ENTERPRISE COMMUNICATIONS 2.0

EMBRACING THE BRING YOUR OWN DEVICE TREND TO IMPROVE EMPLOYEE PRODUCTIVITY

STRATEGIC WHITE PAPER

Accustomed to the freedom they have to access their consumer applications anywhere, at any time and on any device, today's employees want the same seamless, ubiquitous access to enterprise applications on their personal devices whether they are within the work environment or well beyond the enterprise boundary. As a result, they are bringing their personal smartphones, tablets and other portable devices to work, and they expect to continue digital conversations with colleagues, partners and customers on these devices anywhere, at any time and with any application they choose. But the bring your own device (BYOD) trend is creating a higher risk of unauthorized access to sensitive corporate information from the outside whenever these devices are used. Therefore, enterprises must find a way to embrace the trend to serve the communications needs of employees and leverage the paradigm shift to improve employee productivity.

TABLE OF CONTENTS

AT THE EDGE OF A NEW ERA IN ENTERPRISE COMMUNICATIONS

It was bound to happen. Sooner or later, the proliferation of powerful, portable, consumer electronics that have improved personal communications and interactions was going to affect enterprise communications. After all, enterprise employees are, first and foremost, independent consumers. So it stands to reason that they would eventually want and expect the same level of seamless, anywhere, anytime access to communications and information at work that they enjoy in their personal lives. And it's no stretch to accept that if they can't get that experience from "enterprise approved" devices, they're going to bring their personal devices into the work environment to create the experience they want on the devices that they are most comfortable using.

This is creating a considerable challenge for enterprise IT teams worldwide. Because an employee's personal mobile devices are not under the control of the IT team, there is a higher risk of unauthorized access to sensitive corporate information from the outside whenever these devices are used. As a result, IT teams must find a way to regulate the bring your own device (BYOD) trend. But the real challenge is to find a way to embrace the trend to serve the communications needs of employees and leverage the paradigm shift to improve employee productivity.

To meet employee expectations and leverage the BYOD trend effectively, the next generation of enterprise networks must support a variety of personal, smart mobile devices, and individual employee preferences. Therefore, the way organizations offer communications services must change. It is no longer viable for these services to be tied to specific devices. They must become independent of all devices so that they no longer require a user to be confined in the way that they use them.

The enterprise network over which these applications and services travel must also change. The ideal network must be optimized to prioritize an employee's enterprise business traffic over personal, non-critical traffic. This can only be achieved with an intelligent network that can monitor and recognize the nature of the traffic being generated by each user, prioritize critical enterprise traffic, and manage delivery of that traffic at the level of quality required to support enterprise communications processes.

Most importantly, the architecture of the enterprise network must change. A more dynamic architecture is required that can accommodate the new application and traffic delivery models. The new architecture must support seamless interconnection of every user's personal applications so they can work over the enterprise network. In this way, the productivity of end users can be optimized at all times.

THE CONSUMERIZATION OF ENTERPRISE COMMUNICATIONS

The emergence of the BYOD culture and the consumerization of enterprise communications is the direct result of the proliferation of easily portable mobile devices, such as netbooks, smartphones, and tablets. Consumers use these devices in their personal lives to connect to the Internet and build personal clouds by selecting applications that enable them to improve their communications experience or personal productivity. From this initial set up, they shape their personal cloud by adding or discarding applications based on their specific, individual needs at any point in time. And they begin to rely on them. As a result, the personal cloud becomes a personal companion.

At some point, consumers realize that there is a benefit to having their personal clouds support their professional lives. They mold them to address this need by downloading e-mail, word processing, conferencing and document sharing applications to their personal devices that can improve their work productivity. They use these applications whenever they can and, eventually, they become so accustomed to the ease of use their personal clouds offer for business processes, that they don't think twice about leveraging them at work. This pushes enterprises to enter a new PC era, where the Personal Cloud is more important to employees than the Personal Computer.

BYOD trend expected to continue

Market reports confirm that this BYOD trend is well underway. A May 2012 report by Accenture[1] noted that 45 percent of employees find personal devices and applications more useful than those provided by their enterprise. Sixty-six percent don't worry about their organization's IT policies because they just use the technologies they need to do their work. Twenty-three percent use their own devices for work regularly, 27 percent use non-corporate applications to improve their productivity at work, and 32 percent actively recommend good consumer applications to their colleagues. In fact, 27 percent of employees surveyed would be willing to pay for their own devices and applications if they were allowed to use them at work.

Meanwhile, enterprises are starting to accept this reality, although not completely. In December of 2011, Yankee Group reported that 78 percent of IT decision-makers allow personal devices and applications within the enterprise, but less than 20 percent offer full support for them. In addition, personal tablet usage in enterprises has grown by 120 percent, but enterprise-provisioned tablets only grew by 64 percent.[2]

But, change is coming. IDC predicts that commercial and business deployment of media tablets will grow from 4.2 percent of worldwide shipments in 2010 to 14.3 percent by 2015.[3] While Gartner predicts that 90 percent of enterprises are expected to support corporate applications on personal devices by 2014.[4]

Enterprise response options

When personal devices show up on an enterprise network, IT departments must either support them, or banish them. Supporting them is the best option. How they are supported will depend on the enterprise.

Leveraging BYOD to improve productivity is not limited to finding a way to incorporate employee devices into the corporate network. Obviously, authorizing personal devices is the easiest approach. But enterprises can also choose to fund the purchase of selected, pre-authorized devices from which an employee can choose. With this approach enterprises can exert some measure of control over the types of devices that will appear on the network. An employee chooses the device most suited to his or her personal preferences and the enterprise funds the purchase or reimburses the employee after the purchase has been made with personal funds.

1 Accenture, *Consumer IT: The Global Infiltration into the Workforce*, Accenture BlogPodium, May 2012, www.accenture-blogpodium.nl/site.
2 Sandra Palumbo, Denise Lund, George Hamilton, *Webinar Q&A: Embracing Consumerization in the Enterprise*, Yankee Group, December 2011.
3 Carrie MacGillivray, *Tablets in the Enterprise: Opportunities and Challenges for Businesses and Mobile Operators*, IDC, December 2011.
4 Gartner, *Top Predictions for 2011 and Beyond*, Gartner, November 2010, http://www.gartner.com/it/page.jsp?id=1480514.

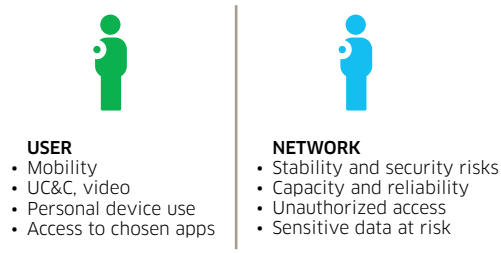
Enterprises can also purchase devices and provide them for employees, in much the same way that desktop PCs are provided today. The device can be a thin client that is configured to simply provide a window into the enterprise network and application suite. Alternatively, it can be a thick client pre-loaded with an authorized operating system and applications programmed to connect to the enterprise network to enable communications with other employees and network-based services.

Whatever the approach chosen, each option requires IT teams to be more vigilant about how devices are incorporated and authorized on the network. If the device is brought in by employees than there are challenges associated with making sure the device is visible on the network and how bandwidth is used, and there are security issues that must be addressed. But if the enterprise provides the device it will have more control over the whole process. In both cases, IT teams must change their approach to the enterprise network and the way applications are offered and managed to leverage the BYOD trend effectively. Ultimately, a new enterprise network strategy is required to accommodate ever-increasing user demands that will dynamically change based on which application or service is used by employees at any given time, at any location, and with any device.

BUILD YOUR OWN DESTINY

The ideal network strategy should address BYOD challenges (Figure 1) by enabling a high quality end user experience with consumer-grade convenience for business conversations based on mobility, application and device freedom. It should ensure all conversations are maintained in context with a high level of service quality. Most importantly, it should provide users with choice and control over all the multiple media and devices available to them, and give them the ability to interact with as many people at a time as they desire, using whatever device they desire.

Figure 1. Leveraging BYOD trend requires enterprises to find a balance between user and network challenges



This new network should be built based on three essential criteria.

First, the network must be able to support an unprecedented and continuously increasing demand for ubiquitous mobility. Employees must be able to access their personal and enterprise clouds from anywhere, at any time, and on any device so they can use mash-ups of personal and enterprise resources, as required. Therefore, the network should be configured to maintain conversations by supporting continuous connections and seamless transitions as employees move across the enterprise boundary and shift between different access technologies: wired, Wi-Fi, 3G, Femtocell, and more.

Second, it must be scalable and elastic. It must be able to allocate the right amount of network resources to every user at all times. Therefore, it must support communications through centralization and virtualization in an enterprise network cloud. This does not mean that the ideal architecture requires more hardware. On the contrary, it means

rationalizing existing network elements to ensure that the right hardware is in place to enable and support the network cloud, and applying advanced traffic management tools, such as load balancing, to optimize the use of all elements at all times

Finally, the ideal network must have the ability to differentiate between personal and enterprise traffic and ensure the security of both. In this way, employees can be assured that their private data is secure at all times, and enterprise IT teams can rest easy knowing enterprise communications and information are secure.

A network built with these criteria in mind will enable enterprises to support the BYOD trend and deliver a high quality end user experience with consumer-grade convenience for all business conversations. But to truly improve employee productivity, enterprise IT teams must also leverage the power of the network by changing the way they deliver applications and services and manage network traffic.

Enable "appification" of applications and services

Improving employee productivity begins with changing the way organizations offer communications services. Enterprise applications and services must become independent of all devices so that users are no longer confined in how they use them and the user experience is seamless and continuous on any device. This is especially important to support employee mobility.

To make this possible, IT departments must match employee experiences and expectations that have been shaped by the way they select and purchase consumer applications and services for their Personal Cloud. Enterprise application provisioning must adopt the convenience, user experience, and deployment model offered by consumer app stores. Therefore, IT teams must either post applications on public app stores or build their own enterprise app store from which employees can download the applications they want. Some call this process "appification".

Select a method of delivery

Obviously, the first step in the appification process requires enterprises to determine just how open the new provisioning process should be. Should it be completely open, or should it be a closed door process? In other words, should applications be delivered via the Internet or via a corporate Intranet?

Typically, large enterprises will want to have an internal app store accessible via a corporate Intranet, while smaller enterprises will probably want to leverage the ubiquity of the public Internet. Whichever approach is chosen, the enterprise app store should be a landing page from which users download an app manager onto their mobile device. Once installed, the app manager provides a convenient way for users to access the enterprise's app store, select apps and download them to the device they are using at the time, a process similar to what employees are already experiencing from consumer app stores.

If it is structured properly, this process will better accommodate individual employee preferences for devices and improve productivity by allowing employees to use their preferred device with corporate applications. For example, some employees may choose to use a unified communications application on their PC, some may use it on their smartphone, and others might use it on both. More importantly, the process will give IT teams more control over applications and devices. The very nature of the BYOD phenomena will require enterprises to provide multiple approved versions of the app — device specific and operating system-specific — that users can access and use on their preferred device.

Maintain security of all applications

One of the key considerations for this type of application delivery will be app usage rights. Because the ultimate objective is to make sure that employee productivity is improved, then the process should ensure that the right people on the right devices can get to the resources they need with a high quality experience, while undesired people or non-compliant devices cannot access any resources.

Ideally, the process should be configured to enable or restrict application downloads based on usage rights associated with each employee's role within the organization. For example, a finance employee may have access to a high level finance application, whereas a factory employee may not. Likewise, a university professor may have the right to download a specific lesson application, but a student may not.

To make this possible, an enterprise must be able to authorize and authenticate users based on their profiles, as well as the devices they are using. Therefore, the first component of any BYOD application provisioning process must be a strong Network Access Control (NAC) solution that authenticates both users and devices.

In addition, it's also important to know that devices entering the network are healthy and will not infect the network or other devices on the network. This was more manageable when only corporate controlled devices were allowed in the workplace. But as the BYOD trend continues, it is important for all enterprises to enable some type of Health Integrity Check (HIC) for any device that attempts to enter the network that is not approved by the IT team. In addition, the process should also provide some level of information about the bandwidth allowed to every user and every device.

With this structure in place, the enterprise will have more control over applications, who can use them, the way they are used, and the network bandwidth required to support them for each user. This allows the network to ensure that quality of service (QoS) parameters are enforced for all user downloads and applications at all times.

Design an intelligent, application fluent network

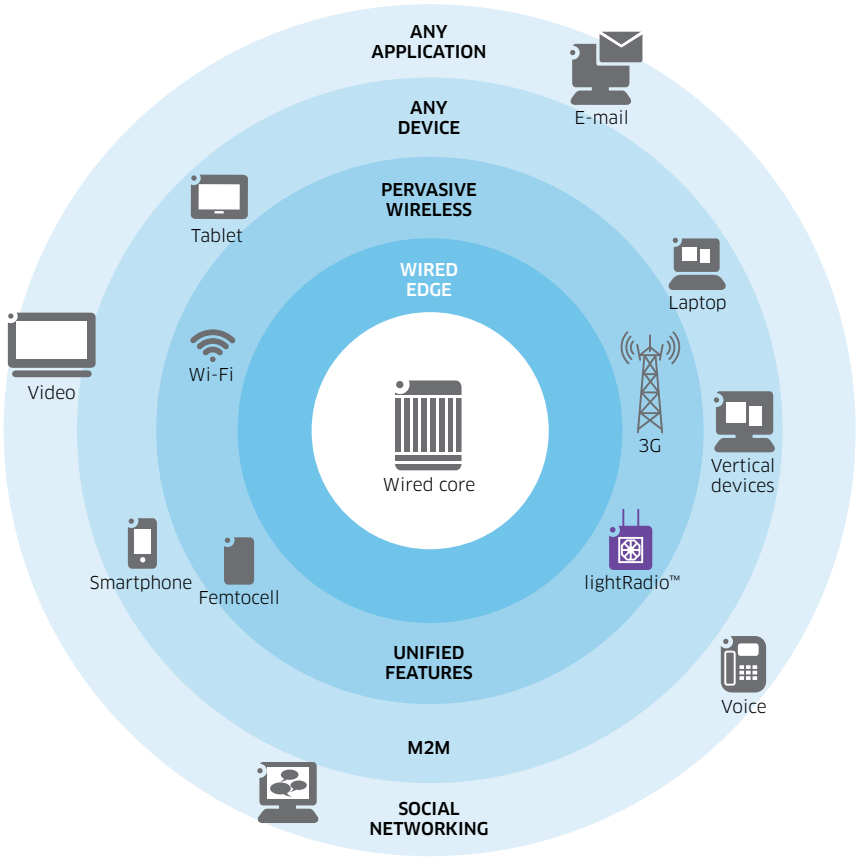
Improving employee productivity based on this level of appification can only be achieved with a network that can manage business conversations effectively and efficiently to create the ideal end user experience. The experience end users expect requires mobility, application, and device freedom that allows conversations to be seamlessly transitioned from one network to another and from one device to another with context and a high level of service quality.

Therefore, the next generation of enterprise network must support employee access to personal clouds over wired and wireless links. It must have the ability to recognize users, applications, and the priority of service for apps and users. In addition, it must be a stable enough to handle the load that will be created by having so many BYOD devices on the network. A converged, intelligent, application fluent network provides higher transmission capacity and automated controls that can deliver the quality user experience needed, while reducing costs and simplifying administration.

Move to a converged infrastructure

Many enterprises have already successfully combined their voice and data networks to the point where voice is viewed as an application or service on the IP network. Convergence will continue to occur with the migration of different applications and associated devices onto the IP network. This will make it necessary to upgrade the network edge and core, and introduce new network service elements. Eventually, a new, network architecture will emerge with a unified access layer and a set of embedded network services for all devices. This convergence process may in turn lead to a seamless hybrid cloud model that enables service delivery on any network, to any device and at any location from private data centers or the public cloud with acceptable QoS and security (Figure 2).

Figure 2. Unification of the access layer to achieve the ideal enterprise end user experience



Create application fluency

Application fluency on a converged network is achieved through a simplified, resilient and low-latency network architecture with built-in security. To improve end user productivity, an application fluent network also features automatic controls for adjusting application delivery based upon profiles, policies and context. And streamlined operations are enabled by automated provisioning and low power consumption.

Creating application fluency can be accomplished in stages. The process should begin with the unification of access management policy and enforcement for the Wi-Fi and wired networks in the enterprise. Unification of the physical wired and wireless networks should follow in areas where this can be achieved with cost savings as the driver.

But the unification of the network access layer cannot stop there. To meet end user expectations for application fluency, enterprises must also integrate Femtocell and 3G/4G technologies to improve the end user experience and reduce costs. This integration may be enabled by the development of new simplified base station technologies, such as lightRadio™.

Enable access control

Complete application fluency also requires complete access control. This can be achieved by migrating from the current wireless control model of using a centralized controller to one in which the control function can be delivered in different forms, based on the existing installed base, network size, and functionalities expected. To make this happen, enterprise IT departments need flexibility and elasticity for the delivery of wireless local area network (WLAN) control functions. For some, a fully distributed model may be necessary. For others a virtualized model makes sense. Some may require a centralized model. While a hybrid model may be the best option for those who may be implementing a campus versus branch office deployment.

In addition, policy enforcement for network access control is required. This can be addressed by the same access layer switches for both wired and Wi-Fi access. Virtualization of the control function and sharing of the policy enforcement point in this way removes the inefficiencies associated with today's controller-based architectures where all traffic is backhauled to a centralized controller.

Embed network service orchestration

Finally, because enabling devices to discover and use available network resources is essential for a seamless user experience, a common provisioning and control function is essential.

To support unified access and enable a seamless user experience the unification of wired and Wi-Fi access can be facilitated by the introduction of a network service orchestration layer that delivers true value to enterprise end users. Network service orchestration allows applications and devices to discover services that are available on the network and enables common service provisioning and control through a single portal. It also ensures interoperability between individual services and supports the ability for all services to easily share a common policy framework.

With service orchestration the network can leverage advances in virtualization and computing technologies to efficiently manage:

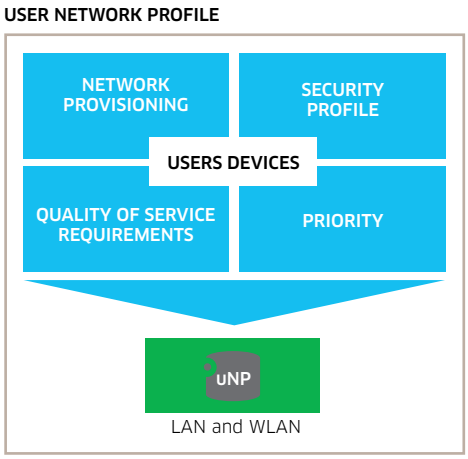
- Security services, such as authentication, firewall, and IPS/IPS
- Access control services, such as traditional IP address management, and Dynamic Host Configuration Protocol (DHCP) can manage, track and control devices via Mac address, as well as Authentication, Authorization, and Accounting (AAA), and role-based access control
- Application fluency services
- Mobility services, such as Wi-Fi control and network handoff
- Application services, such as presence and shared directory services

Manage conversations through user-specific profiles

Ultimately, an intelligent, application fluent network must have something to work with to manage business conversations effectively.

Network conversations can be managed in context by leveraging the unique information associated with each user, application, and device. This can be accomplished by creating a user network profile (uNP) for each employee that provides the network provisioning information, the security profile required by the user of that device, the QoS requirements, and the priority of that user or device within the network (Figure 3).

Figure 3. Network conversations can be managed in context by leveraging a user network profile (uNP)



With this information, the network can recognize users and devices and bind them to a User Network Profile (uNP). This allows it to understand each conversation and automatically adjust to conversation requirements. The network is also able to discover the location of a user or device automatically by monitoring traffic on a specific switch port. It can provision the user and device on that switch port automatically, including security and initial QoS parameters. And it can designate conversations initiated by a particular user on a specific device that are to be measured for actual QoS received.

ALCATEL-LUCENT AND THE COMMERCIALIZATION OF ENTERPRISE COMMUNICATIONS

Alcatel-Lucent offers all the elements enterprises need to create agile architectures, solutions and services that support the BYOD trend and improve end user productivity. With a complete portfolio of wireless and wireline product, communications solutions and service offerings Alcatel-Lucent offers enterprises a variety of ways to enable employee mobility and seamless communication over a personal and enterprise cloud. In addition, Alcatel-Lucent offers communications services for smartphones and tablets that are optimized to enable effective conversation management.

For example, the Alcatel-Lucent Safe Network Access Control (SafeNAC) solution is designed to enable conversation management over an intelligent, application fluent network by managing all of an enterprise's NAC and HIC needs. It can monitor the health and compliance of a device before it enters the network, and notify a network infrastructure of the rights and bandwidth allowed to any user on any device. The solution is engineered to communicate directly with a network infrastructure to enable

conversation management based on each user's uNP. It is fully functional on both wired and wireless devices entering the network, and provides a full featured suite of options for HIC remediation, application filtering, ongoing security checks, and management reporting. Most importantly, it works with a variety of devices, thereby enabling greater freedom for users and peace of mind for IT teams.

Alcatel-Lucent enables access control on enterprise networks with the Alcatel-Lucent VitalQIP™ Appliance Manager (AM) solution, which gives the network the ability to track and associate devices with users. With this solution, a user is assigned a configurable number of devices on the network. Access control is managed through a self-registration user interface. When a user provides a user ID and password through a device, the VitalQIP solution ensures that the Mac address of the device is authorized for that particular user. If the device is not authorized, the solution software has the ability to place the user into a captive portal, which presents a customized web address that provides information for further assistance.

Alcatel-Lucent also offers the OpenTouch™ Communications platform to enable networks to manage multi-party, multi-device, multimedia business conversations more effectively. The platform's architecture and OpenTouch Conversation client application software provide unified management of enterprise telephony, messaging, presence and instant messaging, mobility, audio and web collaboration, and enterprise video applications and services (Figure 4). This allows end users to initiate business conversations with colleagues, partners, and suppliers using whatever device they prefer, and maintain them in context as they move from one device or application to another.

Figure 4. Alcatel-Lucent OpenTouch Communications platform enables multi-party, multi-device, multimedia business conversations

In addition, Alcatel-Lucent offers data center solutions that enable network rationalization and centralization to support communications and information in an enterprise cloud.

CONCLUSION

Given the communications demands being created by the BYOD trend, and more broadly by the never-ending appetite for tablets and smartphones, the reign of the PC as the predominant tool on an enterprise communications network is coming to an end. As employees continue to bring personal devices into an enterprise environment, IT teams must either support them, or banish them. Supporting them is the best option. It allows an enterprise to better serve employee communication requirements, and leverage the BYOD trend to improve productivity.

However, to achieve both objectives, a new enterprise network strategy is required to accommodate ever-increasing user demands that will dynamically change based on which application or service is used by employees at any given time, at any location, and with any device. The ideal network strategy should enable a high quality end user experience with consumer-grade convenience for business conversations based on mobility, application and device freedom. It should ensure all conversations are maintained in context with a high level of service quality. Most importantly, it should provide users with choice and control over all the multiple media and devices available to them, and give them the ability to interact with as many people at a time as they desire, using whatever device they desire.

But to truly improve employee productivity, enterprise IT teams must also leverage the power of the network by changing the way they deliver applications and services and manage network traffic. Enterprise application provisioning must adopt the convenience, user experience, and deployment model offered by consumer app stores. And the enterprise network must have the ability to recognize users, applications, and the priority of service for all apps and users.

By building a new network strategy based on these criteria, enterprises can truly leverage the BYOD trend to build an enterprise 2.0 environment for their employees, while ensuring enterprise communications and information are secure at all times.

ACRONYMS

AAA	Authentication, Authorization, and Accounting
BYOD	bring your own device
DHCP	Dynamic Host Configuration Protocol
HIC	Host Integrity Check
IT	Information Technology
NAC	Network Access Control
uNP	User Network Profile
PC	Personal Computer
QoS	quality of service
uNP	User Network Profile
WLAN	Wireless Local Area Network

Alcatel·Lucent
Enterprise