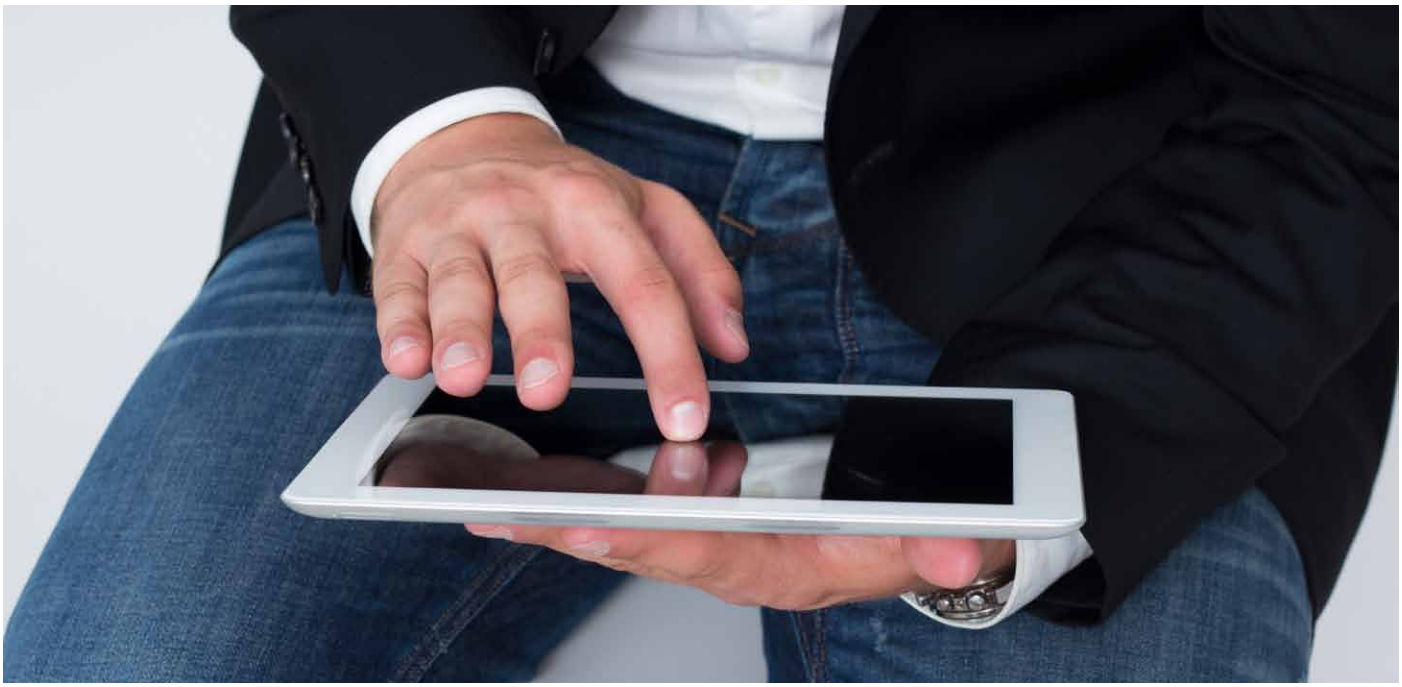


LEVERAGING BRING YOUR OWN DEVICE PROGRAMS

NETWORK SERVICES ENGINEERED TO ENABLE EMPLOYEE CHOICE, MOBILITY AND SECURITY

APPLICATION NOTE

Alcatel·Lucent Enterprise

ABSTRACT

As more enterprises consider how best to leverage Bring Your Own Device (BYOD) programs to improve employee productivity, it is important for IT teams to have the flexibility to develop custom-tailored solutions for their specific needs. Alcatel-Lucent offers all the elements enterprises need to create agile architectures that leverage BYOD programs effectively. The addition of Alcatel-Lucent BYOD services to the Alcatel-Lucent Converged Campus Network Solution ensures that the right users with approved devices can get to the resources they need at all times. It provides all users with the same high quality experience with any application on wired and wireless networks. It enables the freedom of choice employees expect with ubiquitous connectivity, simple access, and always on, anywhere communications. And it restricts unauthorized personnel or non-compliant devices from accessing corporate resources and jeopardizing the integrity and security of corporate information.

TABLE OF CONTENTS

BRING YOUR OWN DEVICE AND ENTERPRISE COMMUNICATIONS

Enterprises have been concerned about the Bring Your Own Device practices of employees for some time. A little over a year ago, a report by Accenture noted that 45 percent of employees find personal devices and applications more useful than those provided by their enterprise.[1] 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, and 27 percent use non-corporate applications to improve their productivity at work.

At the time, this report and others focused on explaining the growing bring your own device (BYOD) trend enterprises of all sizes were facing. One year later, Gartner reports that this trend is becoming more accepted by enterprise IT teams worldwide. In fact, Gartner states enterprise programs designed to leverage BYOD are becoming more commonplace and that by 2016, 38 percent of companies expect to stop providing hardware devices to employees.

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. Users are relying on these devices for more work and life solutions. As a result, applications have become much more mobile and "always on" and more people around the globe are becoming "always on" every day. In this process, employees are becoming more connected to their personal clouds of applications and services than they are to their enterprise networks and they expect the same ease-of-use from all applications.

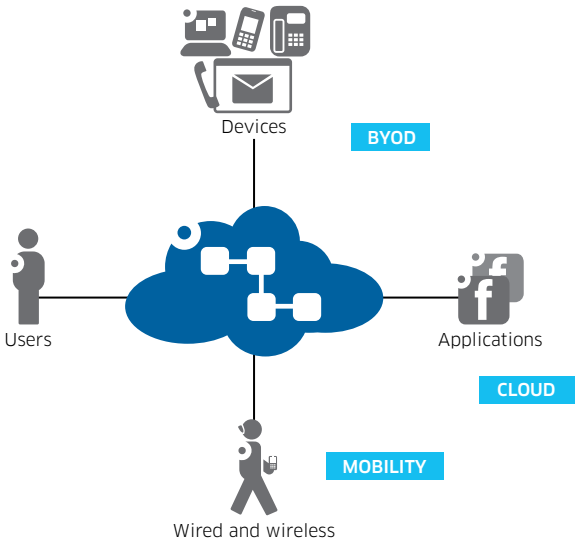
Accustomed to the freedom they have to access their consumer applications anywhere, at any time and on any device, employees want the same seamless, ubiquitous access to enterprise applications on their personal devices whether they are within the work environment or well beyond the enterprise boundary. They want to use their personal devices to continue digital communications with colleagues, partners and customers anywhere, at any time and with any application they choose. And they want to do it over any wired or wireless network they choose.

But BYOD is creating a considerable challenge for enterprise IT teams. Because an employee's personal mobile devices and personal clouds 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 and applications are used. Therefore, enterprises must find a way to not only embrace BYOD to serve the communications needs of employees, they must also leverage the paradigm shift to improve employee productivity and secure their networks from unwanted access.

[1] "Consumer IT: The Global Infiltration into the Workforce", Accenture BlogPodium, May 2012, www.accenture-blogpodium.nl/site.
[2] "Bring Your Own Device: The Facts and the Future", Gartner, http://www.gartner.com/newsroom/id/2466615.a

Alcatel-Lucent offers all the elements enterprises need to create agile architectures, solutions and services that address the evolving communication needs of employees and leverage BYOD programs effectively. With a complete portfolio of wireless and wireline products, communications solutions and service offerings, Alcatel-Lucent offers enterprises a variety of ways to enable employee mobility and seamless communication over a personal cloud and an enterprise network. In addition, Alcatel-Lucent offers communications services for smartphones and tablets that are optimized to enable effective communication management (Figure 1).

Figure 1. Alcatel-Lucent offers communications services optimized to enable effective communication management



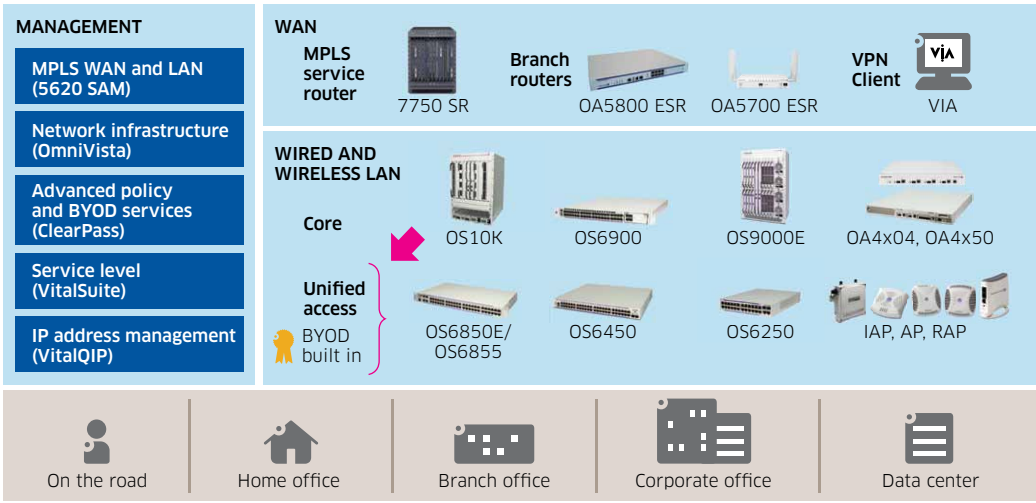
As part of this complete approach, Alcatel-Lucent offers a BYOD enabler as an integral element of its Converged Campus Network Solution. The Alcatel-Lucent approach to BYOD is engineered to ensure that the right users with approved devices can get to the resources they need at all times. It provides all users with a high quality experience with any application. And it enables the freedom of choice employees expect with ubiquitous connectivity, simple access, and always on, anywhere communications. Most importantly, the Alcatel-Lucent solution for BYOD restricts unauthorized personnel or non-compliant devices from accessing corporate resources and jeopardizing the integrity and security of corporate information.

CREATING MOBILITY, APPLICATION AND DEVICE FREEDOM

The Alcatel-Lucent Converged Campus Network Solution supports BYOD by providing a high quality end user experience with consumer-grade convenience for business communications. It ensures all of an enterprise end user's personal and business communications are maintained in context with a high level of service quality. And it provides users with choice and control over all of the media and devices available to them, so they can interact with as many people at a time as they desire, using whatever device they desire.

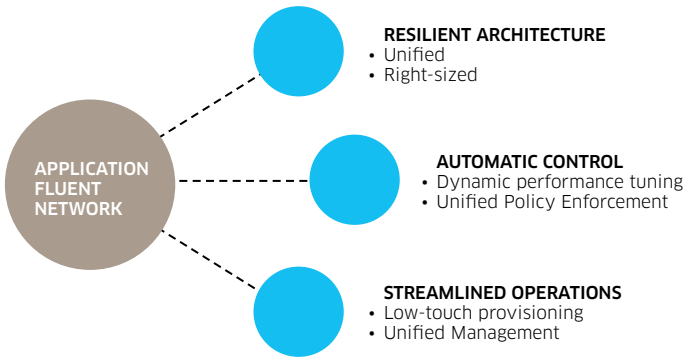
BYOD on enterprise networks built with the Alcatel-Lucent Converged Campus Network Solution is enabled by a comprehensive portfolio of integrated products and solutions engineered to deliver application fluency (Figure 2).

Figure 2. The Alcatel-Lucent Converged Campus Network Solution supports BYOD with products and solutions that enable application fluency



An Application Fluent Network (AFN) built with these elements is equipped to accommodate the new application and traffic delivery models required to support BYOD (Figure 3). The architecture of the network is more intelligent and dynamic. It supports seamless interconnection of every user's personal applications so they can work over the enterprise network. The network monitors and recognizes the nature of the traffic being generated by each user, prioritizes critical enterprise traffic, and manages delivery of that traffic at the level of quality required to support enterprise communications processes. As a result, the productivity of end users is optimized at all times.

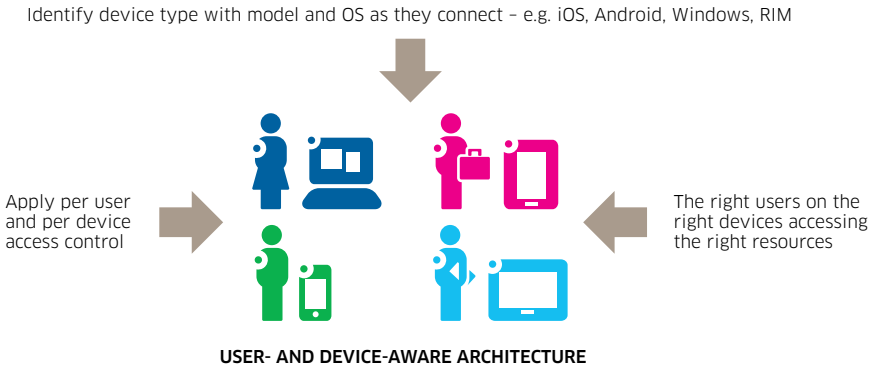
Figure 3. An Alcatel-Lucent Application Fluent Network prioritizes enterprise traffic over personal, non-critical traffic



How it works

The Alcatel-Lucent implementation of BYOD in the Converged Campus Network Solution is based on intelligent device fingerprinting and policy management. These capabilities ensure that the right people with approved devices can get to the communications resources they need and that they receive a high quality experience when they use them (Figure 4). They also restrict unauthorized personnel or non-compliant devices from accessing corporate resources.

Figure 4. Alcatel-Lucent BYOD in the Converged Campus Network Solution is based on intelligent device fingerprinting



Once the device is known, decisions can be made about how to handle the device and the communications applications it is using. This is achieved with:

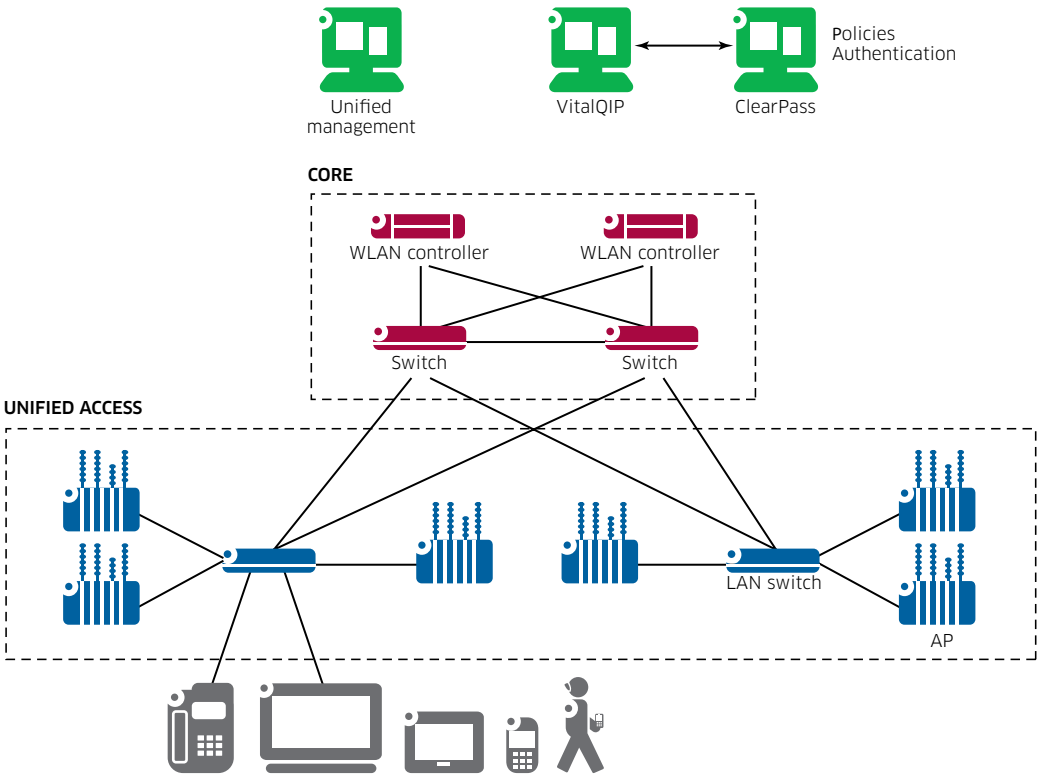
- A strong access control and authorization mechanism, which authenticates both the user and the device
- A posture check, which identifies any non-corporate device that attempts to enter the network and prevents unauthorized applications from using network bandwidth or violating company policies. This ensures that devices connecting to the network do not contain viruses or malicious threats and are not going to infect the network or other devices.
- A quality of service (QoS) and prioritization mechanism, which ensures that all approved applications function properly when they are on the network, and that all traffic is prioritized based on the type of communications the applications generate

With these three elements, Alcatel-Lucent BYOD device fingerprinting and policy management handle all access control needs and also notify the network infrastructure of the rights and bandwidth allowed for any user on any device. Devices such as printers, cameras, and scanners can be added automatically as “white-listed” devices, without IT intervention. From that point, the Alcatel-Lucent Converged Campus Network Solution infrastructure handles the network rights while continuously monitoring the health and compliance of each device. This is done for employees, contractors and guests as they enter the network.

Access control

BYOD unified access capabilities with the Alcatel-Lucent Converged Campus Network Solution are enabled by the Aruba ClearPass™ Policy Manager (CPPM). This platform provides user- and device-based network access control for employees, contractors and guests across any wired, wireless and virtual private network (VPN) infrastructure.

Figure 5. Unified access on the Alcatel-Lucent Converged Campus Network Solution is governed by a policy management platform



With the CPPM, centrally-managed network access policies provide the comprehensive authentication capabilities that are required for today's highly mobile workforce, regardless of device type or device ownership. Automated services let users securely onboard their own devices, register AirPlay- and AirPrint-enabled devices for sharing, and create guest access credentials. The result is a consistent and scalable network access control solution that exceeds BYOD and IT-managed device security requirements.

The CPPM centrally enforces all aspects of BYOD based on granular network access privileges, which are granted based on a user's network profile, device type, device management attributes, device health, location, and time-of-day. Built-in Remote Authentication Dial In User Service (RADIUS), Terminal Access Controller Access-Control System Plus (TACACS+), profiling, onboarding, guest access and health checks, and the ability to leverage third-party mobile device management solutions, ensure seamless policy enforcement across the entire network.

Application fluency

By managing access in this way, Alcatel-Lucent is able to deliver complete application fluency. This is achieved by creating differentiated access control levels to accommodate the practical working concerns of different user groups.

For example, the functional departments in an organization may be granted access privileges for specific resources and applications. In addition, device classes can be established for users in each department. With this approach, a BYOD device class may be given different access privileges than corporate issued devices.

But differentiated access also allows IT teams to control the number of devices a user can bring to work. For example, executives or sales personnel may be allowed to onboard up to two personal devices because high mobility and constant customer interaction are expected of this group. On the other hand, office-based employees may be limited to one personal device because they are likely to spend most of their time on a corporate-issued computer.

Visitors to the enterprise are also a discrete group with their own access needs. A guest-access solution can be used to separate guest traffic, customize the experience for each user and provide visibility on who is connecting. Blended access solutions of this nature also provide IT teams with the necessary data to adjust bandwidth requirements for different user groups, as well as for planning purposes and user-based network audits. To simplify visitor management, the CPPM also offers guest management features. The CPPM Guest™ feature streamlines workflow processes and allows operators or sponsors, such as receptionists, event coordinators and other non-IT staff, to create temporary accounts for Wi-Fi® access.

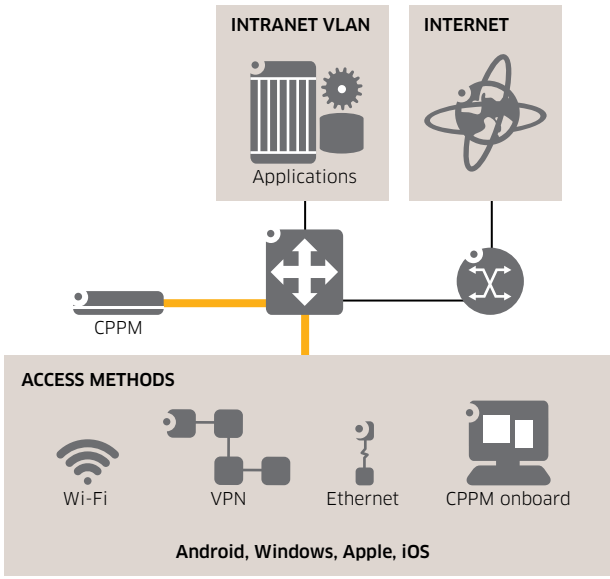
Guests can also self-register for network access. Once registered, CPPM Guest delivers account login credentials to users via Short Message Service (SMS) text message or e-mail. Accounts can be set to expire automatically after a specific number of hours or days.

Because it operates off the CPPM platform, the CPPM Guest feature is enabled by the CPPM platform's core set of authentication, authorization, accounting, and policy enforcement capabilities. The CPPM scales seamlessly across multivendor wireless, wired and VPNs, and supports a variety of identity stores. Therefore, the CPPM Guest feature can scale to support the needs of large enterprises and multi-site networks and manage secure, user-based access for hundreds of thousands of concurrent users. Plus, with complete visibility into each visitor's network access activities, CPPM Guest makes it easy to measure network usage, identify Wi-Fi coverage requirements, and meet corporate and industry compliance mandates.

Device on-boarding

The CPPM also manages device on-boarding. With the CPPM, the solution is able to automatically provision and configure an employee's personal mobile devices (Windows®, Mac OS® X, iOS® and Android™ 2.2 and above) and enable each device to connect to the network securely. This is achieved with the CPPM Onboard™ feature (Figure 6).

Figure 6. The CPPM manages device on-boarding with the Onboard feature



CPPM Onboard allows employees, contractors and partners to self-configure their own mobile devices. The CPPM registration portal automatically detects a device's operating system and presents the user with the appropriate configuration package. It then offers a simple way to configure wireless, wired and VPN settings, apply unique device credentials, and ensure that users securely connect their devices to 802.1X-enabled networks with minimal IT involvement.

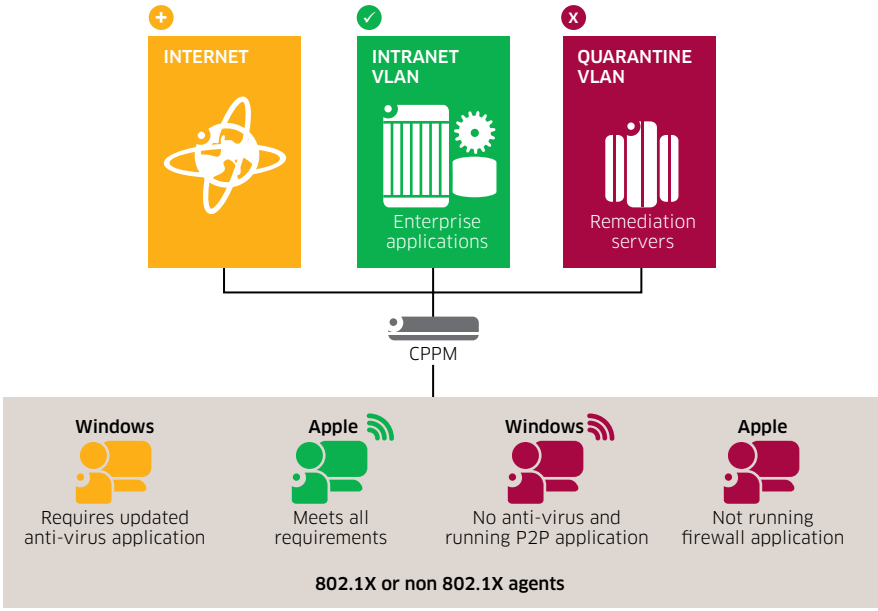
The CPPM Onboard feature leverages the certificate authorization capabilities of the CPPM platform to publish unique credentials that include certificate information as well as user and device data. The distribution of published device credentials through CPPM Onboard protects organizations that want to adopt BYOD initiatives without implementing an external certificate authority. Easy-to-use search and menu-driven capabilities ensure the rapid revocation and deletion of certificates for specific mobile devices if a user leaves an organization or the mobile device is lost or stolen.

This simple on-boarding process streamlines workflow for IT help desks. It allows IT personnel to automate and secure multiple processes that are required to successfully carry out BYOD initiatives while improving the user experience.

Posture checking

Posture assessments and health checks are managed with CPPM OnGuard™. This feature provides enterprise-class protection with advanced end point posture assessments on leading computer operating systems to ensure compliance is met before devices connect. These assessments and checks are performed in addition to anti-virus, anti-spyware and personal firewall audits performed by traditional network access control (NAC) and network access protection (NAP) processes. This ensures the network is always protected with a greater level of end point compliance (Figure 7).

Figure 7. Posture assessments and health checks are managed by CPPM OnGuard



The advanced NAC and NAP framework in CPPM OnGuard offers exceptional safeguards against vulnerabilities. If unhealthy end points do not meet compliance requirements, the user receives a message about the end point status and instructions on how to achieve compliance if auto-remediation is not used. For added protection, CPPM OnGuard health checks can check for more granular data than with the standard NAP agents. OnGuard can also be used to assess product-specific attributes, such as product, engine and data file versions for anti-virus applications.

Mobile Application Management

Mobile Application Management (MAM) is provided by the CPPM application, WorkSpace. This feature allows IT teams to secure, distribute and manage enterprise apps on personal mobile devices. It also includes the WorkSpace mobile app, which lets users onboard their own devices, organize and manage their work apps, and provision network access for their guests.

WorkSpace makes it easy for enterprise IT departments to create policies that control how work apps are used and data is secured. An automatic VPN session can be initiated when specific work apps are used on public networks. Work apps can also be locked based on a location or geo-tracking status.

For users, the WorkSpace mobile app offers unprecedented control for as many personal devices as the user is allowed to bring onto the network. It provides visibility into app policy status, access to an enterprise app store, and a single sign-on for work apps. It also lets users create and manage temporary guest Wi-Fi accounts, instead of having IT or the reception desk provision guest access.

WorkSpace supports one of the largest ecosystems of enterprise mobile apps in the industry. IT can easily secure, distribute and manage more than 40 leading third-party enterprise productivity apps as well as internally-developed apps. Granular policy controls and automatic updates allow IT teams to apply policy changes per app without the need to redeploy or rewrap apps already on devices.

With the WorkSpace feature, IT teams can also distribute and manage corporate-approved apps from an internal app store. A user's network profile is used to determine which apps are automatically pushed to the device. The IT department can also track which enterprise apps are being used and quickly make updates to any app without touching a user's device.

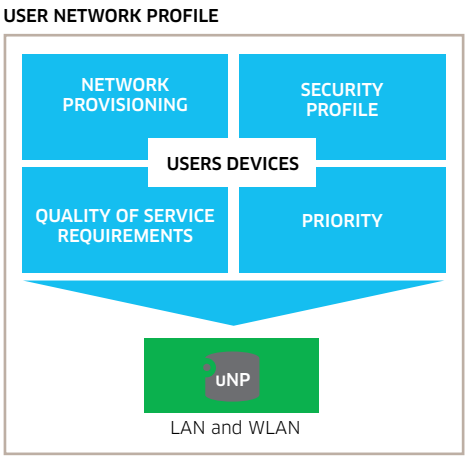
Finally, WorkSpace eliminates corporate liability issues related to privacy by preventing IT teams from accessing a user's personal information. With WorkSpace, IT teams can wipe or lock enterprise apps and data, but cannot view a user's private information.

QoS Control with User Network Profiles

Of course, all communications on an enterprise network must be managed to deliver a high QoS. The Alcatel-Lucent Converged Campus Network solution coupled with CPPM, ensures users continue to experience the highest quality for their business and personal communications by leveraging the unique attributes of user network profiles.

All network communications in the Alcatel-Lucent implementation of BYOD are managed in context by leveraging the unique information associated with each user, application, and device. This is accomplished by creating user network profiles (uNPs) that each employee/device/application combination fits into. The uNP is preset to define the security and QoS parameters to be used for each user in a particular situation. The switches then become the enforcement points for the security and QoS parameters. The uNP can also assign VLAN membership. (Figure 8).

Figure 8. Network conversations in the Alcatel-Lucent implementation of BYOD are managed with user network profiles



With this information, the network can recognize users and devices and bind them to a uNP. This allows it to understand each communication and automatically adjust to specific 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 identify communications initiated by a particular user on a specific device that are to be measured for actual QoS received.

Unified Access and Communication Management

Unified access and communication based on uNPs are managed by the simplified, flatter architecture and network virtualization technology at the heart of the Alcatel-Lucent Converged Campus Network Solution (Figure 9). This architecture is engineered to improve resiliency and optimize the use of network resources. It includes all the elements needed to enable efficient unified access and application fluency, including:

- The ability to manage communications in context with the uNPs, which are embedded in the access layer switches.
- Access layer switches enabled to detect and examine communications upon initiation, and manage QoS, as required, for an optimal end user experience.
- A service orchestration layer, which allows applications and devices to discover services on the network and provides a common service provisioning and control portal to ensure interoperability between individual services, including the ability to share a common policy framework.

Figure 9. The simplified, flatter architecture of the Alcatel-Lucent Converged Campus Network Solution

The 10 and 40 GigE wire-rate core of the architecture is enabled by the OmniSwitch™ 10K and OmniSwitch 6900 Local Area Network (LAN) switches. These switches analyze and process different types of traffic based on the granular classification enabled by uNPs. As a result, enterprises can assign priority to applications, users or both. The distributed architecture processes traffic at the ingress, allowing it to be intelligently forwarded to other elements without a central choke point. It also lets enterprises scale their environment based on growing needs without compromising performance and bandwidth.

The converged network also includes a unified access layer where a single policy framework, a common authentication scheme, a single user database and a single set of location-aware variables are applied for both wired and wireless devices.

Wired network access is provided by the OmniSwitch 6850E and the ruggedized OmniSwitch 6855 stackable series, the OmniSwitch 6450 series and the OmniSwitch 6250 series LAN switches. Wireless access is provided by wireless access points connected directly to access layer switches, and control is provided by the OmniAccess™ 6000/4000 Wireless Local Area Network (WLAN) controllers. Also available are instant access point technologies, with integrated virtualized controller functions embedded in the access points.

CONCLUSION

As more enterprises consider how best to leverage BYOD programs to improve employee productivity, it is important for IT teams to have the flexibility to develop custom-tailored solutions for their specific needs.

The Alcatel-Lucent implementation of BYOD with the Alcatel-Lucent Converged Campus Network Solution provides the flexibility IT managers need to implement a BYOD strategy immediately and evolve it over time as requirements change. It is engineered to handle all of an enterprise's access control needs and notify an enterprise network infrastructure of the rights and bandwidth allowed for any user, on any device. From that point on, the Alcatel-Lucent infrastructure will handle the network rights while continuously monitoring the health and compliance of each device. This level of control can be configured for all employees, contractors and guests as they enter the wired or wireless network.

The advanced, application fluent network architecture that is the foundation of the Alcatel-Lucent solution for BYOD is designed to communicate directly with all enterprise network elements, collect critical user information, and provide instructions as to which user network profile (uNP) to use given the user/device combination. The network profile can incorporate such parameters as firewall, bandwidth management, traffic anomaly detection, virtual local area network (VLAN) identity and more, thereby ensuring that the network always delivers a pleasant experience to all users.

Unlike other BYOD solutions, the Alcatel-Lucent implementation of BYOD is fully functional on both wired and wireless devices entering the network. It provides a full-featured suite of options for remediation, application filtering, ongoing security checks and management reporting. And it is engineered to accommodate guests entering the network in a variety of ways, including sponsored or unsponsored access, all the while ensuring proper access, security and management.

This scalable approach works with a broad range of devices. It provides end users with greater freedom, while giving network managers greater peace of mind.

ACRONYMS

AFN	Application Fluent Network
BYOD	Bring Your Own Device
LAN	Local Area Network
MAM	Mobile Application Management
NAC	network access control
NAP	network access protection
QoS	quality of service
RADIUS	Remote Authentication Dial In User Service
TACACS+	Terminal Access Controller Access-Control System Plus
uNP	user network profile
VLAN	virtual local area network
VPN	virtual private network
WLAN	Wireless Local Area Network

Alcatel·Lucent Enterprise