Unified Communications

e book

www.voiceanddata.com.au

voiceanddata
.com.au
Information & communications technology

WESTWICK-FARROW MEDIA

Unified communications (UC) has many potential benefits for organisations.

Some of these benefits include cost savings, through the use of IP telephony. By getting rid of a traditional phone system and instead routing calls as VoIP over a data network, companies can save significant dollars on calls, as well as telephony administration.

But the more interesting benefits of UC are less tangible, coming in the form of smoother communication between staff members, and to customers. This is thanks to UC's integration of various forms of communication, such as email, telephony, instant messaging, videoconferencing and more.

For example: pre-UC, two staff members in separate offices spending time trying to catch one another on the phone, in order to organise an in-person meeting, to work on some project, taking days in the process.

With UC, staff member A can leave a voicemail that is converted to text and sent straight to staff member B's email. When both are at their desks, a presence utility can notify the workers that they are both available. They can launch a collaboration application at the click of a mouse button, enabling them to complete their project - while discussing it via videoconferencing - without leaving their offices.

By reducing the latency that comes from employees using disparate forms of communication, organisations can get things done quicker.

This UC eBook features several articles on emerging movements in UC, including cloud-based UC, mobile device management, collaboration technologies and several guides to implementing UC.

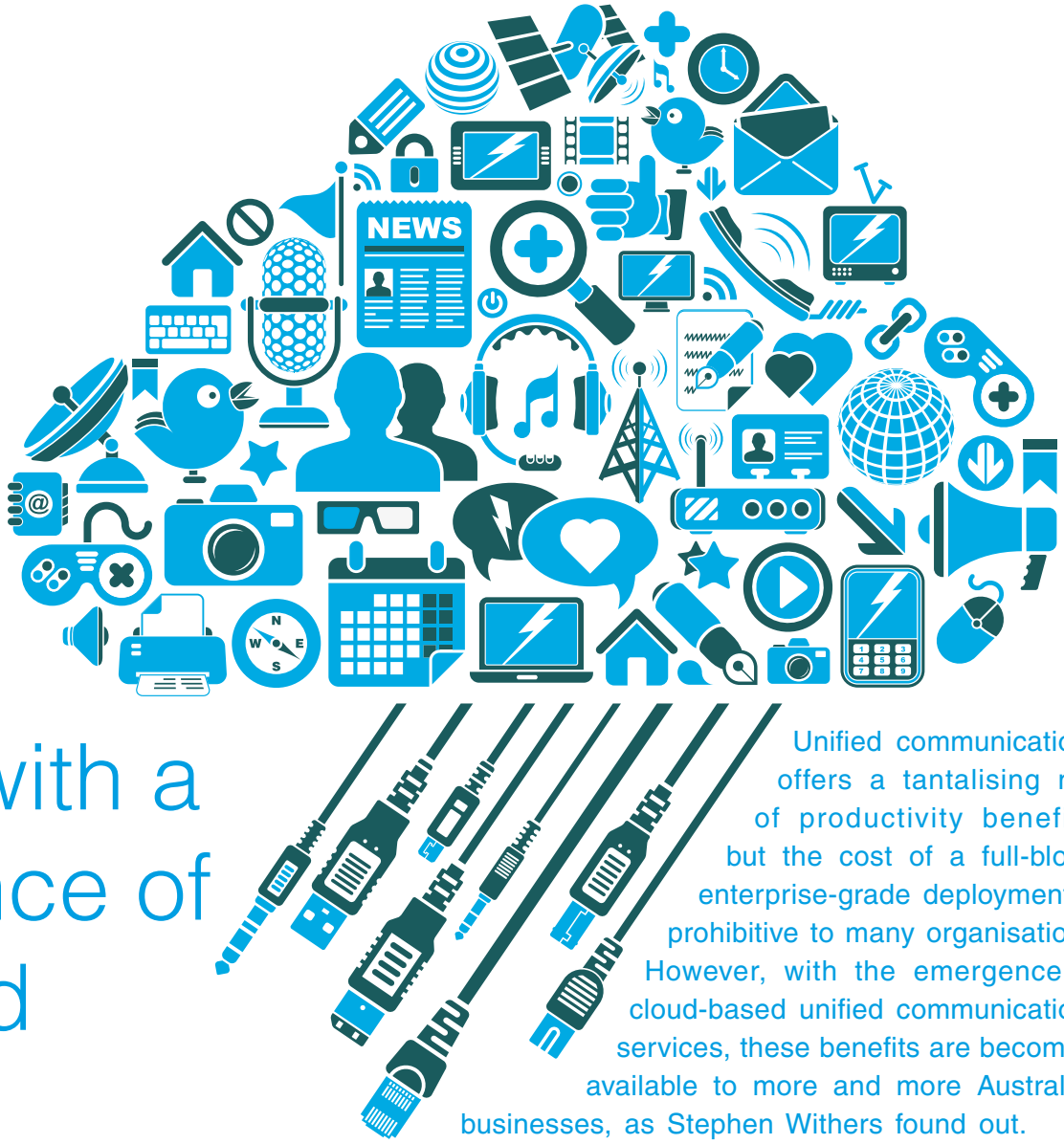
Andrew Collins
Editor – *Voice+Data*

Contents

3 UC with a chance of cloud

6 How planning will make your UC project more successful, more sustainable and less risky

10 Managing the mobile



UC with a chance of cloud

Unified communications offers a tantalising mix of productivity benefits, but the cost of a full-blown enterprise-grade deployment is prohibitive to many organisations. However, with the emergence of cloud-based unified communications services, these benefits are becoming available to more and more Australian businesses, as Stephen Withers found out.

Traditionally, a unified communications (UC) implementation has involved either taking on the configuration and management of fairly complex servers or cobbling together a collection of often consumer-grade services, but the shift towards hosted and cloud systems means that enterprise-grade services are, or soon will be, available to even the smallest businesses.

Audrey William, ICT Research Director at analyst firm Frost & Sullivan, says the hosted/cloud UC (or UCaaS - UC as a service) market is still at the early stages of growth, but the concept provides several key advantages. These include: flexibility, including support for telecommuters and mobile staff; ease of management, the provider takes care of the technical issues and provides customers with a simple interface for adds, moves and changes; scalability, users can be added or moved as required; and portability, if a company moves its office, it simply continues using the service from the new location. Consequently, she predicts a move away from on-premises systems.

But she draws a distinction between the real-time and non-real-time aspects of UC. Since voice and video are more demanding, she says some organisations like to keep that part of the system on-premises, even if they use a cloud or hosted services provider for the rest. William expects this hybrid model to remain commonplace, at least in the short to medium term. Around 50% of respondents to a recent local Frost & Sullivan survey said they were using no hosted UC components at all, and only a small percentage said they were using hosted telephony systems.

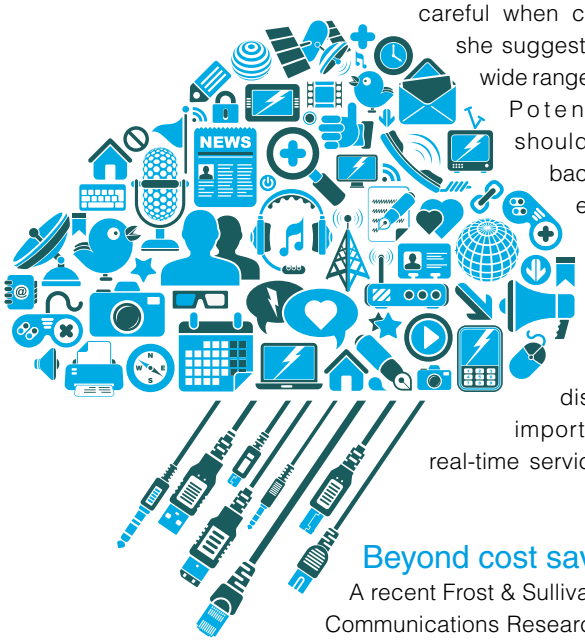
"The market will eventually mature," she said, but for now "some customers don't feel like taking the risk." Frost & Sullivan's prediction is that UCaaS will become the preferred model by 2015, and William expects to see a lot of hybrid and UCaaS trials in the next one to two years.

"Enterprise mobility will be a big driver," said William. In addition to the tendency for employees to stay out of the office, whether that is so they can work at home or on clients' premises, the growing use of mobile devices means the ability to use UC applications, via a browser, is a very powerful concept.

And SMEs are "definitely going to find this model very attractive" especially in the five to 10 employee range as the pay-per-use pricing of cloud systems allows usage to scale up and down with employee numbers and avoids the need for capital expenditure.

William says all the leading UC vendors in Australia - such as Cisco, Siemens, Avaya and NEC - offer hosted or cloud UC systems. So do the carriers: "They control the network and they have the scale," she said, and they will offer cloud and hybrid UC services to SMEs right through to enterprise customers.

Large organisations need to be especially careful when choosing a supplier, she suggests, as there will be a wide range of UCaaS providers. Potential customers should check providers' backgrounds thoroughly, especially with regard to their track records for service management and reliability. Resilience and fast disaster recovery are important, especially for real-time services.



Beyond cost savings

A recent Frost & Sullivan report ('Enterprise Communications Research: 2011') noted that "Businesses are realising that UC not only offers cost savings but also a competitive advantage through better knowledge sharing among employees and advanced communication tools."

While some customers have had valid concerns about hosted communications services (notably around security and control), the growing complexity of converged communications and IT solutions is contributing to renewed interest in hosted and cloud services. In addition to lower and more predictable costs and improved agility, UCaaS is coming to be seen as a way of enhancing business continuity and resilience.

Gartner's position is that we're at least five years away from a single enterprise UC client (the firm prefers to talk about unified communications and collaboration - UCC - but our working definition includes aspects of collaboration, so we'll stick to UC for consistency), and most businesses will be using at least three UC clients, eg for telephony, email and messaging and social networking.

The firm concluded that "The broad adoption of comprehensive UC suites, such as Microsoft Lync, IBM Lotus Sametime and Cisco UC 8.x, and their improving maturity into UCaaS, such as Microsoft Office 365 or Cisco Hosted Collaboration Service with dominant telecommunications service providers, reflects the expectation that UCC and related solutions will increasingly be delivered via the cloud."

Gartner predicts UCaaS will become mainstream in the next two to five years and deliver high business benefits. The firm notes that vendors fall into two categories: email-centric (eg, Google and Microsoft) and voice-centric (typically telcos such as Telstra or specialist providers running systems such as Cisco's Hosted Collaboration Solution). It also expects many major systems integrators to enter the UCaaS market during 2012, but warns that UCaaS functionality is 12 to 18 months behind on-premises equivalents and that some vendors' offerings do not really deserve the 'unified' label.

Local options

For many organisations, voice is the heart of UC. And when you think of voice, you think of phone companies, and then typically of Telstra. Telstra's IP Telephony (TIPT) service is "growing exceptionally well," according to John Fasso, General Manager of UC marketing. TIPT use is doubling annually, he says, with thousands of handsets being installed each month. The Broadcom-based system includes video calling and video conferencing facilities and Telstra plans to launch these aspects for medium sized businesses in the coming months.

TIPT can provide small businesses (as few as two seats) with enterprise-style functionality such as click-to-call, remote office and simultaneous ring on multiple handsets including Next G mobiles. According to Fasso, Australian SMEs currently show little interest in other UC facilities such as presence and text messaging, although Telstra is working with Microsoft in this area. A 2011 survey conducted for Telstra found that just over half of Australian small businesses have a moderate to high interest in ICT, so that leaves some 350,000 with little or no interest.

Given that 65% of small businesses have at least one member of staff spending the majority of their time away from the office, there is clearly an opportunity to use UC to help overcome this separation. But the biggest barrier to technology adoption is seen to be the upfront cost, which is where UCaaS comes in.

Another example is iiNet's Business Voice, a hosted voice service that provides features including advanced call routing (such as selective forwarding), music on hold, voicemail to email and conferencing, at prices starting from $39.95 per seat per month, including a handset, line rental and local and national calls. The service is hosted on iiNet's own servers. One downside is that you can't scale down without incurring penalty charges, but they appear to be related to the cost of the supplied handset.

"The beauty of a hosted solution means every dollar that's spent on your phone system goes

towards business productivity," says Greg Bader, head of iiNet Business. "There's no initial cost for buying the hardware and no added costs for upgrades."

Back in 2009, Avaya adopted a new UC architecture called Aura that accommodates a combination of in-house and cloud or hosted services - the hybrid model. APAC Technical Director Muneyb Minhazuddin explained that running everything in-house can be expensive, and this arrangement allows organisations with an existing investment in infrastructure to switch on selected new services for particular groups of users without having to buy more hardware or software.

While greenfields customers tend to look to the cloud from the outset, "what we've seen is a gradual migration" from on-premises to cloud or hosted systems as new functions are implemented in the cloud or through hosting services and on-premises equipment is phased out, Minhazuddin explains.

A growing organisation with an existing 100-user PABX may need to accommodate another 100 users at the same location or elsewhere. Those new users can be served from the cloud, with full interoperability with the legacy PABX. "It's not a rip and replace [upgrade]," he says.

While Avaya provides cloud services in some parts of the world, in Australia they are generally delivered through the company's partners. "Partners are enterprise-grade systems integrators as well as some service providers [ie, telcos]," Minhazuddin says, emphasising that it is a true cloud offering with rapid self-service provisioning and the option of per user, per month pricing.

Dedicated hosting is another option for situations where that is more appropriate than cloud. Avaya offers "a fully flexible model" from completely on-premises through a blend of on-premises, hosted and cloud, to pure cloud. While government agencies may be especially concerned about keeping their systems isolated from other customers, midrange organisations are more interested in the economic benefits of UCaaS, says Minhazuddin.

Pure UCaaS customers tend to be at the smaller end of town and are attracted by the 'no capex, pay by the month' model, while larger enterprises are accommodated by service providers that can take on the management of their existing hardware and offer additional services. "Uptake is at all levels."

Avaya's offerings cover a wide spectrum of customer sizes, ranging from a single user to 250,000 users in 250 locations around the world. "We've got hundreds of millions of lines worldwide," he said.

According to Minhazuddin, Avaya's UC products use true multichannel sessions, so users can, for example, jump from instant messaging to voice, or voice to video as required. "Nobody else can do that, because they're not doing the architectural change," he claims.

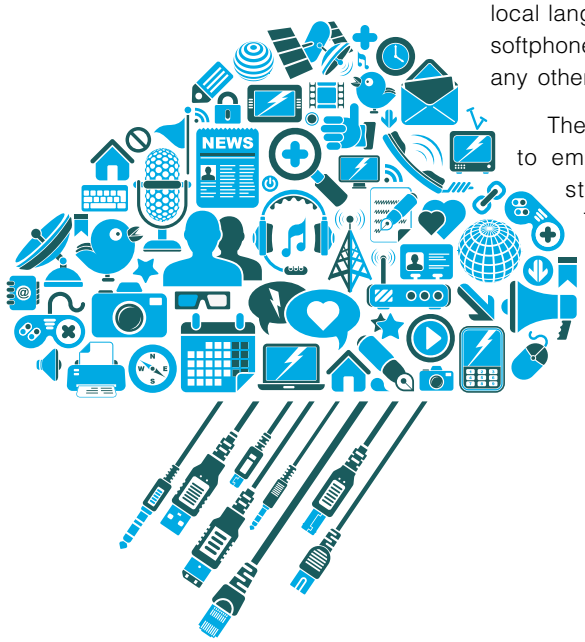
Colin Thomas, IT Manager at Teachers Credit Union, says his organisation installed an on-premises implementation of Interactive Intelligence's UC system around three years ago, but if he was making the decision today he would give serious consideration to the otherwise similar cloud or hosted system that is now offered.

"The time is ripe for that kind of product," and hosted UC is "absolutely perfect" for greenfields situations in some industries, he said. "You have to look very seriously at all options," even though cloud isn't the panacea some business leaders think it is, suggests Thomas.

Marcus Moufarrige, Chief Information Officer at virtual office provider Servcorp, says his company offers a cloud UC system to its clients. Based on Cisco hardware, the system was developed entirely in house.

Clients can self-provision the service within five minutes, he says. With 130 centres in 22 countries, Servcorp can provide phone numbers in each city that can be answered by a receptionist in the local language or English, or routed to the client's softphone or home, office or mobile number, or any other number, as required.

The system includes such features as voice to email and fax to email, but not (at this stage) presence or instant messaging. There has been a "fantastic response" to the system from clients, Moufarrige said, and the feedback "has been really phenomenal." ■



As published on www.voiceanddata.com.au

How planning will make your UC project more successful, more sustainable and less risky

Unified communications (UC) is a concept rather than a defined set of communications tools or a specific communications capability within an organisation. The historical positioning of UC as a technology to allow many modes of communications to be funnelled onto a single user device or application remains valid, but this should no longer be the principal concept. Unified communications should primarily:

Success criterion 1: *Provide a richer, more effective communications and collaboration environment that will increase efficiency and drive better organisational outcomes.*

Using this as the key concept might broaden the scope of UC and this is a good thing. A unified communications strategy should be predominantly focused on understanding and defining the organisational outcomes achievable through UC.

The typical challenges associated with delivering unified communications are associated with application integration, user adoption and operational enablement. How do you overcome these challenges? And is the result 'ubiquitous communications'?

This paper provides an overview of the approach that should be taken when planning for UC in order to ensure project success and operational enablement, and provide a user experience that is as ubiquitous as possible.

What is unified communications?

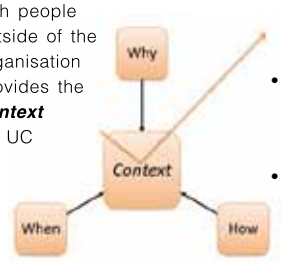
It is important to start a UC project with a key objective in mind; that is, to define what UC is for your organisation as soon as possible in the process. The assumption that the base-line deployment of a UC desktop application that caters for myriad types of communications modes (such as presence, instant message, email, video, voice and collaboration) will result in a successful UC project is a dangerous one. It is not just the delivery of the applications that makes the project successful; what is more important is the use of the applications by end users, the availability of the applications to end users, alignment with broader business strategies and, therefore, the positive impact UC has on the organisation as a whole.

To create a definition of what unified communications is to your organisation should be a primary objective of the UC business-requirements specification process. That definition allows you to understand how UC should be used and where it can be used from as opposed to simply what it should functionally provide and 'do'.

Success criterion 2: *Establish a defined and managable communications and collaboration services portfolio based on a detailed business-requirements specification.*

To support this approach, use the following high-level parameters in this definition process.

Understanding:
why how, and **when** ...
... people communicate with each other within the organisation and with people outside of the organisation provides the ***context*** for UC



The ***context*** allows you to:

- identify gaps that can be filled by UC and issues within the current communications environment that must be addressed
- understand which UC tools will be required and under what circumstances
- optimise the organisational relevance of UC maximise user adoption

The shaping of these three parameters for your particular environment will allow an initial profile (or groups of profiles) to be developed for all communications users.

It is only these communications profiles and associated user profiles and requirements that are able to provide the necessary baseline and context to continue developing your UC strategy in an optimal way. It is important to complete this process in advance of making definitive decisions around a UC vendor or platform: that decision must hinge on the output of the business-requirements specification rather than being an input.

Taking the time to specifically define unified communications within the context of your environment makes UC more tangible for the end users and stakeholders. The approach also mitigates the risk associated with building a UC environment based on a solution or vendor in isolation of broader business input and requirements specification.

In addition, taking the correct approach significantly increases the value of the requirements-specification process and the business value of the resulting UC environment. By understanding

more in advance, you can start to tackle the key challenges and success criteria around a typical UC project.

Success criterion 3: *Broad, but relevant, application integration*

Unified communications is inherently not going to be provided by a single platform or vendor. High-level and low-level applications must be integrated in order to enable unified communications to become unified and/or ubiquitous. Application integration includes planning around desktop applications, mobile applications, server applications, network applications and the supporting IP network layers required to transport UC and enable the user experience to be as constant and consistent as possible. Communication requirements and challenges associated with existing business processes should also be understood, as the UC integration scope and user adoption will be influenced by how effectively these processes can be enhanced.

Success criterion 4: *Organisational relevance and user adoption*

Although use case scenarios are essential, this is an area that is often overlooked in the planning and discovery phases. When establishing with the user base what UC tools and functions will be available to them, it is essential that the interoperation of those tools (ie, the real-time usage of voice, video, instant message, email, etc) is flexible and functional enough to meet mobility requirements, different preferences and workforce strategies (such as using UC to enable more remote/home working).

Again, with UC inherently encompassing a variety of applications (both data and communications), there is an expectation that everything is accessible and easy to use. Precise use case scenarios should be established before design and deployment to ensure that the solution is viable and that the resulting usability of the environment meets the stakeholders' requirements and expectations.

Success criterion 5: *Operational enablement*

This is a broad challenge for unified communications deployments that are made somewhat more challenging as the deployment aims to become more ubiquitous. At a high level, the operational enablement is greatly facilitated by understanding and addressing the application-integration and user-adoption challenges. Operational capability and any required adjustments to that capability or cost should be understood as soon as possible within the planning and discovery phases as ultimately they will affect what will be in the UC services portfolio and the subsequent rollout strategy.

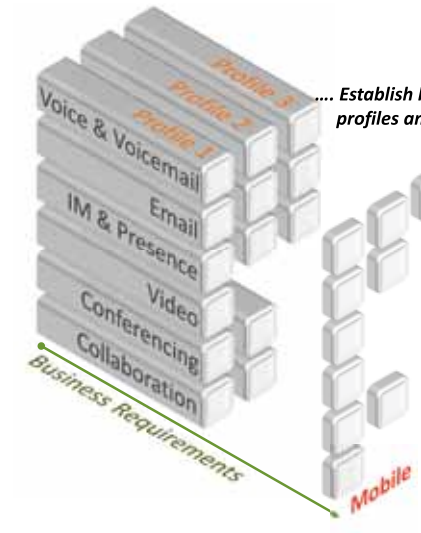
What is interoperability within UC? And why is it so important?

Interoperability analysis should start with profiling the UC business requirements.

…. Establish UC profiles and UC application filters

Not everyone in the organisation necessarily needs access to all UC applications

The value might be reduced by simply deploying everything, everywhere to everyone and expecting them to use it at all, or use it effectively. Equally the operational cost is higher than it needs to be



…. Establish locations, develop profiles and fine-tune filters accordingly

Mobility, accessibility and flexibility are all key terms for UC and provide the basis for 'Ubiquity'

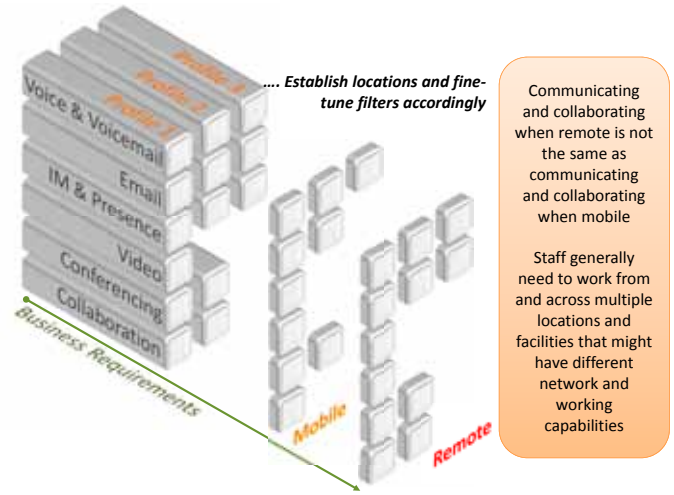
How does this affect the profiling in principle?

What services should be available under what circumstances to whom?

- Once why, how and when people need to communicate with and within the organisation are understood, the specific UC services and tools can be better identified.
- Interoperability is initially identified at the user level. It is not easy and relevant for users to use the tools defined for them in the profiling, then they will either not use the tools at all or not use them effectively or within the context of the UC strategy and required outcomes.
- Interoperability should only then be addressed at the product and infrastructure level because, before this point, you don't really know what needs to be achieved, on what scale, in which locations and circumstances and, therefore, what products, applications and supporting network infrastructure are required for a particular use case.

A note on business-requirements specification

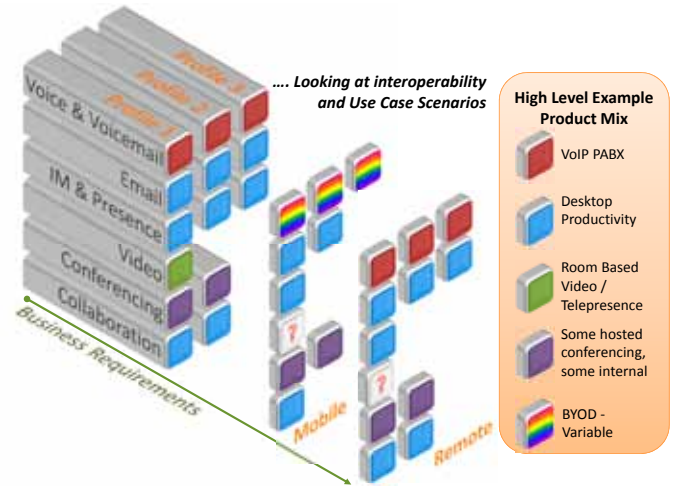
Generating business-requirements specifications for UC should not be about simply sitting down



.... Establish locations and fine-tune filters accordingly

Communicating and collaborating when remote is not the same as communicating and collaborating when mobile

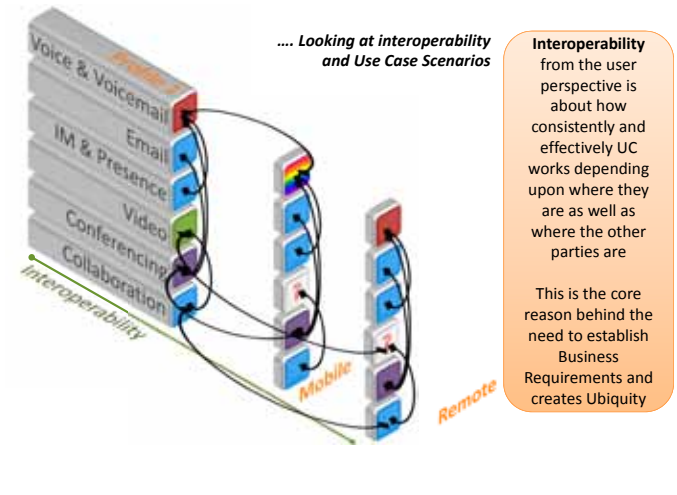
Staff generally need to work from and across multiple locations and facilities that might have different network and working capabilities



.... Looking at interoperability and Use Case Scenarios

High Level Example Product Mix

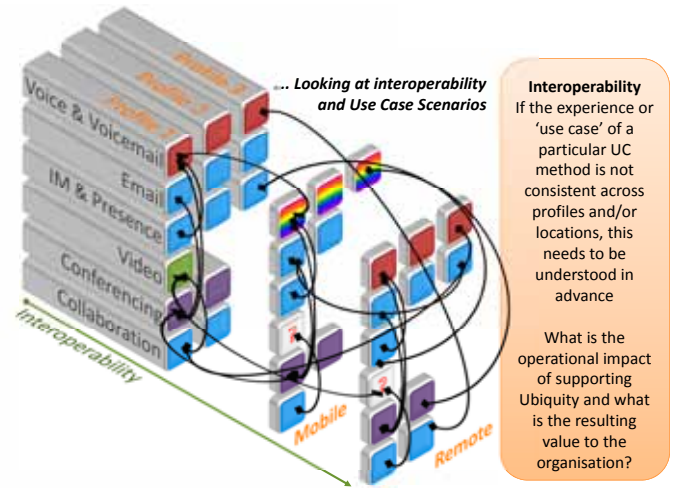
- VoIP PABX
- Desktop Productivity
- Room Based Video / Telepresence
- Some hosted conferencing, some internal
- BYOD - Variable



.... Looking at interoperability and Use Case Scenarios

Interoperability from the user perspective is about how consistently and effectively UC works depending upon where they are as well as where the other parties are

This is the core reason behind the need to establish Business Requirements and creates Ubiquity



.... Looking at interoperability and Use Case Scenarios

Interoperability If the experience or 'use case' of a particular UC method is not consistent across profiles and/or locations, this needs to be understood in advance

What is the operational impact of supporting Ubiquity and what is the resulting value to the organisation?

with a range of users and asking them what they want. This misconception and subsequent reluctance to engage with the business properly has led to many UC projects being based around the capability of a product and assumptions around how it might best be used. This is not necessarily an incorrect approach, but it is certainly less than optimal and can become disruptive to the ongoing development of UC beyond the initial deployment. It is important to understand that gathering business-requirements specifications for UC is about empathy with, and understanding of, the business challenges and inefficiencies associated with the current communications environment. Solve current communications issues, reduce organisational inefficiency and align the UC strategy to other organisational focused strategies and your project will be:

- more successful,
- more sustainable,
- and will involve less risk.

An ideal approach

Profiling is the key to ensuring that the principal factors outlined so far drive your UC project. It represents an opportunity for IT to increase business and stakeholder focus on, and association with, the project.

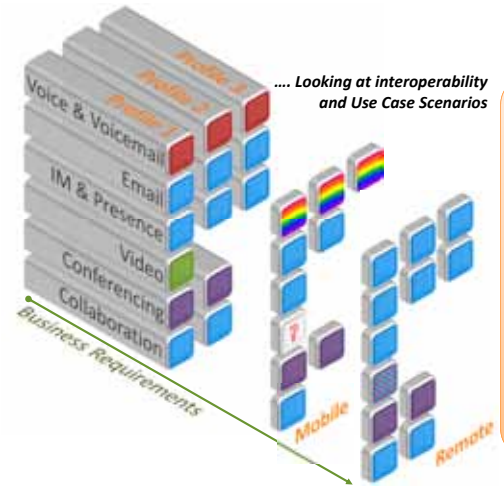
On the following pages, a typical range of UC services is used, including:

- voice services and voicemail
- collaboration
- email
- conferencing
- instant message and presence
- video

An increased number of services or a more granular breakdown of collaboration services, for example, might be required, depending on your required outcomes.

Conclusion

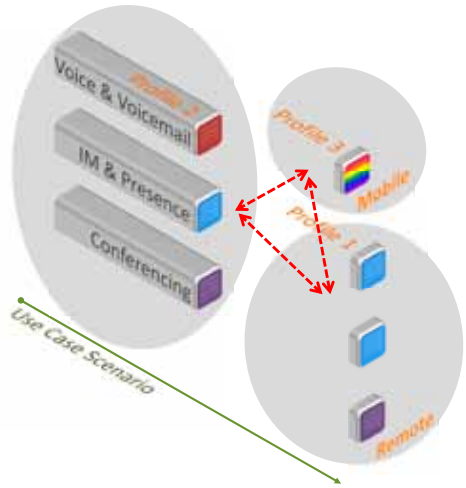
Setting the correct success criteria around a unified communications project and taking an organisational-centric approach will allow you to address current communications issues, reduce



…. Looking at interoperability and Use Case Scenarios

What is a Use Case Scenario?

Specifically in the following example: A user in Profile 1 is remote. They need to set up a conference (voice and multi-media) with a user in Profile 2 who is on campus. Half way through they need to bring a Mobile user from Profile 3 in to the conference…



In this particular use case – how easy it for these three users to interact in the required way?

What is the organisational outcome of enabling access to this scenario – what is the value vs. the cost of supporting?

How does the setup differ to other user cases?

inefficiency and align the UC strategy to other organisational strategies. This will mean that the project will be:

	more successful	more sustainable	and will involve less risk
because	UC will have higher level of business and organisational relevance.	UC will have stronger and broader endorse-ment within the organisation and a more tangible value.	Fewer assumptions are required around the operational requirements, accessibility, scalability, flexibility and complexity, along with their associated costs.
which means	UC will have dramatically enhanced user-adoption levels and therefore have a greater positive organisational impact.	The underpin-ning UC strategy will be allowed to move forward with more readily available funding and develop in unison with other IT and organisa-tional strategies.	IT can properly plan for the operational impact of UC, which is typically quite high. Unexpected, costly operational overheads as well as unpredicted business demands on the UC environment will generate an impression of failure of a UC project however well it has been technically implemented – this risk can be avoided.

It is, of course, an imperative to deliver a solution that works from a technical perspective. But limiting success factors to technical delivery backed only, as is often the case, by outcomes defined in limited 'proof of concept' environments is likely to result in a less than satisfactory outcome from an organisational perspective. The costs typically associated with taking the approach outlined in this paper are always a fraction of the costs associated with deploying and operating the new UC environment and yet the value is significant.

Ubiquitous communications is not necessarily a natural outcome of deploying unified communications, but it is certainly an extension or leveraging of unified communications. The distinctions are really that:

- Ubiquitous communications is more the concept of being continually connected through a variety of means, methods and applications. A current analogy is where the boundaries between UC and social media are starting to blur and merge.
- Unified communications is all about increasing efficiencies and the overall capability of an organisation to achieve its goals and strategies.

Ubiquitous communications will provide an additional, passive layer to unified communications: the recipient and how they might use that communication are unknown, which - if you think about it - is actually contradictory to this principal of unified communications. Ubiquitous communications is distinct in as much as it allows recipients to choose whether or not to respond or add to the communication, or, indeed, even 'consume' it in the first place. ■

Author

This white paper was authored by Stuart Kirkby, Domain Expert/Solution Architect (Unified Communications) at NSC Group. Stuart has been working in multiple roles within the unified communications industry for over 16 years, spanning architecture, engineering, service delivery and organisational change.

Stuart has worked for NSC Group for the past seven years, primarily within Avaya and Microsoft unified communications and messaging technologies.

While working with NSC Group, Stuart has enabled unified communications for tens of thousands of users within business, government and educational organisations. This experience has brought him to his current role within NSC's Consultancy Group as a UC domain expert and solution architect where he is responsible for pioneering NSC's evolutionary approach to delivering communications capability to its customers.

Managing the mobile

The proliferation of mobile devices - company-owned and BYOD - is boosting corporate productivity. But it also presents a new management issue to IT, which needs straightforward ways to ensure these devices are appropriately and securely configured and to oversee compliance with usage policies. Enter mobile device management (MDM).

Multiple surveys show the widespread use of personal devices in corporate environments. In an August 2011 global survey, conducted for Dell KACE, 87% of respondents said employees were using their own devices for work purposes. It seems to be even more widespread in Australia - a January 2012 survey conducted for VMware found 93% of surveyed organisations know that employees are using their own devices. 51% of respondents (all executives) said they worked more efficiently when able to choose what web-based or customised software and apps they use at work.

The problem for IT is to provide appropriate governance (eg, taking steps to ensure that sensitive information isn't stored on the device, that all corporate information can be wiped from the device if it is reported lost or stolen and that password complexity rules are applied).

Such steps need to be taken without unduly interfering with the user. If you want full control over devices, then buy them for your users - but don't be surprised if they still opt to use personal devices for work purposes. On the other hand, if you're paying the phone bill, it's legitimate to ask a particular employee why they're consuming more data on weekends than they are between Monday and Friday - to do that conveniently, you'll need the right tools.

"You can't actually control these devices… so it's about governance. We call it the carrot and stick approach," said Robertson Roe, managing director, Australia and New Zealand, AirWatch. For example, it isn't possible to prevent an iOS device owner jailbreaking it, but if they do, mobile device management (MDM) software can respond, perhaps by remotely wiping all the corporate assets it contains.

"Most companies lack the people, processes and tools to manage the rapidly expanding number of mobile devices that require access to corporate information. Enterprises are struggling with smartphone and tablet (mobile endpoint) management, which results in increased security risk, growing usage costs and diminished IT control," said Michael Disabato, research vice president, Gartner.

"The era of fully supporting a single-vendor, company-owned, enterprise-class device (eg, BlackBerry) is declining while the era of offering tiered support for multivendor, employee-owned, consumer-class devices (eg, iPhone and Android) is growing. Mobile device management solutions help enterprises manage smartphones and tablets by providing centralised, multivendor device management that results in lower risk and improved cost of ownership." AirWatch and Good Technology are among the vendors that Gartner regards as leaders in MDM.

And according to Brian Duckering, senior manager, product marketing, Symantec: "when all the hype dies down, mobile devices are just another endpoint" that needs to be managed. The question then becomes "what are the policy settings and controls that are right for your company, industry and location?"

Provisioning

Setting up a device with the right set of applications, support files and settings can be a chore. The list can include: generally available apps that you want on your users' devices (free and paid; the absence of volume licensing for Australian customers of Apple's App Store will hopefully be remedied soon, in which case the ability to manage iOS licence codes will become important); apps that you don't want them to use (eg, a mechanism for removing blacklisted apps, although that can be a contentious issue and there are other ways of maintaining the corporate/personal separation - see below); company-specific apps; security certificates (eg, for VPN access); settings such as forcing the use of a passcode; and configuring a corporate email account.

It will also help if the MDM software can operate on a self-service basis when an employee arrives with a new device. This will most likely require integration with Active Directory or another directory service so that the device receives the right configuration, based on the user's identity or membership of particular groups.

Since BYOD extends to notebook computers, it may be worth looking for software that handles Windows and Mac OS X as well as iOS, Android and other mobile platforms.

Secure storage

There is particular (and perhaps excessive) concern about the risk of losing - or losing control of - sensitive data stored on mobile devices in the event they are stolen or mislaid or when the owner of the device leaves the company.

There are two basic approaches: either avoid storing data on the device in the first place or use encryption to make life difficult for the finder.

The first approach typically involves using web apps or virtualisation. The software runs on a remote server rather than on the device itself and only the results are displayed. If the device is lost, the information cannot be extracted from local storage. The downside is that such applications aren't available if the device is offline (eg, when travelling by air).

"I have no concern about security," said Peter James, food service division general manager at Craig Mostyn Group, even though his sales staff use unmanaged iPads. That's because the ERP and CRM data remains on the server, so the issues are the same as they would be in a traditional environment.

Encryption can either be applied to individual files or to a 'container' holding the corporate apps and data on the device. The latter approach is used by Good Technology. "We are by far the largest player in our market," said Jim Watson, vice president and corporate general manager APAC, Good Technology, with major Australian customers in the banking, mining, legal, professional services, and healthcare sectors. Good for Enterprise provides a native-like experience for calendars, contacts and so on, while allowing optional integration with the native equivalents.

With implementations for iOS, Android, Windows Phone and others, Good for Enterprise also provides provisioning (including support for self service), policy management by user or group, remote lock/wipe and more.

An advantage of being able to remotely wipe just the container is that "if you find the device… you've still got all your personal data," said Watson. Good also offers third-party developers an API to containerise their apps in this way.

Mobile users are accustomed to the convenience of services such as Dropbox, so companies such as AirWatch have built secure equivalents into their MDM offerings. "We see people so worried about Dropbox," said Roe, explaining that his company uses 256-bit AES encryption to protect the data on the device and SSL to protect it in transit. Documents can be downloaded automatically or on demand and may be time limited (eg, so a price list can only be seen during its period of validity). There's also a mechanism to stop them being saved as normal files on the device.

Network access

There are two main aspects to network access for mobile devices. The first is ensuring that only 'authorised' devices can connect to the organisation's network and other resources; the second is managing expenditure on carrier networks (for phone calls and data).

Connecting devices securely to corporate networks is a well-defined process. The role of MDM software, in this regard, is to simplify and automate it as much as possible. An employee may be able to arrive at work with a new device and

make an initial wireless connection that triggers an enrolment process (based on the user's identity as verified through a password and possibly another authentication mechanism). The process would provision the device, as described above, and grant access to the relevant resources.

Managing the use of carrier networks is more about gaining immediate visibility of how and when the device is being used, especially if the organisation is picking up the bill. The data collected can be used to provide guidance to any employees that may be going beyond the realms of reasonable private use.

A related issue is internet filtering. While in-house use may be controlled at the firewall, there is sometimes a desire to control off-premises browsing on company sanctioned (though privately owned) devices.

AirWatch plans to add a 'secure browser' to its product which will enforce blacklists or whitelists, even when the device is not connected to a corporate network. This would be used in conjunction with the product's ability to block the device's standard browser.

Good Technology recently announced Good Mobile Access for Android, a secure mobile browser for access to behind-the-firewall applications (such as SharePoint) and other resources, without the need for a VPN. Cookies, caches and other browser data are encrypted within the Good container, on the device.

Duckering notes that Symantec's software can restrict the use of certain apps to particular geographical areas without maintaining a record of where the device has been.

If you're concerned with self-service provisioning, including secure network access but not detailed device management, Aruba Networks' ClearPath provides an alternative to full-blown MDM products. "Our job is to get the device onto the network," explained Mark Verbloot, director of systems engineering for Asia Pacific. The onboarding process can include checking that important operating system and application updates have been applied.

Break glass in event of emergency

If a mobile device is lost or stolen it can be useful to be able to locate it. MDM software may offer this capability by tracking the location of the device using its built-in GPS functionality (much like Apple's Find My iPhone service but under corporate control), but it is appropriate (and in some situations mandatory) to obtain the individual's consent.

GPS tracking is regarded as "a dangerous precedent" by most of Good's customers, said Watson. However, there may be times when the ability to locate a device is necessary, so MDM often includes this capability. What's needed is a set of procedures and safeguards to minimise the risk of misuse and thus show respect for employees' expectations of privacy in the hope they will agree to tracking.

Whether or not location capability is available, it may be considered important, or even essential, to delete any corporate information and apps as quickly as possible. Given that the provisioning and data management aspects of an MDM product should make it quick and easy to restore this material to a found or replacement device, it is hard to argue against prompt remote wiping. However, it does require network access to the device, so this is not an excuse for failing to encrypt sensitive information.

That leaves the question of whether user data should be wiped at the same time, as MDM software can provide a complete remote wipe (aka device reset) without requiring the user's explicit permission. Again, it is up to the IT organisation to put the right processes in motion. Put yourself into the shoes of a user who has just captured a once in a lifetime video clip and then loses their smartphone before backing it up. You probably wouldn't want your personal files wiped along with the corporate data unless you were sure the device was gone forever. Possibilities include various combinations of self-service remote wipe, building consent into the acceptable use policy for personal devices, and allowing first-level support staff to wipe corporate data, while requiring escalation for a complete wipe.

Monitoring

Location tracking may be a delicate issue, but it is easy to justify usage monitoring when the organisation is picking up the phone bill. MDM software may be able to track and report on voice and data usage, disable international roaming (even if it can't stop the user turning it back on), check the MDM agent on the device is still running and generally indicate that settings and usage remains in compliance with policy.

Cloud or on premises?

Cloud implementations of MDM are particularly convenient for smaller organisations with relatively unsophisticated IT. There's no need to install and manage software, just pay each month for the number of devices your people are currently using. For example, AirWatch charges $3.50 per device per month and it has servers in Australia, taking care of data sovereignty issues.

According to Phil Offer, director, mobility and convergence at Optus Business, organisations have been waiting for a carrier to provide a MDM service and the latest update to Optus Mobile Device Management will provide comprehensive cover for company and employee-owned devices. The service is a rebranding of an unspecified vendor's product - customers wanted to deal directly with Optus, he said. Optus MDM is offered on a 24-month contract in batches of 25 device

licences. Offer said the service was relevant to "any organisation with a large smartphone fleet."

Organisations that already use a systems management tool may prefer an MDM product that fits into that framework. Duckering said Symantec's recent acquisition of Odyssey Software had given it a mechanism to provide MDM to users of Microsoft System Center Configuration Manager, along with support for Android and Windows Phone 7, in addition to iOS.

Similarly, McAfee Enterprise Mobility Management supports iOS, Android, Windows Phone 7 and BlackBerry devices and integrates with McAfee ePolicy Orchestrator and other corporate IT services. Likewise, Kaseya's Mobile Device Management (for iOS, Android, BlackBerry and others) integrates with the rest of the Kaseya IT Automation Framework so mobile devices, desktops and servers can all be managed from one place. ■

As published on www.voiceanddata.com.au

An anonymous example

An Australian professional body found it was issuing board members with as many as 500 pages of papers prior to meetings, which was particularly inconvenient when travelling. Delivering the material via tablet was an attractive alternative, but the nature of some of the material meant the organisation wanted a mechanism to remotely lock or wipe lost or stolen tablets. Another consideration was the desire to easily provision tablets for different groups of users, explained the organisation's business solutions manager. (Corporate policy prevented him from identifying his organisation.)

At that time, there were just a few vendors in the MDM space and it found AirWatch was the only one prepared to make its people available during Australian business hours (the company now has an Australian presence). In addition to meeting the needs set out above, AirWatch also provides the ability to manage devices in terms of unacceptable apps, excessive data use and overseas roaming for data.

resources

from our sponsor

NSC Group: leading the way in customer contact

NSC Group helps medium and large organisations communicate with their customers and their staff. We use insight and technical expertise to design, implement and support sophisticated communication systems across a range of media: voice, web, email, social media, messaging and video.

We work with you to identify, explore and document the business issues before proposing relevant technologies that deliver genuine benefits. We offer end-to-end solutions and an integrated, seamless approach to organisational communication. After commencing with consulting and planning, we can then design, install, integrate and provide ongoing support for your communication systems.

For more information on how we can help your organisation:

phone us on: 1300 366 304

visit our website: www.nsc.net.au