Making Everything Easier!™

Avaya Custom Edition

Midmarket Collaboration

FOR DUMMIES®

A Wiley Brand

Learn to:

- **Benefit your business with a collaboration solution**
- **Engage a distributed, mobile workforce**
- **Produce faster, smarter decisions that lead to better business**

Brought to you by

AVAYA

The Power of We™

Lawrence C. Miller, CISSP

Midmarket Collaboration

FOR DUMMIES®
A Wiley Brand

Avaya Custom Edition

by Lawrence C. Miller, CISSP

FOR DUMMIES®
A Wiley Brand

Midmarket Collaboration For Dummies®, Avaya Custom Edition

Published by
John Wiley & Sons, Inc.
111 River St.
Hoboken, NJ 07030-5774
www.wiley.com

ISBN 978-1-118-91427-4 (pbk); ISBN 978-1-118-91515-8 (ebk)

Manufactured in the United States of America

10 9 8 7 6 5 4 3 2 1

Publisher's Acknowledgments

Some of the people who helped bring this book to market include the following:

Senior Project Editor: Zoë Wykes

Acquisitions Editor: Katie Mohr

Editorial Manager: Rev Mengle

Business Development Representative: Sue Blessing

Custom Publishing Project Specialist: Michael Sullivan

Project Coordinator: Melissa Cossell

Special Help from Avaya: Gary Proefke, Eric Lai, Richard Solosky, Matt Young, Luke Stangel

Table of Contents

Introduction

How well connected are you? That's the challenge in today's mobile, virtual business landscape as companies strive for consistent communications between employees, business partners, and clients. Too often, a remote working world can feel splintered, disconnected, and complicated, resulting in lower productivity and lost opportunity. What you need is a rich, seamless environment that instantly keeps everyone connected, effortlessly collaborating and sacrificing nothing in the process. It's the difference between simply doing business and doing business simply.

About This Book

As a midsize company, you have the same goals and objectives as larger enterprises — but you don't necessarily have the same resources to achieve them. You need a cost-effective, easy-to-implement-and-maintain collaboration solution, one that gives you the agility and flexibility that your business demands.

Midmarket Collaboration For Dummies, Avaya Custom Edition, explores the midmarket business trends in collaboration, how collaboration can drive productivity and strategic advantage, the networking and security challenges for midmarket businesses, and much more!

Foolish Assumptions

It's been said that most assumptions have outlived their uselessness, but I'll assume a few things nonetheless!

First, I assume that you're part of a midsize business or organization with communication and collaboration challenges. Perhaps you're trying to increase productivity among a group of remote or mobile workers. Or you need to improve your collaboration capabilities with customers and business partners. Or

you're trying to figure out how to manage the "Bring Your Own Device" trend in your organization. If any or all of these challenges apply to you, keep reading — this is the book for you!

As a midsize business or organization, you most likely don't have the same technical resources as a large enterprise. Your IT department may consist of a handful of very dedicated and knowledgeable technology generalists, rather than large teams of siloed specialists with more defined — and limited — roles and responsibilities. Your IT department is expected to know a little about everything; if it has a power cord, they support it! In this book, you learn about collaboration solutions designed for just such an environment.

Icons Used in This Book

Throughout this book, you'll occasionally see special icons to call attention to important information. You won't see any smiley faces winking at you or any other cute little emoticons, but you'll definitely want to take note! Here's what you can expect:

This icon points out information that may well be worth committing to your nonvolatile memory, your gray matter, or your noggin — along with anniversaries and birthdays!

You won't find a map of the human genome here (or maybe you will, hmm), but if you seek to attain the seventh level of NERD-vana, perk up! This icon explains the jargon beneath the jargon and is the stuff legends — well, nerds — are made of!

Thank you for reading, hope you enjoy the book, please take care of your writers! Seriously, this icon points out helpful suggestions and useful nuggets of information.

Proceed at your own risk . . . well, okay — it's actually nothing *that* hazardous. These helpful alerts offer practical advice to help you avoid making potentially costly mistakes.

Beyond the Book

Although this book is chock-full of information, there's only so much I can cover in 72 pages! So, if you find yourself at the end of this book, thinking "gosh, this was an amazing book, where can I learn more?" just go to `www.avaya.com`. There, you can learn more about Avaya's collaboration solutions for midsize businesses.

Where to Go from Here

With our apologies to Lewis Carroll, Alice, and the Cheshire Cat:

"Would you tell me, please, which way I ought to go from here?"

"That depends a good deal on where you want to get to," said the Cat — err, the Dummies Man.

"I don't much care where. . .," said Alice.

"Then it doesn't matter which way you go!"

That's certainly true of *Midmarket Collaboration For Dummies,* Avaya Custom Edition, which, like *Alice in Wonderland,* is destined to become a timeless classic!

If you don't know where you're going, any chapter will get you there — but Chapter 1 might be a good place to start! However, if you see a particular topic that piques your interest, feel free to jump ahead to that chapter. Each chapter is individually wrapped (but not packaged for individual sale) and written to stand on its own, so feel free to start reading anywhere and skip around! Read this book in any order that suits you (although I don't recommend upside down or backward). I promise that you won't get lost falling down the rabbit hole!

Chapter 1

The Business Case for Midmarket Collaboration

In This Chapter

- Recognizing the business benefits of collaboration
- Taking a look at the midmarket economy
- Understanding important midmarket trends
- Talking about UC&C use cases

In this chapter, I talk about Unified Communications and Collaboration (UC&C) and the business benefits of a UC&C solution. I also discuss the definition of the midmarket, important trends, and how they affect your business.

What Collaboration Is and How It Can Help Your Business

Making your organization's employees more efficient and productive is an important goal for any business or organization. In a recent survey, 87 percent of business leaders stated that they believe collaboration improves productivity. For midsize businesses competing with much larger enterprises in a global marketplace, collaboration solutions built for a business like yours are crucial for gaining a strategic advantage.

For example, a UC&C solution enables organizations to connect employees in multiple locations with one another, with partners, and with customers — anywhere, anytime, and from any device — professionally, efficiently, and cost

effectively. This capability is key to empowering a distributed, mobile workforce to build crucial relationships, collaborate more effectively, and shorten time to decision. Such a solution enables an organization's employees to find, communicate, and collaborate instantly with one another and with others, which, in turn, drives better and faster business decisions. The majority of midmarket businesses have deployed some sort of unified communications solution or are seriously considering one (see Figure 1-1).

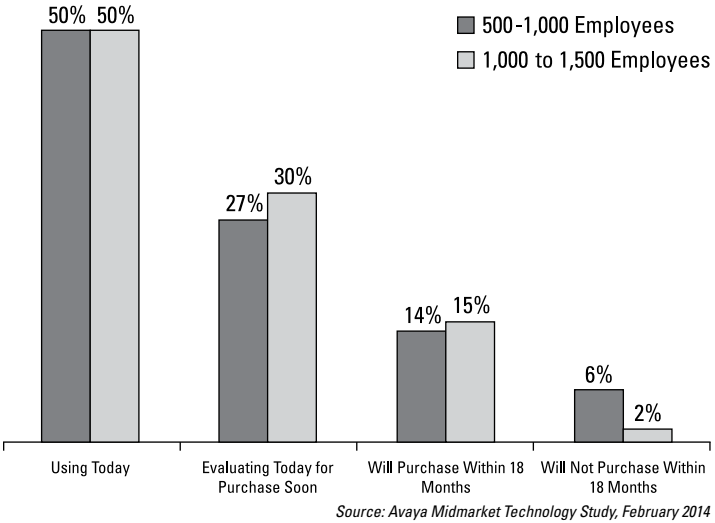


Figure 1-1: Midmarket companies that are planning to deploy UC&C.

Midmarket, Midsize — What It All Means

Is your company in the midmarket, and if so, why should you care? Although no commonly accepted definition for the term *midmarket* really exists, it is an important consideration. Midmarket companies share common attributes, and your technology provider needs to know how these attributes affect your business to recommend solutions that meet your unique needs.

In the U.S., The National Center for the Middle Market — a collaboration between Ohio State University and GE Capital — produces a quarterly performance update and economic outlook for companies with annual revenues between $10 million

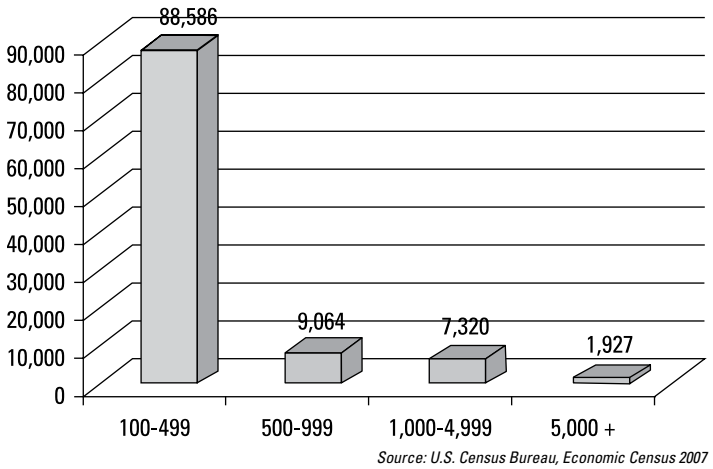
and $1 billion (see Figure 1-2). According to that report, roughly 197,000 businesses fit this description and employ 43 million people, representing a third of the private sector gross domestic product (GDP). So, if your business fits this description, congratulations! Your company matters to the world economy.

Revenue Growth **MIDDLE MARKET**		Employment Growth **MIDDLE MARKET**	
PAST 12 MO.	**NEXT 12 MO.**	**PAST 12 MO.**	**NEXT 12 MO.**
4Q'13 5.0%	4Q'13 4.3%	4Q'13 2.5%	4Q'13 2.2%
3Q'13 5.5% 4Q'12 7.0%	3Q'13 4.4% 4Q'12 5.2%	3Q'13 2.8% 4Q'12 2.7%	3Q'13 2.1% 4Q'12 2.3%
S&P 500		**ADP (PAST 12 MO.)**	
PAST 12 MO.	**NEXT 12 MO.**	**LARGE CORP.**	**SMALL BUS.**
4Q'13 1.0%	4Q'13 0.8%	4Q'13 2.3%	4Q'13 2.0%
3Q'13 2.6% 4Q'12 2.9%	3Q'13 1.0% 4Q'12 3.5%	3Q'13 2.4% 4Q'12 2.3%	3Q'13 1.8% 4Q'12 1.6%

Source: National Center for the Middle Market Q4 2014 Middle Market Indicator

Figure 1-2: Midmarket revenue and employment growth.

In the U.S., small and medium-sized businesses (SMBs) are generally defined in terms of headcount: small businesses constitute entities with less than 100 employees and medium-sized businesses consist of those having 100 to 999 employees (see Figure 1-3).



Source: U.S. Census Bureau, Economic Census 2007

Figure 1-3: U.S. midmarket and large businesses by employee count.

In the EU, small and midsized enterprises (SMEs) are defined as a category of micro, small, and midsized enterprises that employ fewer than 250 people and have an annual turnover not exceeding 50 million euros. These businesses may be eligible for EU business-support programs and may have fewer requirements or reduced fees for EU administrative compliance.

But when it comes to the midmarket, varying descriptions enter in — between 250 and 1,000 employees, less than 2,500 employees, and so on. And even if there were agreement, what does company size say about how your requirements differ from those of a large enterprise?

Some industry analysts see the midmarket as a "tweener" market — a company-size segment situated between SMB and enterprise markets. But going beyond company size, the midmarket is better defined by a company's adoption of technology and its support characteristics.

Much like a large enterprise, midmarket companies think about technology strategically and have a distributed multi-office profile. Unlike most SMBs, however, midmarket companies have an IT department, albeit one limited in staff in some areas. Think of a midmarket company as one with enterprise aspirations but limited IT resources.

A midmarket company needs a UC&C solution that is custom-built. Such a solution is

- Powerful, but with simplicity and value.
- Well-integrated with existing networks and systems.
- Easy to manage and reduces risk for the company.

Aligning Your Business with Midmarket Trends

Midmarket considerations and drivers include the following:

- **Workforce**
  - Working outside the office (nearly half of all information workers)
  - Using smartphones, tablets, and other mobile devices as standard business equipment

- **IT trends**
  - Enhancing and extending mobile infrastructure
  - Securing the "Bring Your Own Device" (BYOD) organization
  - Virtualizing servers
  - Optimizing infrastructure
- **IT support**
  - Working with limited IT staff
  - Minimizing exposure to risk
  - Dealing with complexity in applications and operations

A vendor or solution provider offering a collaboration solution should understand these trends and present a complete solution — one that meets requirements, yet is simple, with minimal exposure to risk. Further, the provider should demonstrate an understanding of the implications that deploying a collaboration solution may have on your existing infrastructure.

For example:

- Additional bandwidth and network capacity may be required to support additional devices and technologies, including video. In fact, the typical employee now uses more devices (such as desk phones, smartphones, desktop PCs, and tablets) during a workday than ever before.
- Securing UC&C is different than securing a data network.
- More robust routing strategies and dial plans may be needed as multi-site configurations are extended and flattened.

Finally, an increasingly mobile workforce using a variety of devices remains a major driver of UC&C solutions. Both large and small companies share four priorities related to UC&C:

- Extend internal systems for mobile access
- Improve mobile security
- Support smartphones
- Support tablets

Within that context, midsize businesses are exploring the means of optimizing their IT infrastructure, including server virtualization, cloud services, and other ways of reducing capital expenditures (CAPEX) and the IT footprint while simplifying management overall.

Looking at UC&C Use Cases

Here's a look at some common midmarket use cases for UC&C solutions.

Work from anywhere

A recent study by Business Impacts states that, on average, executives spend 37 percent of their workweek away from their primary work location and that 40 percent of U.S. information workers regularly or occasionally work outside the office. As a result, 59 percent of midmarket companies either have reduced or plan to reduce office space because flexible/remote workers need fewer desks.

A UC&C solution supports a distributed and mobile workforce in a variety of situations, enabling employees to appear as if they are in the office while not sacrificing productivity, regardless of where they may be.

For example, knowledge workers can work from home — or just about anywhere — taking calls, participating in meetings, and answering e-mails just as if they were in the office. Line managers can stay connected with their teams wherever they are. Parents with a sick child at home can quickly and easily get connected with the office and still tend to personal matters. And program managers can stay close to a project with lots of moving people and parts.

Access on the go

The BYOD trend has certainly revolutionized the way we all work and collaborate with one another and has blurred the line between our work and personal lives. According to Business

Impacts, 60 percent of information workers use mobile devices for both work and personal purposes, and 52 percent use two or more devices for work. These devices include smartphones, tablets, and laptop computers, among others.

The ability to have access on the go empowers midmarket employees in a number of ways. A sales executive can increase product sales, while a sales generalist can consult an expert from anywhere. Similarly, a support manager can be more accessible to customers, and a mobile technician can be more effective and efficient in the field.

More powerful collaboration

Collaboration is extremely important to the midmarket. UC&C enables midmarket businesses to collaborate in a number of powerful ways (see Figure 1-4). For example, training departments can expand their reach and control, distributed teams can keep a project on track, human resources departments can reduce recruiting costs, and engineering departments can easily consult with experts across the globe.

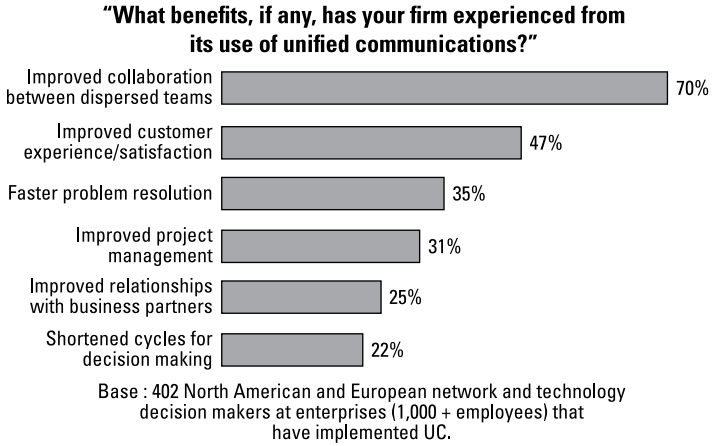


Figure 1-4: The top benefit of UC&C is improved collaboration.

How the workforce works together

UC&C empowers a mobile, distributed workforce to collaborate in powerful new ways.

Imagine a salesperson on the road using his smartphone to contact a product manager in the office about an issue.

- The salesperson securely connects to the corporate network via a session border controller (SBC, which I talk about in Chapter 3), locates the product manager using presence, then sends her an instant message (IM) that he needs to talk to the vendor about the product.
- The product manager receives the IM on her tablet and then makes a call from her tablet to the salesperson to get more details about the issue. She then sends an e-mail invitation to the vendor and the salesperson to join a video collaboration session so that the three of them can quickly work out a solution for the customer.

With powerful UC&C solutions, midmarket businesses can compete with the same professionalism and efficiency of much larger enterprises, without all of the resources and overhead.

Chapter 2

Mobile Collaboration

In This Chapter

- Looking at the challenges of a mobile workforce
- Having remote accessibility
- Collaborating through videoconferencing
- Embracing BYOD

An increasingly mobile workforce using a variety of devices remains a major driver of Unified Communications and Collaboration (UC&C) solutions. A recent survey by Forrester Research of both large and small companies found that more than 40 percent of businesses shared four priorities: to extend internal systems for mobile access, to improve mobile security, to support smartphones, and to support tablets.

In this chapter, I discuss UC&C for a mobile, distributed workforce.

Understanding Mobile, Distributed Workforce Challenges

As the workforce moves more and more onto mobile devices, UC&C capabilities are rapidly becoming essential to businesses. Safely enabling and empowering these devices becomes an ever bigger issue. How big of an issue? The number of mobile-connected devices is projected to exceed the world's population by the end of 2014.

A recent Gartner, Inc., report found that knowledge workers typically use at least three different mobile devices (for example, smartphones, laptops, and tablets), not all of which are owned by the business. According to AMI Partners, 40 to 50 percent of all cellular calls are made and received while the user is in the office and in range of Wi-Fi. Therefore, it's not surprising that, according to Forrester Research, 76 percent of midmarket businesses say that it's a high or critical priority to provide more mobility support for employees both inside and outside the office, and a recent Avaya study further confirms this need (see Figure 2-1).

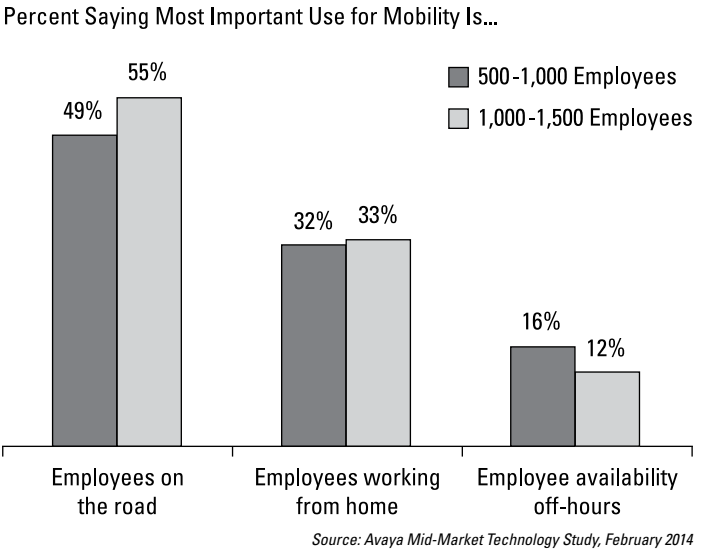


Figure 2-1: Supporting a mobile, distributed workforce is a top priority for midmarket businesses.

Access on the Go

According to a recent survey sponsored by Avaya, more than 50 percent of midmarket companies say that supporting workers on the road is their single most important use for mobility. Users stay connected and productive while on the move, and callers need remember only a single business number.

In addition to simplifying contacts with vendors and customers, the ability to have "one person, one number" is also critically important to effective real-estate consolidation strategies, such

as hoteling, flextime, and virtual offices — which are becoming much more common in the modern workplace. In fact, Forrester Research reports that 59 percent of midmarket companies have reduced or planned to reduce office space because of flexible/remote workers needing fewer desks.

Companies must not lose sight of the impact that mobility has on modern information workers in their day-to-day routine. Recent findings suggest that nearly half of an employee's impact on business profitability comes from the ability to help others perform, which reinforces the business case for mobile collaboration tools.

With robust mobility capabilities built into a UC&C solution, mobile workers can use their mobile devices to place and receive calls, send and receive instant messages, view their colleagues' presence, and conduct multiparty audio conferences, just as if they were in the office. Mobility capabilities also can enable workers to use their mobile devices to place low-cost VoIP calls through the corporate wireless network, reducing cellular costs.

Powerful Video Collaboration

Businesses should include video collaboration deployment in a wider unified communications strategy, not as a standalone purchase decision. Just as with other mobile applications, video needs to follow information workers to their homes, other offices, and on the road, and be available to them in a readily usable, integrated way.

In a recent survey sponsored by Avaya, the most important use cited for videoconferencing among midmarket companies is conferences within the company itself (take a look at Figure 2-2). In addition to the hard-dollar benefit of reducing travel costs, video provides much greater personal interaction than a voice call, allowing distributed individuals and teams to forge stronger relationships through face-to-face communication. An effective video collaboration solution will integrate seamlessly with other UC&C capabilities to enable anytime, anywhere video collaboration via virtually any device, including smartphones and tablets for employees, partners, and customers.

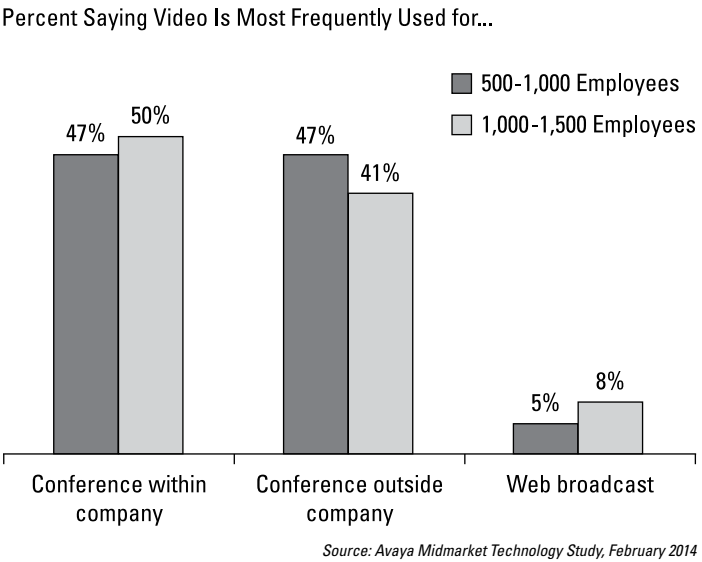


Figure 2-2: Video conference use in midmarket businesses.

With these new capabilities, videoconferencing has rapidly moved from an expensive enterprise status symbol to a functional must-have. Nearly 50 percent of midsize companies report that they have some videoconferencing capabilities already, and the average projected spend on this technology is more than $100,000 per midmarket company over the next 18 months — mainstream indeed!

The Bring-Your-Own-Device Party Is Getting Bigger

Mobile devices are an integral — and expected — part of doing business. The trend to Bring Your Own Device (BYOD) has become much bigger than you may realize. Nearly three-quarters of companies now allow some sort of personal device to be used for business purposes. According to Gartner, Inc., many businesses find that having a BYOD solution enables their workers to do more, helps them address problems faster, and improves overall customer satisfaction.

The statistics behind these findings also are interesting. According to a Frost and Sullivan survey, nearly 40 percent of employees identified their cellular phone as the primary device used for business communications. Perhaps more telling, Forrester Research found that 53 percent of information workers use their own devices, applications, or services because they aren't satisfied with the solutions that their company offers.

Just ask any one of your employees. You may find that they're using solutions you'd prefer they weren't, and opening security holes you want to keep closed.

BYOD isn't a yes or no question. And a one-size-fits-all approach to BYOD won't work. Instead, you need to develop a BYOD policy that meets the specific needs of your business and addresses several key considerations and questions, including

- **Productivity:** Who is likely to benefit most if permitted to use their own devices? What do they need and from where are they likely to want access?
- **Infrastructure:** Will your network be able to support the greater capacity, performance, and resiliency that a BYOD policy requires?
- **Compatibility:** Are the devices your employees want to use able to interoperate with each other and with your network and the applications you support?
- **Legal issues:** Are there regulatory or privacy concerns that you need to address?
- **Security:** What new security risks does a BYOD policy introduce for your business? Are your firewalls, VPNs, and anti-malware solutions robust enough to protect smartphones and tablets?

In Chapter 3, I talk about Session Border Controllers (SBCs) and Identity Engines and how they work together to help you securely enable BYOD as part of your UC&C solution.

Chapter 3

Looking at Network and Security Considerations

In This Chapter

- Understanding the networking impact of UC&C
- Recognizing security challenges
- Looking at unique threats
- Making a case for Session Border Controllers
- Delving into the Bring Your Own Device trend
- Having a look at some real-world use cases

Effective collaboration begins with your network, and when it comes to your network, age does matter. Deploying Unified Communications and Collaboration (UC&C) solutions requires a full assessment of the underlying infrastructure to ensure that it is sufficient to support all the requirements of the new solution.

Security requires a new perspective, too. Securing UC&C beyond the borders of the enterprise requires a very different approach than securing data. To be truly effective, the approach must work in real time, understand the latency requirements of voice and video traffic, and be able to reflect call states — things that firewalls aren't typically designed to do.

This chapter is about the network and security implications of a UC&C deployment for your enterprise.

How UC&C Affects the Network

Deploying a new UC&C solution directly impacts your network. The implementation of new real-time video, voice, mobility, and conferencing capabilities requires a high-performing, reliable, and controllable network infrastructure. Such an undertaking creates an opportunity to revisit your underlying networking assets and ensures that the right infrastructure is in place.

Capacity

In addition to having the right networking infrastructure, you also need to ensure that your network has the capacity to support UC&C. Capacity considerations include making sure that you have

- Network bandwidth sufficient to support additional voice, video, and other collaboration features.
- Quality of Service (QoS) for traffic prioritization.
- Network switches with available Power over Ethernet (PoE) ports for UC&C endpoints.

Configuration

Your network must always be compliant with the applications that ride on it, which is why you need to take an application-first approach to networking. Ultimately, the critical business applications and their performance are what matter most to your business and your employees. As you're adding UC&C capabilities to your network, you need to carefully assess their impact on your existing applications. Security changes (discussed later in this chapter) are also likely to have an impact on the performance of your applications, so you will need to take a holistic approach to network and security design.

Next, you need to separate your voice, video, and data traffic on your network. This is usually done with QoS and traffic shaping. QoS allows you to prioritize the traffic on your network according to protocol or IP address, for example. With QoS, you can ensure that your voice and video have a higher priority over data when traversing your network, so that you minimize latency and packet loss that negatively impact voice and video quality.

Traffic shaping works together with QoS to ensure that the flow of packets through a given interface is throttled or limited in order to prevent a particular interface from being congested with network traffic.

Another method for separating voice, video, and data is to create virtual LANs (VLANs) for each application type, or place voice and video on completely separate networks (for example, voice and video on a 172.16.0.0 network and data on a 10.0.0.0 network).

Ease of management

Finally, a UC&C deployment shouldn't complicate your network design and infrastructure needlessly. Management tools need to be in place that can enable you to quickly and easily identify and isolate network performance issues. In a UC&C environment, users commonly move equipment around within the office, such as a desk phone to be plugged into different offices or cubicles. Mobile devices (discussed later in this chapter) must also be easily identified and managed because these devices are a key component of UC&C capabilities and adoption.

Taking a Look at UC&C Security Challenges

Midsize businesses are under constant security threats. Increased usage of collaboration tools means security threats are more of a concern and are different from in the past. Threats now include

- Toll fraud, where attackers seek to control UC&C and VoIP servers and use them to resell long-distance minutes
- Denial-of-Service (DoS) attacks, including call/registration overload and/or malformed messages (also called *fuzzing*)
- Vulnerability from configuration errors, such as misconfigured devices or operator and application errors
- Theft of service via unauthorized users or unauthorized media types

- Viruses and other malware, spread via Session Initiation Protocol (SIP) messages and instant messaging (IM) sessions
- Spam over IP Telephony (SPIT) and other unwanted traffic

UC&C security is different from data security

Although data communications seems instantaneous to users, sufficient latency is built into transmissions to assess and address dangers. UC&C environments don't have the luxury of this store-and-forward approach. Phone calls need to occur in real time and thus require seamless communications rather than choppy bits of information being passed back and forth.

Security mandates and compliance

A host of laws and regulations governing the activities of financial services firms, healthcare providers, and other businesses — both in the U.S. and globally — require threat mitigation to prevent theft of real-time information.

Contemporary threat mitigation efforts include keeping a communication private, or encrypted, for as long as possible and ensuring that users are authenticated to access and pass that information over a communication network. An example of this is the Payment Card Industry's (PCI) Data Security Standard (DSS), which requires that best effort be employed every time credit card information is transmitted, even via voice communication, with severe penalties for noncompliance.

A Menu of Threats

UC&C environments are vulnerable to both external and internal dangers that can imperil business operations, data, and customers.

Toll fraud

Far and away, the most significant threat in a UC&C environment is toll fraud, which has seen a large spike in prevalence over the last couple of years. Well-organized networks of attackers continuously probe for UC&C and VoIP servers that are not protected properly. Once attackers have control of vulnerable systems, they use them to resell long-distance minutes or to place calls to premium rate numbers that they themselves own, running up huge bills for the business.

The FBI has estimated that one such ring of attackers hacked the private branch exchanges (PBXs) of 2,200 enterprises in the U.S. and ran up charges in excess of $50 million. In such cases, it is not uncommon for an unprotected midsize business to suddenly get a phone bill that is hundreds of times larger than its typical phone bill.

Vishing: VoIP phishing

Other vulnerabilities in a UC&C environment include exposure to VoIP phishing, or *vishing,* in which fraudulent automated calls lure unsuspecting consumers into providing credit card numbers and other information.

Telephony Denial-of-Service attacks

Mobile malware can be used to conduct Telephony Denial-of-Service (TDoS) attacks and to steal information such as mobile banking credentials from devices. In a TDoS attack, perpetrators launch high volumes of calls against the target network, tying up the system so that it can't receive legitimate calls.

The Case for Session Border Controllers

As midmarket businesses rapidly adopt the Session Initiation Protocol (SIP) for UC&C connections to service providers, hosted application providers, extranet partners, and remote

workers via SIP trunks, a commonly asked question is, "Since my SIP trunk provider already has a session border controller (SBC) in its network, do I need an on-premise SBC as well?" This section helps you answer that question!

Security

An SBC provides essential SIP security regardless of whether the public SIP trunk service is delivered as a dedicated connection from the provider or via a shared multiprotocol label switching (MPLS) network. VoIP is a service that runs on an IP network, just like e-mail and web browsing.

An SBC enforces your unique VoIP security policies — just like a firewall does for data — and ensures that any regulatory requirements for voice security are met. See Figure 3-1.

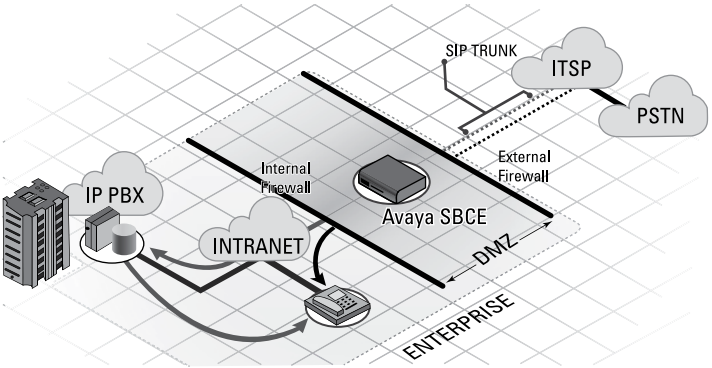


Figure 3-1: UC&C security with SIP trunking and SBC controls.

The SBC hides the complete network topology, including SIP signaling and real-time transport protocol (RTP) media. Thus, an SBC mitigates the risk of exposing large ranges of private IP addresses to an externally controlled entity and the associated possibilities of intentional or unintentional (misconfiguration) attack.

Unlike a firewall, an SBC is specifically designed for deep packet inspection and to manipulate the SIP headers, if necessary, to ensure protocol-compliant formatting. The SBC

is able to enforce signaling, rate limiting, and media bandwidth policing, and reduce the impact of DoS attacks by using dynamic access lists triggered by behavioral analysis of users and traffic.

The SBC also can enable secure remote access connections from smartphones and tablets without the need for a virtual private network (VPN) connection, further extending easy-to-use security capabilities to protect the business.

Flexibility

By installing an SBC on premise, the specific requirements and policies of the business can be addressed quickly and easily without complicated requests for changes from the service provider. The SBC provides an ideal reference interface for network border interoperability testing by normalizing the signaling and RTP streams into the business.

Additionally, the business may want to work with multiple SIP trunk providers. The SBC enables more than one provider to terminate SIP trunks to the business, providing a common demarcation point for normalization.

Accountability

An SBC also can generate per-call statistics including QoS measurements for independent service-level agreement (SLA) monitoring. It also can provide reports on intrusion attempts and provide session replication for call recording to meet industry or regulatory requirements.

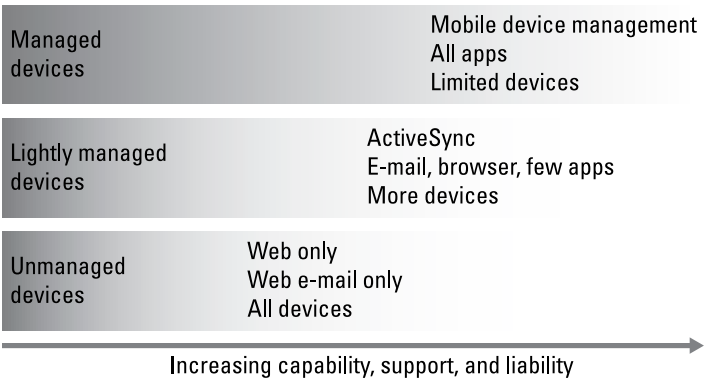
You wouldn't build a data network without a firewall; you shouldn't build UC&C without an SBC. Adding an SBC provides complete security for your UC&C solution. It secures SIP trunks, secures remote connections without a VPN, encrypts remote connections to prevent eavesdropping, and includes intrusion detection/intrusion protection systems to help guard against DoS attacks, call hijacking, and toll fraud.

The BYOD Trend

In addition to dealing with viruses, spam, and DoS attacks, enterprise IT security managers must adapt to the growing requirements of mobile and remote workers using smartphones, tablets, laptops, and soft clients.

Although IT organizations initially resisted this trend toward Bring Your Own Device (BYOD), many businesses are now embracing it for cost savings and employee productivity.

IT leaders are charged now with finding ways to deploy appropriate security measures that encompass personal devices used for work (see Figure 3-2).



Source: Forrester Research, Inc.

Figure 3-2: Tiering mobile device management based on applications and security.

The first step in securing BYOD is to establish appropriate access policies. Do you expose your entire network to all mobile devices or restrict mobile devices to only certain areas? And what mobile device management tools do you have available for enforcing such policies?

Ideally, access policies should be based on a user's role, location, and device type. For example, certain users will need access to critical business applications from everywhere, such as a salesperson requiring access to Salesforce.com. However, you need to be able to accurately identify those users and

devices. A hardware address, or generic user-generated device name, such as "Emily's iPad" or "Nick's iPhone," isn't very helpful for identifying and managing thousands of devices in a BYOD organization. Beyond merely identifying users, you also need to be able to accurately identify devices and security features, such as anti-malware software or whether a device has been compromised through *jailbreaking* or *rooting.* This is the role of an Identity Engine in your UC&C security architecture.

Jailbreaking is the term for hacking an Apple device so that users can bypass security features for the purpose of customizing the operating system in a way unsanctioned by Apple, or for downloading pirated applications. *Rooting* is the Google Android equivalent of jailbreaking.

Policy Servers

A Policy Server, or Identity Engine, gives you granular control of both users and devices to set the policies you need. For example, a user who connects wirelessly to the corporate network via a work-provided laptop can be granted full network access if the user is running the latest security and anti-virus software. However, the same user connecting via a personal iPad may be granted restricted access to avoid jeopardizing the security of the network.

Key benefits of an Identity Engine include

- **Improved security and granular control:** Secures wireless and guest access, role-based access control, and compartmentalization of the network to segment and protect data.
- **Reduced costs:** Supports current network infrastructures and identity stores and protects your investments via its standards-based solution.
- **Simplicity:** Provides centralized policy decisions (breaking down silos), policy expressions in plain language (not tied to technology), and simplified policy creation through virtual groups.
- **Regulatory compliance:** Offers full network visibility and comprehensive reporting and policies.

Use Cases in the Real World

Here's a look at some real-world examples of an Identity Engine at work in a BYOD environment.

Guest access

Guest access was once an all-or-nothing proposition: You either locked down your network, preventing guests from entering, or left it wide open, allowing any wireless user to tap in and consume your resources.

Now, with an Identity Engine solution, you can control who enters, where in the network a user is allowed to go, and for how long. All that's required to accomplish this is filling in a template. No technical expertise and/or resources are required, and it can be done in real time.

Guests receive a user ID on the spot, and a password is sent to their smartphones.

Posture checking

Verifying that connecting devices are virus free and running up-to-date software is a key element in enforcing network security. An Identity Engine enables you to perform posture assessments to ensure that connecting devices are equipped with valid antivirus software, updates, a personal firewall, and other appropriate security measures.

In the event that a client fails a health check, a number of options are available to the administrator, who can choose to grant limited access on a remediation network, allow Internet-only access, or deny access altogether.

Authorized fixed assets

An Identity Engine enables you to define authorized fixed assets or non-interactive devices such as IP phones, printers, and fax machines. You can conduct hardware address-level

authentication to help make sure that only authorized devices connect to the network and connect only where they're expected to connect.

This prevents intruders from unplugging a printer and accessing the network and prevents employees from bringing in their own wireless access points and sharing network services, compromising network security.

Chapter 4

Customer Interactions

In This Chapter

- Building customer loyalty with customer service
- Understanding what multichannel does for customers and businesses
- Looking at multichannel use cases
- Bringing customer experience management to your business
- Taking call centers to the next level with customer experience management

Technologies that support customer interactions are going through a transition in response to changing demographics and the means, or "channels," customers now choose to use. Companies can benefit from this transformation — extending and enhancing their level of customer engagement — by implementing end-to-end customer experience management solutions across their businesses.

This chapter introduces multichannel contact centers and their role in supporting more efficient and more profitable customer interactions.

Customer Service Is the Key to Customer Loyalty

The importance of customer service in driving sales through competitive differentiation, customer loyalty and retention, and overall brand advocacy has been long established. According to an Avaya survey of U.S. and U.K. consumers, 73 percent of Millenials say they will stop doing business with a company after just one bad experience, whereas 82 percent report that they will buy more from companies that make it

easy to do business. Having to budget time to make a phone call to get information rather than using an intuitive self-service website portal can be a real business detractor.

Surprisingly, despite all the talk of customer service, a gap is growing between customers' service expectations and the ability of companies to fulfill them.

- Although 80 percent of companies believe that they deliver a good or superior customer experience, only 20 percent of their customers agree, according to a recent contact center survey conducted by Webtorials.
- The Customer Service Scoreboard website (`www.customerservicescoreboard.com`) states the matter bluntly: "Most people believe they receive inadequate customer service from most companies today."

Companies cannot afford this disconnect, given that the vast majority of consumers report that their experiences with the contact center are either "important" or "very important" in shaping their opinions about a company's image.

With all of the resources devoted to customer service, this situation may seem paradoxical. In reality, the situation is decidedly familiar: Customer service is a dynamic business function; like the nature of business itself, it continually evolves. In fact, midmarket businesses now face a major paradigm shift in customer service brought about by changing demographics, new technologies, and new forms of communication and interaction — including the powerful impact of social media. Customers today expect to be able to do business using the channel of their choice — whether through a website, chat, e-mail, social media, or a simple phone call.

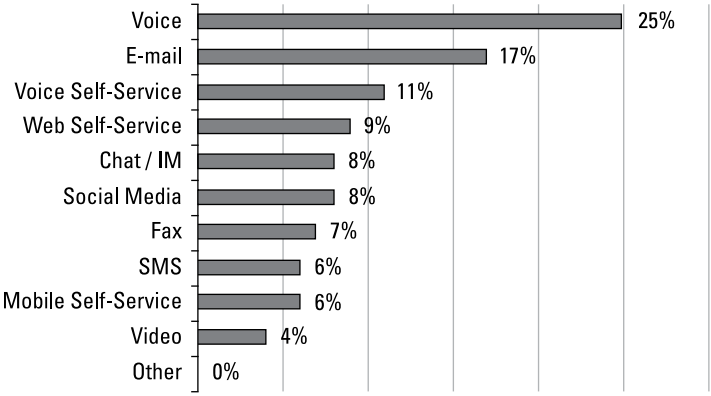
What Multichannel Means and Why You Should Care

How often have you heard something like this from a customer?

"I sent your company an e-mail describing issues I am having, but you never got back to me so I called your company and spoke to an agent who didn't know anything about me, my

problem, or the e-mail I sent! Having to explain my issue all over again really made me angry."

Perhaps more often than you'd like. (See Figure 4-1.)



Source: Business Technographics Networks and Telecommunications Survey. Q1 2013.

Figure 4-1: Customer interactions across the contact center.

Trying to support customer interactions with a simple call center, based on small phone-hunt groups, is no longer a satisfactory option. Even small contact centers should now explore multichannel capabilities, where all voice, e-mail, and chat sessions are handled by a common, integrated system that unifies all customer interactions, activities, and data.

A *phone-hunt group* consists of a small group of phones that ring simultaneously or sequentially after a preset number of rings. Less commonly, a hunt group can be configured to ring to a phone that has been idle the longest in a group, or to ring phones in a round-robin manner with the first call going to one phone, the second call to the next phone, and so on.

Multichannel capabilities give your customers the channels for interaction they use, want, and expect. Your customers find you where they want to, and you're ready when they get there.

In a multichannel contact center, interactions from all channels are universally queued and easily routed to the most suitable agent. Customers and agents move seamlessly between channels, resulting in enhanced customer service, increased productivity, and real business benefits.

Exploring Multichannel Use Cases

Your multichannel contact center serves different business needs and priorities. Here's a look at some real-world examples to see what multichannel can mean for your business (see Figure 4-2).

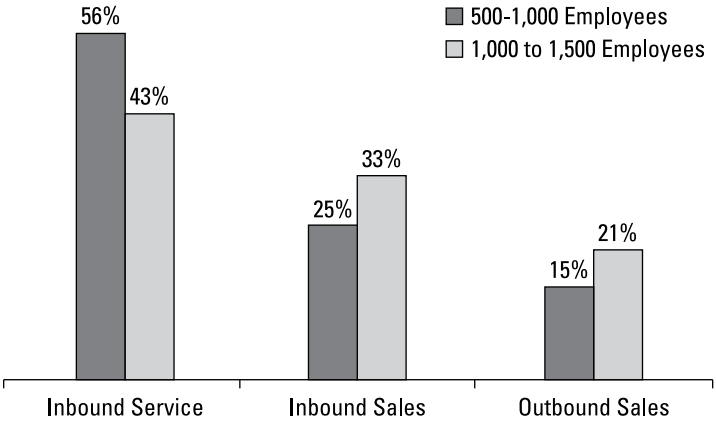


Figure 4-2: What is the single most important use for your contact center?

Inbound service

How your business handles customer service issues *after* a sale is critical to retaining customers and building loyalty. The cost of acquiring new customers is always higher than the cost of retaining existing ones, so keeping those new customers happy should be a primary goal for any business.

Yet the customer service leader must balance customer satisfaction and customer loyalty against the ever-increasing volume of customer contacts that the business receives. And, when issues arise, customers increasingly prefer website portals, e-mail, chat sessions, even social media, over voice. Blending all of these options for your customers helps ensure that you address their issues in the manner they want, while improving agent efficiency so that your customers don't go somewhere else.

Inbound sales

E-commerce is ubiquitous in our modern economy. Businesses that aren't selling on the Internet are missing out on a major sales channel. The convenience of e-commerce to a customer is undeniable, but online shoppers still want a personalized experience. The ability to open a chat session with an inside sales representative to help a customer navigate a website can help. Being able to quickly escalate the chat session into a voice call will not only greatly enhance the overall customer experience but also create opportunities to drive incremental sales.

Outbound sales

Outbound campaigns targeting existing customers or new prospects represent yet another opportunity to engage customers in a meaningful way. A fully integrated, multichannel contact center empowers your agents to do more than just cold-call a lead and fish for an opportunity. Equipped with information about previous conversations, e-mails, chat sessions, and the customer's website behavior can enable agents to engage the customer in a meaningful way and improve the desired result — increased sales.

Benefits of Multichannel

Deploying a blended multichannel contact center solution can help do the following:

- **Reduce voice traffic and lower contact center costs:** A voice call costs between $3 and $10, while an e-mail interaction costs between $1 and $3. Based on cost-per-transaction and the fact that one agent can handle multiple web chat sessions and respond to several e-mails in the time it would take to handle a single voice call, multichannel solutions can reduce costs by up to two-thirds.
- **Boost agent productivity:**
  - Reduced call volume allows e-mail queries to be queued for agents during lulls in voice traffic, increasing productivity.

- Using a multichannel contact center platform also enables agents to dynamically switch from one channel to another, as needed.
- In addition to optimizing agent utilization, allowing agents to switch from one channel to another can reduce agent fatigue and improve retention.

- **Increase sales:** An analysis by the Baymard Institute showed that online shopping carts are abandoned at an average rate of around 65 percent. Web chat and assisted browsing can help keep customers interested and engaged and speed them through the virtual checkout line, increasing sales and customer loyalty.
- **Improve decision making:** With a unified customer contact system, contact center managers have a single reporting structure across all channels and, therefore, more accurate data on which to base decisions.
- **Enhance customer experience:**
  - Customers can choose their preferred communication channel and switch between channels as desired.
  - Giving customers non-real-time ways to get problems addressed, such as sending an e-mail rather than calling the contact center and waiting on hold, enables them to use the channel that makes most sense to them based on their current situation.
  - Combining the visual richness of the web with the personalized treatment of a contact center enhances the customer experience by giving customers assistance when they need or want it.

Going Beyond the Call Center with Customer Experience Management

Innovations in contact center and communications technologies have made a new era of customer experience management possible, providing enhanced capabilities for improving access, managing interactions, adapting workflows, creating and preserving context, expanding the scope of performance evaluations, and much more.

Ultimately, successful implementation is a multi-pronged effort that requires careful adaptation to market needs, societal/generational trends, infrastructure, and cost considerations. For example, although voice may not be the first choice of everyone who needs customer service — and remains the most expensive interaction channel, it is still the medium that rates highest for customer satisfaction. While interaction methods such as self-service create the opportunity to reduce the cost of transactions, surveys show that many people still want costly live-agent support.

The challenge is to determine and deploy the right combination of automated and assisted experience-management capabilities to achieve exemplary customer service while optimizing capital and operational expenses.

Contact centers must be able to handle almost any type of contact, including phone calls, e-mails, online communications (such as instant messaging or chat windows), and the web.

To be implemented successfully, customer experience management requires a focus on the following core components:

- **Connected/open business:** Easily and cost-effectively integrate communications, information, and processes inside the contact center and across the business.
- **Application integration:** Integrate real-time communications with business applications, information, and processes.
- **Orchestrated experience:** Meet customers on their terms; proactively manage all interactions across all media and modes, agent-assisted and self-service, including warm handoffs.
- **Full context in every session:** Collect, grow, and leverage information about customers and their environment to improve the quality of every interaction and transaction.
- **Fully immersed agent experience:** Provide a unified and contextual desktop to empower agents and experts outside the contact center with real-time information to address customer needs.
- **Management and development tools:** Deliver a closed-loop process for leveraging historic and real-time insights to manage operations and continuously adapt.

Evaluating contact center solutions for the midmarket

Does your midmarket business need a contact center solution? If so, you should consider several important questions when evaluating solutions.

For starters, what is the primary focus of your contact center? Is it inbound service? Inbound sales? Outbound calling? Or perhaps a combination of some or all of these functions?

Here are some additional questions to consider:

- Do you have other connected locations and need to support agents in those locations?
- Do you support teleworking and want to attract agents in other states or even other countries?
- Do your customers want to use channels other than voice and expect you to respond in a timely fashion?
- Do you want your agents to be more productive and efficient and to handle more and different types of transactions?
- Do you want your supervisors to have a "cradle to grave" view of all your transactions in the contact center? And act on them?
- Are your customers waiting too long to get answered?
- Can your agents proactively make outbound calls to increase sales today?
- Could you implement a self-service strategy to complete all or part of a customer transaction?
- Recording calls improves agent-to-customer interaction and can quickly resolve conflicts. Is this important to you?
- Can an agent stop recording calls in the middle of a conversation, for example, when collecting personal or financial information (for HIPAA or PCI compliance)?
- Do you have agents that have different skills (languages, products, and so on) and would you like to route calls to those agents first?

Chapter 5

How to Get It All Done

In This Chapter

- Building a collaboration strategy for your business
- Choosing a single or multiple vendor solution
- Working with a partner

Organizations often struggle with Unified Communications and Collaboration (UC&C) deployments and with updates needed in networking and security to support new applications. But don't be intimidated. This chapter helps you create a UC&C strategy, assess fully integrated versus best-of-breed solutions, and understand the role of a technology partner.

Defining Your UC&C Strategy

Defining a UC&C strategy for your business consists of the following five tasks:

- Understand how a collaboration solution can address your business needs and objectives.
- Create profiles for the users in your company — in the office, at a desk, on the operations floor, in the warehouse, at a remote office, and in the field.
- Identify the communications capabilities you need for each of these user profiles.
- Assess your current communications, networking, and security infrastructure and readiness.
- Develop a timeline for rolling out your solution, including getting your employees trained.

Having a strategy will give your business a clear direction on the UC&C solution you need and help you to stay focused on your business goals and objectives.

Understanding your business needs

You should begin developing your UC&C strategy by conducting a *business assessment.* What exactly are you trying to achieve with UC&C, and how does that map to your overall business strategy? This assessment will be the foundation for designing and implementing your UC&C solution, so it's important to clearly articulate your goals for the technology, including the following:

- Evaluating how your employees communicate, who they communicate with, and where they perform their work activities
- Determining the specific UC&C capabilities you want for each type of user, including mobility, conferencing, video, and customer interaction requirements
- Specifying and prioritizing the timelines for delivering those capabilities

You need to consider four basic environments when developing your UC&C strategy: main office, remote or branch office, home or virtual office, and mobile office.

Main office

Your main office (or location) has employees who primarily work in offices or cubicles or at workstations at a company site. You may perform all or some of your business operations, administration, and support functions at this location, and communications and technology equipment is typically fixed (such as PCs and desk phones) and assigned to specific individuals. Capabilities may include conference calling, voicemail, e-mail, instant messaging (IM), and presence.

Remote or branch office

The remote office is a satellite location with mostly standalone operations that need to regularly communicate with the main office.

Employees who work from remote locations should have access to the same capabilities as in the main office, but the company should also expand these capabilities to enhance communications between the main office and various remote locations.

Additionally, remote offices present some unique challenges, particularly with regard to networking and security (refer to Chapter 3 to learn more).

Home or virtual office

The home office is exactly as it sounds — the employee's primary office is at home. The employee could be a sales person, a worker in another geographic location, or someone who doesn't want to commute, often referred to as *teleworking* or *telecommuting*.

Communications systems need to provide the same level of accessibility to your teleworking employees as they do to those in the main office. Coworkers need to be able to communicate seamlessly with one another, and your customers expect the same level of service and support, regardless of where folks are actually located.

You don't want employees installing and configuring complicated software settings. Your employees are busy people who may not be technologically savvy, and they definitely don't want to spend their time troubleshooting communications issues.

Mobile office

People who work from a mobile office are always on the go and use a variety of devices, each with the means to provide a variety of capabilities. Mobile devices include smartphones, tablets, laptops, and practically any computer with access to the Internet. These employees can work from many places, including the main office, a virtual home office, a branch office, a hotel conference room, an airport terminal, a coffee shop, or the back seat of a taxi cab.

In fact, if UC&C is implemented correctly, your customers should never have any idea that your employees may not be in the main office. In order to deliver that level of service and support, your employees need to be able to access various resources easily, whether working from home, on the go, or in the cubicle next door.

Specifying the capabilities you need

With a clear understanding of your business objectives, you should next specify the communications and collaboration capabilities that your business needs to achieve your objectives, including

- **Basic voice communications:** Simplified dial plans, auto attendant, call routing, and call recording.
- **Basic UC&C features:** Voicemail, e-mail, IM, presence, and click-to-dial features.
- **Mobility:** Single-number reach and full functionality on smartphones and tablets, whether company or employee owned, with similar, if not identical, user interfaces.
- **Collaboration:** Conferencing, video, document sharing, interactive whiteboard capabilities, one-to-one and one-to-many features.
- **System administration:** Business and communication continuity, seamless mobility, customizable settings, applications integration, enhanced administration capabilities, and deployment options.

Your UC&C strategy must provide access to the communication and collaboration tools that your workers need from wherever they are.

Knowing the situations that are applicable and the options your employees require will help you establish a UC&C strategy that increases productivity and improves customer service.

Developing a timeline and getting your users ready

As you develop your UC&C strategy, cost will always be an important consideration. Remember that when implementing your UC&C solution, you define the pace. You can ease into it, adding capabilities as your budget and business strategy permit, or you can go for the whole enchilada!

Because UC&C is so tightly integrated with many other communications technologies, you'll quite possibly be able to replace certain technologies and reduce or eliminate some costs.

UC&C also will bring new communications and collaboration capabilities to your business, so you'll need to develop policies and procedures for all of this new technology and train your employees on how to get the most from it!

Finally, considering support options in your UC&C strategy is important. Although a UC&C solution isn't complex necessarily, you may need additional support staff or a service contract that provides highly responsive support when you need it.

Comparing Single Vendor and Best-of-Breed Solutions

The question of whether to deploy a complete, single-vendor solution or a best-of-breed solution comprised of various components from different vendors is a classic buy-or-build business decision.

Some people use a string-of-pearls analogy to describe how best-of-breed solutions work: By taking pearls from various applications and stringing them together, you can create a beautiful necklace. But UC&C solutions aren't necklaces. In some cases, components have to use features with their least-common denominators set to work together. Each component has its own lifecycle and upgrade path. For example, one component might get a new release and no longer work with the others, be they different editions of an office communication program or a mobile video app.

With a single-vendor, fully integrated solution, you don't have a loose coupling of individual components. Everything is built to work better together, not only UC&C, but also networking, security, video, and contact center. A single-vendor solution can reduce integration risk and delays, speed time-to-results, and lower total cost of ownership.

Well-integrated, single-vendor solutions:

- **Are innovative and validated:** Individual components are pre-built, pre-configured, pre-tested, and certified to work together.
- **Focus on real-time communications:** A purpose-built UC&C solution is comprised of components and devices — including networking and security — that are optimized for real-time communications and collaboration.
- **Are easier to provision with faster time-to-service:** Provisioning a complete system from a single vendor rather than long bills of materials (BOMs) from multiple vendors reduces errors and speeds the entire provisioning and deploying process.
- **Require significantly less capital and operating expense:** A complete solution is typically less expensive to acquire, implement, and maintain than best-of-breed solutions.
- **Provide a single-support model:** When an issue arises, you don't want to be dependent on multiple vendors who want to claim that their individual component is not at fault, pointing fingers at other vendors instead of fixing your issue!

Understanding the Role of Your Business Partner

Choosing the right technology partner for your UC&C deployment is a crucial first step. Find a partner that you can look to as a trusted advisor, an extension of your IT department. The partner should be proficient — and certified — in all aspects of the solution: unified communications, collaboration, contact center, video, networking, and security.

Your employees (and perhaps you personally) will need assistance operating, maintaining, and troubleshooting the hardware, software, and various end-user devices of a UC&C solution. Be sure that your partner is capable of providing the support you need, along with support from the vendor. Trained support personnel must be readily accessible when you need them.

Chapter 6

Exploring Avaya Midmarket Collaboration Solutions

In This Chapter

- Learning about Avaya IP Office
- Taking a look at Avaya's complete collaboration suite
- Discussing flexible deployment models

This chapter introduces Avaya's comprehensive Unified Communications and Collaboration (UC&C) solution for midsize businesses, based on the Avaya IP Office Platform, surrounded by the Avaya contact center, video collaboration, networking, and security — a complete solution from a single source.

A Complete Midmarket Solution

Avaya surrounds its Avaya IP Office collaboration software platform with Avaya contact center, networking, security, video, and support (see Figure 6-1). This platform enables your Avaya partner to deliver a comprehensive solution for your midsize company from a single source — designed to work together — reducing integration risk while speeding return on investment.

Avaya Comprehensive Midmarket Solution
Built on IP Office as the Core – Power with Simplicity and Value

Figure 6-1: The Avaya IP Office platform provides a complete midmarket solution.

Avaya IP Office

Avaya IP Office is a flexible midmarket collaboration platform — simple to use and manage, yet powerful enough for the demanding needs of a distributed, mobile workforce.

The Avaya IP Office Platform extends Avaya innovation in UC&C to midsize businesses, delivering a seamless experience for voice, video, mobility, and collaboration.

Avaya IP Office software can run inside a virtual machine, on a server or appliance, or be deployed as a mix of these. The solution scales to support as many as 2,000 users at up to 32 locations in a single solution and supports a broad range of end points: analog, digital, IP, and softphones; PCs, Macs, and Android or iOS smartphones and tablets. This deployment flexibility enables investment protection for businesses that choose to migrate to unified communications in phases.

The latest release of Avaya IP Office software contains more than 100 feature enhancements, including

- Simplified scalability of up to 2,000 users, so your solution can grow with your business
- Flexible deployment options to reduce hardware footprint and associated costs

- Rich unified communications, mobility, and video collaboration options to deliver a superior experience that engages your workforce
- Simplified administration and management, reducing IT overhead

By offering a proven, comprehensive collaboration solution that is designed for the midmarket and easy to deploy, use, and manage, Avaya helps reduce integration risk and delays, speed time-to-results, and lower total cost of ownership.

Avaya IP Office is currently deployed in more than 300,000 businesses worldwide, with more than a decade of experience and customer feedback to guide development.

Contact center

Customer expectations have risen dramatically, requiring companies to develop a far broader set of capabilities for their customer interactions. To be successful today, midsize businesses must be capable of responding to their customers swiftly, efficiently, and accurately, no matter which channel of interaction — or combination of channels — customers choose.

Contact Center Solutions for IP Office extend Avaya innovation in customer experience management to midsize businesses, with the simplicity and value they require. Avaya Contact Center Solutions for IP Office:

- Support blended multichannel inbound and outbound contacts (voice, e-mail, chat, SMS text, and fax)
- Feature agent and supervisor desktops, call recording, and reporting
- Offer flexible deployments — a dedicated server or in a virtualized environment
- Are priced for midsize businesses
- Can be deployed in hours, instead of days
- Are easy to set up, maintain, and manage

Video

Many midmarket companies are looking to enable video in their organizations to build relationships, improve collaboration, and speed time-to-decision.

Avaya's flexible, affordable video collaboration infrastructure, applications, and clients offer simplicity, performance, scalability, and broad interoperability with multi-vendor videoconferencing solutions and devices, including a broad range of mobile consumer devices, desktop, and room-based systems.

The Avaya Video Collaboration Solution for IP Office combines desktop, mobile, and high-definition (HD) room-based video collaboration in an affordable package.

The Avaya Video Collaboration Solution:

- Creates a virtual conference room
- Combines room system, desktop, and mobile devices
- Supports Bring Your Own Device (BYOD) and third-party devices
- Is comprehensive, simple, and affordable

Networking

Companies deploying UC&C solutions will often need to consider the state of the underlying network infrastructure to determine whether it is sufficient to support the requirements of the new solution. Not addressing network considerations can affect the performance of the solution negatively. Bringing in a separate vendor for networking adds complexity and integration risk to the deployment.

Avaya Ethernet Switches can be deployed as part of an Avaya IP Office solution with a single command that launches automated provisioning of voice and data virtual LANs (VLANs) and gateway IP addressing, enabling plug-and-play installation of an IP phone in less than a minute.

Avaya networking solutions and features include

- **Avaya ERS 3500/4800**
  - Auto-provisioning for IP Office in minutes
  - One-minute plug-and-play capabilities for IP phones and automatic QoS (Quality of Service) and provisioning
  - Power over Ethernet (PoE)/POE+ models for powered connection of IP phones and other devices
  - 100-plus deployed enterprise features
  - 50 percent lower TCO than other competitive switching solutions
- **Avaya Wireless LAN 8100**
  - Optimized support for data, voice, video, and messaging applications
  - Always-on architecture
  - Guest access and management
  - Wireless intrusion detection

Security

Securing unified communications beyond the borders of the enterprise requires a different approach from securing data. The approach must work in real time, understand the latency requirements of voice and video traffic, and be able to reflect call states. A firewall is not well suited for this task.

An Avaya Session Border Controller (SBC) provides a comprehensive approach to securing unified communications based on Session Initiation Protocol (SIP), including securing SIP trunks, securing remote connections without a VPN, encrypting remote connections to prevent eavesdropping, and intrusion detection/intrusion protection systems to guard against denial-of-service attacks, call hijacking, and toll fraud.

Avaya Identity Engines provide a complete, policy-based, secure BYOD solution with guest and network access for employees, guests, and business partners. This is particularly relevant in industries such as education, finance, and healthcare, where regulations such as SOX (Sarbanes-Oxley-Act), HIPAA (Health

Insurance Portability and Accountability Act), and PCI (Payment Card Industry) are important.

Avaya security solutions and features include

- **Avaya Session Border Controller**
  - Border signaling/media control
  - Denial-of-service (DoS) and distributed denial-of-service (DDoS) attack mitigation
  - Intrusion detection/prevention
  - Toll fraud prevention
  - Border access control
  - Mobile access without VPN
- **Avaya Identity Engines**
  - Centralized policy management
  - Network and device agnostic

Flexible Deployment Models

Server virtualization is being widely adopted by midmarket organizations as they seek to reduce their hardware footprint, capital expenditures (CAPEX), and operating expenses (OPEX). The design approach of some UC&C solutions runs counter to this trend, requiring the addition of multiple appliances to the network to achieve the needed scale.

For midmarket organizations that have virtualized their data centers, or are planning to, Avaya IP Office software offers a deployment model that aligns with that effort. Significantly, an IP Office solution can consist of virtualized and non-virtualized components, extending deployment options even further (see Figure 6-2).

Avaya has been shipping virtualized software since late 2012, when it released Avaya Aura Virtualized Environment (Avaya Aura VE). This release was designated as VMware Ready, which is VMware's highest level of endorsement for virtualization technologies.

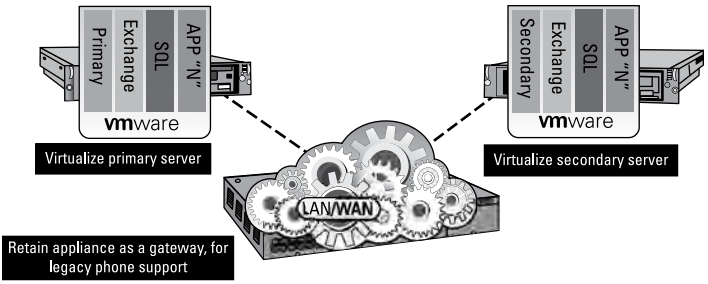


Figure 6-2: Flexible Avaya IP Office deployment options.

When deployed as virtualized software, Avaya IP Office provides the following benefits:

- Leverages VMware investment
- Makes collaboration more resilient and easy to manage
- Consolidates voice, messaging, and mobility in a single application
- Installs as a turnkey, pre-configured OVA (Open Virtual Appliance) package
- Lowers costs with shared licensing and no additional hardware to purchase
- Adds resiliency when deployed on a second physical server or virtual image (see Figure 6-3).

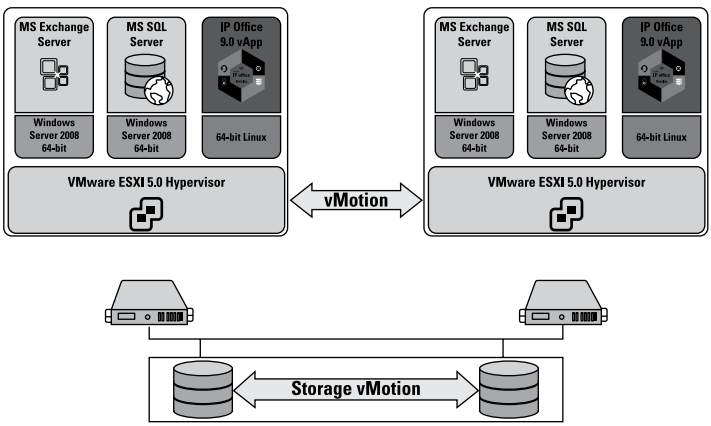


Figure 6-3: Avaya IP Office adds resiliency to your UC&C environment.

When choosing a deployment model for your organization, you should look at your overall IT hardware and software strategy and select a UC&C solution that offers the flexibility to support that strategy.

A final deployment option is to have your UC&C environment hosted by a cloud service provider — but hosted UC&C isn't for everyone! Hosted UC&C is most appropriate for emerging companies where the size of the workforce could fluctuate widely, and for companies that aren't yet ready to make the investment in UC&C.

The breakeven point for a hosted/cloud UC&C solution versus an on-premise UC&C solution is typically 15 to 18 months. Beyond that, hosted is no longer the most cost-effective solution.

Chapter 7

Ten Simple Actions for Deploying Midmarket Collaboration

In This Chapter

- Deciding on the person to manage your project
- Complying with regulatory requirements
- Interacting with customers
- Looking at midmarket solutions
- Coming up with a technology partner
- Establishing a design and deployment plan

In this chapter, I outline ten simple actions that will help you deploy a midmarket collaboration solution for your business — from finding the right project manager to successfully adopting a new technology solution.

Appoint a Project Manager

Plain and simple, if your UC&C initiative is to be successful, you need a responsible individual to oversee all aspects of the effort, including

- Creating and maintaining the project plan and milestone schedule
- Managing and coordinating all activities and personnel associated with the project

- Documenting and proactively communicating the status of those activities
- Ensuring tight change control

Although these tasks may seem straightforward enough, effective project management comes with many challenges.

Your project manager needs to be more than just a figurehead or a sacrificial lamb who is good at checking off a to-do list and holding meetings. The individual needs to be an effective manager and an experienced leader — and may come from outside the IT department.

Many complex tasks are required for a successful implementation, and tight coordination of many activities and organizations is a must. Your project manager may have management responsibilities for your collaboration initiative that transcend his normal position in your organization and may cross departmental or functional boundaries.

The ability to communicate effectively with other managers and work with a diverse group of people with differing positions, skill sets, and priorities is key to successful project management.

Finally, your project manager needs to be able to "just say no!" Effective change control helps you avoid "scope creep," which in turn helps you avoid "cost creep." An effective project manager will help you stay on time and on budget.

Conduct a Business Assessment

Once a project manager is in place, the next task is to determine exactly what you want your UC&C solution to accomplish. After all, you can't measure success if you don't know where you are going.

Here are some things to consider:

- What challenges and objectives can the solution help address? Can it improve productivity? Extend mobility? Secure BYOD? Improve customer satisfaction? Optimize your infrastructure?

- How many sites do you have? How many employees? What types, in-house, remote? How should the solution touch each of these?
- How do your employees collaborate today with others who aren't in the same location?
- How sophisticated would you like your UC&C solution to be? Should video be a part of it?
- What about customer interactions?

Address Regulatory Compliance

Virtually every industry today is touched by the alphabet soup of acronym regulations. Healthcare has HIPAA, the Health Insurance Portability and Accountability Act; retail has PCI DSS, the Payment Card Industry Data Security Standards, which is a set of security requirements for credit card processors; and virtually every public company must adhere to SOX, the Sarbanes Oxley Act of 2002. It's beyond the scope of this book to go into detail on the implications of regulations on your UC&C solution, but your solution *must* address certain regulatory considerations.

Define Mobility Policies

The high-level goal of a mobility solution is to enable employees working outside the office to be as productive as they would be in the office, with access to the same tools. Considerations begin with a simple review of staffing and continue with the more in-depth requirements of secure BYOD policies.

- How many outside salespeople do you have? Do they use smartphones and tablets regularly in their day-to-day selling activities?
- What about remote workers? Do you support telecommuting?
- Would you like to support mobility in the office? Wireless phones? Enable employees to make calls from their mobile devices over the corporate Wi-Fi network to save toll charges?

- To what extent do you want to support BYOD? How should access differ based on role, location, or device?
- What about secure guest access?
- Do any of the policies in this list require regulatory considerations (discussed earlier in this chapter)?

Consider Customer Interactions

Although technically not part of a UC&C solution, customer interactions are discussed in this book (see Chapter 4) because contact center solutions can use the same communications infrastructure and run over the same network, with the same security protection. Considerations include

- What are your objectives for customer experience? What is your Satisfaction/Net Promoter Score? Agent efficiency? Customer Lifetime Value?
- Is a contact center important to your business or mission critical?
- What is the primary focus of your contact center? Inbound service? Inbound sales? Outbound campaigns?
- How many agents do you need to support? How many supervisors? Do any agents work remotely? How is work distributed?
- What contact channels do you support today? How? What are the business requirements for each channel?
- Do you want to integrate customer relationship management (CRM) or other applications into the agent interface?
- What call recording/reporting capabilities do you need?

Conduct a Network Assessment

Once the needs and expectations of the business are understood clearly, you need to conduct a detailed network and security assessment and inventory that document the following:

- Do the existing network elements support the local area network (LAN), wide area network (WAN), and remote access connectivity?
- Is the available network bandwidth sufficient to support additional voice, video, contact center, and other collaboration features?
- Can your existing infrastructure support Quality of Service (QoS) for traffic prioritization?
- Do your network switches support Power over Ethernet (PoE) to connect and power new UC&C end points?
- How will you secure communications? Remote workers? BYOD? The contact center? Will you be able to detect and mitigate toll fraud, telephony denial-of-service, vishing, or other attacks?

Evaluate Midmarket Solutions

As discussed in Chapter 1, some consider the midmarket a "tweener" market, which sits between the small and midsize business (SMB) and the enterprise market. The first question to ask is whether the vendor, and the proposed solution, are really designed for a midsize business:

- Is the solution powerful and full featured enough to meet your requirements?
- Can the solution scale, simply and effectively, to grow with your business and with your changing needs?
- Can you integrate the solution with your existing networks and systems? Can you use existing analog and/or digital phones with the new solution?
- Does the solution offer deployment options — to align the solution with your infrastructure objectives?
- Will the solution be easy to deploy and easy to manage?
- Does the solution offer the simplicity and value that your limited IT resources and budgets require?
- Is the vendor committed to the midmarket?

Identify a Technology Partner

The right technology partner can serve as an extension of your team, guiding you through the processes outlined in this chapter. Clearly, your partner must demonstrate specialized UC&C expertise and be willing to invest the time required to truly understand your business and your objectives. Your partner also needs to:

- Take a holistic view of the solution and its impact on your infrastructure.
- Be equally competent in assessing, recommending, and deploying networking, security, video, and contact center components.
- Understand core interoperability standards (such as the Session Initiation Protocol, or SIP) and have solid working relationships with other industry providers.
- Have strong skills in security assessment, solution development, and implementation.
- Be able to handle all aspects of deployment and offer options for long-term maintenance and support.

Create a Design and Deployment Plan

Your collaboration solution design should be optimized for maximum performance, interoperability, and business impact at each stage of implementation.

Once any needed modifications have been incorporated into the design of your collaboration solution, the final step in the planning phase is to develop a detailed deployment plan. The plan should conform to required budgets and milestones, maximize appropriate reuse of existing investments, and address the needed level of security and business continuity.

Your deployment plan should specify the deployment sequence, including the exact mechanisms and schedules for transitioning existing communication capabilities and configurations to the new collaboration solution. Your plan also should address any

coexistence issues that may occur during the transition period from your old system to your new collaboration solution.

Finally, you need to plan for the unexpected, by developing contingency plans for each phase of deployment and by building flexibility into the deployment schedule.

Validate Readiness and Go

Before proceeding with any key phase, the project manager must assess "go/no go" readiness, including the following:

- Ordering, receipt, configuration, and testing of all new hardware, software, and LAN/WAN connectivity components.
- Development and testing of all required interoperability and networking attributes of the solution.
- Training of system administrators and end users.
- Notification of organizational stakeholders. (Are they informed and ready? Do they know what is expected of them? Do they know how they will be impacted?)
- Completion of technical dependencies and requirements. (Are release levels of component applications and operating systems in place? Is the network ready?)

Ultimately, the human factor remains one of the largest variables that determines whether a new technology solution is adopted successfully.

Glossary

auto attendant: An automated system that enables callers to be transferred automatically to an extension without an operator or receptionist.

bot: A computer that has been infected with malware and is under the control of an attacker.

botnet: A large number of bots, perhaps tens of thousands, under the control of one or several attackers.

Bring Your Own Device (BYOD): A prevalent trend in the modern workplace in which employees are permitted to use their own mobile devices, such as smartphones and tablets, to perform work-related functions.

call routing: The process of routing telephone calls across the Public Switched Telephone Network. See ***Public Switched Telephone Network***

click-to-dial: Allows a person to dial a phone number by clicking a link or icon in an application, such as an e-mail or a web page. Also known as click-to-talk.

contact center: A facility designed to provide agents access to customers and clients through a variety of media, such as phone, e-mail, chat, video, and fax.

Customer Relationship Management (CRM): An application for managing a company's interactions with current and prospective customers through all media, including e-mail, phone, and face-to-face meetings.

Denial-of-Service (DoS): The purpose of a DoS attack is to make a computer, application, or network unavailable to its intended users.

dial plan: Specifies the sequence of numbers to be dialed in a phone system. For example, you may require that 9 be dialed for external phone numbers, and you might enable internal numbers to be dialed simply by entering the last four digits of a phone number extension.

Distributed Denial-of-Service (DDoS): A large-scale attack that typically uses bots in a botnet to crash a targeted network or server. See ***bots*** and ***botnet***

Health Insurance Portability and Accountability Act (HIPAA): A U.S. Department of Health and Human Services (HHS) regulatory requirement for health entities that establishes rules for security, data privacy, and breach notification.

hunt group: A method for distributing a single phone number across multiple phones. For example, you might have a single phone number ring to several phones simultaneously or sequentially.

instant messaging (IM): A program that provides real-time text transmissions across a network, such as the Internet.

Interactive Voice Response (IVR): A technology that enables callers to select different call-routing options based on voice or keypad input on a phone system.

jailbreaking: The term for hacking an Apple device so that users can bypass security features for the purpose of customizing the operating system in a way unsanctioned by Apple, or for downloading pirated applications.

Multiprotocol Label Switching (MPLS): A protocol used in wide area networks (WANs) to provide high-speed data transmission without requiring routing table lookups.

Open Virtual Appliance (OVA): A virtual machine that is built on an open standards platform.

Payment Card Industry Data Security Standards (PCI DSS): An industry standard created by the major payment card brands including American Express, Discover Financial Services, JCB International, MasterCard, and Visa Inc. PCI DSS is applicable to any organization, regardless of size or industry, that processes or stores credit or debit card transactions.

Power over Ethernet (PoE): Provides electrical power over an Ethernet network cable and is commonly used to power IP telephones and wireless access points in a network.

presence: A feature in Voice over IP phone systems that enables users to indicate whether they are available to other callers without needing to actually call the user.

Private Branch Exchange (PBX): A telephone switch that manages a business or organization's telecommunications services.

Public Switched Telephone Network (PSTN): The infrastructure and services provided by national, regional, and local telephone service providers.

Quality of Service (QoS): QoS provides the means to prioritize traffic on a network so that voice and video, for example, will always have priority over web browsing if a network is otherwise congested.

Real-time Transport Protocol (RTP): A protocol for transporting audio and video packets over IP networks.

rooting: The term for hacking a Google Android device so that users can bypass security features for the purpose of customizing the operating system in a way unsanctioned by Google, or for downloading pirated applications.

Sarbanes-Oxley Act of 2002 (SOX): A U.S. regulation for security and governance that is applicable to all U.S. public companies, management, and accounting firms.

Service-Level Agreement (SLA): A contractual agreement that specifies the performance levels to be maintained by a service provider.

Session Border Controller (SBC): A security appliance deployed in VoIP networks to provide security functionality similar to a firewall in data networks but designed and optimized specifically for real-time communication protocols.

Session Initiation Protocol (SIP): A signaling communications protocol commonly used for voice and video calls in an IP network.

Short Message Service (SMS) text: A text messaging system used on phones, web, or mobile communication systems.

small and midsized business (SMB): In the U.S., SMBs are generally defined in terms of headcount: small businesses constitute entities with less than 100 employees and midsized businesses consist of those having 100 to 999 employees.

small and midsized enterprises (SME): In the European Union, SMEs are defined as a category of micro, small, and midsized enterprises that employ fewer than 250 personnel and have an annual turnover not exceeding 50 million euro.

Spam over IP Telephony (SPIT): Prerecorded phone messages that are unsolicited and automatically dialed to bulk phone numbers, similar to e-mail spam. Also known as VoIP spam.

virtual local area network (VLAN): A logical partitioning of a layer 2 local area network (LAN) that creates distinct broadcast domains in a network.

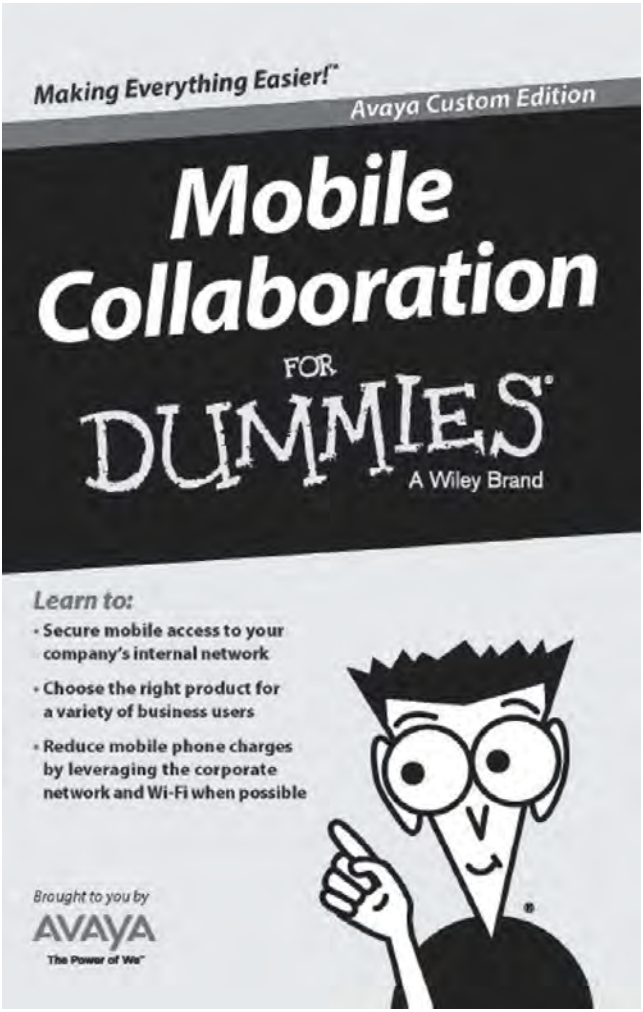
virtual private network (VPN): Securely extends a private network across a public network, such as the Internet.

vishing: A social engineering attack that uses a telephone system to get sensitive information, such as passwords or financial information. The VoIP equivalent of e-mail phishing. Also known as *voice phishing*.

Voice over IP (VoIP): Voice and multimedia communications sessions delivered over an IP network.

Notes

The fast way to make the smart moves on Mobility!



Go to avaya.com/mobility4d

Realize the full potential of Unified Communications and Collaboration

Midmarket companies face unique challenges to improve their competitiveness against larger enterprises. With employees, suppliers, partners, and customers scattered across the globe, Unified Communications and Collaboration (UC&C) solutions are a key technology to enable business growth and maximize productivity.

- ***Define a collaboration solution* — *understand your business needs, assess your current infrastructure, develop a plan, and deploy the solution***
- ***Understand advanced UC features* — *including presence, mobility, and video***
- ***Use multichannel communications* — *to engage your customers and to deliver an exceptional customer experience***
- ***Use a flexible deployment model* — *virtualized software, a dedicated server, an appliance or a mix, all based on your infrastructure objectives***

Open the book and find:

- **What UC&C can do for your business**
- **How to enable employees to be as productive on the move as they are in the office**
- **Why securing UC&C is different from securing traditional data**

Go to Dummies.com®
for videos, step-by-step examples, how-to articles, or to shop!

FOR DUMMIES®
A Wiley Brand

ISBN: 978-1-118-91427-4