AVAYA

Smooth Sailing: Best Practices for Implementing an IP Contact Center

March, 2005

Table of Contents

Section 1: Opening Statements

Among the most successful 16th-century mariners competing to explore the New World was the renowned Captain Drake. Many countries were rushing expeditions into this uncharted territory. Drake, however, had an advantage: from foreign ships he had kidnapped navigators who knew the coastline from previous voyages. With their help, Drake navigated the dangerous waters and went on to establish routes that others would follow for centuries to come.

When you run a contact center, the alluring territory of internet protocol (IP) telephony can seem uncharted and perilous. Fortunately, Avaya knows these waters well. Our experience can guide you through a successful journey. And you don't have to abduct Avaya experts to get that experience. In this paper we have compiled the lessons of our long history of IP contact center deployments. Think of this paper as your Niño daSilva.[1]

Section 2: Executive Summary

Over the years, conventional circuit-switched technologies have earned the loyalty of IT managers. But these technologies have limitations, making it complicated and costly to deploy today's advanced solutions throughout the enterprise.

IP telephony, meanwhile, is proving itself as an architecture that is flexible and cost effective. Savings and efficiencies can be gained by migrating to IP telephony — and lost by stumbling into common pitfalls. Adhering to best practices during your planning and implementation will help to avoid the snags and ensure success. This paper outlines the hazards and best practices as collected from an Avaya history with contact centers and IP telephony.

Conventional contact center solutions include a rich set of advanced features, the loss of which can harm the contact center's performance metrics. Avoid a backward step by preserving that full feature set, including third-party applications, in the transition to IP.

The tests of IP telephony are call quality and reliability. A detailed network assessment is essential to identifying weaknesses. Define your organization's service level agreements (SLAs) and standards for QoS up front, to avoid shifting expectations.

As the voice and data networks converge, voice over IP (VoIP) communication must be protected. Think in terms of the "security trinity" in your network design. Implement measures that will protect your assets, detect a breach, and enable you to respond quickly.

Convergence raises questions regarding the responsibility for managing integrated systems. Think beyond appointing roles for the usual functions. Concentrate instead on who will be in charge of monitoring, managing, and reporting.

Be prepared to support your company's plans for growth. Deploy a system that has proven itself handling thousands of lines. Verify that the solution you choose will support your plans to pool contact centers and interflow calls between them.

Making the jump to pure IP telephony is not the best path for every contact center. Uprooting existing private branch exchange (PBX) infrastructure and integrating new voice servers with the data network could be disruptive and costly. If yours is an established center with a digital PBX, consider IP enabling the existing PBX to protect your existing investments.

[1] Niño daSilva was one of Drake's most willing and valuable Portuguese navigators, having been to South America on previous journeys.

Avaya recognizes that the financial commitment of a VoIP infrastructure can be significant. You must choose the right path for migration. Avaya lets you take each step at your own pace. Choosing Avaya reflects the choices you make about technology directions, protecting investments and, above all, serving customers.

Section 3: IP Contact Center: Opportunity and Risk

There is a certain warm comfort that comes with the tried and true. Conventional circuit-switched PBXs and automatic call distribution (ACD) have been around for a long time. They are secure, reliable, and have sophisticated capabilities for contact centers. Over the decades, they have earned the loyalty of conservative managers who have spent years fine-tuning their contact centers to most efficiently use their agents.

The winds of change, once a distant rustling, now are pushing the status quo toward a new course. Distributed contact centers are increasingly important to global organizations. This, in turn, strengthens the interest in centralized administration, especially where sophisticated, industry-specific telephony applications are involved. Cost control and efficiency are the battle hymn of almost every industry.

These trends in contact centers are filling the sails of IP telephony. Circuit-switched contact center technologies have their limitations, making it complicated and costly to deploy the next level of advanced capabilities throughout your enterprise. By contrast, an IP-based architecture is flexible and cost effective. Analysts agree that it is not a matter of whether IP telephony will become mainstream, but when — and the projected timeframe is short.

While IP telephony can be justified on cost savings and efficiency, one major deployment problem could wipe out the savings. And if the new solution does not provide better efficiency with the same functionality, the cost savings could be consumed by additional staffing costs.

Fortunately, the switch to IP does not have to be risky. This paper outlines the hazards and best practices as collected from a long history with contact centers and IP telephony.

Section 4: Issues and Corresponding Best Practices

The following eight sections describe the themes that may arise during the transition to IP telephony, and the best practices for avoiding or overcoming issues.

Section 4.1: Capabilities essential to the contact center

Conventional contact center systems include a rich set of advanced features that work together to improve customer service and agent efficiency. Since the largest cost component in a contact center is staffing,[2] the loss of any of these features can harm the contact center's performance metrics.

Basic call operations, such as transfer and conference, are standard features in any IP PBX. Advanced contact center features are much more complex and should not be assumed.

Call routing, for example, which gives callers faster service, bases its decisions on expected wait times that are derived from internal data such as the number of agents staffed, number of calls in queue, call priorities, and average handle times. Features using sophisticated predictive algorithms based on current staffing and past behavior are providing even more flexibility for contact routing. Less sophisticated routing can result in extended wait times and frustrated callers. Adding staff to compensate may wipe out any cost savings achieved.

[2] According to CIO Magazine, personnel accounts for about 70 percent of each call center's costs; the rest goes to rent, phone bills, and computer and telephone equipment. ("Working Smart: Airborne Freight's Call Center Management System," April 15, 1999 [www.cio.com/archive/041599_smart.html].

Best practices for preserving productivity

The move to IP telephony should expand the capabilities of your contact center, not diminish them. Work with your vendor to ensure absolutely that your center will continue to enjoy all of the features it depends on today. Your current staffing levels (and therefore costs) are based on having the rich, mature applications you use now. Avoid a backward step by preserving that full feature set, including third-party applications, in the transition to IP telephony.

A robust IP contact center architecture separates the *application* layer from the *transport* layer. Contact center features are the function of software applications, while the transport — whether TDM or IP — is hardware dependent. When applications operate independently of their transport layer, they can continue uninterrupted when the transport is migrated from TDM to IP.

One of the promises of IP telephony is that it enables ubiquitous access to applications from every enterprise location. Whether the agent is headquarters based, in a branch office, or a home agent, they can and should enjoy the same feature set. Validate each vendor's complete support of your set of devices, with standardized capabilities and appropriate user interfaces.

Continued performance improvement in your contact center will depend in part on future enhancements to your applications. Avoid committing the enterprise to a proprietary environment that would limit rapid enhancements or become a dead-end technology. Evaluate any IP telephony offering on its open architecture and broad support from the development community.

Section 4.2: Deployment success begins with assessment

The supreme test of IP telephony in the contact center is call quality and reliability. These topics are so critical that we have included sections on each in the pages that follow. Overall voice performance is affected by the performance of each network component, so the burning questions are: "Can the IP network handle voice?" and "How will we know in advance?"

Of course, the network eventually will handle voice, but Gartner estimates that 85 percent of today's large enterprise LANs will require hardware or software upgrades before they are ready to support IP telephony. In other words, the first weeks and months on IP telephony can be rough ones, if issues are not identified and resolved beforehand. During a difficult deployment, the community of concerned collaborators can expand considerably. Expectations can become a moving target, amidst unwelcome attention to the project. Key personnel can spend untold hours tinkering with the network and managing perceptions.

Best practices for identifying network weaknesses

To avert a difficult deployment, involve the right people early in the planning process. Contact center management and IT should collaborate especially closely to actively address each of the issues outlined in this paper.

An objective, detailed network assessment is essential to identifying weaknesses. Assessment requires asking the right questions pertaining to quality, reliability, and the prioritization of voice on the IP network. The assessment should endeavor to anticipate growth, planned restructuring, acquisitions and divestitures, to the degree possible.

Assessments require specific technical capabilities and tools. It is often advantageous to engage an outside service provider for this stage of the process. They will be able to locate assessment hosts within the network in such a way as to accurately measure end-to-end performance. The tools they use will be specifically designed for IP telephony environments.

Once the assessment is complete, proceed with the indicated network upgrades and changes. Quality and reliability depend on it, and are worthwhile exploring in more depth now.

Section 4.3: Quality of service vital for voice traffic

The quality of service (QoS) requirements for voice are different than for data. Some people remember the experiences of the early years of VoIP. Their first question is whether the voice quality will be acceptable.

The main QoS issues to consider are those that might result in the perception that a caller has a bad connection. Voice over IP is digitized and broken down into data packets, each containing a fraction of a second of sound. Voice is a real-time function, and quality can be adversely affected by delay or packet loss caused by any underperforming component on the network.

Delay introduces an unnatural audible effect to the conversation. It occurs when there is a delay as voice is being compressed, packetized, transmitted, reassembled and decompressed — a formidable job that must be performed in an imperceptible length of time, every time. "Latency" and "jitter" are terms applied to describe the source of delay problems more precisely.

Packet loss happens when a high percentage of packets are not successfully routed from end to end. Nominal packet loss goes unnoticed; high packet loss causes poor sound quality or a static-like noise. With data, lost packets can be re-sent; but re-sent voice packets would arrive too late to be delivered in the correct sequence. The voice contained in the lost packets, however minute, is discarded.

Best practices for ensuring QoS

The definition of adequate QoS varies from company to company. The key to achieving QoS goals is for stakeholders to reach agreement early on the definition of QoS and the assumptions that affect it. Define your organization's standards for QoS up front, to avoid the moving-target conundrum of expectations.

QoS deserves special attention in WAN infrastructures, or where Real-time Transport Protocol will be used, for example, to deliver videoconferencing.

QoS is closely related to other areas — reliability, manageability and scalability — where potential issues will be uncovered in the network assessment. Service levels will depend on defining the standards and heeding the assessment results.

Section 4.4: Reliability takes on new meaning

Is IP technology reliable enough to send customer calls over it? In terms of "uptime," we already know that IP data networks can achieve 99.999 percent (five nines) reliability.

As long as an IP network is delivering data, it is considered to be "up." When the IP network becomes the voice network, reliability standards are more stringent. Voice network downtime is unacceptable for most contact centers. The new measure of reliability is a combination of *availability* and call *continuity*.

Reliability in data networks is achieved by thinking in duplicates — redundant servers, redundant routers, redundant power supplies — to make interruptions go almost unnoticed. Redundancy alone does not guarantee call continuity. Even if almost all downtime is eliminated, calls can be dropped in the split-second switch from primary to failover systems. Call continuity requires maintaining active calls during a failover event. Otherwise, a brief power failure could disconnect all conversations in progress.

There are powerful alternatives in reliable data networks. For example, Avaya and Extreme Networks have a strategic alliance for best-of-breed converged networking solutions. Extreme Networks provides the robust data solutions to meet the rigorous security, availability, and performance demands of converged networks, while

Avaya brings to the table advanced voice IP applications. Together, this powerful alliance provides enterprise customers advanced converged networking solutions and services not available anywhere else in the market, i.e., truly best-of-breed solutions.

Voice network availability is a factor of uptime and sufficient voice quality. A data application might respond slowly during a minor network problem, but the same network problem can cripple a voice application. If the connection quality is so degraded that the participants terminate the call, then there has been a perceived episode of unavailability.

Best practices for preserving availability and call continuity

Network failures can take many forms, from brief slowdowns to complete outages. Define service level agreements (SLAs) and then contrast them to a spectrum of failure scenarios. Using the network assessment as a guide, judge the ability of the LAN or WAN to meet the SLAs. Use the results of this analysis as the basis for any necessary upgrades in response to the network assessment.

Confirm that your vendor can deliver high availability and call continuity. This level of reliability requires sophisticated software design that allows for call state information to be shared between primary and failover components.

Build redundancy into the network with the goal that users and callers should never perceive an interruption of service. There are several approaches that should be considered during the assessment:

- Duplicate network paths supported by multiple service providers, WAN access points and switches

- Duplicate servers for applications and core IP network services

- Duplicate IP interfaces so that, if one fails, IP endpoints can be redirected to another interface without interruption

- Virtual router redundancy protocol (VRRP) on large networks with layer 3 devices

Global enterprises with multiple contact centers can, with the right technology, choose to treat all centers across the enterprise as one pool of agents. This enables a *country n +1* strategy of redundancy, where a failure in one center is accommodated by sending overflow to another. Consider this possibility and build it into your requirements as needed.

Section 4.5: Security on many levels

Toll fraud was once the main security concern of contact center managers when adopting new technologies. IP telephony sprouts its own crop of potential security risks:

- Eavesdropping on unencrypted voice communications

- Denial-of-service attacks

- Viruses and malicious code

- Hacking and data theft

- Unauthorized inside access via the LAN

- Abuse of external access provided for remote or virtual agents

None of these risks is new to data networks, but the conventional voice network has not been previously subjected to them. Voice communication is an important function that must be protected as the voice and data networks converge. Shortcomings in products deployed, as well as shortcuts and overlooked security risks, create "holes" that are convenient for attackers.

Best practices for securing VoIP communications

Security stems from design as much as from implementation. A network assessment will uncover security risks, and those should be dealt with at the outset of your deployment. Think in terms of the "security trinity" — incorporate prevention, detection and response in your network design.

Involve all of your technology and business stakeholders to collectively anticipate potential threats. Identify what you are protecting, and from whom or what you are protecting it. Prioritize the most likely threats. Then implement cost-effective measures that will protect your assets, detect a breach, and enable you to respond quickly.

The best security policies are those that can be implemented through system administration and published guidelines. In the former case they are enforceable with security tools; in the latter, with consequences for violation. The Internet Engineering Task Force has identified the components of a good security policy,[3] ranging from technology purchasing and maintenance to access and authentication.

Consider these broad categories of security measures:

- Data security — passwords, encryption

- Code security — firewalls, virus protection

- Physical security — locks on doors, alarm systems

- Corporate security — written policies, regulatory compliance

- Assigned responsibility for security

That final point is important, and not only for the resulting accountability. Security and compliance are a changing landscape. A person or role must be responsible for continuously reviewing and improving your security measures.

Section 4.6: Manageability issues

Who will manage the converged network and deal with issues that arise? Voice and data networking were previously managed by separate functions, using their respective sets of tools. Convergence raises questions regarding the responsibility for managing the integrated systems.

Monitoring network performance will be essential to the contact center's performance. Tools designed for data network monitoring will not be adequate for monitoring voice on the network. Likewise, the tools used to manage the voice network were never intended for the rigors of data network management.

Best practices for network management

When assigning responsibility for management of integrated system, think beyond appointing roles for the usual move-add-change functions. Identify who will be in charge of monitoring, managing, and reporting.

IP telephony enables new levels of monitoring for call quality — even monitoring every call, if desired. Incorporate the monitoring level that is right for your contact center. In some cases, real-time continuous monitoring, or even remote monitoring, may be needed. With adequate monitoring, you or your remote monitoring provider can often fix a problem before agents know it exists.

Equip network managers with an integrated tool set that is designed for IP telephony. Ensure that the tools are capable of managing a multi-vendor environment and integrating with your existing technologies and processes.

[3] IETF "Security Handbook," RFC 2196 pp. 8-9, www.IETF.org, 1997.

Outline your strategy for handling network issues after deployment. Assess what problem scenarios could arise, how they will be detected, and how they will be dealt with. You will have averted most of them by following the recommendations in this paper; nevertheless, the unexpected can happen and it need not be disruptive.

Section 4.7: Scalability concerns

How will your IP network scale as your contact center expands? This question is important for two reasons. First, you must be prepared to support your company's plans for growth, or risk experiencing very visible growing pains at each of your contact centers. Second, IP telephony enables you to treat multiple contact centers like one center, so your scalability requirements likely will comprise your total number of combined lines for all centers.

Best practices for handling growth
Scalability is addressed simply: Deploy a system that has proven itself handling thousands of lines. Verify that the solution you choose will support your plans to pool contact centers and interflow calls between them.

During periods of exceedingly high call volumes, interflowing calls over IP can stress any network. Consider configuring your network to overflow some calls to the PSTN when the data channel is too busy to maintain your standards of quality.

Section 4.8: Evolution vs. revolution

Your company's PBX equipment represents an investment in TDM infrastructure. What will happen to that investment if you move to an IP-based voice network? Justifying IP telephony is a reasonable concern, especially if the PBX is a recent upgrade to the current generation of TDM technology.

Uprooting existing PBX infrastructure and integrating new voice servers with the data network can be disruptive and costly. There is the software required to deliver the full capabilities you need. There is the hardware necessary for redundancy. If you choose to deploy IP end-to-end, there is the task of replacing digital and analog desk sets with IP phones. Then there are the LAN or WAN upgrades that may be deemed necessary in the network assessment.

Best practices for protecting your investment
Making the leap to *pure IP* telephony is not always the best path for every existing contact center. If yours is an established center with a digital PBX, consider IP enabling the existing PBX. You can retain your investment in existing equipment, as well as familiarity with the current system's features and user interface, and yet take advantage of using IP where and when it makes sense for your business.

This factor is most evident in the decision to deploy IP phones. A flexible IP environment will allow agents to keep their familiar TDM phones, unless there is a business rationale to switch to IP hard phones. Agents who work some days from home (e.g., for workforce flexibility or business continuity reasons) may prefer IP soft phones, so their interfaces will be the same in both locations. And for new centers or expansions, IP phones generally make the most sense.

Make new investments that will endure through to a pure IP stage. If your company is planning to expand, or if you are currently evaluating a new or upgraded PBX platform or contact center system, it is important that the wiring and contact center platforms under consideration support the direction of your company toward IP.

Evaluate IP telephony vendors based on all of the best practices outlined in this paper. Consider their ability to provide assessment, hardware, software and services, as well as the best tools for security and management.

Take time to work through the details of your implementation plans with your vendor. Make sure their application interfaces use an IP connection, so no change to the interfaces will be required during the move to an IP infrastructure. Announcements and music on hold should be sourced where it makes sense for the business, regardless of whether the infrastructure is IP. Likewise, IP and SIP trunks can be used within IP contact centers if there is a business reason to use them.

Section 5: Avaya Takes IP Contact Centers Seriously

Avaya recognizes that the financial commitment of moving contact center traffic to a VoIP infrastructure can be significant, and that you will base your decision on the unique requirements of your business. Each company must evaluate IP telephony for their unique situation and choose the right path for migration. A contact center must take each step at its own pace, without rushing into unnecessary forklift upgrades. Your choice of vendors reflects the choices you make about technology directions, protecting investments and, above all, serving customers.

Whether you choose the pure-IP path, or to IP-enable your existing PBX, Avaya offers both approaches to convergence. With Avaya, you have several alternatives for introducing IP telephony into your contact center. You can add IP to your existing Avaya contact center, or you can implement LAN-based solutions. Additionally, Avaya offers options to deploy a network-based, or hosted, contact center solution that allows you to access the same contact center functionality, but you can pay for usage on a monthly basis and avoid upfront costs.

Alternatively, you can choose Avaya servers and gateways that allow your endpoints to be flexible. For outside connectivity, you can continue to select from the public network, tie lines, ISDN, an ATM network, or an IP broadband network provided by an Avaya certified Network Service Provider. At the agent desk, you may want to keep your digital or analog phones, use IP hard phones or IP soft phones, or have a mix of these.

In addition, Avaya knows that alliances help individual companies focus on their strengths and build solutions that are more comprehensive, faster to implement, and more cost effective for their customers. While some organizations are successfully finding their own way to the advantages of IP telephony, the complexity of this challenge is significant. IP telephony technology and systems have reached a level of maturity where they must be treated in a holistic manner in terms of overall network performance, security and reliability, and the business activities they support. Alliances, such as Avaya and IBM for example, can help maximize the benefits of complex technologies like IP telephony and help companies to minimize risk and reduce the time it takes to implement a solution. This relationship, and other alliances, ensure that vendors focus on the development of business solutions and minimize the inter-vendor conflicts that might otherwise develop. In this way, Avaya can help individual companies focus on their strengths and build solutions that are more comprehensive, faster to implement, and more cost effective for our mutual customers.

Avaya offers companion white papers that address the business value of moving to an IP contact center and that help you map these suggestions to Avaya solutions and services. For more information on how Avaya can help you safely navigate your way to IP telephony, contact your Avaya Client Executive or Authorized Avaya BusinessPartner, or visit us at www.avaya.com (go to Research By/Resource Type/White Papers). Some examples are "Three Best Practices for Today's Profitable Contact Centers", "IP Telephony Migrations: Alliances Make Solutions Work" and "The Decision to Deploy a Hosted Contact Center".

About Avaya

Avaya enables businesses to achieve superior results by designing, building and managing their communications infrastructure and solutions. For over one million businesses worldwide, including more than 90 percent of the FORTUNE 500®, Avaya's embedded solutions help businesses enhance value, improve productivity and create competitive advantage by allowing people to be more productive and create more intelligent processes that satisfy customers.

For businesses large and small, Avaya is a world leader in secure, reliable IP telephony systems, communications applications and full life-cycle services. Driving the convergence of embedded voice and data communications with business applications, Avaya is distinguished by its combination of comprehensive, world-class products and services. Avaya helps customers across the globe leverage existing and new networks to achieve superior business results.

AVAYA

**COMMUNICATIONS
AT THE HEART OF BUSINESS**

avaya.com