OVUM

WHITE PAPER

Global Conferencing Challenges

sponsored by 

About the Authors

Ian Jacobs

Principal Analyst, Ovum Research
Enterprise Telecoms

Ian Jacobs is a principal analyst on the Customer Interaction Technologies team, covering contact center markets and technologies. With a strong focus on core routing technologies, customer experience issues, social media and its impact on service, and customer interaction chains, Ian monitors and analyzes emerging trends, technologies, and market dynamics in the contact center, speech, and CRM industries.

Ian has authored numerous research studies on automatic call distributor systems, IP contact centers, the intersection of social media and customer service, routing technologies in the enterprise, CRM enablement, customer service and support applications, IVR systems, and offshore outsourcing of customer support. Ian has led several consulting projects on fostering excellent customer experiences, improving contact center processes, and building awareness of excellence through marketing for clients in multiple countries. He is frequently cited in the media on contact center and CRM issues. An award-winning columnist, Ian also contributes regular columns to leading industry publications.

He brings with him more than 15 years' experience as a marketer, journalist, and analyst in the enterprise software market. Ian Jacobs received an MA in journalism from Stanford University, where he was a recipient of a McClatchy Fellowship. He received a BA in both comparative literature and sociology from Rutgers University.

Mike Sapien

Principal Analyst, Ovum Research
Enterprise Telecoms

Mike Sapien is responsible for Ovum's US Enterprise Practice. Based in southern California, Mike is focused on North American and global enterprise telecom markets. This includes WAN, managed, and advanced voice and data services to address Global MNC, large enterprise, and SMB customers. His focus areas also include data center services, emerging cloud and hosted services, enterprise mobility services and related product development, market launch, and channel programs of enterprise services.

Mike leads the design, development, and implementation of Ovum's research and advisory services on enterprise network services and managed solutions in North America with a major emphasis on the tier 1 carriers, infrastructure vendors and providers. He is a regular contributor to Ovum's enterprise research, and provides analysis of industry, vendor, and product trends included emerging managed services such as SIP trunking, unified communications, VoIP, and complex managed services.

Mike has over 27 years in the telecoms and internet services industry including executive positions at large carriers, CLEC, and a data center provider. Mike was one of the first published authors to write about ISDN applications for IT personnel (Mastering ISDN by Sybex – 1997). Mike is a graduate of Loyola Marymount University (BBA & MBA) and Columbia University executive management program.

Global Conferencing Challenges

Why it can't be the same everywhere

Authors: Mike Sapien and Ian Jacobs

EXECUTIVE SUMMARY

Ovum overview

The global market for audio conferencing will hit $5.5bn in 2015, up from $5.0bn in 2010. Much of that growth will come from emerging markets in Asia, the Middle East and Africa, and Central and South America, each of which is projected to rise at a minimum compound annual growth rate (CAGR) of 4%, while certain regions will hit a torrid 8% growth rate. Some of that emerging market growth will come from organic, domestic usage, but much of it will come from multinational corporations extending their conferencing reach into the various regions in which they operate.

Extending conferencing services into emerging regions requires enterprises to recognize the issues they are likely to face. Regulatory and technological infrastructure differences between countries can make even basic conferencing a complicated endeavor. A rapid uptick in usage of mobile devices will challenge enterprises' ability to provide easy, toll-free conferencing around the world. Operating in regions more susceptible to fraud makes security a concern that companies will need to plan for before they roll out any conferencing services. It will demand constant monitoring to provide peace-of-mind going forward. Selecting a partner that understands all of these issues and can help companies navigate the tricky waters of multinational conferencing will make life much simpler, and allow them to better focus on their core business.

Key messages

- Enterprises do not properly recognize the number and severity of the challenges brought on by extending conferencing services to emerging countries.
- Regulatory environments can vary tremendously from country to country, and can change with little notice. Attempting to keep track of all the permutations and interactions between regulations can be exasperating.
- Infrastructure differences around the world will make conferencing standardization and stability a constant challenge for enterprises. Unreliable or non-existent interconnections between carriers, even carriers within the same country, are typical of the infrastructure-related issues that could confound enterprises.

- Using methods such as social engineering, criminals have been successfully gaining illegitimate access to conference bridges. Once fraudsters can access a bridge, they often resell that access as toll-free calling in their home countries.

Considerations for customers

Companies in developed regions such as North America and Western Europe often assume their experiences are universal and that doing business in other regions is the same as at home. Because audio conferencing is relatively simple and hassle-free to set up and to use in their home countries, companies often expect the same state of affairs to occur in emerging market countries. This fallacious reasoning can easily set companies up for failure when they actually attempt to extend their conferencing services to new countries.

Although it sounds simplistic, Ovum believes that companies need to be reminded that countries such as Brazil, Pakistan, and Sierra Leone do not have the same infrastructure, the same regulations and the same levels of security as developed countries such as the US or France. Only when companies recognize the scale of the difficulties they are likely to encounter can they then begin to properly plan, assess their own capabilities, and decide on the best course of action.

To construct a stable, multinational audio conferencing facility, a company would need to unravel the tangled skein of regulations from every country in which calls might originate. It would need to evaluate the capabilities of multiple carriers and then create relationships with all of those required to provide the necessary coverage. It would also need to establish a fraud identification and prevention system.

In most cases, the efforts required to accomplish all of these tasks would easily exhaust the resources of even large companies. Ovum believes that companies would make much better use of their time and money by working with a third-party conferencing services provider that has already done all the groundwork to facilitate conferencing around the globe, and that can help fight potential fraud. Such a relationship will allow companies to focus their internal resources on their primary business activities.

GEO-POLITICAL ENVIRONMENT WITH REGULATORY CHAOS

Geo-political differences outside North America

Audio conferencing is on the rise in emerging markets

Table 1 details the rapid growth of audio conferencing across several emerging markets, using data from Ovum's report *Audio and Web Conferencing Services, Volume and Revenue Forecast: 2010–15*.

The figures show the CAGR from 2010–15 for audio conferencing revenues. Ovum defines agentless audio conferencing (also known as unattended or reservationless conferencing) as a conference set up by one of the participants in the call, and not requiring operator assistance or scheduling. Operator-assisted audio conferencing (also called managed audio conferencing)

includes conferences scheduled in advance and managed by an operator, who may provide functions such as event moderation, registration, and call admission.

Table 1: Audio conferencing revenue growth 2010–15

Country (selected)	CAGR for agentless audio conferencing revenues	CAGR for operator-assisted audio conferencing revenues	CAGR for total audio conferencing revenues
Brazil	11.61%	-2.95%	9.24%
China	10.12%	-5.34%	8.07%
India	9.56%	-5.35%	7.37%
Pakistan	8.22%	-3.74%	7.00%
Egypt	6.24%	-5.40%	4.94%
Czech Republic	5.18%	-5.72%	2.69%

Source: Ovum

These figures clearly demonstrate that the demand for conferencing services to and from emerging markets is on the rise. However, all that growth brings with it numerous difficulties with which enterprises must cope.

Regions and countries differ greatly and have restrictions and limitations

Most companies are very comfortable working within the stable and mature telecoms industry of North America (the US and Canada). This stability is a result of many years of consistent investment in the telecoms infrastructure, a consistent regulatory environment, and a standard numbering plan (the North American Numbering Plan). This allows carriers and conferencing vendors to provide high-quality services and interconnection between incumbent telecoms carriers and the many competitive providers. Wireline and wireless operators provide services that allow roaming and numbering plans that enable national coverage and interconnection. This environment provides a very consistent platform for conferencing services, and many enterprises have developed homegrown or internally developed conferencing systems that can be implemented with relatively little complexity within North America. Many other enterprises have turned to conferencing services providers, looking to tap into their expertise and their already built-out infrastructure.

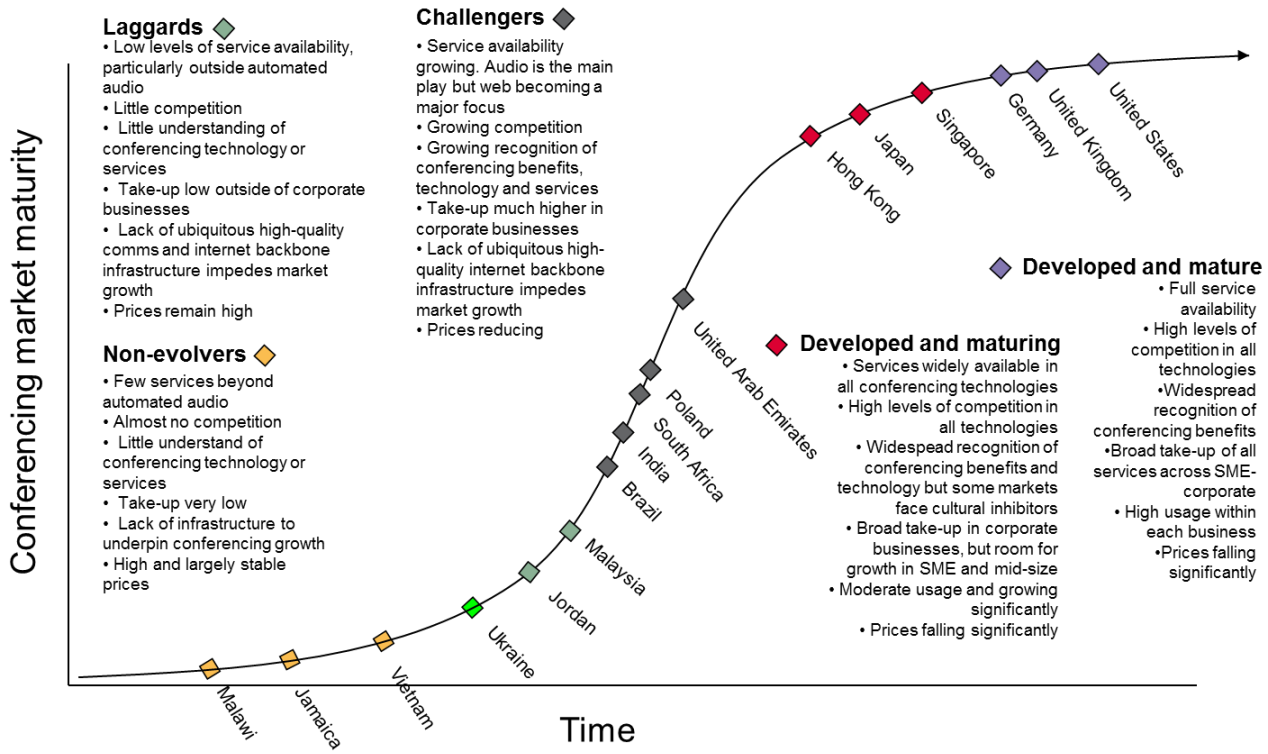
To enable global service coverage, however, the complexity is greatly increased. Some regions and countries lack numbering plan interconnection, roaming, and stability. With many countries still maintaining government ownership of the incumbent telecoms provider, and some still maintaining a monopoly in the telecoms environment, some services are either not available or extremely costly. In some countries, mobile network operators do not provide interconnection with the wireline operator. In other countries, including China and Japan, the government has split the market between two wireline incumbents, each with a monopoly in its own region.

In the BRIC countries (Brazil, Russia, India, and China),which include the three highest growth markets, there are situations where IP traffic cannot be mixed with TDM traffic for conferencing services. In India there are also many cases where the mobile operators are not interconnected, creating situations where mobile customers cannot call each other or connect to conferencing

resources. This lack of interconnection is a problem in many emerging countries. Furthermore, the regulation of conferencing services can be ill-defined or vague, allowing for liberal interpretation and often resulting in “gray” situations, in which interconnection or carrier coverage can be very difficult.

The challenge of trying to mix TDM and IP networks, as well as providing interconnection between carriers and networks, makes it very hard for most enterprise customers to build out and maintain voice connectivity for reliable, global conferencing services.

Figure 1: Conferencing maturity model



Source: Ovum

Figure 1 illustrates the current level of maturity and the path of technology adoption for conference services in selected countries around the world. Ovum breaks countries into five categories. On one end of the scale there are the “non-evolvers”: poorer nations without the economic impetus or technology infrastructure to drive internal conferencing growth. Some audio conferencing services are available in these countries, but there is insufficient telephony to drive uptake. Prices are high due to a lack of competition and limited economies of scale.

On the other end of the scale are the “developed and mature” and “developed and maturing” nations, which include countries in North America, Western Europe, and developed parts of Asia-Pacific. These nations have the choice of the full range of automated audio, managed audio,

streamed event, web, and desktop- and room-based video services, and have the infrastructure and advanced business processes necessary to yield the benefits.

The countries identified in Figure 1 are typical examples of each group. Enterprises looking for conferencing services to and from countries in the “non-evolvers,” “laggards,” and “challengers” categories will face a greater degree of difficulty, with issues including regulation, infrastructure, rapidly increasing uptake of mobile technologies, and higher levels of fraud. This report highlights many of these issues, providing enterprises with a host of topics to discuss with any conferencing service provider.

The regulatory challenge increases with change management

Understanding the regulatory environment

One challenge to the implementation of global conferencing services is the constant change of regulation and policy in many countries outside the US. One example of this is the switch from 11 to 12 digit phone numbers in Germany. In India, meanwhile, the government may mandate that the carriers interconnect with each other and then subsequently issue orders to prohibit interconnecting with certain mobile operators.

For enterprises, change management can include issues around increased tax liability, local phone number availability, toll-free services, and voice termination/origination. These challenges can have a major impact on companies’ basic conferencing service capabilities.

It often seems that just when enterprises start to understand the different regulatory environments and complete major deployments, the rules change and require last minute changes or modifications to support basic conferencing services. The effort required to understand the regulations can be much smaller than the effort to keep up with the changes in emerging countries such as India, China, and Brazil.

Regional examples and highlights

The challenge of keeping up to date in the Middle East

Many of the issues mentioned above are present in the Middle East. Some countries in the region do not allow VoIP services. In others, enterprises cannot mix the IP and TDM networks. This requires the duplication of infrastructure or the use of “gray” gateway vendors to connect the two technologies and networks. In some countries, foreign companies and providers cannot get local phone numbers, while in others phone numbers may be restricted to only wireline service or only mobile services.

At the same time, the propensity of regulation to change adds to the complexity of operating in this region. Incumbent providers often have the authority to develop and implement changes at their own discretion, and when these operators are the exclusive mobile or wireline carriers, enterprises are unable to avoid their restrictive policies. All the major challenges of providing reliable conferencing services are present in the Middle East, and must be faced by enterprise customers expanding their presence in the region.

TELEPHONY INFRASTRUCTURE, INCLUDING MOBILITY

Global differences prevent conferencing standardization and stability

MNCs have to realize that global coverage raises the investment requirement

The North American numbering system may be dated, but it has provided a consistent, standard model for telephony services. It can be considered both a blessing and a curse, in that it applies only to the North American market: other parts of the world have different number plans and policies, and these can vary by country and by region. The variations in dialing plans, phone number allocation, use policy, and number distribution add to the challenge of providing the voice connectivity required for a global conferencing platform.

In the US, it is very easy to get the voice infrastructure necessary for national coverage with just a few large carriers. The US carriers all have networks with strong coverage, and provide interconnection between themselves as well as with all the major mobile operators. Customers have long forgotten about the roaming issue, as all the major mobile operators have gone to a blended usage model, without extra charges for mobile roaming. The simplicity of the US system makes it easy to deploy and maintain voice infrastructure for conferencing services. Unfortunately it is much more complex to expand to the global coverage required by most MNCs and large enterprises.

Outside North America, many more carriers are required to provide the necessary connectivity for global conferencing coverage. In many regions, multiple carriers are required within a single country to cover the geographic, mobile, and regulatory divisions. Sourcing and managing all these carrier relationships can quickly consume all of an enterprise's internal network staff resources, leaving its other internal IT priorities at risk.

In countries such as India, the Philippines, Indonesia, Malaysia, and Thailand, the incumbent telecoms provider controls most of the infrastructure, and has a great deal of sway with the regulatory bodies. Enterprises looking to extend their conferencing capabilities into such countries face many uncertainties, ranging from parsing the nuances of regulations, through to the actual physical connections. The complexity increases exponentially when enterprises attempt to set up multi-country conferencing systems. In fact, it seems as if the one constant for enterprises looking to build out their own global conferencing infrastructure is that there is another unknown lying in wait around every corner.

In addition to the increased number of direct carrier relationships, multi-tier carrier relationships are needed in order to get the global coverage necessary for conferencing services. In many cases the coverage will require a number of small, regional carriers that can provide the needed interconnection or reach. This complexity is one reason that many enterprises turn to conferencing partners that have already navigated the waters of multi-carrier, multi-country relationships.

It is almost impossible for an enterprise without a good handle on its conferencing volume by region or country to design and build out the network infrastructure or carrier commitments needed to manage the costs and traffic volumes effectively. Many over-build their networks for conferencing, or have to expand their networks at the last minute. This is both costly and difficult to manage, and in some regions network expansion can take as long as 90 days. This means that the service is either blocked or unavailable until the network expansion is completed.

Other issues enterprises face when building out conferencing capacity include the need to plan for predictable, but difficult to manage, spikes in volume. For example, cultural norms mean employees typically schedule conference calls on the hour or the half hour. This results in heavy spikes in conferencing volumes twice an hour during business hours.

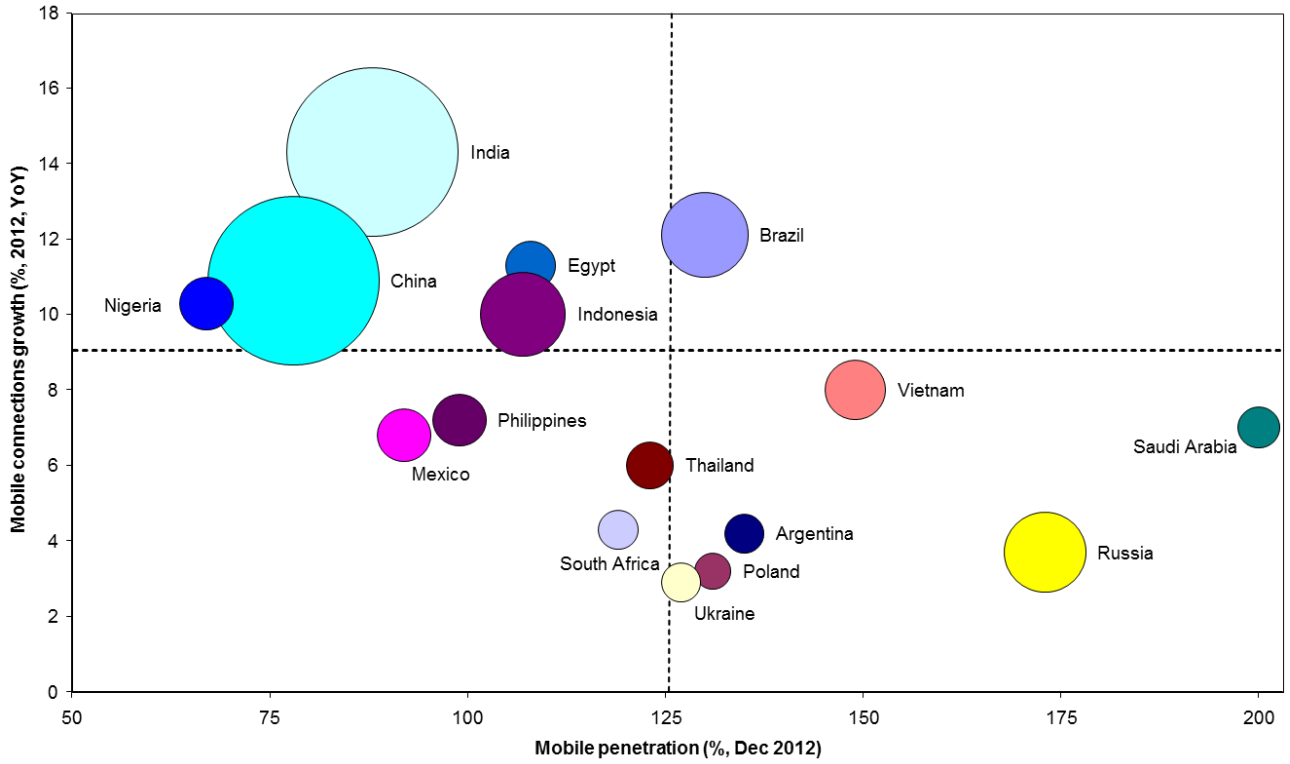
Managing existing capacity and forecasting the need for additional network infrastructure for conferencing services can often expand beyond the customer's budget, staffing, and expertise. This is another reason for enterprises to turn to a trusted partner with experience in forecasting requirements, understanding the elasticity available to enterprises, and managing the multiple carrier relationships required to meet shifting conferencing demands.

Mobility creates numerous challenges

Quality of service and a lack of interconnection make mobile access tricky

Accessing conferencing services is a major challenge in many countries, but enterprise customers see it as important for its knowledge workers and sales teams. The issue of quality of service (QoS) also creates major challenges outside the US, especially in emerging markets, where mobile service may be the only option.

Figure 2: Mobile connections growth in selected markets: 2012



Source: Ovum

Emerging markets continued to see double-digit mobile connections growth in 2012. In the report *Trends for 2012: Emerging Markets*, Ovum explained that large markets with relatively low mobile penetration – such as China, India, Brazil, Nigeria, and Indonesia – will be the key drivers of emerging market connections growth. This trend is illustrated in Figure 2, in which the size of the bubble indicates a country's total market size, as measured by connections.

Most mobile services outside the US have very expensive roaming charges or lack interconnections with other mobile networks. In many emerging countries, poor voice quality is a major problem, and this makes connecting to any conferencing service a challenge. The limited QoS and the lack of interconnection mean that most mobile end users are left with few choices in terms of conferencing services.

Even basic access from mobile devices can be an issue. In some countries, international toll-free numbers – the type favored by many conferencing customers – are blocked for mobile users. This blocking often happens with very little notice, as was the case with calls for Finnish mobile users in 2012. Sometimes conferencing providers can open up that international toll-free access for a charge, but that fee often outweighs the benefits the customer would receive. Even when everything does work and mobile callers can access the conference service with a toll-free number, the toll structure for those calls makes access unfeasible. The cost of a call from a mobile

device can sometimes run to more than 20 times the cost of a similar call from a landline. In such cases, enterprises will likely need to work with their conferencing service partner to contact the local carrier and ensure that mobile phones are blocked. The alternative approach for such situations is to source a local, in-country number, but as mentioned previously, such local access may not always be available.

How to improve the mobile experience

As the increasing reliance on mobile devices in emerging markets makes clear, enterprises looking to extend their conferencing capabilities into such regions will need to accommodate mobile users. Some conferencing providers have taken solid steps towards optimizing the mobile conferencing experience, building mobile conferencing applications. The best of these applications, such as the iPhone application built by InterCall, shown in Figure 3, give users a great deal of control over their conferencing experience, both as meeting organizers and participants.

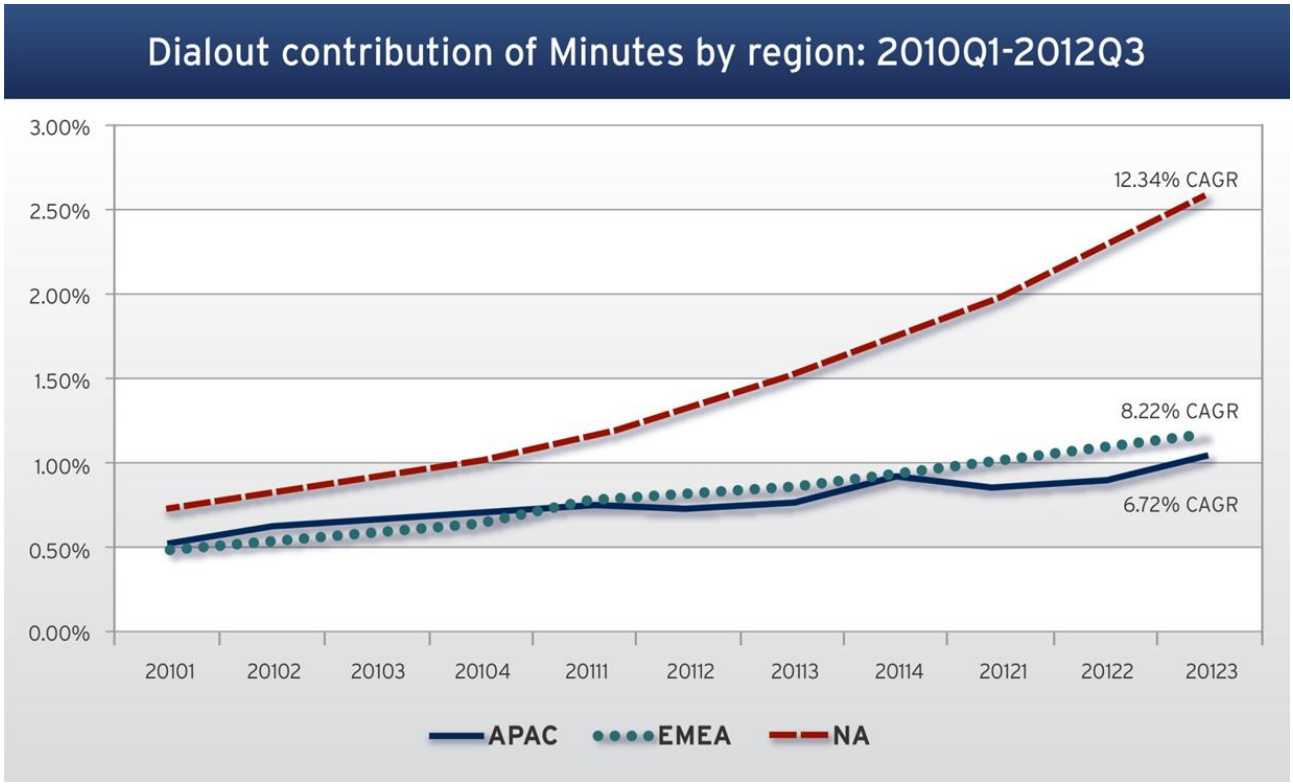
Figure 3: Example of a purpose-built mobile conferencing user interface

Source: InterCall

The increased penetration of mobile devices in emerging markets is also feeding demand for dial-out options. These allow users to request a call from the conferencing system, often by clicking a link in an email invitation. This dial-out functionality provides mobile users with a streamlined experience, with no need to enter a 10- or 15-digit number followed by a 10-digit access code. In “caller pays” situations, such functionality also helps enterprises to keep their mobile costs in check. In some cases, dial-out is the only way for critical participants to join a conference.

Figure 4, from conference provider InterCall, shows the rapid growth in dial-out minutes as a percentage of total conferencing minutes. Although the benefits of dial-out are most acutely felt in developing regions, users in developed countries also like the simplicity and easy experience that the function offers.

Figure 4: Quarterly dial-out minute growth of a leading conferencing vendor (2010–13)



Source: InterCall

Regional differences in infrastructure

Wireline and wireless operators differ by region and country

Brazil and India offer differing examples of the issues enterprises face in multinational conferencing. India does not allow PSTN or TDM traffic to mix with IP traffic, which means that a conferencing service would have to backhaul traffic out of the country. Brazil, on the other hand, has more than 40 mobile providers available to enterprises. Not all of those mobile operators have agreements in place to allow connection to each other's networks. Some do not support the different phone number configurations of other operators, and there is no regulatory requirement for operators to provide such interconnections.

In both India and Brazil, growth in demand has outgrown the existing telecoms infrastructure, making even simple services a challenge in some areas. At the same time, the rapid growth in

these two markets means that most MNCs require services there. Enterprises are therefore forced to accept what they can get within these countries, or find third-party solutions. The key point here is that every country has its own idiosyncratic issues, and tackling them all would tax the resources of even very large enterprises.

Although working with a trusted partner can make life much easier for enterprises, they must go into such relationships recognizing the limits of what that partner controls. While conferencing providers can help with provisioning numbers and creating bridges, they must themselves use partners, some of which will also use partners of their own, to provide access to users in other countries. Enterprises need to work with their conferencing provider partners to ensure the optimal level of coverage and quality of service with the minimum of hassle.

FRAUD AND SECURITY OVERVIEW

Major fraud and security principles in conferencing

Constant monitoring is the key

Companies looking to build multinational conferencing facilities must plan to combat fraud, and should build processes and technology to increase security. The issues are complex, and differ somewhat from region to region, and there are several reasons why companies should seek help in understanding the numerous ways to combat fraud and improve security.

While companies that operate only within a single geography are also susceptible to fraud, any fraudulent activity tends to be easier to spot. A company that only ever uses conferencing services within the US and Canada, for example, would be likely to notice participants using one of its conferences bridges from Latvia or Pakistan. If, however, a company actually has frequent conferences that include participants from around the world, fraudulent activities become much harder to spot. Companies in such situations might benefit significantly from the help of a conferencing provider with experience in dealing with multinational fraud. Such providers can provide practical advice on how to prevent fraud, as well as algorithmic help in identifying out-of-the-ordinary usage.

Enterprises with multinational conferencing facilities are likely to face two main categories of fraud. The first is when someone in a foreign country uses a company's bridge and network for unauthorized purposes, such as calling friends and family members, or even for more nefarious purposes such as making the bridge available to terrorist or criminal networks. The second is when a fraudster gains access to the conferencing bridge and then sells that access, often by means of a prepaid calling card. This type of fraud tends to be perpetrated by organized criminal entities, rather than a single individual.

In either type of fraud, criminals construct organized attacks to break the security of the conference bridge, often using social engineering to obtain the required information. However, enterprises are frequently lax when it comes to creating, instituting, and enforcing security policies internally. For

example, some companies publish conferencing information (including PINs) on their websites. Such slipshod security is a gift to would-be fraudsters who are seeking such information.

To better hide their usage, fraudulent users will often try to utilize the conferencing bridges at weekends and on public holidays, when network monitoring may be more relaxed. Understanding the patterns that indicate fraud takes time and experience. Ovum believes that enterprises would be wise to seek out partners that have fraud management systems in place. Such systems monitor conferencing bridges, and constantly seek out new ways that legitimate credentials can be illicitly acquired. They should have automatic alert thresholds so that when a potential fraud is detected, the conferencing provider will receive notifications immediately, allowing it to rapidly take corrective actions.

Look for conferencing platforms with built-in security features

Any conferencing system should itself be designed to thwart fraud. Some leading conferencing providers have adopted a simple approach: if a user attempts to log in with incorrect credentials three times they are locked out of the system. Some conferencing systems build in another layer of security using the same idea: whenever a user attempts to do anything in the system incorrectly three times in succession, that function is locked.

Another approach to providing additional security is to parse the calls coming into the system to ensure that they are legitimate. Conferencing bridges should be flexible enough to have user- and system-generated blacklists for numbers and countries that will automatically be rejected by the system. The conferencing bridge should also check that the telephone number associated with an incoming call matches the customer profile.

Smaller security features can also help to reduce fraud. Conferencing provider InterCall estimates that more than 85% of all fraud on its systems is associated with accounts with security codes of seven digits or fewer. To help make fraud more difficult, enterprises should require users to have longer security codes; InterCall claims that 10 digits would make for a more secure environment.

Security includes social engineering

Balancing security best practice and usability is tricky

The types of people that attempt to gain fraudulent access to conferencing bridges are certainly not shy and retiring. They typically have seemingly endless patience for piecing together whatever bits of information they can gather, but they also often resort to more brazen approaches to information gathering. Social engineering – manipulating others into revealing confidential information – is a favorite tactic.

Fraudsters will call a conference bridge's helpline and attempt to obtain information from the customer service representative. They will often pretend to be legitimate users who have lost their security credentials. Deceitful callers can be very convincing, but security policies can help thwart even the best social engineers. For example, conferencing services should create policies that ensure that even if a fraudulent caller fools the customer service representative, they still cannot

get the required information. A conferencing service provider could, for instance, allow only call center agents to email security codes, and require them to send such emails only to specific, registered corporate accounts, and not to personal accounts such Gmail or Yahoo Mail. Such a policy would mean that a would-be fraudster would need to have hacked a company's email system before they could gain access to its conference bridge.

Regional consistencies in fraud incidents

Be aware of specific hotspots

Although criminals attempting fraudulent access to conferencing systems come from all over the world, certain hotspots bear extra scrutiny, and conferencing service security policies should be fine-tuned with those areas in mind. According to conferencing services provider InterCall, high levels of fraud have been noted in Latvia, Pakistan, and several African countries.

There are numerous examples of detected fraud. One company found its conference service access numbers, along with active security credentials, published as a free conferencing service in India. Others have found the access details to their conference bridges being sold as calling cards in Pakistan.

One way to curb such fraud would be to simply block dial-in from and dial-out to those countries that are considered hotspots. However, if a company truly needs to provide access from those countries, there are approaches available. For example, while most conferencing users have shifted towards agentless conference bridges that allow individuals to initiate their own conferences, companies could require that any call coming in from specific countries be routed to an agent. This would give the company another line of defense in verifying that all usage is legitimate.

Conclusion

Partner for safety, sanity and effective communications

Enterprises clearly know best how they will use conferencing services and how such services can act as transformative tools for building a collaborative culture. But enterprises would be wise to recognize the need for expertise when it comes to designing, securing and operating such services. Attempting to navigate the tricky waters of interoperability between operators, securing conferencing services against fraud and other security intrusions and optimizing for the ideal level of capacity could easily consume an enterprise's IT department to the point that it negatively impacted that enterprise's core business functions. Therefore, enterprises should be seeking out partners qualified to handle the complexity of multinational conferencing and that can truly allow them to focus on excelling in their main business.