



Unified Communications & Collaboration Clean-Up Guide

All the steps you need to help assure the availability and quality of your UC&C services.

INSIDE ▶▶▶

Time to Optimize Your UC&C Services

Page 2

Clean Up QoS in Your Network

Page 4

Clean Up Your SIP and SIP Trunking Environment

Page 7

Clean Up Your Multivendor UC&C Environment

Page 10

Clean Up Your Video Conferencing Environment

Page 13

Clean Up Your Voice Quality

Page 15

A Single Application to Monitor Voice, Video, and Data Services

Page 17

SPONSORED BY

NETSCOUT

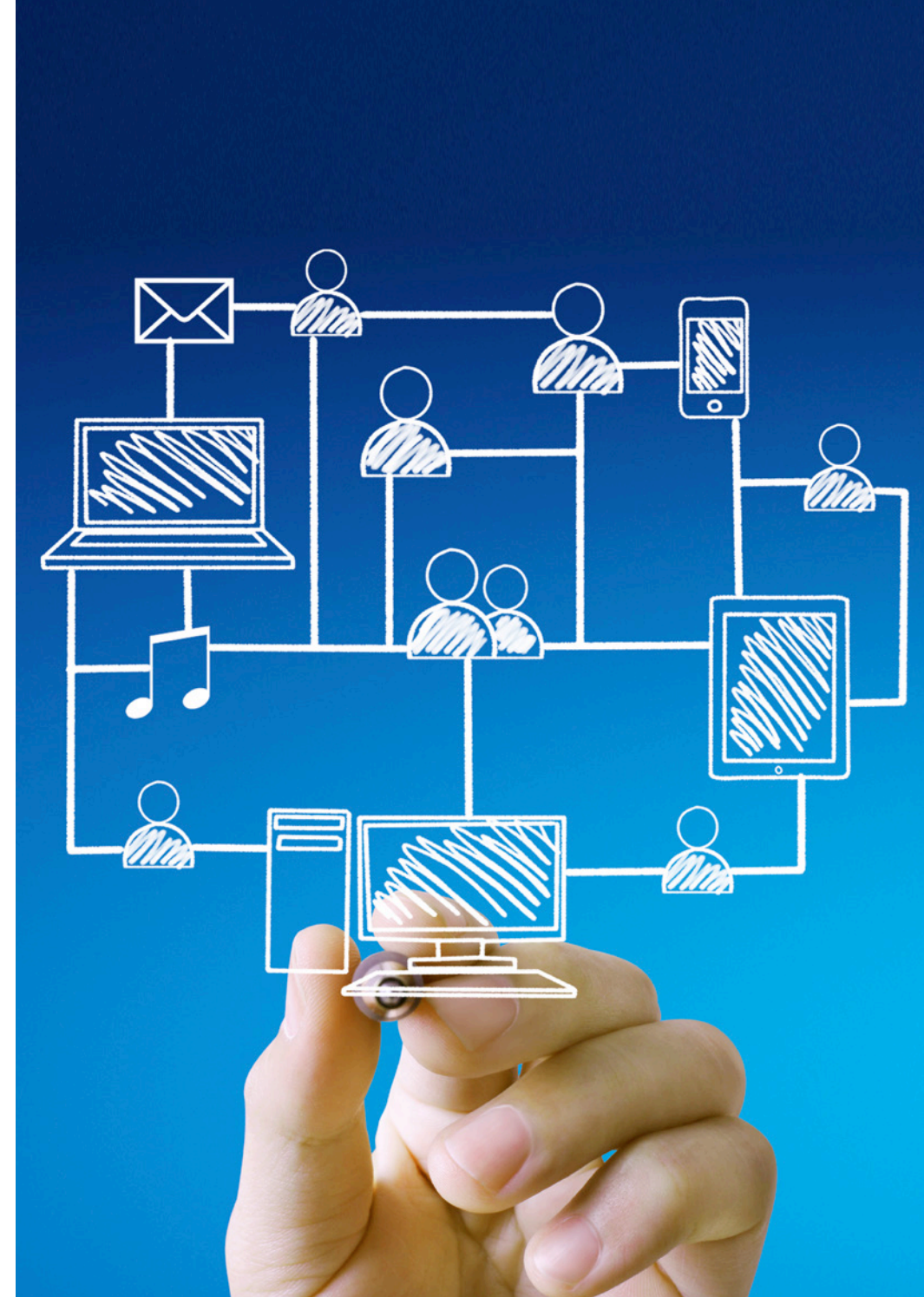


Time to Optimize Your UC&C Services

Don't wait for your Unified Communications and Collaboration (UC&C) services to be in crisis before you start thinking about how you monitor and manage them.

With the increasing importance of UC&C services in your organization, poor performance, underutilization, application unavailability, and service disruptions in your voice and video call quality will likely:

- **Cost you money** in terms of lost revenue, costly service repairs, poor customer satisfaction and lost customers
- **Waste your valuable time** pinpointing problems in complex UC&C environments or finger-pointing with both internal and external participants





- **Negatively affect people** through lost productivity, communication breakdowns, customer complaints, and high frustration

Yet, even in today's complex, multivendor environment, simple ongoing preventive actions can minimize painful service degradations or unplanned outages and assure the availability and quality of your UC&C system.

This short checklist of regular, pre-emptive activities is based on best practices from some of the largest, most intricate unified communication networks in the world and over 10 years of UC monitoring implementation and support. It will help save money and time, avoid headaches, and protect the quality of your UC&C environment.

Where Problems Can Hide

The current UC&C estate is often a blend of several different vendor solutions where voice, video conferencing, and instant messaging are tightly coupled with other IT



systems such as email, calendar, authentication, and DNS systems over the converged IP network.

This complex landscape creates ample opportunities for a problem to remain hidden and deteriorate further without anyone realizing it has occurred. Throwing the problem to your third-party provider does not always guarantee a quick or full resolution. Instead, seeing and understanding the key areas of your UC&C deployment, infrastructure components, and service-enabling protocols, vendors, and

platforms, and their interdependencies will keep them operational and highly available.

Let's not forget, it is called "converged" for a reason. Voice, video, AND data services converge on the same enterprise network, and their behaviors have an impact on one another. Unexpected spikes in utilization of one business service can absorb bandwidth otherwise available to UC&C services. The cause of poor-quality phone calls may be hidden behind the activity of another business service application or activity.



Clean Up **QoS** in Your Network



The Problem

Voice and video are latency-sensitive applications running over your infrastructure. Once a network slows down or becomes congested, quality can suffer unless this traffic is suitably prioritized over the network.

This is why Quality of Service (QoS) is so important.

QoS problems may be some of the trickiest issues to tackle. But they're probably also the most important because QoS helps ensure that you get the best user experience over your network. Some IT professionals discount the value of QoS where bandwidth



availability seems plentiful. But experience teaches us that what may be fine today may not work tomorrow because nobody really knows what is coming around the corner. As UC&C service uptake increases, you get more video conferencing and new business applications layered onto your converged infrastructure, all of which consume bandwidth. Therefore, a strong, continuous focus on QoS should be part of everyone's strategy.

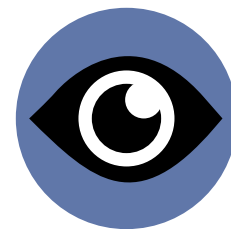
You might not even be aware that the QoS is not set correctly until people start to complain. But where do you look?

QoS can be set almost anywhere in the network. The phone or endpoint typically sets it from the start. Switches and routers can also make changes to classifications en route to the destination but also need to "honor" the quality and prioritize the traffic throughout its journey. There are lots of moving parts, and if QoS is not set correctly, or becomes misconfigured throughout the call's journey, quality will likely suffer.



What Monitoring Do You Have?

You can start by monitoring your call quality. Vendor management tools typically provide endpoint statistics of call quality or Mean Opinion Score (MOS), with metrics on packet loss and jitter. This gives you an indication of possible congestion affecting the quality of the traffic going to the endpoint. You now have statistics indicating that the call was bad for that user, but unless you have more data, it will be hard to utilize just those metrics to "clean up" call quality.



The Visibility Needed

What's needed is increased visibility and specific metrics that will help you pinpoint where in the network the congestion exists. Identify where the QoS is set, where there

are mismatches, or whether QoS changes throughout the journey of the call.

The only way to achieve this visibility is to have instrumentation along the call path. You can then see the quality and the QoS settings as the call makes its way through the network across the data center, across the WAN to the endpoint. This provides information on the quality of the calls to an endpoint or location. You will see the QoS setting in both directions and would expect them to be set to the high priority AF (assured forwarding) or EF (expedited forwarding) queues with the same prioritization in both directions. You should expect consistent QoS everywhere you see the call through the instrumentation.

Additionally, having visibility into all the traffic running over the links, including VoIP, video and signaling, and application traffic, will help you discover bandwidth hogs that may be contributing to congestion and thereby causing quality issues.



The Cleanup

Now that you have the visibility, you can prioritize, drill down, and clean up QoS issues.



- **Information on MOS scores**

for various locations: This insight lets you prioritize your cleanup. You will probably want to fix what is visibly broken (the bad calls) first!

- **Information on QoS mismatch:** This info enables you see and prioritize what

needs to be fixed. Because a QoS mismatch means that things are not set up correctly, this makes it a good target for early resolution.

- **Information on which locations have voice and video with inappropriate QoS settings:**

Here you get the ability to check the paths of the traffic going to those locations with incorrect QoS, rather than having to check each one in turn.

- **Information on the traffic over your links for**

each QoS queue: This info lets you see what other traffic is contending with the voice traffic and what the priority should be. For example, discovering that a large-file backup was occurring midday across the WAN on the high priority queue is a problem. The intention had been to schedule this late at night, but inadvertently the configuration did not turn out that way.

- **Business data application mistakenly in the priority QoS class:** This situation can create quality issues for the voice and video traffic.



Clean Up Your SIP and SIP Trunking Environment



The Problem

The big benefits of SIP trunking are cost savings and agility. Many next-generation IT initiatives are focused on flexibility to provide new features and infrastructure that new business services can consume. Cost savings can be substantial because of cheaper long distance voice costs, but none of this should come at the expense of service quality. Becoming more efficient (reducing costs) while decreasing one's effectiveness (losing customers, revenue, etc.) is not a recipe for long-term success.

While there are several standard and proprietary signaling protocols



available, SIP is becoming ubiquitous. SIP preserves interoperability with all systems, and the migration to SIP is inevitable. But if SIP is not operating efficiently in your network, calls will not connect, or they will be slow to connect.

The key technological strength of SIP trunks is that they are IP based, replacing the need to have gateways translating to TDM or POTS analog technology. This means that the calls typically will not need to be coded, recoded, and then translated back again, ultimately improving call quality.

With SIP trunks, you now have a new piece of hardware to be placed into the infrastructure, a Session Border Controller, or SBC, which can provide security, routing, and prioritization of voice signaling and voice traffic. However, if the SBC is not configured correctly, you may see performance or connection issues.

The other thing, of course, is that calls are being made to remote parties through the SBCs. So when it comes to issues of voice or video quality, it is important to be aware of where the problem exists and who owns the responsibility

for fixing it — you or the provider? If it is your issue, such as voice quality from within your infrastructure or signaling issues from your Call Servers and SBCs, you can start to rectify things. But if the provider owns the problem and the resolution, you need to present that provider with some clear evidence to encourage a speedy resolution.



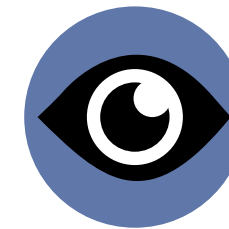
What Monitoring Do You Have?

You may be surprised at the lack of visibility into SIP trunk performance. Frequently providers deliver monthly service reports, saying they have met SLAs that typically relate to availability but not necessarily to service quality.

But the day-to-day issues around SIP and SIP trunking involve more than just uptime. Slow connections, connection failures, codec mismatches, one-way audio, drops, poor quality, etc., are all meaningful metrics that can be used to define overall system health.

You already have statistics on SIP call

signaling, such as calls made, successful calls, failed calls, and dropped calls. And perhaps you have summary information on the quality side, such as average MOS, packet loss, and jitter for the trunk. But it is difficult to improve service quality by using only these basic metrics.



The Visibility Needed

Let's look at the metrics on signaling. Basic information will give you statistics on the number of calls and the responsiveness of the requests to the Call Servers, as well as errors. All of these can help indicate the source of call setup issues.

For SIP trunking to be successful, it is really important to know the number of calls that are being made. Call setup stats will give you this and prove that the SIP trunk is being utilized. Also, if you are using multiple trunks, you can compare their performance, balance their utilization, and make sure you're getting the most from your provider.

Voice and video quality (MOS, packet loss,

and jitter) for calls traveling through the SBC and SIP trunk are also very important because you want to know the source of any quality issues. Determining whether the problem lies in your network or that of the provider is critical. It is also useful to have visibility on both sides of the SBC because that gives you insight into where the problem truly resides.

Codec selection is also relevant when it comes to VoIP quality. Don't underestimate how much impact that could have on overall service quality. Using the wrong codec not only affects quality, but it also affects how much bandwidth is used. So, although high-fidelity codecs promise better quality, the extra bandwidth could cause congestion and compromise your system. Moreover, without the right QoS configuration and sufficient high-priority QoS reservation, you might start to see packets dropping and quality suffering.

QoS visibility for SIP trunking is also essential. But if it is not set up correctly, you may see issues with UC quality. Knowing whether an issue

originates from the network or the trunk is important. Don't forget that the SBC can, and often does, reclassify the traffic. If this configuration is not done correctly, you're back to square one!

The Cleanup

With the right metrics in place, in terms of voice, video, and signaling that travel across your enterprise and into (and out of) the SIP trunk, you now have a platform from which to fine-tune the system:



- **Signaling issues:** Check out the errors over your environment. See whether they are consistently coming from specific SBCs, Gateways, or Call Servers and are indicative of configuration and service issues. The errors may not specifically affect the availability of the trunk (i.e., an outage) but may mean that these servers are unnecessarily processing calls, routing calls inefficiently, or just causing delays in call setup and teardown.

- **Voice and video quality and QoS:** If you can see the quality going in and out of your infrastructure, you can determine whether it is your problem or the provider's. This is fundamental to SIP trunking success. Is it QoS, bandwidth, congestion, or the infrastructure that is gradually affecting service quality?
- **Codec analysis:** See what's running in your estate. How many calls for each codec? Do you have any codec surprises coming from certain locations or SIP trunks? If you do, that's a great place to start cleaning.
- **Multiple or mismatches of codec and signaling protocols in the same network:** For instance, people are running SIP but find Cisco Skinny running or find two different codecs in use (especially between different offices, as can be found in merger-and-acquisition situations). Other common causes include policy changes or a simple misconfiguration.



Clean Up Your Multivendor UC&C Environment

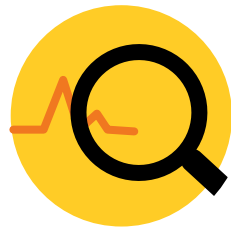


The Problem

Today, it's unlikely that you have a single vendor solution of UC equipment deployed across your entire environment. There are many reasons for this, including overall design strategy, best-of-breed component selection, specific feature requirements, infrastructure components, or inheriting existing technology through merger or acquisition. As a result, most people have to assume that even if their environment is single vendor today, that may not last long as the business evolves and grows, and new UC&C technology is added. Systems today are more complex with more interconnected pieces. Quality issues are more likely

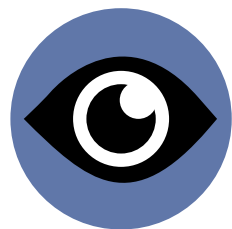


to occur because of minor incompatibilities with the equipment or the need for mediation or transcoding between systems provided by gateway functions. Rationalization could be a solution, but investments have already been made. What is most needed is fine-tuning.



What Monitoring Do You Have?

It's no surprise that the equipment vendors themselves each have a separate tool for monitoring the performance of their systems and can provide valuable insight into performance. However, what each individual tool often lacks is visibility into the other systems that play significant roles in UC&C service delivery and the end-user experience.



The Visibility Needed

When it comes to evaluating quality, getting a consistent

view of the performance of a call or video conference as it transitions between the components, vendors, or domains really provides a helpful way of understanding end-to-end quality. Additionally, if there is a problem, it will let you pinpoint the source or domain of the issue. So make sure you can get a perspective of quality — both into and out of each domain. Metrics that provide the right sort of information include voice quality in each domain, network performance (e.g., MOS), packet loss or jitter, signaling protocols in use, codec in use, QoS, bandwidth utilization, and single-direction calls.

The Cleanup

You will want to have instrumentation that provides the appropriate quality metrics at the strategic points in the network, which may include high concentrations of call volume



and demarcation points among the vendors. Then you can obtain the right context and insight to fine-tune each of the systems.

The variety of issues you will be able to clean up will be diverse, but each piece of fine-tuning will guard against system failure or quality complaints from users. Some areas of importance that may start small but can quickly escalate out of control are:

- **QoS classification:** When there is change along the call path, check the source of the change (e.g., SBC, WAN, Service Provider, or router).
- **QoS mismatch of QoS settings for inbound and outbound calls:** Again, this is important, since it is indicative of a misconfiguration, and you would expect the same QoS in both directions.
- **Single-direction calls:** This is indicative of diverse routing running through your



network — should it be like that? Or are things routing inefficiently.

- **Incorrect codec in use or a change of codec between systems:** This could be the cause of quality issues, but it could also increase the amount of bandwidth the system uses.
- **Increase of bandwidth used by one of the systems:** Why is this happening? Is it a direct

result of service uptake or codecs taking up more bandwidth?

- **Increasing packet loss or jitter from a firewall or SBC:** Are the firewalls, SBCs, or other components in the network the cause of the drops?
- **Voice quality issues from a mediation gateway:** A great demarcation point, as this can help pinpoint the domain responsibility of

issues in the environment. Are these devices canceling echo effectively?

Of course, this same methodology can be used to help remediate critical issues. The Mean Time to Know (MTTK) will help you escalate the problem with suitable evidence to the correct team (or vendor or service provider) to fix the issue quickly and minimize downtime.



Clean Up Your Video Conferencing Environment

The Problem



If you are on a video call and the video stops but the audio remains, you can continue. However, once you lose audio, regardless of what happens to the video, communication effectively stops.





What Monitoring Do You Have?

The video conferencing vendor's management tools will typically provide statistics of conferences and conference-quality information. This will help you understand the calls and conferencing that have taken place. Unfortunately, they do not have the view of the underlying infrastructure. So if quality degrades, it is extremely difficult to diagnose the root cause and to do so in real time as the call is taking place.



The Visibility Needed

There are some key metrics on both voice and video that should be very valuable when cleaning up your operation. Most importantly, you need underlying network metrics. You need to know what signaling protocols, codecs, and QoS your audio and video are set to and the amount of band-

width that the service is using. Quality metrics such as MOS, packet loss, and jitter are all essential to combine with this information to fine-tune what is really going on.

An additional useful metric for video is compression degradation and how much it is affecting quality. Compression degradation is an indication that the clever video codecs are starting to negotiate down the resolution or frame rate (and therefore the quality) of the video to perhaps accommodate for network congestion on your links. This metric provides a valuable early warning that things are starting to suffer, and you need to tidy up your operation.

Finally, don't forget metrics on audio quality. Positioning of the microphone is essential for good video-call experience. Misplaced or misconfigured microphones can mean that audio quality will suffer. Audio metrics such as voice levels, noise, and echo will all help fine-tune video conference audio quality.

The Cleanup

As use of the video conferencing service increases, you should continually review the following:



- **QoS setup and bandwidth utilization:** This is essential to maintain the high quality of the service throughout its lifetime.
- **Codecs in use:** These will directly relate to the quality you will get from your equipment, as well as to the amount of bandwidth required for the service.
- **Video-compression degradation:** Such degradation can be an early indicator of issues in the underlying network infrastructure, so understanding its source is vital.
- **Audio quality beyond the network metrics:** This will help you position the microphones in the video conferencing rooms to optimize them.



Clean Up Your Voice Quality

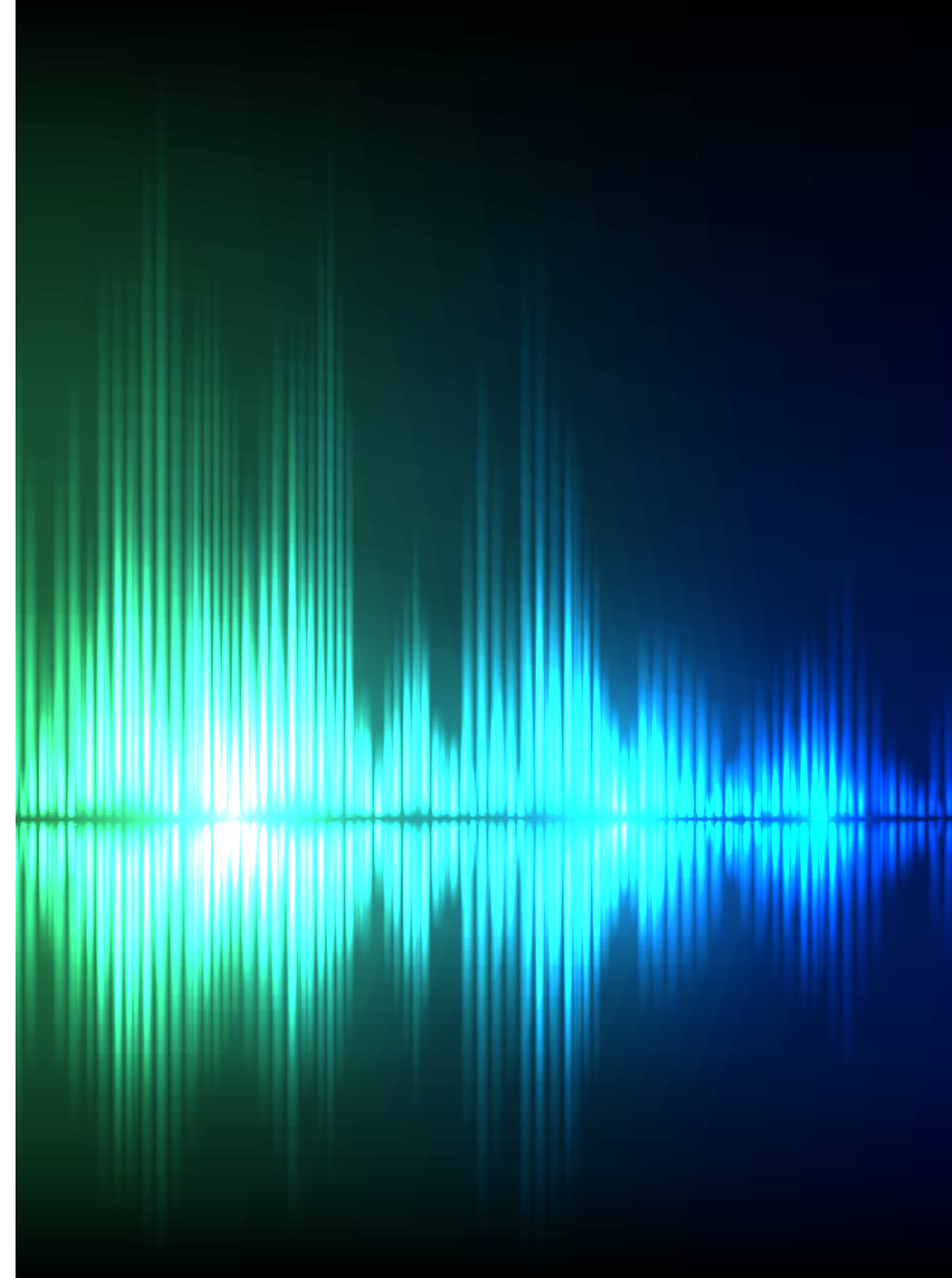


The Problem

Large offices and contact center environments are often highly complex with many components connecting your customers to the right people in your organization. Getting visibility along the path or at the demarcation points between the network, UC vendor equipment, and service providers will help ensure that the service is performing to its best ability.

In a call center, keeping an agent's equipment connected and at peak performance affects how your customers perceive your company. Customer service and satisfaction suffer when voice quality is compromised and the agent can't hear the customer, the customer hears background noise, or the customer can't understand the agent because of poor audio quality. When this occurs, it presents a poor image of the company and can affect your brand and even bottom-line revenue.

Additionally, if call center agents struggle with the voice equipment and have

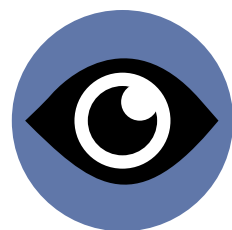


difficulty communicating with customers, it just makes their job harder and more tedious. That, in turn, increases agent turnover, which then costs the company time and money to recruit, hire, and train replacements.



What Monitoring Do You Have?

Although quality of calls is generally paramount, sometimes monitoring of the actual voice calls gets overlooked. Other metrics include length of time to answer calls, numbers of calls, and queue length. Don't overlook the regular "monitoring" of end-user hardware performance.



The Visibility Needed

"Seeing" the quality of calls going to and from staff with metrics such as MOS, packet loss, and jitter is valuable. These network-type degradations can be diagnosed and quickly resolved with network tools and config-

uration efforts. However, such metrics cannot detect non-network-oriented aspects of the work environment, which could cause quality to suffer. Examples include bad microphones, specific agents' use of the equipment, or a noisy office environment. It is essential to get deeper metrics than just basic network metrics, such as codec use, and extended voice metrics, such as echo, volume levels, and noise, to help isolate environmental issues.

The Cleanup

Once you have metrics for each user on voice quality, you will be able to fine-tune the work environment by analyzing:



- **Network and voice metrics:**

This will help you understand whether the network infrastructure is the underlying cause of voice-quality issues in the office or call center.

- **Codec usage:** This will help you

isolate quality issues due to use of inappropriate codecs.

- **Extended voice metrics will isolate:**

- users with consistently underperforming microphones
- agents who are not using their equipment effectively, e.g., volume settings, microphone position, or an incompatible microphone deployed by the user
- office design where perhaps partitioning between users is too low, resulting in a noisy environment

This clean-up operation is essential to assure quality in the workplace and should be a normal part of your best practices and reviewed regularly. Coupled with regular user training, this can prevent bad habits from forming and can affect the quality of the interaction with the customer.

You should never forget that customers always have a choice, and if their user experience is compromised, they may dial up a competitor next time.



A Single Application to Monitor Voice, Video, and Data Services

Supporting a proactive, continuous program to “clean up” the UC&C estate will go a long way toward reducing service disruptions or degradations that have a negative impact on you and your organization.

Yet the performance of UC services is highly dependent on a sound infrastructure and seamless interoperability in multivendor environments. Unfortunately, the infrastructure

is often challenging, and interoperability is anything but seamless.

Managing this is hard enough for experienced IT teams, but doing so without strong performance management visibility is exponentially more difficult.

A more effective and efficient approach to problem identification, service triage, and resolution of issues with your UC&C services would be a single monitoring application that

includes voice, video, and data services. This approach overcomes the time-consuming limitations of vendor-specific, UC&C-only point tools that cannot see the broader environment. It also ensures that your UC&C service continues working at peak performance — and, most importantly serving your customers effectively.

To learn more, visit www.netscout.com/Connect/unified-communications-at-a-glance.

About NETSCOUT

NETSCOUT SYSTEMS INC., (NASDAQ: NTCT) is a market leader in real-time service assurance and cybersecurity solutions for today's most demanding service provider, enterprise and government networks. NETSCOUT's Adaptive Service Intelligence (ASI) technology continuously monitors the service delivery environment to identify performance issues and provides insight into network-based security threats, helping teams to quickly resolve issues that can cause business disruptions or impact user experience. NETSCOUT delivers virtually unmatched service visibility and protects the digital infrastructure that supports our connected world.