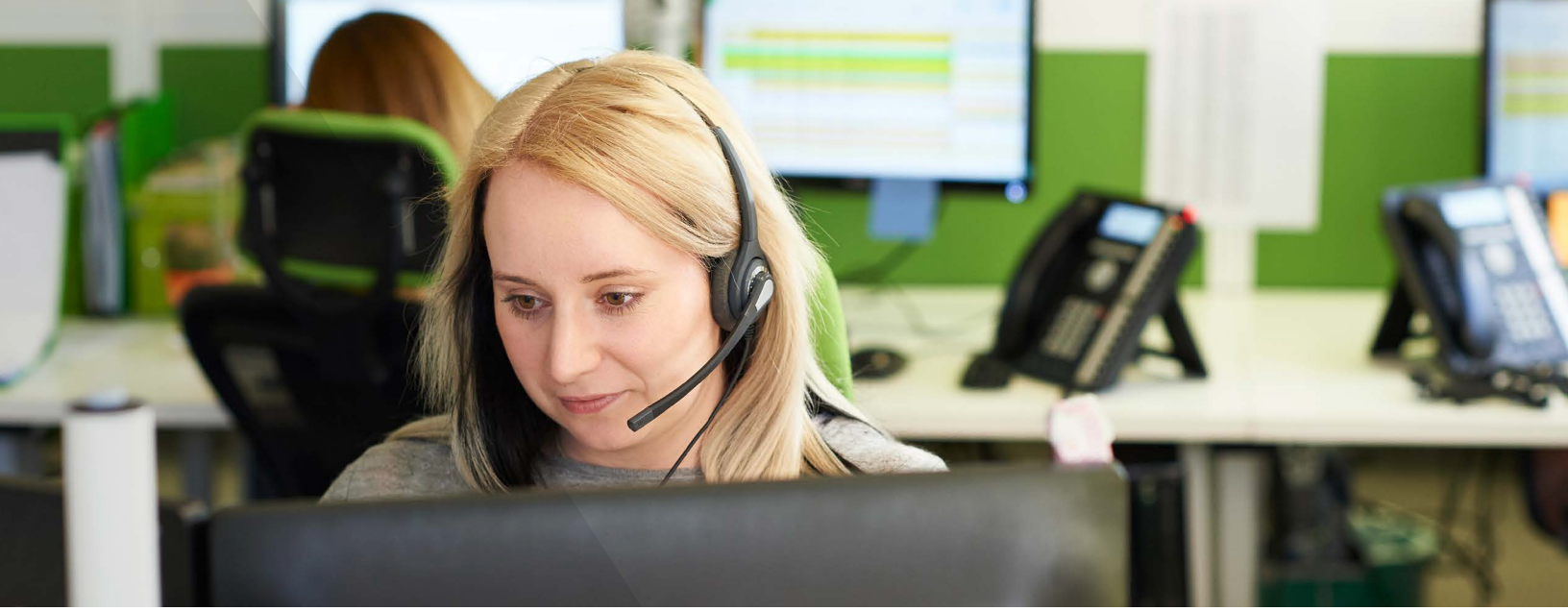
INTERMEDIA
CLOUD COMMUNICATIONS

ROCKY KNOLL TECHNOLOGIES LLC

Not All Voice Clouds Are Created Equal

A Technical White Paper Describing Intermedia's Voice Network

CONTENTS



INTRODUCTION

A high-quality "Voice Cloud" is determined by not only the strength and robustness of its network's infrastructure but, equally important, by the expertise of its architects and engineers. Intermedia's 20+ years of VoIP experience sets itself apart from other communication leaders with its unrivaled, industry proven Voice Cloud.

Intermedia's Voice Cloud, by definition, is our voice network for delivering Voice over Internet Protocol (VoIP) service to our customers. Seasoned architects and engineers first developed our Voice Cloud in 1998, and have constantly evolved it to keep ahead of both customer growth and our own extremely high benchmarks for reliability, security, and Quality of Service (QoS).

In fact, these three components are essential to the high-quality VoIP service we deliver:

- **Network Reliability & Redundancy.** Intermedia's Voice Cloud is purpose-built to deliver 99.999% uptime. We back this uptime promise with an industry-leading, financially backed Service Level Agreement (SLA).
- **Security.** Our single greatest responsibility is to keep customer data secure and private. This commitment permeates every aspect of our cloud and extends across our entire company and into the Intermedia services you use.
- **Quality of Service (QoS).** We've developed many significant programs and processes to assure high-quality calling, including customer site pre-qualification as well as constant real-time monitoring of our network for any QoS issues.

This white paper offers a deep dive into our proprietary technology. It explains how our Voice Cloud is architected to achieve or exceed our benchmarks for reliability, security and QoS. But as you read on—and as you consider your options for a move to a cloud voice provider—remember: when it comes to choosing a provider that will become an essential partner with your business, a provider's legacy and experience is just as important as raw technological specifications.

INTERMEDIA

ROCKY KNOLL TECHNOLOGIES

VOICE CLOUD RELIABILITY

Intermedia's Voice Cloud network delivers 99.999% (five nines) uptime for our voice services. We support our 99.999% uptime guarantee with a financially backed Service Level Agreement.

This level of reliability—which calculates to less than 26 seconds of unplanned downtime per month—is possible because our architects and engineers have applied their deep expertise to seven key technological components:

1. Network architecture
2. Failure-resistant SIP gateway, AKA "Uber Cluster"
3. World-class multi-region datacenters
4. Aggregation of Tier 1 telecom carriers
5. Constant network resiliency/readiness testing
6. Our software deployment strategy
7. Scalabilit

Geographic dispersion

The Intermedia Voice Cloud is hosted in geographically dispersed tier 1 datacenters. Each datacenter has multiple full-peer connections to Internet and telecom backbone carriers. The primary data path between datacenters for exchanging data is through redundant private circuits.

Our redundant architecture prevents multiple component failures from impacting our customers, helping to ensure uptime even in the event of individual component failures.

1. Network Architecture

The Intermedia Voice Cloud architecture has three contexts, or layers, providing clear abstraction and a well-defined communication via interfaces or APIs. This layered approach isolates the various platform functional areas, which enables us to meet our extremely high criteria for reliability, security and QoS.

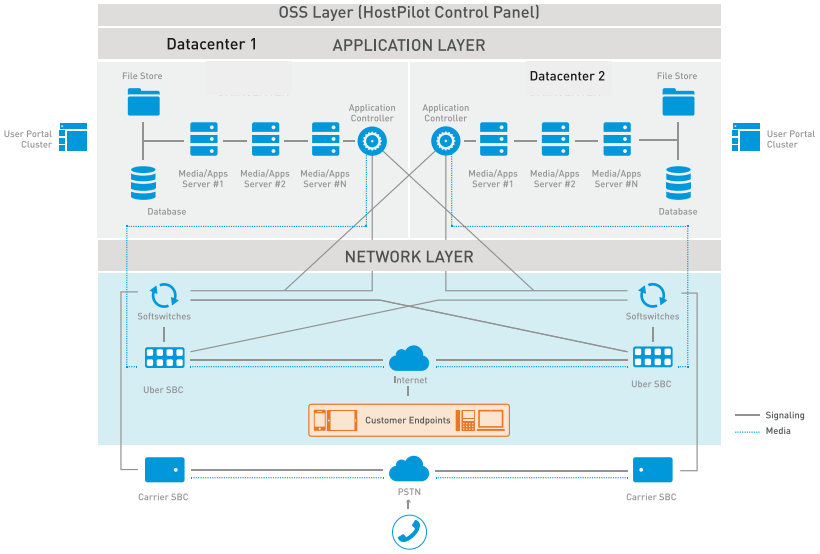
The network layer routes calls to the application layer based on criteria including the availability of the application server, the load on the application server and the proximity of an application server to the call ingress point. To any specific application layer instance, the network layer is abstracted and presented as the network API. Application components—such as "play and record voicemail", "calculate call routing" or authentication of phones—are built as resource pools.

This design simplifies issues around application failures and redundancy while easing capacity growth and network management. This is all provided transparently and automatically through the network API (via the network layer.)

The network layer is the foundation of the service delivery platform. It's responsible for all the basic call or session setup functions, the interconnection of all external public and private telephony environments, and for the routing of calls among application layer services.

The below diagram represents a typical data center deployment model for our Voice Cloud service globally across North America, EMEA and the Asia Pacific markets.

Example deployment model



1. Failure-resistant SIP gateway, AKA "Uber Cluster"

Our "Uber Cluster", as we call it, brings reliability and redundancy to Intermedia's Voice Cloud. "Uber Cluster" is a set of distributed servers, which peers with end-user SIP devices and handles SIP registration and call processing. The Uber Cluster design is modular and built on scalable network technologies that power the world's largest networks, including Anycast technology, the inherent multipath and fault tolerance features of the Border Gateway Protocol (BGP) and Open Shortest Path First (OSPF).

Uber Cluster's simple design allows end customers to reach Intermedia with a single IP address, using the best available path to seamlessly route around network issues.

BGP allows different networks to find each other. The benefit of applying the BGP fault tolerance features to Uber Cluster's design is necessary in the event of a catastrophic incident that causes the network to lose an entire datacenter. In this situation, Uber Cluster migrates the traffic over to the nearest datacenter instantly. If the network loses a server within a datacenter, traffic will migrate to the nearest active server. In the event of such failure, the maximum customer impact would result in a dropped call—as opposed to a lengthy service outage.

INTERMEDIA

ROCKY KNOLL TECHNOLOGIES

Anycast is implemented by using BGP to simultaneously announce the same destination IP address range from multiple points on the Internet. Rather than having multiple servers with unique IP addresses, all servers share one Anycast IP address. Customers connecting to the Anycast IP address will simultaneously connect to any one of these servers, generally connecting to the one geographically closest to them, which leads to lower latency and better QoS.

2. Network Reliability

The network's highly redundant design is geographically dispersed, using stateless soft switches, SBC clusters, and application resource pools that are deployed in multiple groups. This provides reliable and redundant service availability to our customers regardless of endpoint capability.

Intermedia stringently controls change of management within our network, limiting planned maintenance and minimizing potential impact to our customers. In addition, we have implemented unique resilient solutions for different failure types that occur within the carrier domains outside of the network. For example, with inbound toll-free traffic, we use a four-carrier mask for toll-free routing. This spreads call volume across four carriers so if any of the carriers are experiencing regional/national issues with toll-free traffic, we can drop that carrier from routing within minutes.

3. Network Resiliency Testing

We proactively validate our network resiliency with quarterly component failure and failover testing. During testing, we exercise both of our datacenters to ensure they can handle the full capacity of the network. Our testing helps ensure every component of our network is available, especially in the event of an outage. In addition, we look at phone lines failing to reconnect, incomplete calls, and our ability to send and receive calls to each of our carriers. We also validate that application-level components are functioning, such as voicemail, faxing and enhanced routing.

4. Carrier Reliability

Intermedia currently maintains and monitors over 3 million phone numbers. Each month, we handle over 40 million calls and over 100 million minutes of voice traffic. To maintain the highest level of service for our customers, Intermedia has partnered with several different tier 1 voice carriers. Each of our carriers is selected for Quality of Service (QoS), coverage, cost and reliability. Partnering with multiple top-tier carriers provides maximum reliability and redundancy across our highly trafficked Voice Cloud.

Intermedia performs ongoing evaluations of each carrier, automatically eliminating any carrier negatively impacting the quality of voice traffic.

In addition, our failover routing design provides coverage to over 98% of Metropolitan Statistical Areas. Each call is routed between carriers based on individual carrier service level, availability, geographic proximity and cost. This provides quality VoIP traffic and low cost to our customers.

INTERMEDIA

ROCKY KNOLL TECHNOLOGIES LLC

5. Software Deployment Strategy

When new software and updates are deployed to Intermedia's Voice Cloud, our Change Control Board reviews each change and written Method of Procedure (MOP). Once the software/update and MOP is approved, changes are scheduled and deployed to our Voice Cloud.

The process for a standard network change or software upgrade is as follows:

1. All proposed network changes run through a full standardized regression testing procedure on our in-house QA network, and results are reviewed by the Change Control Board.
2. Approved changes are then installed on our non-production "Beta" system and run for a minimum of two weeks prior to loading it into production.
3. Once step two is successful, then 25% of the systems in each datacenter node will be upgraded during the next weekly maintenance window in order to minimize impact to any individual customer.
4. Following the success of step three, 25% of the remaining systems will be upgraded during the next weekly maintenance window, and so on, until all nodes are upgraded.

This stringent approach to scheduled software updates helps ensure customers are not impacted in the unlikely event a bug or issue is introduce.

7. Scalability

Every component of our Voice Cloud has been designed to scale, which allows our network to grow with our customers' needs. To maximize scalability, the network layer soft switches so customers see no difference between any components of the application layer, the network layer, or any call processing device on our network. This allows for a scalable network architecture that is not continuously encumbered by the special needs of each application service, carrier partner or customer being connected to it.

The network layer is comprised exclusively of Intermedia's proprietary software running on industry standard servers. Intermedia's scalable voice architecture enables the easy addition of functional elements, such as soft switches, Session Border Controllers (SBC) and app servers to accommodate customer growth. This uniformity also provides for ease of administration and the reduction in the number of problems. Additionally, the Session Border Controller software is the exact same binary image produced, whether the SBC has been deployed for the carrier interface or for SIP endpoints, which improves the efficiencies throughout the operational areas of our business.

VOICE CLOUD SECURITY

At Intermedia, one of our greatest responsibilities is to secure your information and service. Our Voice Cloud was developed with three comprehensive levels of security:

1. Physical and network security
2. SIP endpoint security (phones and devices)
3. Toll-fraud monitoring/detection

1. Physical & Network Security

Intermedia's Voice Cloud is hosted in geographically dispersed, highly secure and monitored datacenters by top tier providers. Each datacenter has restricted access, biometric controls, and complete tracking of access and changes.

As with our network resiliency analysis, Intermedia conducts penetration testing of our cloud infrastructure on a quarterly basis. During testing, we attempt to infiltrate our systems and check for vulnerabilities and open ports in the network. In addition, we also regularly scan our network with our robust vulnerability management system that scans our systems and servers, inside and out, on a weekly basis to detect open ports and vulnerabilities.

INTERMEDIA

ROCKY KNOLL TECHNOLOGIES LLC

Our network specifically is protected in a number of critical ways:

- Commercial-grade edge routers are configured to resist IP-based network attacks
- Intermedia subscribes to Distributed Denial of Service (DDos) protection through Verisign, one of the leading providers of network security
- With Commercial-grade firewalls, only needed ports and protocols are allowed
- Custom-built intrusion detection systems detect and stop incoming attacks
- Production network is physically and logically separated with highly restricted access

Our Voice Cloud also meets industry leading compliance standards including PCI, CPNI and HIPAA. KPMG and other top-level firms perform a security audit of the organization for specific processes related to HIPAA requirements. We use such results to help ensure our Voice Cloud facilitates compliance in an ever-changing standards landscape. We internally conduct background checks on all support staff and authenticate all customers that call in through a list of approved contacts.

For PCI compliance (credit card security), we validate card numbers entered into our system through pattern matching. Invalid cards are added to an existing list of fraudulent credit cards for future detection.

2. SIP Endpoint Security (phones & devices)

The second level of our Voice Cloud security safeguards all SIP endpoints on our network. To verify phones and devices are secure from cyber threats and attacks like eavesdropping, we require strong passwords on all SIP endpoints.

We are constantly monitoring customer site vulnerability and endpoints by looking at call patterns. Through this process, we can detect and limit simultaneous calls per device, phone registration from multiple IP addresses, and attacks on device and account credentials. IP filtering of hostile areas is done to block access from high fraud IP addresses. When any threat is detected, service is suspended and customers are notified immediately.

3. Toll Fraud Detection

Toll fraud is the illegal use of a company's telecommunications system by a third party (e.g. a hacker) from a remote location.

The most common toll fraud is international toll fraud, whereby hackers obtain access to passwords and accounts to exploit companies for international calls. In this form of fraud, criminals scan the public Internet for applications that make phone calls.

Once they detect these applications, they attempt to crack the authentication credentials and make phone calls (for which the customer will be charged).

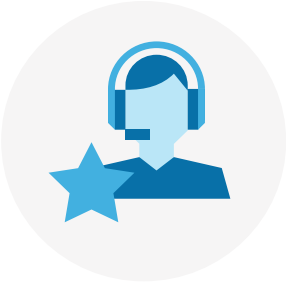
Intermedia's policy requires all SIP endpoints to be installed in a securely trusted zone behind a firewall and not exposed to the public Internet. The firewall must block all inbound untrusted Internet traffic to the SIP endpoint. The firewall can be configured to allow inbound traffic from trusted devices from remote locations. Filtering based on source or destination address is useful because it enables the user to allow or deny traffic based on the computers or networks that are sending or receiving the traffic.

In addition, Intermedia scans the network of connected devices to determine if any of our SIP endpoints are open to the public Internet. If an endpoint (a phone, phone system or gateway) is determined to be open to the public Internet, a notification is sent to the customer requiring them to secure the SIP endpoints behind a firewall.

Intermedia monitors call patterns to international (and high-cost) locations on a constant basis and continually looks to improve our fraud monitoring systems. If any customer exceeds the call thresholds for any international areas, Intermedia will disable international calling, and send an email notification to the customer informing them that international calling has been disabled based on possible fraudulent activity. To protect the customer, we will not enable international calling until the account holder has given Intermedia authorization.

VOICE CLOUD QUALITY OF SERVICE (QOS)

Intermedia relies on four elements to provide customers with a high-quality experience for every call on our network:



1. Network Call Quality Monitoring
2. New Customer QoS Testing & Support
3. VoIP Scout for Partners
4. Smartwatcher for QoS Troubleshooting
5. QoS Dashboard

1. Network Call Quality Monitoring

Intermedia proactively monitors the Voice Cloud to enable the highest call quality for our customers. As calls flow through our Voice Cloud and the different network components (PBXs, SBCs and network routers), each component collects statistics. The statistics are added to call-detail-records, which are then added to an internal database. Every minute, internal systems query the database looking for problems related to connectivity loss, latency, (packets taking too long to arrive), jitter (inconsistency in packet timing) and packet-loss (dropped packets due to congestion) on a trunk-by-trunk basis.

By constantly monitoring each call in depth, we can automatically or manually intervene and resolve QoS issues without any customer involvement. And by constantly monitoring our entire Voice Cloud, we can conduct a real-time analysis of regional and carrier issues, allowing us to evaluate our carrier performance proactively and eliminating carriers preventing high quality voice calls.

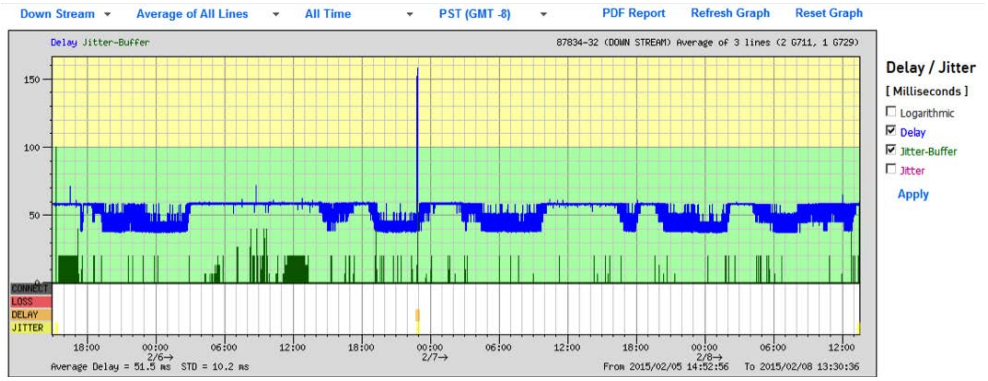
2. New Customer QoS Testing & Support

Intermedia knows that a great VoIP experience starts with great QoS. The best way to insure great QoS is by testing for QoS issues BEFORE customers sign up for our voice services.

Many QoS issues can be easily identified and fixed before initiating our voice services. Intermedia will only bring a customer onto our system once we're confident their network will support VoIP and provide great QoS. As such, we work with our customers during the sales process by testing their systems and making sure it is ready for high quality VoIP.

Intermedia pre-qualifies each customer's data connectivity and network by verifying that:

- The customer's Internet circuit has sufficient capacity for VoIP using our bandwidth test;
- The customer's Internet circuit is reliable and has consistent quality using our VoIP Scout tool (3+ day simulation of voice traffic at the customers site);
- The ISP is reliable and can support VoIP; and
- The network equipment supports VoIP.



In addition, we re-qualify the network during the onboarding process because environments and situations are not static and can change over time. This process includes:

- Reconfirming bandwidth, compatible ISP and network equipment;
- Optimizing network equipment for VoIP; and
- Verifying that our equipment will register and make a quality phone call

INTERMEDIA

ROCKY KNOLL TECHNOLOGIES LLC

3. VoIP Scout for Partners

Intermedia has also developed a set of powerful tools, called VoIP Scout, enabling our partners to provide self-service, pro-active network and data circuit testing, which allows high quality VoIP calls for their customers. Intermedia's VoIP Scout consists of three core components:

1. The VoIP Scout Appliance for running tests onsite via dedicated hardware (ideal for locations with no available PCs and/or dedicated voice networks);

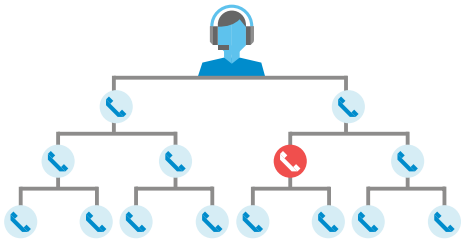
2. The VoIP Scout Soft Client for running tests via on-site computer; and

3. The VoIP Scout Management Portal for scheduling,reviewing and managing network tests.

These tools help our partners alleviate the potential for a poor customer experience and save the additional cost of emergency post-sale troubleshooting, which can ultimately damage the customer relationship.

4. Smartwatcher for QoS Troubleshooting

When customers contact Intermedia's support with QoS issues, we troubleshoot calls using the Smartwatcher interface. Smartwatcher is a set of tools offering a complete view of all service interactions between network components on a simple display.



With Smartwatcher, a customer service professional can quickly drill down to the customer calling in, get a list of phone calls associated with the customer and find out which call potentially was impacted. In this single interface, we have the signaling and quality of service information on the portion of the call which is using a carrier partner, the ability to see which applications features are triggered in the network, quality information as it relates to our ability to deliver the phone call to the end-user, and all relevant information, such as what touchtone digits the user used during the call.

We have the ability to cross-reference the information gathered from Smartwatcher with output from our real-time, round-the-clock QoS tester that the network operates against all customer on-premise equipment. Should it be necessary, the tool extracts the capture of this phone call for later analysis and troubleshooting.

to evolve our Voice Cloud, which allows us to continuously provide high-quality VoIP services to our customers. Intermedia is a proven communication leader with a Voice Cloud focused on each of your business needs: reliability, security and QoS.

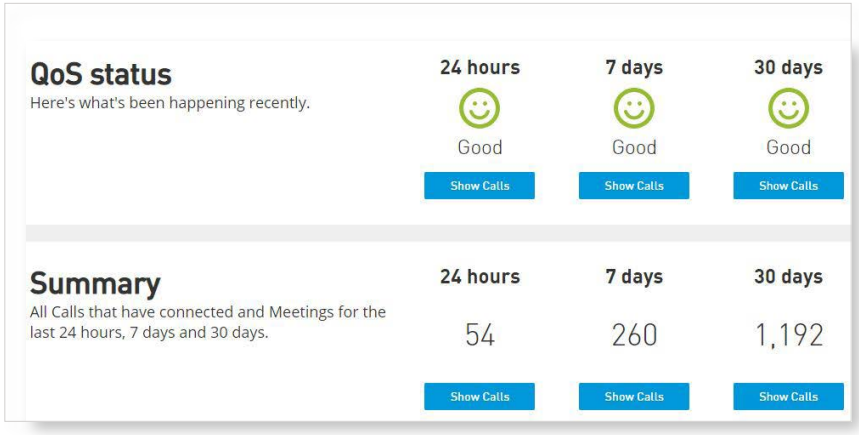
INTERMEDIA

ROCKY KNOLL TECHNOLOGIES

5. QoS Dashboard

The QoS Dashboard provides administrators with Quality of Service (QoS) analytics to easily view, diagnose, and solve network issues that could lead to a negative voice or video quality experience for users.

The Dashboard identifies QoS trends by aggregating all of an organization's calling data into rich, toplevel graphical visualizations of call quality. If they wish, administrators can then drill down into these representations for more granular information. Examples of this data include: the names of carrier(s) and call parties within individual calls, the specific call quality issue that was experienced (i.e. packet loss, jitter or latency,) and issue origination and direction



CONCLUSION

When you consider a cloud voice service provider for your business, remember that experience is crucial. While certain providers appear to meet your business needs, consider the package as a whole. It is not just the technology—it's how it was implemented that determines your experience.

With 20+ years of experience, our seasoned architects and engineers work tirelessly to evolve our Voice Cloud, which allows us to continuously provide high-quality VoIP services to our customers. Intermedia is a proven communication leader with a Voice Cloud focused on each of your business needs: reliability, security and QoS.