

Unified Communications Management Platform Architecture:

The Story of Correlated Diagnostics in the Complex World of UC Monitoring and Diagnostics

WHITE PAPER



Table of Contents

The Promise of Unified Communications	4
The Value of UC	4
The Challenges of UC	4
Managing a UC Deployment	4
The Reality of Managing a UC Deployment	4
The 3 Domains of a UC Deployment	
Partnering to Optimize the Enterprise's UC User Experience	7
The "Powered by Nectar" Advantage	
Correlating Diagnostics – Nectar's UCMP	8
Modular	8
Scalable	9
Multi-Tenant	9
Cross-Platform	9
UCMP Elements Overview	10
UC Foundation (UCF)	
Perspective	10
UC Diagnostics (UCD)	10
Intelli-Q.	10
Application Health – UC Foundation	11
UCF Value Drivers	11
UCF Functionality	11
UCF Architecture	13
Network Readiness - Perspective	14
Perspective Use Cases	
Perspective Functionality	16
Perspective Architecture	17
Network Health – Real-Time Quality with UC Diagnostics	18
UCD Value Drivers	19
UCD Functionality	19
UCD Diagnostics Architecture	
UCD – The Case for Probes	21
End User Health - Advanced Analytics	22
Advanced Analytics Value Drivers	
Advanced Analytics Functionality	



Powering The UC Service Provider Practice	23
Intelli-Q – Fitting into the Service Provider Processes	. 23
Architected for the Service Provider	24
UCMP and the Service Provider Value Proposition	24
Service throughout the UC life cycle	24
Offering Various Levels of Service	25
In the Clouds	25
Summary	27
About Nectar Services Corp.	27

Nectar Services Corp. Copyright 2017. All rights reserved.

The Promise of Unified Communications

The Value of UC

When the term "unified communications" (UC) entered the enterprise IT lexicon in the mid-1990s, it brought the promise of increased business productivity through enhanced collaboration and individual employee efficiency. The potential value of UC is in driving operational efficiencies by removing the "friction" in the way individuals, groups, and companies interact and perform.

From an architecture perspective, UC encompasses a suite of products that provides a consistent user experience across multiple devices and media types. UC solutions may consist of individual products or suites from a single vendor or, more commonly, a portfolio of integrated applications and platforms that span multiple vendors. In many cases, UC technology is deployed to extend and add functionality to a company's established communications investments.

The Challenges of UC

Although UC offers the promise of increased user productivity, business agility, and effective control of operational costs, companies continue to face difficult choices in terms of implementation and migration strategies, as well as how to effectively manage the more complex environment of a UC deployment.

Applications like conferencing, mobility, video, and collaboration have massive performance and availability requirements that often fail to meet the high expectations of users. Delivering on these expectations becomes an even more onerous goal in today's world with the contention of network bandwidth-intensive solutions, the variability of Bring Your Own Device (BYOD), the latency and load of layered security, and the complexity of cloudand hybrid-deplyoyed solutions. Most UC management offerings today cannot pinpoint the exact problem, nor can they deliver real-time monitoring to provide the consistent, reliable collaboration infrastructure that most enterprises require.

Managing a UC Deployment

Most analysts note that UC best practices for users and system integrators are still maturing. With regard to emerging UC services, Frost & Sullivan suggests that service providers and enterprise IT staff must be able to manage and monitor the applications, servers, endpoints, and network infrastructure that drive the way today's work gets done in order to ensure an optimal user experience. To effectively do this, an enterprise needs to leverage the right tools.

The Reality of Managing a UC Deployment

Gartner has found that many network teams are illequipped to manage, troubleshoot and diagnose the varied issues with which most enterprise businesses continue to struggle. Gartner further notes in its October 2016 Market Guide for Unified Communications Monitoring that:

 Real-time voice and video are the most networksensitive applications. When network performance is challenged by congestion, these typically break first.

Inectar

- Troubleshooting complex UC solutions requires a combination of vendor-derived, end-user, protocoland packet-based data sources for in-depth understanding and diagnosis of issues.
- Migrating between legacy and new UC platforms often involves changing network and service providers. This results in bifurcated unified communications monitoring (UCM) requirements.

The 3 Domains of a UC Deployment

The flip side of UC's promise of user enablement and an enhanced user experience is the added complexity of trying to monitor and troubleshoot across a much more complex environment. Gone are the days of a phone connected via a dedicated wire to circuit pack in a PBX cabinet. Troubleshooting today's UC conversations means trying to correlate across 3 different domains.



Application Domain

With the adoption of UC, every communications platform has become a server running software. The application domain is the UC software itself and the servers and services that host this software. If the servers and platform software are not running optimally, the user experience could suffer.

When evaluating the potential impact of the application domain on the health of a UC deployment, here are some key questions to consider:

- Does high CPU utilization negatively affect how the servers process codecs or register/users calls?
- Is low disk space slowing down processing time or jeopardizing the retention of key records?
- Did someone accidently let certificates expire, thus bringing the entire UC deployment down?

Network Domain

Interview

One of the advantages of UC is that it converts voice, video, and other communications into packets that can run across the existing data infrastructure. One of the challenges of UC is that real time communications is high bandwidth and extremely time sensitive, which means it is highly dependent on an efficient network, while at the same time adding a heavy burden to that same network. Any congestion on the network or configuration drift could impact how real-time communications traffic is transported over the data network and could negatively impact the user experience.

When evaluating the potential impact of the network domain on the health of a UC deployment, here are some key questions to consider:

- Is the network properly architected to support expected UC traffic?
- Is the network configured to properly prioritize UC traffic?
- If there are call quality issues, was the network a factor?
- If the network was a factor, which network segment(s) created the issue?
- If the network was a factor, what happened in the network to create the issue?
- If the network was a factor, what other users/calls may have been impacted by the same issue?

End User Domain

Even if the platform is running optimally and the data network is transferring communications packets in the most efficient way, the end user can still heavily influence their own user experience. The connectivity to the network (wired, WiFi, mobile), the device itself (hard phone, PC, tablet, mobile, etc.) and even the headset/ speakerphone will impact the experience of the user and everyone they communicate with. The end user domain has the unique position of being the area with both the most variability and the least control by the IT staff.

When evaluating the potential impact of the end user domain on the health of a UC deployment, here are some key questions to consider:

- Is the user on a wired or wireless connection?
- Is the user using a supported-device (headset, speakerphone, etc.)?
- Is there a consistent pattern of poor user experiences based on device (manufacturer, OS, client, etc.), headset or wireless SSID; with a single user or across a group of users?

Correlated Diagnostics

So, when there is a poor user experience, was it caused by the application? The network? The end user's environment? How do you know? What if it was a little of each? Nectar's UCMP offers correlated diagnostics that allows service providers to see the conversation across all 3 domains and efficiently troubleshoot any issues.

The 3 Functions of Managing to An Optimal UC User Experience

In an effort to simplify the complexities of managing a UC environment, many tools providers and services providers combine monitoring, reporting, and diagnostics into a single "monitoring" label. The reality is that each of these functions is distinct and brings unique value to the ongoing optimization of the UC deployment.

Monitoring

In the world of UC optimization, monitoring is the ongoing observation of the UC environment over a period of time. It is a systematic review of the health of the UC infrastructure and components. When monitoring the health of various system components (servers, etc.), UC monitoring tools will capture, report, and alert on relevant performance metrics, sometimes called key health indicators (KHI's).

Reporting

While monitoring is more ongoing in nature, reporting is a historical analysis of the UC environment. Through effective reporting, enterprises or their service providers can begin to track patterns over time. Sometimes these patterns highlight usage adoption, both positive and negative. These patterns can also illuminate issues within the end user domain mentioned above. Reporting can also create snapshots of monitoring output to analyze potential patterns with service levels and performance metrics over time.

Diagnostics

Diagnostics is the practice of identifying the root cause of poor user experiences by an examination of the "symptoms" and the environment during the time span of the call or in real time. Diagnostics allows service providers to investigate specific user sessions and within the context of what was actually going on in the network (media and signaling) at the time of that call, potentially even as the call is happening. Diagnostics can also help illuminate specific network segments that are negatively impacting UC conversations.



Partnering to Optimize the Enterprise's UC User Experience

Relying on a Service Provider

Given the complexities of effectively managing a UC deployment, most enterprises look for a service provider they can trust to monitor, diagnose and remediate their UC environment. The exceptional service providers are able to demonstrate their value by providing effective reports on the health of the UC environment, the work they have done to optimize the health, and the usage and adoption that the UC deployment has achieved.

Since UC is their core competency, service providers have both the breadth and depth of personnel to help enterprises with their UC deployment. Most enterprises don't have the IT staff to effectively manage a UC deployment across all 3 domains 24 hours per day, 7 days per week, especially if their users span global geographies. Even if the enterprise did have the headcount, it is expensive to invest in training their internal staff on each underlying component of the UC infrastructure. The focus of a service provider on UC management justifies the investment in a staff with enough people to support all of the users of all of their clients as well as the individual expertise to go deep in the troubleshooting and remediation of a variety of specific components.

Service providers have also developed an effective process for maintaining and managing an enterprise's UC deployment. Since their entire business value is based on effectively and efficiently monitoring and troubleshooting potential UC issues, they provide this service at a cost most enterprises could not match internally.

In addition to the people and the processes, service providers have the tools to effectively maintain and

manage a UC deployment. Based on their experience and expertise, service providers have evaluated the market and determined the best tools for optimizing the UC user experience of their clients. They have also invested in the training to understand how to best utilize those tools. Since they are leveraging the tool across multiple enterprise clients, they are using the tools daily and therefore their training remains current and fresh.

Services "Powered by Nectar"

Nectar is the industry leader in tools for monitoring, diagnostics, and reporting on UC deployments. Nectar's tools were built to be leveraged by service providers to optimize their ability to handle the UC management requirements of their enterprise clients. Services powered by Nectar are a clear competitive differentiator when enterprises are selecting the service provider to care for their UC deployment.

The "Powered by Nectar" Advantage

UC is a valuable tool for driving enterprise productivity by facilitating collaboration across the enterprise. The distributed and flexible deployment options for UC make it complex to architect, deploy, manage, and maintain.

Enterprises who want to maximize their UC investment and optimize their user experience need to select a service provider with the people, processes, and tools to monitor, diagnose, and report on their UC deployment.

Nectar agrees. This is why our company has devoted its considerable years of experience and expertise to the development of a real-time, vendor-agnostic communications management architecture that takes a holistic approach to providing inventory, monitoring,

alarm, root-cause-analysis, capacity, and performance management while enabling remediation for real time communications systems.

Nectar's holistic approach to UC monitoring and diagnostics is specifically designed to provide complete visibility throughout a multi-vendor UC environment via a 'single-pane of glass', multi-site, multi-location view that can support hundreds of thousands of end users worldwide. Because the UCMP architecture is designed to be vendor- and technology-agnostic, it enables service providers to deliver significant economies of scale to their client's deployments while assuring an easy path for future technology needs and business growth. This agnostic approach enables Nectar to deliver real-time visibility into the quality of each UC user's experience, regardless of vendor platform or network configuration – on-premises, cloud-based, or hybrid.

This whitepaper will identify how Nectar's Unified Communications Management Platform (UCMP) enables service providers to effectively deliver services wherein their highly trained staffs can work across a multitude of systems centrally, gaining economies of scale and collaboration amongst multiple, diverse engineering departments. Available in both SaaS (operating expense) and traditional software purchase (capital expense) business models, the UCMP solution is engineered to operate in distributed, large, overlapping IP address environments, pass information through firewalls via a single encrypted connection, and scale both inside a customer's large global enterprise, as well as externally for service provider installations.



Correlating Diagnostics – Nectar's UCMP

Nectar UCMP is a modular, scalable, multi-tenant, crossplatform UC management/diagnostics suite architected from the ground up to offer service providers the correlated diagnostics they need to optimize the UC user experience for their clients. UCMP provides the ability to maintain a complete, centralized, multi-vendor UC environment with a single tool. It also allows service providers to quickly adapt to their customers' changing UC environments, effectively manage complexity, and maximize their total cost of ownership.

At its core, the Nectar UCMP architecture delivers exceptional system health and availability with a single 360-degree view of all voice and data assets. Pre and ongoing network assessment and UC monitoring is made possible via infrastructure auto-discovery, a multi-tenant NOC interface, root cause analysis, contextual monitoring, and at-a-glance troubleshooting. The Nectar architecture provides for enhanced performance by focusing on the entire UC ecosystem via integrated capabilities such as resource trending and utilization, capacity monitoring and planning, and comprehensive reporting and analytics.

Modular

Nectar's UCMP leverages 5 different modules to create a correlated tool to help service providers optimize the application, network, and end user domains of the UC deployment. The modular structure of UCMP grants service providers flexibility in how they incorporate Nectar into their service offerings. The service provider can

leverage different combinations of modules based on the needs of each enterprise client environment and/or or the level of service the enterprise client wants to purchase from the service provider. We will discuss the various modules and their impact on the specific UC domains throughout this whitepaper.

Scalable

UCMP is not only modular in terms of the software components that can be activated, but the overall architecture is modular, which makes a Nectar deployment very scalable, both within a specific enterprise client and across the entire customer base of a service provider. This scalability means that Nectar can grow with the service provider and their clients. Scalability is also a key consideration as some service providers look to bring a hosted UC as a Service (UCaaS) offer to market. Nectar scales to provide monitoring, diagnostics, and reporting to a large, multi-tenant hosted deployment.

Multi-Tenant

From its inception, Nectar developed a software platform that was purpose-built for service providers. For any service provider with more than one client, multi-tenancy becomes critical. UCMP was designed to allow service providers to monitor and manage their entire portfolio of enterprise clients with a single pane of glass. The data of each client is insulated for security and privacy, while alerts and alarms and presented in a centralized view so the service provider NOC can effectively and efficiently prioritize and track all issues.

Cross-Platform

Over the years, Nectar has developed pre-defined collections/alerting packs known as Vendor Knowledge Modules (VKM's). Nectar has VKM's for the big 3 UC platforms (Avaya, Cisco, and Microsoft Skype for Business). Nectar also has VKM's for Sonus gateways and slightly less automated collections packs for a variety of infrastructure vendors within the UC ecosystem. The ability to poll for SNMP strings and receive SNMP traps extends Nectar's reach to nearly any component in a UC deployment. Nectar's ability to provide monitoring and diagnostics across multiple platforms means that service providers can support Cisco, Avaya, and Skype for Business environments and their supporting ecosystems with a single tool. This expands the market for those service providers, including those enterprises with a variety of platforms within their environment.

Through this type of unified, architecture-based integration, the UCMP solution enables service providers to quickly identify, isolate, and remediate UC performance issues while controlling costs. Regardless of the type of multi-vendor enterprise UC environment – on-premises, hybrid, or cloud-based – the Nectar UCMP solution can support each customer's unique business needs with a variety of customizable software modules and services that ensure peak performance and optimum utilization of UC system resources.

Nectar enables simple access to voice quality metrics that include trace route and IP network visibility, real-time media analysis, and immediate UC network awareness. Further, comprehensive troubleshooting tools enable synthetic call testing, remote access and call tracing, file transfer and secure chat capabilities, alarm management, and SLA tracking and management.

UCMP Elements Overview

The correlated UCMP diagnostics story is supported by 5 integrated components. UC Foundation, UC Diagnostics, Perspective, Analytics, and Intelli-Q work together help services providers to efficiently and effectively correlate diagnostics across all 3 UC domains.

UC Foundation (UCF)

Nectar's UC Foundation module relies on information from the various platforms and infrastructure/ecosystem components to monitor application health and availability. UCF uses SNMP, RESTful API, and a variety of manufacturer-specific protocols to gather data on performance metrics. UCF then uses this data to alert/ alarm once certain thresholds are met or when certain components have stopped functioning properly.

Perspective

Perspective generates its own RTP traffic to monitor and measure how UC traffic is "behaving" over the network. Perspective generates traffic between agents on the network and captures key metrics like DSCP, MOS, jitter, and route path to ensure UC traffic is being optimized on the network. If anything on the network changes that could affect how UC traffic traverses the network, Perspective will alert and alarm to minimize the potential user impact.

UC Diagnostics (UCD)

Nectar's UC Diagnostics module uses manufacturer protocols and analyzers on the network to analyze the actual signaling and media of a UC conversation. By capturing information on the actual packets of the conversation, UCD can identify where in the network congestion or other issues impacted the communications quality of a specific conversation. By capturing and correlating the SIP signaling, UCD can also help troubleshoot issues when the conversation changes network domains (e.g. when a call moves from the enterprise's network to the public SIP carrier network).

Advanced Analytics

For reporting, Nectar leverages its Advanced Analytics module, which captures and correlates data from the underlying UC platforms and the other Nectar modules to create a holistic view of the UC user experience. Service providers can use this information to identify intermittent issues, especially those caused within the end user domain or to report on usage and adoption across the enterprise.

Intelli-Q

Inectar

Intelli-Q is the routing engine for all alerts and alarms. Intelli-Q can either exist standalone and present alerts and alarms to various engineers based on the routing rules that were established or integrate into other help desk applications to route alerts/alarms as tickets within a service provider or enterprise environment.

Each of these elements will be discussed below in detail within the context of the UC domain(s) they impact.

Acadication Health: Dashboards & Monitoring Deployed on a VM adjacent to UC pool Functions as head-end to other modules Multiple deployment roles (Genoming) Deployed as a VM adjacent to UC pool Deployed as a VM adjacent to UC pool Deployed as AVM adjacent to UC po



Application Health – UC Foundation

The application domain is the core of any UC deployment. The platform software and the servers and services that run it impact every UC conversation in that environment. Every conference call terminates on an MCU that is part of that application domain.

Nectar's UC Foundation (UCF) module helps service providers monitor and optimize the application domain of an enterprise's UC deployment. UCF is the fundamental layer of the Nectar UCMP framework, providing centralized operations dashboards & alerting capabilities for comprehensive, active health and performance monitoring and analytics.

UCF Value Drivers

UCF brings value to service providers by helping them optimize the uptime and performance of the application domain in a powerful, efficient and cost effective manner.

The Power of Cross-Platform

UCF optimizes the application health of the Avaya, Cisco, and Skype for Business platforms as well as many of the ecosystem components (gateways, SBC's, etc.). This flexibility allows service providers to support heterogeneous enterprise environments with a single tool. A single interface means less tooling within the NOC, fewer screens to view, and simplified training for NOC personnel. Service providers can support a wider base of enterprise clients as well as portfolio of enterprises with hybrid deployments. The Efficiency of Auto Inventory/Auto Update UCF's auto discovery and auto update functionality significantly reduce the time and cost of service providers onboarding client environments. With the Vendor Knowledge Module (VKM) auto discovering the relevant components of an enterprise's Cisco, Avaya, and/or Microsoft UC deployment, a service provider can be monitoring the application domain of their client within hours rather than days or weeks. UCF's checking every night to determine changes in the configuration means that the service provider can be proactive in identifying any components that have been added by the client.

The Flexibility of Customizable Dashboards

UCF gathers a broad spectrum of data from the underlying UC platform and gives the service provider tremendous flexibility in how this information is displayed, how alerts/alarms are generated, and how they are routed. No client is the same and UCF allows the service provider to provide that personal level of touch to every environment they manage.

UCF Functionality

UCF gathers information from the monitored platforms and surfaces this data through a variety of dashboard components based on a customizable set of thresholds.

The Information Flow

UCF uses a variety of protocols to gather information from the underlying platform. For the core 3 platforms (Avaya, Cisco, Microsoft), UCF leverages their manufacturer-based protocols as well as standard protocols like SNMP. For the broader ecosystem, UCF can leverage SNMP or RESTful API's to gather the relevant data.



Gathering the Data (Pollers and Trap Packs)

UCF's pollers and trap packs gather the information from the monitored device/component (agent). Pollers are scripts that "interrogate" the device and pull monitored parameters, while trap packs receive SNMP traps pushed from the monitored device/component.

Processing the Data (Collection and Alignment)

Periodically (typically every 24 hours), UCF will inventory an agent (monitored device/component) and capture that inventory as a collection. Then, UCF will reconcile the current collection with the prior collection (alignment). Based on this alignment, UCF will update pollers accordingly.

Evaluating the Data

Pollers and other measures are only as valuable as their context. For context, UCF has thresholds that trigger actions. Based on certain service provider-determined thresholds, alerts and/or alarms are generated, surfaced on a dashboard and, if applicable, routed to the appropriate service provider or client resource.

Putting Alarms in in Context – Dependency Trees

A core function of the Nectar UCMP system is the ability to identify the relationships of disparate silos of technology, events, and data. Dependency trees are the underlying capability that enables such correlation within the platform. A dependency tree provides a visual representation of all the components, services, and integration required to deliver an application to enterprise customers. It shows what is working, what is not, and which users and/or departments are affected. This context-sensitive display identifies any broken link in the chain in real-time, so service provider staff can quickly focus their remediation efforts.

Dependency trees are automatically generated through VKM's or they can also be manually created to illustrate – in real-time – the complex relationships between different and the dependent technologies.

Visualizing the Data with Relevance - Dashboards

UCF dashboards provide highly detailed, real-time information in a format that allows service providers to track all aspects of application performance and status. Dashboards can be customized to fit the unique needs of each customer deployment, and can be launched at the service provider level (CIP), the enterprise level (EIP) or individual platform level (RIG). Dashboard information can also be customized to suit the specific needs of different users, including IT support teams and/or executive-level staff.



UC Foundation Dashboard

Examples of Nectar UCMP real-time dashboards include:

- WAN/LAN bandwidth utilization
- CPU, RAM, and disk consumption
- Active, ESS, and LSP modes for the Avaya Communications Manager VKM
- SLAs on network links and facilities
- Trunk status and usage statistics
- DSP and CLAN resources

Automating the Process – Vendor Knowledge Modules (VKM's)

To reduce the time, effort, and cost of onboarding a customer, Nectar has developed Vendor Knowledge Modules (VKM's) for certain platforms. The VKM is a "bundled" set of pollers, trap definitions, thresholds, alert definitions, collections, and dependency trees for a given environment. An installation wizard completes the automation and ease of deployment. VKM's are designed to help a service provider can up and running with monitoring an enterprise client's UC environment minutes, instead of days or weeks.

VKM-generated dependency trees are automatically mapped to depict all of the inter-related, co-dependent elements that are required for a specific application or service to function. This mapping process provides rapid first level root case analysis. If there is an issue, a service provider is directed to the broken link in the chain, so they can focus on fixing the problem instead of trying to find it.

A complete list of current VKM's can be found in the partner portal and is included in the release notes for each version of the software.

Semi-Automation – The InformationPack

For some platforms, components, or manufacturers where a full VKM has not yet been developed, Nectar

has Information Packs. Information packs are a collection of pollers and thresholds developed for specific components/devices. Information packs encompass both live and historical data collection and representation for the critical data elements within a converged network. Information packs include pollers (SNMP Gets & Traps), live dashboards and historical reports for any SNMP device. They can also facilitate the generation of dependency trees, with some manual intervention. Though not as robust as VKM's, information packs can still ease the deployment burden on some monitoring for some components that do not have VKM's yet. For a list of applicable infopoller packs ask your Channel Account Manager or refer to the partner portal.

UCF Architecture

Nectar

UCF was designed and developed to be modular so it could meet the scalability and flexibility needs of service providers. At a high level, UCF has 3 components, the RIG, the EIP, and the CIP.



This section includes detail on the RIG and the EIP. The CIP will be covered in the Service Provider section of this white paper.

Remote Intelligence Gateway (RIG)

The Remote Intelligence Gateway (RIG) is the fundamental component of a UCF deployment. It is a server appliance



that typically resides next to the UC platform, within the customer's datacenter and is the data collection point for a customer's UC application environment. The RIG collects and forensically looks at all of the data from the UC network that is being managed. It gives service providers visibility into the customer environment in order to manage all data connections. In some cases, depending on the managed service, the customer can also view alerts and other data in order to troubleshoot or co-troubleshoot issues along with the service provider.

A RIG can be either a Windows-based or Linux-based physical or virtual server. It operates in a store-andforward manner for information channel feeds. Since RIG's have local data stores, there is a persistence of collected information at all times. It is important to note that customer relevant data always remains on-premises at the customer site. Only alarms flow upstream to the NOC.

Key Features

- Monitors UC servers and application health
- Powered by VKMs
- Deployed as VM or as hardware
- Adjacent to UC server infrastructure
- Provides polling, alarming, etc.
- Enables basic reporting of application health

Enterprise Intelligence Portal (EIP) – Enterprise Level

A RIG is deployed for every instance of an enterprise's UC platform. If a customer has their global Skype for Business infrastructure consolidated in regional data centers, for example, they would need a separate RIG for their APAC pool, their EMEA pool, and their Americas pool. Similarly, if a customer had a mixed communications environment, it is recommended they have a separate RIG for their Cisco UCM, Avaya Aura, and Skype for Business pool. Nectar's Enterprise Intelligence Portal (EIP) consolidates the alerts and alarms from all of the enterprise's RIG's into a centralized management console.

The EIP is typically deployed on a separate server. The EIP houses registration and communication proxy systems and provides a consolidated, global view of environments with multiple Remote Intelligence Gateway (RIG) deployments. The EIP enables global dashboards and acts as the launch point for the consolidation of customer dashboards from multiple downstream RIGs, providing centralized alarming of all RIGs.

In a large enterprise deployment, the EIP that resides onpremises can connect to the external Central Intelligence Platform (CIP) – described later in this paper - is typically housed within the service provider environment. Administrators can securely connect to downstream RIGs in order to pass commands and subscribe to information channels between the equipment that the RIG is providing proxy access to and the administrator.

Key Features

- Consolidated dashboards aggregate various RIGs for service providers
- Can be deployed as a VM or as hardware
- RIGs can be single or multi-home to EIP/CIP
- Includes Intelli-Q gateway



Network Readiness - Perspective

There is tremendous power and flexibility when voice, video, and application sharing can be converted to packets and sent over the existing network infrastructure. There is also significant complexity in making sure that all



of those packets arrive (low packet loss), arrive quickly (low latency) and arrive at roughly the same frequency (low jitter). If the network cannot effectively prioritize and route voice, video, and application sharing packets (QoS), the conversation quality suffers and user experience suffers. A key factor in optimizing the UC user experience is making the sure the network is always as ready as possible to transport those UC packets.

Within a distributed UC network, traditional packet flow can cross multiple paths based on their source and destination. This makes it impractical, if not impossible, for traditional vendor solutions to proactively monitor anticipated voice and video quality. The Nectar Perspective[™] module solves this problem by generating synthetic UC packets across the network between "agents" that measure key network metrics like MOS, jitter, delay, and DSCP.

This advanced technology enables network support staff to simultaneously monitor network readiness from different locations within a distributed UC environment – enabling support staff to maintain a consistent quality level based on an enterprise customer's corporate QoS design. Typical Perspective assessment scenarios include:

Perspective Use Cases

Ensuring the network is effectively transporting UC traffic

is critical to a successful UC deployment. Perspective can help validate network readiness in 3 different use cases.

Pre-deployment/transition – Network Assessment

Before ever deploying UC, an enterprise needs to confirm that their network is ready to effectively handle the proposed traffic. The best way to test network readiness before a deployment is to generate synthetic UC traffic equivalent packets and confirm they do not experience unreasonable levels of loss, latency, and jitter. Service providers can help their enterprise clients prepare for a UC deployment by using Perspective to generate traffic loads equivalent (or slightly above) what is expected from users once they are on-boarded to the UC platform. Potential triggers for a Perspective-drive network assessment include:

- Migration from IP PBX to UC (Lync/Skype4B)
- Migration from PRIs to SIP Trunks
- Load Testing
- Throughout the UC migration to ensure network supportability of additional users/workloads

Troubleshooting

Often, enterprises will experience poor conversation quality between groups of users in specific locations. Often a key first step in resolving the issue is understanding to what extent, if any, the network is the source of those issues. If there are not already diagnostics tools (probes) in place to evaluate the actual conversation packets, a series of synthetic transactions can help service providers understand how the network is handling the UC traffic between those locations. Either there will be clear issues with the network metrics that the service provider can address or the network segment will come back "clean", which enables the service provider to focus on





the other domains (application or end user).

Continuous Assessment

Networks are inherently dynamic. Configuration drift is a constant as routers are replaced, upgraded, or configured to support various IT initiatives. Often, the groups updating the network configurations do not fully understand the impact of these changes on how the network effectively prioritizes and routes UC packets. A simple router upgrade can drop QoS prioritization and UC conversations no longer get through the congested network in time or in order.

With a constant series of synthetic conversations, Perspective can immediately identify if the expected path of the packets has changed, the QoS prioritization changed, or if the network is down all together. Any call instability will generate an alert. Perspective enables support staff to review network path, delay, jitter, and packet loss metrics from the simulated calls. In a continuous assessment deployment, Perspective allows service providers to be proactive and alert their clients if configuration drift has potentially negatively impacted how the network is handling UC traffic.



Perspective Continuous Assessment

Perspective Functionality

Perspective generates RTP traffic between software agents. These agents initiate "conversations" between each other and measure the key metrics:

Network Path – Which routers did the packets pass through to get from one agent to another?Loss – Did every packet that was sent by one agent get to the other agent?

Delay – Did every packet that was sent by one agent get to the other agent in a fast enough time to be tolerable for real time communications?

Jitter – Did the packets arrive with a consistent spacing between the packetsor at least close enough that the network could re-order them before delivering them? **QoS** – Did the prioritization (DSCP value) that the first agent set to ensure packets were routed as efficiently possible stay with the packet all the way to the other agent or was it dropped and the UC packets had no prioritization?

Topologies

In order to match the projected UC traffic patterns, Perspective can be configured to run three different topologies:

Mesh – Every agent sends packets to every other agent in the enterprise environment.

Hub-and-Spoke – There is a centralized agent that sends and receives packets from every other agent in the enterprise environment.

Site-to-Site – Two agents sending packets back and forth. This topology is most often used in a troubleshooting scenario where there is consistent trend of poor calls between two enterprise locations.

Scheduling

Service providers can configure Perspective to run different tests at different times of day or different days of week. Service providers would leverage scheduling in 3 different scenarios:

Non-Work Day Impacting Assessment – If there is already voice/video traffic on the network during working hours, Perspective can generate a low volume of traffic during the day to test MoS, path, and QoS and then increase that volume after hours to test the network at load without impacting the enterprise's day-to-day operations.

Mirroring Anticipated Traffic – UC traffic patterns are not just based on location, they can sometimes be based on time of day or day of week, especially in a call center or sales environment. Service providers can fine tune the schedules to demonstrate exactly how the network will handle the proposed UC traffic based on anticipated call volumes at a given time on a given day.

Non-Work Day Impacting Monitoring – In some environments, especially contact centers, any additional traffic during the day could be business-impacting. Contact centers also want to make sure that nothing has happened in the off hours to prevent customers from calling. In these environments, service providers can schedule Perspective to generate and test traffic after hours and especially right before the business hours of the contact center begin.

Alerts/Alarms

If the network path changes, if QoS prioritization (DSCP) drops, or if MOS falls below a certain level, Perspective will generate an alert that will be sent to the UCF RIG and can processed with the other alerts/alarms within the service provider environment. These alerts allow the service provider to be as proactive as possible.

Reports

In addition to the alerts/alarms with specific network conditions, Perspective collects all the data captured by agents and surfaces them in a series of reports. These reports can give a picture of the overall health of the network and can highlight potential issues based on location, time-of-day, or day-of-week. Reports are a very effective way for service providers to communicate what Perspective is doing to ensure the network is optimized for UC traffic.

Perspective Architecture

To allow service providers to effectively simulate UC traffic, analyze its impact on the network, react to any network issues and present results to their enterprise clients, Perspective has 3 basic architectural components.



Controller

The Perspective controller is a service that runs on the UCF RIG and manages the assessment and aggregates the data for analysis and reporting purposes. The controller is also the management interface for configuring the assessments, including topology and scheduling. Finally, the controller receives the alerts/alarms from the agents and incorporates them into established UCF routing processes. The controller can either reside within the enterprise client environment or the service provider's data center.

Perspective Agent

Perspective agents (PA's) are the software that generates the actual RTP traffic. Agents reside at the sites that represent the endpoint of the targeted UC conversation.

Agents are standalone software that can reside on a VM, but are typically deployed on an Intel NUC. The Intel NUC has the advantage of being purpose-built for this function and comes with the agent software preloaded and pre-configured through the Nectar Appliance program, which makes it very easy to deploy.

Sessions

Sessions are the actual synthetic conversations between PA's. Sessions can be configured to mimic a variety of standard UC voice codecs.

Reporting

In many respects, the power of any tool is how it represents what it does in a way that in consumable and actionable by each potential stakeholder group. Perspective offers two reporting options:

Native Controller – The Perspective controller has a set canned reports that are an easy way to quickly present the output of the assessment.

Advanced Analytics – For more flexibility, the service provider can also leverage Nectar's Advanced Analytics modules for customizable dashboards with a variety of filters and views.

The Perspective module has everything needed to maintain a centralized view of real-time and historical measurements; centrally administer synthetic transaction sessions; and provide alarms and alert IT staff based on customizable performance thresholds.



Network Health – Real-Time Quality with UC Diagnostics

An important element of the UCMP software suite is the Nectar UC Diagnostics (UCD) module. UCD provides real-time visibility into the overall quality of the user experience by unobtrusively monitoring content, session, and network topology data. While UCF offers services providers manufacturer-provided quality statistics, UCD utilizes probe-based analyzer technology to fill in manufacturer blind spots, thereby creating true real-time, complete call diagnostics for every session, regardless of platform or client type. UCD collects comprehensive data from the actual UC conversations relating to packet loss, jitter, delay, echo, MOS, and other key metrics. This visibility offers service providers IP network issue correlation and comprehensive insight for fast resolution, a lower total cost of ownership, and a superior user experience. Without the use of network probes, support staff cannot track real time voice quality, segment the conversation, diagnose issues across multiple platforms, or correlate SIP signaling.



UCD - Quality of Session Table



UCD Value Drivers

Real Time Quality

The true value of UC Diagnostics is that it can see, and report, on how the actual packets of a conversation are being handled on the network. It can either show this in real-time or create a correlated snapshot for later review. Whereas Perspective can demonstrate how the network will likely handle UC traffic at a specific time, UCD can tell the service provider how the network handled the specific user's specific conversation.

SBC Bracketing

In addition to the media packets, UCD tracks the signaling packets and correlates the signaling to the associated UC conversation. This correlation is especially valuable when enterprise clients have deployed SIP trunks. Strategically placed analyzers (probes) can capture the signaling between the enterprise network and the SIP carrier and identify any signaling errors that may have been the source of the issue.

SDN API

Microsoft encrypts the media and signaling for all of its Skype for Business calls. This makes it impossible to, with certainty, associate specific packets with a given Skype for Business conversation. Microsoft addressed this with the SDN API which passes the necessary data at the beginning of a call to identify the packets on the network. As one of the inaugural SDN API development partners, Nectar's UCD has the longest track record of leveraging the SDN API to identify and diagnose Microsoft UC calls on the network.

UCD Functionality

UCD is a powerful tool that allows service providers to quickly identify any network or SIP signaling issues that are the cause of a specific user's specific poor conversation or a group of user's whose calls passed through the same burdened network interface.

Specific-Session Look-up

Through the UCD management interface, a service provider can look up a specific session. The sessions can be searched and filtered based on the caller (SIP URI, phone number, called phone number), the session type (voice, video, application sharing), how the call was rated, and how the call ended. The search can be limited to calls within the last hour or within in any time range in the past 30 days.

Correlated Sessions – Conference Calls

On a conference call, a user experiencing a poor quality call may assume it is their line or device causing the issue. When in fact, it could be an issue with any one of the users on the call. Simply checking the affected users stream for poor quality would not find that the source was actually another user. For instance, if the speaker has a bad connection, the other participants have the poor experience and are the ones likely to escalate an issue to the service provider. UCD allows the service provider to find the related sessions of the other participants in the conference call. The service provider can then identify which party had the poor connection and begin to diagnose the root cause.

Correlated Sessions – Network Interface

A common network-related source of poor conversation quality is a congested network interface. The number of concurrent calls going through that interface has exceeded the priority queue assigned to it. In this case,

there is likely more than one conversation and therefore more than one user impacted by the network condition. With another related sessions lookup, a service provider can identify all calls that were impacted by that network congestion and all of the users on those calls. At the very least, this allows the service provider to communicate the overall impact of the network congestion to their enterprise client. For an additional level of service, the partner could reach out to the impacted users proactively to communicate that they noticed they may have had a poor call, but the issue has been identified and is being addressed.

Alerts/Alarms

Since UCD is monitoring the networking, it will be able to identify certain network conditions that could impact overall conversation quality (congested ports, network route instability, etc.). UCD will alert on these conditions. Alerts and notification targets are configurable through interactive dashboards.

Reporting

Visualization of historical trends allows for executive-level tracking, management, and decision making in order to improve the user's experience and anticipate operational requirements such as capacity planning.

UCD Diagnostics Architecture

UC Diagnostics includes the following deployment roles:



Management Console (UCD-M)

The UCD-M is the management console for UCD. It is the user interface where the service provider can configure the tool and do all of the investigation and diagnostics. The UCD-M includes dashboards that provide the following data:

- Network alerts and site performance
- Network, Signaling, and Media KPIs
- Trending and Reporting

The UCD-M is also the interface to the UCF and will send all of the alerts and alarms to the RIG to be processed accordingly.

Point (UCD-P)

The UCD-P performs the protocol and signaling analysis. It consumes the Microsoft SDN API feed to identify Skype for Business calls on the network. It will also capture and process SIP signaling that can be exported into a SIP ladder diagram. Any network peering or polling also happens via the UCD-P.

Analyzer (UCD-A)

The UCD-A is the infamous "probe". The UCD does all of the media (voice and video) analysis. The analyzer segments the conversation on the network and provide real-time media analysis. Finally, the UCD-A captures the bandwidth, MOS, delay, jitter, packet loss and other key quality metrics of the conversation. The codec is then determined by the P from looking at the session signaling. The UCD- A determines the codec if it can but it cannot auto-detect dynamic codecs.

These roles can be deployed on individual servers or any combination can co-reside on a single server.

UCD – The Case for Probes

Some monitoring tools in the market that do not have the correlated diagnostics capabilities of Nectar's UCMP, claim they can do everything Nectar can do without probes. Their positioning blacklists "probes" that effectively narrow the problem domain and correlate network events to help service providers effectively identify, diagnose, and remediate network issues that are impacting the communications traffic and the user experience. The purpose of this section is to provide a quick overview of the case for probes.

What You Can Do With Probes

Since probes sit on the network and analyze UC media and signaling packets in real time, they are able to better correlate network activity and identify the location and nature of network events that are impacting UC traffic. Specifically, the value of probes can be seen in these four use cases:

- Tracking Real Time Voice Quality Observing every packet in a UC conversation and capturing metrics, probes can track key measures of call quality like MOS, jitter, latency, and packet loss in realtime throughout the duration of the call. Most UC platforms neither capture, nor pass on this level of real-time detail, so a probe is the only way to gather it.
- Segmenting the Conversation Since UC conversations are ultimately two, one-way streams, strategically placed probes can help identify which segment of the network impacted the conversation quality based on which directional stream showed the poor quality.
- Diagnosing Across Multiple Platforms In this era of transitioning infrastructures and hybrid deployments, many conversations pass through multiple platforms.

In many large enterprises it is not unusual for conversations to traverse from an Avaya user to a Cisco or Microsoft user or vice versa. Only with probes can a service provider segment between the various platforms and correlate a singular view of the conversation. Imagine a conference call with internal users from a variety of platforms.

4. Correlating SIP Signaling - Since the T1 was introduced in the 1960's, there have been challenges as voice left the private customer domain and entered the public carrier domain. That challenge lives on today in the form of SIP trunks and SIP carriers. Nectar analyzers can correlate poor user calls with SIP errors and produce a SIP ladder diagram that helps pinpoint the issue and gives the right people the information they need to remediate.

What You Have to Do If You Can't Produce Probes

So these monitoring companies that cannot leverage probe technology have to attempt to emulate the concept of network awareness. How do they do it?

- Traceroute Some monitoring tools will leverage a traceroute after the conversation is completed to try and recreate the network path of the call and capture network statistics. There are four fundamental challenges to the traceroute approach:
 - There is no guarantee that traceroute will report the same network path used by a call.
 - Many routers are configured to not to respond to traceroute.
 - Traceroute does not provide the egress interface.
 - Network devices will not treat traceroute packets the same as the UC RTP packets.

2. Regurgitate Manufacturer-Provided Data

Especially in the Microsoft UC world, most non-probe monitoring tools rely on the statistics provided by the UC platform. These platforms have very little actual

Inectar

network awareness, so the monitoring tool is subject to the same limitations as the manufacturer-reported data.

- Poll The Network Without probes, you could leverage SNMP or other protocols to poll the network. There are two challenges with this approach:
 - How do you correlate the packets with a given conversation?
 - Network devices don't capture MOS.



End User Health - Advanced Analytics

Reporting is a key component of any service provider offer because it articulates to the enterprise client the value the service provider is delivering. The Nectar Advanced Analytics module is a comprehensive reporting tool that provides advanced business intelligence and analytics. The Advanced Analytics platform offers flexible dashboards and scheduled reports that can help service providers and enterprise clients troubleshoot systemic user issues and report on overall usage and adoption, bad call pattern analytics, and conference call usage. It operates across multiple platform databases and correlates with other data points – such as SBCs, Gateways and WiFi for Skype for Business, Avaya, and Cisco – to provide robust trending and analysis, as well as performance reports during the pre-assessment phase.

In much the same way as their counterparts in business functions are challenged with making data-driven decisions easily and quickly, IT professionals are under pressure to gain insight into their own operations. By using Advanced Analytics, service providers can help their clients' IT pros explore beyond standard operational dashboards to gain deep awareness into areas of concern where the answer is not immediately visible, such as SLA performance analysis, network traffic optimization, root cause analysis, license utilization, and IT asset management.

Advanced Analytics Value Drivers

Effective reporting not only helps with the identification of intermittent issues within the end user domain, it can also help justify the UC investment or highlight areas of further investment with objective data on user adoption.

Intermittent End User Issues

The power of the flexibility of a UC deployment also adds complexity in diagnosing poor user experiences because there is some variability in the end user domain. When investigating a single call, it can be hard to attribute the poor quality to any single factor (WiFi, headset, PC, etc.). Looking at a series of poor calls, however, the service provider can begin to see trends with specific components. For example, if 2/3 of a user's poor calls have an unsupported headset, the headset is likely contributing, at least to some extent, the overall poor user experience. Or, if all the users connecting via a certain WiFi access point have a higher proportion of poor calls over a period of time, that would justify looking further into that access point's performance.

Usage and Adoption

A migration to UC can be expensive for enterprises and the ROI is not always obvious. The ROI, however, is heavily dependent on usage and adoption. If an overwhelming majority of the targeted users are not using the UC platform, then the justification is much more difficult. Effective reporting can demonstrate who is using



UC and which modalities (voice, video, collaboration, etc.). Where usage is high, the investment is validated. Where usage is lower than expected, however, it gives the service provider an opportunity to engage in a user experience initiative. To realize the full benefits of their UC investment, many enterprises will pay their service providers to analyze user feedback and develop training and other programs to increase adoption.

Advanced Analytics Functionality

Nectar's Advanced Analytics gathers data from a variety of sources (the monitored platform, ecosystem components, UCF, UCD, Perspective, etc. and presents them in a series of dashboards and reports. The dashboards are built to be flexible with a variety of filters and views that allow service providers to represent the data in a way that is most relevant to their enterprise clients. Reports are a convenient and consistent way to present the same data over time. A weekly report of usage and adoption may be a valuable contribution to a weekly management call. Intuitive reports can provide user experience detail across voice, conferencing, video, and IM technologies. Other Advanced Analytics reports include:

- Call diagnostics summary
- List of conference participants
- Conference summary
- Modality report
- MOS detail
- Peer-to-peer activity summary
- Server performance
- User activity report
- User registration

Reporting and advanced analytics provide insight into the end user environment and adoption modalities, including enterprise-level to user-level reporting, adoption statistics, and deep data analysis. The ability to troubleshoot systemic user issues and report on overall usage and adoption is directly related to the ROI of any UC investment.

Powering The UC Service Provider Practice

Nectar's UCMP was designed to empower service providers to generate value by bringing a superior level of service to their enterprise clients. This section highlights on the aspects of the Nectar suite that drive this value.



Intelli-Q – Fitting into the Service Provider Processes

Nectar Intelli-Q[™] is an automated Network Operations Center (NOC) workflow engine that acts as a call center for alarms and events. It can operate in a multi-tenant or standalone mode, offering service providers and/or enterprise customers a central management console, skills-based routing capabilities, alarm notification, and ticket system integration. Intelli-Q helps categorize, prioritize, and escalate issues using business rules to ensure proper notification and response by the operations team. The Intelli-Q module provides queues – or issue buckets – for different types of problems. Engineering resources are then assigned to the queues that best match individual skill sets.

For example, when an alarm or event hits the system, automation software offers options to send an email, SMS notification, and/or visual notification to a team member or group. As each NOC engineer or technician logs into Nectar's UCMP system, they are immediately presented



with the Intelli-Q "war board", a live list of all issues they have been assigned, as well as an 'all unassigned issues' group. These issues are color-coded based on device alert levels, and prioritized based on client service windows.

With Intelli-Q, NOC team members are able to create various service offerings to clients that go beyond simple alarm receipt and forwarding. NOC team members can be assigned to queues based on product knowledge, job function or service window. For instance, equipment failure alarms can be placed in one queue while application related problems and after-hours support are placed in others. In conjunction with alarm notifications, issues are routed quickly and efficiently to the correct group so that team members deliver faster response times and faster resolution of critical issues.

Intelli-Q makes it simple for service providers to adhere to business SLAs and customer contract agreements by providing the ability to assign levels of importance to outage types and define proper escalation procedures. This capability ensures optimal service delivery for clients of any size, with any type of problem, at any time.

Architected for the Service Provider

UCMP was specifically architected, from the ground up, to drive efficiency and value for the service provider.

Central Intelligence Platform (CIP) – Service Provider Level

The Central Intelligence Portal is a service provider aggregation point that enables a top-down view into multiple enterprise customer environments and their individual networks. The CIP operates as a georedundant server cluster (providing N+1 for scalability) that is hosted within the Nectar cloud. It houses registration and communication proxy systems that allow service providers to receive alarms and securely connect to customer deployed premise equipment in order to pass commands and subscribe to information channels between the service provider and the customer location.

Secure Remote Session Transport Protocol (SRSTP)

The Secure Remote Session Transport Protocol is a patented communications protocol that acts as the nervous system of the UCMP platform and links all components by utilizing a 256-bit outer encryption shell and proprietary internal command structure. It allows service providers to gain secure access into the client's network via a protected, single point of entry. This communications package creates an infrastructure that allows for the dynamic creation of information, command, and transport channels to be routed through an authorized connection between and amongst Nectar UCMP system components. The SRSTP system utilizes TCP port 443 for all communications that pass through internal and external systems to reach registered UCMP components.

The Publish and Subscribe system capability allows customer relevant data to always remain on-premises at the customer site. This feature makes data securely accessible to authorized service provider representatives and engineering resources in both always-on and on-demand fashion when the on-premises system is connected to the external CIP system component.

UCMP and the Service Provider Value Proposition

Service throughout the UC life cycle

The modular nature of Nectar's UCMP portfolio allows service providers to deliver value to their enterprise clients throughout the UC lifecycle. This holistic approach deepens and lengthens the relationship with the client and facilitates more revenue opportunities.

Planning for UC

Perspective is the most obvious module to leverage while planning for a UC deployment. If the network cannot effectively handle the projected UC traffic, user experience will suffer and the enterprise will not get the adoption necessary to justify the investment. Network assessments should be part of planning for any UC deployment and Perspective gives service providers a cost effective tool for delivering them. Perspective has



the added benefit that it can be left in place for a ongoing network readiness monitoring, which can be a standalone service or part of the broader service provider offer.

UC Foundation has a unique application in the Planning phase of UC project. Since the VKM's can auto discover Avaya, Cisco, and Skype for Business environments, service providers could use it as a tool to make planning around users and trunk capacity more efficient. If UCF can detect in a day that the current voice infrastructure is only using 40% of their trunks enterprise-wide, the service provider could save their client money with a plan to reduce the overall trunking when the new platform is deployed.

Deploying UC

The role of UCF in the deployment phase of the UC lifecycle is a bit more minor, but can still bring some real value. Since UCF monitors application health, it can be a great initial test to ensure the deployment as planned.

It can determine which services are up and running and which ones are not. This is a crucial next step before users are added and traffic increases.

Operating UC

Nectar

The application of Nectar UCMP in the Operating phase is straightforward and the purpose of the bulk of this content. The various modules enable service providers to bring value in monitoring, supporting, reporting on, tuning, and fixing their enterprise client's UC environment.

Offering Various Levels of Service

The breakdown of UCMP into modules helps service providers integrate Nectar into various levels of service offerings for their enterprise clients. The application domain is a fundamental level of basic service that leverages UCF. For those clients that want a higher level of user care, adding advanced analytics for end user health is a source of additional value (and potentially revenue). Finally, Perspective and UCD allow the service provider to be more real time and to proactively delve into the complexities of the network health. With diagnostics and network health, the UC service provider can set themselves apart from their competition and drive a long term, high value relationship with their enterprise market.

In the Clouds

The market buzz is around moving UC to the cloud. In some ways, the cloud is a risk to service providers because it moves some of the processing out of the control of the enterprise. In essence, the value of monitoring the application health domain diminishes significantly, if not entirely. Still, strategic service providers can still provide value as enterprises migrate UC to the cloud and continue to operate in hosted deployment.



Moving to the cloud does change the nature of the application domain, but it does not lessen the requirements of the network nor end user domains. Actually, it puts more pressure on the enterprise to ensure those domains are running optimally so that any issues that are caused by the hosted provider are clearly identified as such. It also adds complexity to the network domain by incorporating the carrier domain with the trunks/data lines that connect the enterprise locations



to their hosted provider. In the move to the cloud, Perspective and UCD both allow service providers to continue to bring ongoing value to their clients.

Is The Enterprise Network Ready for Hosted UC?

Again, moving the application domain to a UCaaS provider does not magically remove responsibility from the enterprise's network domain. If anything, it increases the pressure on the enterprise and their service provider to ensure the network is transporting the application as effectively as possible. Before deploying a hosted UC environment, every enterprise should perform a network assessment from a qualified service provider. This helps eliminate the network as a potential risk area of a cloudbased UC deployment.



Protecting the Edge with UC Diagnostics

With the additional complexity of a cloud UC deployment, the onus is on the enterprise to "protect their edge." In other words, if there is a poor user experience, was it caused by the hosted provider, the carrier, or the enterprise's network? UCD's ability to segment the conversation with analyzers, allows service providers to determine where call quality suffered. Analyzers at the intersection of the carrier and hosted provider domain and the carrier and enterprise domain can pinpoint whether the packets are entering and leaving each domain with good call quality.



Joining the Cloud Crowd – Perspective as a Service

As more and more enterprises migrate to UC, network assessments and ongoing network readiness monitoring



solutions are become a required service. Nectar's Perspective as a Service model allows service providers to cost effectively and efficiently deliver network assessments to a variety of clients simultaneously from a cloud-based controller.

Perspective as a Service means easy-to-deploy, easy-tooperate, high margin network assessments for the Nectar service provider community.

Summary

Nectar is spearheading the delivery of unparalleled network assessment, monitoring, and diagnostics tools for service providers and enterprise customers. Regardless of other vendor or technology platforms operating within the same network environment, Nectar's full suite of software provides seamless insight, metrics, and root-cause analysis of issues that may affect voice and video quality and the overall user experience. With Nectar, service providers can deploy, support, and manage their multi-vendor client's UC environments from the enterprise to the cloud and beyond.

About Nectar Services Corp.

Nectar is a global market leader. The company provides the most comprehensive monitoring and diagnostics software solutions for Unified Communication services, enabling IT and operation organizations to proactively ensure the end-user experience. Nectar's flagship Unified Communications Management Platform (UCMP) improves visibility and service delivery across integrated voice, video, and data application solutions by providing unique and critical performance information. Nectar provides monitoring and diagnostics for millions of enterprise endpoints to more than 1,400 enterprises in over 86 countries — including the largest global banking, search engine, healthcare, and manufacturing organizations in the world. Visit www.nectarcorp.com for more information.

For more information:

Americas — <u>info@americas.com</u> Europe, Middle East, and Africa – <u>info@emea.com</u> Latin America – <u>info@latam.com</u> Asia Pacific – <u>infor@apac.com</u>

Corporate Headquarters

366 North Broadway, #201 Jericho, NY 11753 +1 (888) 811-8647

The Nectar logo is a trademark of Nectar Services Corp. Other company, product, or service names mentioned herein may be trademarks or service marks of their respective companies. This document may contain forward-looking statements regarding future events or product enhancements. All statements other than present and historical facts and conditions contained in this document are predictions and reflect our current beliefs and expectations with respect to future events. Any forward-looking statements are based on information available to Nectar as of the copyright date, and Nectar assumes no obligation regarding such statements.