

# Automating Diagnostics using SDN

---

*Version 1.02 (December 10, 2015)*

## **Copyright Statement and Disclaimer**

Copyright 2015 International Multimedia Telecommunications Consortium, Inc. ("IMTC"). All rights reserved, except as expressly delineated herein. May include contributions for which Copyright is owned by IMTC contributors. See IMTC Copyright Policy [[www.imtc.org/documents/policy-documents/](http://www.imtc.org/documents/policy-documents/)] for additional information.

Unless authorized by the IMTC in writing, this document (including translations) may only be copied, distributed, or used for the purpose of implementing the specification in the document or preparing suggested revisions for consideration by the IMTC. Except as provided in the preceding sentence, the document may not be modified. If you reproduce or translate this document, this copyright notice and the disclaimer notice provided below must be included on the first page of any copy or translation. If you translate this document, you must translate the notice and the disclaimer notice provided below in the language used in the rest of the translation.

**DISCLAIMER OF WARRANTIES:** The specification in this document is provided "AS IS". IMTC and every contributor to the specification contained in this document hereby disclaim to the greatest extent possible under applicable law all warranties, express or implied, including but not limited to any warranty of merchantability, fitness for a particular purpose, or non-infringement. You are advised that Implementation of the specification may require licenses to patents or other intellectual property rights owned by IMTC, by contributors to the IMTC, or by third parties. IMTC disclaims ANY representation that any such intellectual property rights will be available to you.

---

# 1. Introduction

Today's Unified Communication and Collaboration (UC&C) systems are critically dependent on the underlying network to provide a high quality of experience to end-users. While most data applications are quite tolerant of network delays and can recover just fine from intermittent packet loss, real-time communication has much stricter network requirements since it involves human two-way interactions and issues like latency and packet loss can have a significant effect on the end-user experience. To deliver a high Quality of Experience (QoE) for UC&C, enterprises need to configure Quality of Service (QoS) on their networks to prioritize the latency-sensitive voice and video traffic ahead of other data traffic.

However, even when properly configured, traditional networks are generally oblivious to UC&C applications and unaware when users are experiencing voice or video quality related problems. Similarly, UC&C applications have limited visibility into the network which makes it difficult to determine the root cause of any quality of experience-related problems. Delivering a consistently high quality of experience to end-users requires diagnostics and management systems that integrate and correlate both network and application-centric information.

This document describes the use of Software Defined Networking (SDN) to allow UC&C applications to interact with the network with the goal of creating accurate and timely reports of QoE, assisting with root cause analysis of those issues, and automating problem resolution.

We introduce an **Automated Diagnostics Service (ADS)** that leverages SDN to access and control network elements and defines a set of Automated Diagnostics Application Programming Interfaces (APIs) that allow UC&C applications, SDN controllers and management tools to exchange pertinent information in real-time, to provide comprehensive visibility and to automate problem resolution.

# 2. Definitions

The following definitions apply to this document:

**Automated Diagnostics Service (ADS):** A service described in this document that leverages SDN to interact with both the network infrastructure and UC&C applications to provide comprehensive visibility and automate problem resolution.

**Advanced Video Coding (AVC):** is a common video coding format standard that offers a high level of compression, also known as H.264 or MPEG-4 Part 10.

**Mean Opinion Score (MOS):** a standardized measurement predicting the perceived quality of the media after transmission across the network. The value is 1 to 5, with 1 the worst and 5 the best theoretical possible. The maximum value and the impact of network impairments varies based on codec type used.

**Network Controller:** A logically centralized entity that controls the forwarding behavior of multiple network elements.

**Northbound Interface (NBI):** In an SDN architecture, northbound interfaces are used to communicate between the SDN Controller and higher layer services and applications.

*Perceptual Evaluation of Video Quality (PEVQ)*: a standardized measurement predicting the perceived quality of a video after transmission across the network.

*Quality of Experience (QoE)*: A measure of a user's entire experience with a service (e.g. phone call, video conference, etc.)

*Quality of Service (QoS)*: A model that provides differentiated treatment for different Classes of Service.

*Real-time Transport Protocol (RTP)*: A network protocol for delivering audio, video and multimedia over IP networks. RTP is used extensively in communication and entertainment systems that involve real-time media [3].

*RTP Control Protocol (RTCP)*: A sister protocol of RTP. RTCP provides out-of-band statistics and control information for an RTP session [3].

*SDN Domain*: A portion of the network being managed by the same SDN control plane.

*Service Level Agreement (SLA)*: a contract between a service provider and a customer that specifies, in measurable terms, what quality, capacity and reliability of network services are to be provided for different classes of service.

*Software Defined Networking (SDN)*: The physical separation of the network control plane from the forwarding plane where a control plane controls several devices.

*Southbound Interface (SBI)*: In an SDN architecture, southbound interfaces are used to communicate between the SDN Controller and the network elements (e.g. switches, routers, etc.)

*Scalable Video Coding (SVC)*: is an extension of the H.264/AVC video compression standard that also contains one or more subset bitstreams.

*Traffic Engineering*: The set of methods used for optimizing the performance of a network by dynamically analyzing, predicting, and regulating the behavior of data transmitted over that network.

### 3. Problem Statement

Organizations that deploy UC&C applications face the following network challenges:

1. Active health monitoring
2. Timely problem reporting
3. Effective troubleshooting
4. Rapid error resolution
5. Capacity planning

#### Active Health Monitoring

Gauging the health of a system typically involves monitoring for alerts that notify administrators of system failures. The absence of any such alerts is generally interpreted as an indication of good overall system health.

However, for UC&C systems the absence of alerts does not always imply that the UC&C applications are delivering an acceptable quality of experience (QoE) to the end-users. This is because QoE problems are typically not the result of equipment failures and instead are often the result of configuration errors or due to network congestion. For example, voice and video quality might suffer when QoS is misconfigured or if any link along the path of the network is oversubscribed.

What is needed instead for proper UC&C health monitoring is the ability to obtain **positive** feedback from UC&C applications that the overall system is operating correctly with a high QoE.

These feedback indicators should answer the following questions:

- Is the UC&C application performance consistent with Service Level Agreements (SLAs)?
- Is the network behaving properly?
- Is the overall UC&C system delivering acceptable quality?

Without such positive feedback, administrators cannot be confident that the overall UC&C system is operating properly, as many users do not report QoE issues and may choose other forms of communication instead.

Being able to provide a **system is healthy** message when no quality issues have been identified could also allow UC&C endpoints and applications to optimize the user experience by allowing them to operate at their highest performance and bitrate that does not negatively impact other sessions on the network.

#### Timely Problem Reporting

As stated before, UC&C quality of experience (QoE) problems are generally not easy to report using traditional management tools. For example, anecdotal industry data suggests there are three main causes for audio or video QoE issues:

1. Incorrect QoS configuration on the network
2. Wireless Access Point issues (e.g. misconfigured, insufficient coverage, interference or overlapping channels)

3. 3<sup>rd</sup>-party network problems (e.g. networks run by service providers that lack sufficient visibility or control, for example a wide area network)

None of these issues are easily identified or exposed by traditional network monitoring tools. As a result, network administrators are often forced to rely on end-user trouble tickets to become aware of such problems. Unfortunately:

- End-users tend to significantly under-report problems.
- Trouble tickets take time to submit and additional delay to be processed, which makes troubleshooting difficult since network conditions may have changed since the time when the problem occurred.

Significantly better reporting mechanisms are required to support monitoring all UC&C session quality information in real-time so that potential problems can be detected proactively and addressed in a timely fashion. These mechanisms should allow UC&C endpoints and applications to exchange quality information without any user intervention required. Also, for many issues it is important to be able to capture the situation while it is occurring and collect all the relevant environmental information to be able to identify and address the root cause.

## Effective Troubleshooting

When users experience intermittent QoE problems, it is often extremely difficult to identify the root cause. Identifying the root cause quickly is critical to be able to deliver on SLAs and guarantee a high quality of experience:

- Obviously, network administrators will be able to resolve the issue more quickly if they can identify the root cause more quickly.
- By having SDN Controllers identify the root cause and communicating it to the application, applications can avoid taking wrong corrective actions. For example, when UC&C applications see packet loss, they may apply Forward Error Correction (FEC) and send redundant voice and video packets by assuming the dropped packets are caused by poor signal quality in the wireless network. However, if the root cause of packet loss is network congestion, FEC may compound the problem.

By correlating detailed quality reports generated by the UC&C application with network topology information, it will be possible to quickly and accurately pinpoint the root cause of most UC&C quality issues.

## Rapid Error Resolution

If the root cause is determined to be due to a network misconfiguration, the problem is typically addressed using manual reconfiguration by a network administrator. Unfortunately, manual processes are generally time consuming and often error prone. It would be preferable if the system could apply the necessary corrective action automatically in response to identified quality issues. If quality reports from UC&C applications include sufficient information to pinpoint a network problem as the culprit of voice or video quality problems, it should then be possible to automatically correct many of these network issues as well.

## Capacity Planning

Even when QoS is configured properly, UC&C sessions may still experience intermittent quality problems because of network congestion anywhere along the path. Network administrators need visibility into QoE issues resulting from insufficient network capacity or incorrectly sized SLAs across the various classes of services, to be able to properly plan for peak usage scenarios. In this case, the individual QoE issues are less relevant, but it is necessary to be able to correlate the aggregate and the load behavior across multiple UC&C sessions.

Furthermore, administrators should also be able to identify trends that give early warnings about potential future capacity issues. For example, quality in certain locations may be trending down because usage in those locations is trending up. This means that quality trends could be a good early indicator of insufficient network bandwidth in specific locations or along certain paths. Ideally, network administrators should have the necessary visibility into these trends to allow them to add additional bandwidth capacity, adjust SLAs or limit application usage before congestion and poor QoE becomes a significant issue.

Ongoing capacity planning involves answering the following questions:

1. What is the anticipated usage between user groups and locations?
2. How much bandwidth will each session consume?
3. How much nominal and peak capacity should the organization plan for

Answering these questions is challenging in dynamic environments where users are mobile and multiple media modalities are available, each with different bandwidth requirements.

Addressing these challenges requires detailed analytics that can:

1. Capture historical UC&C session data and bandwidth utilization per user and location
2. Identify trends in the historical utilization with the goal of predicting future bandwidth requirements

## 4. Shortcomings of Current Solutions

Network administrators typically rely on the following mechanism for diagnosing UC&C quality problems:

1. Network counters and statistics
2. Probes
3. Synthetics

While these mechanisms are useful for diagnosing UC&C related problems, this document introduces a more effective and automated mechanism for monitoring and diagnosing UC&C quality issues.

### Counters and Statistics

Traditional network management systems periodically retrieve counters and statistics from network elements to get information about bandwidth utilization and packet loss across various network interfaces. These systems typically monitor all relevant interfaces on the network and do so at sufficiently large intervals to avoid the following scalability challenges:

- Excessive monitoring may overload the CPU or other resources of the network elements.
- Monitoring data might overload the network and have a negative effect on the production data that are being monitored.
- Excessive data collection may overload the network monitoring applications that collect, aggregate, and correlate all the data.

As a result, traditional network counters and statistics are not granular enough to effectively diagnose UC&C quality problems:

- UC&C systems require fine-grain monitoring, since even transient problem that only create brief sub-second disruptions in media streams may result in perceptible quality of experience issues to end-users.
- It can be difficult to determine which UC&C sessions are affected by problems observed at the network level without visibility into application-level state. Conversely, when UC&C sessions experience problems, it can be difficult to identify which network elements and paths are contributing to impairments of affected sessions.

More targeted and better integrated monitoring approaches are required to address the fine-grain diagnostics requirements of UC&C applications.

### Probes

While counters and statistics provide network-centric information, some network administrators also rely on probes to provide more detailed monitoring about the voice and video quality experienced by end-users:

- Probes *passively inspect* voice and video traffic on specific network segments and process this traffic to extract quality-related parameters such as latency, jitter, MOS scores, etc.



When voice and video traffic needs to be monitored by probes, network administrators typically configure **port mirroring** on network switches which instructs the switch to forward a copy of all network packets on specified switch ports (or an entire VLAN) to the switch monitor port where the probe is connected. As a result, the traffic seen by the probe “mirrors” the traffic on the switch ports (or VLAN) being monitored.

Alternatively, probes can be deployed **in-line** to monitor all voice and video traffic flowing through a specific interface. This deployment scenario is especially useful at demarcation points between different administrative zones, since it allows administrators to monitor quality of traffic that enters from or leaves into zones to which they don’t have administrative control or access.

While at first glance probes might look like an adequate solution for UC&C monitoring and diagnostics, they suffer from the following issues:

- The effectiveness of probes for root cause analysis is dependent on where and how many probes are deployed. Ideally, probes should be deployed at every router and switch in order to get pinpoint accuracy. This is unlikely to happen, since the cost to deploy probes adds an increased capital cost to the adoption and deployment of UC&C applications.
- And finally, probes may not be able to detect and analyze encrypted UC&C media flows which further reduces their effectiveness.

More effective and lower cost mechanisms are required for obtaining session-level quality metrics for voice and video traffic.

## Synthetics

Additionally, some network administrators use synthetics to periodically test network performance:

- Synthetics is **active testing** that generate “artificial” test traffic that simulates voice and video sessions with the goal of analyzing and predicting the quality and capacity that can be expected between specific network locations and paths being tested.

While synthetics are quite useful for capacity planning and network pre-assessment, they suffer from the following limitations:

- Synthetics are most commonly used during the UC&C installation process or during off-peak hours when they are not likely to interfere with live production traffic. In fact, using synthetics to help diagnose problems with live production traffic may actually exacerbate the problem.

A less intrusive and more real-time mechanism is required to address the fine-grain diagnostics requirements of UC&C applications.

## 5. Automated Diagnostics Service

While traditional network management tools provide high-level information about general network performance and traffic utilization, UC&C specific management tools must provide richer UC&C session details and quality metrics, to support monitoring individual UC&C sessions, along with networking topology awareness for determining how voice and video sessions are forwarded across the network. These management tools must interact with both the network infrastructure and the UC&C applications to provide comprehensive visibility into all aspects of UC&C quality and performance.

This document introduces an **Automated Diagnostics Service (ADS)** that leverages SDN to provide comprehensive visibility, to assist with root cause analysis of UC&C quality issues and to automate problem resolution, without requiring dedicated probes. UC&C applications inform the ADS using the SDN API, with a rich set of quality information whenever new UC&C sessions are being setup and/or being torn down and when quality problems occur. This enables the following interactions:

1. The ADS interacts with UC&C applications to track UC&C sessions that are active on the network. It leverages SDN Controllers to obtain topology and path information for these sessions and to monitor the network interfaces along these paths. This approach enables **targeted monitoring**, which addresses some of the scalability constraints of traditional network management tools.
2. The ADS interacts with UC&C applications using the SDN API, to collect metrics that provide a comprehensive end-to-end view of the quality of active and completed sessions. These metrics are significantly more effective than those that could be collected from using only probes, since these metrics are available for any network on which UC&C endpoints are deployed, not just the network segments with probes connected to them.
3. Based on information about session quality and their paths, the ADS can correlate network-centric metrics, like throughput and packet loss with application-centric metrics about voice and video quality to provide a comprehensive view of the overall health of the system.
4. The ADS receives notifications from UC&C applications that indicate it should perform more detailed analysis of a given flow. This may be in response to session quality thresholds being exceeded, or specific requests to monitor a given session or set of endpoints. In response to these notifications, the ADS could increase the frequency at which network counters and statistics are being polled, or request more detailed metrics from the network controller, with the goal of pinpointing the exact network interface, link, or devices contributing to the quality issue.
5. The ADS may interact with other UC SDN components to automatically resolve quality issues (such as the [Dynamic Traffic Engineering functionality of the Automated QoE Service](#) [12]).

The functional architecture of the Automated Diagnostics Service is shown in Figure 1 below:

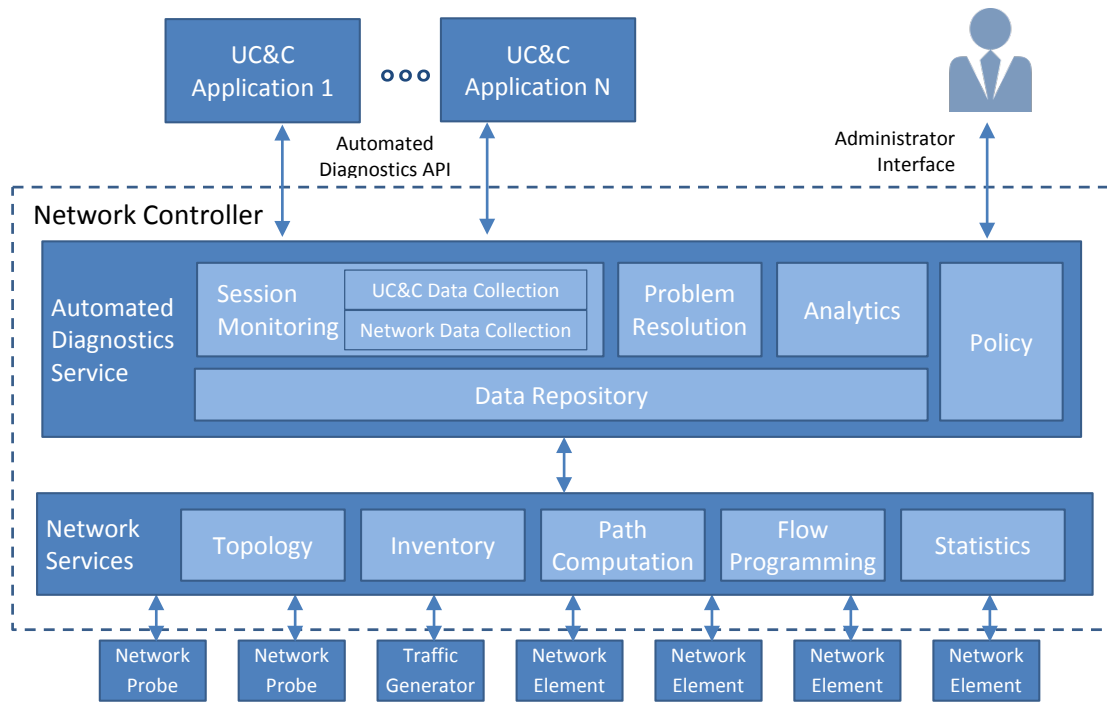


Figure 1. *Automated Diagnostics Service Functional Architecture*

As shown in Figure 1, the Automated Diagnostics Service includes the following functional modules:

1. **Session Monitoring:** this module tracks active session on the network and collects the relevant quality metrics for these sessions using the following two submodules:
  - a. **UC&C Data Collection:** this module interfaces with UC&C applications to collect diagnostics information from the associated applications and corresponding endpoints.
  - b. **Network Data Collection:** this modules interfaces with network elements to collect diagnostics information from the associated network interfaces.
2. **Problem Resolution:** this module is responsible for identifying root causes of quality problems and resolving issues if possible. Note that this module could interact with the Automated QoE module if necessary (for example to invoke the Dynamic Traffic Engineering functionality [12]).
3. **Data Repository:** this module is responsible for storing all session quality and monitoring-related data collected by the ADS.
4. **Analytics:** this module provides an analytics engine or similar system to try and identify specific patterns or trends that are a likely source of quality issues or may perform data correlation to identify and categorize known issues for more efficient troubleshooting.
5. **Policy:** this module allows Administrators to create the desired policies and custom thresholds for the session monitoring, data collection, and analytics modules.

## 6. Use Cases

As shown in Figure 1, the Automated Diagnostics Service (ADS) supports the following functions that are not easily accomplished with traditional network management solutions:

1. Session Monitoring
2. Automated problem resolution
3. Analytics

### Session Monitoring

The ADS includes a ***session monitoring*** module that addresses the shortcomings of existing solution by including the following functions:

1. Targeted network data collection
2. UC&C data collection
3. Automated problem reporting
4. Fine-grain network data collection

### Targeted Network Data Collection

The first function of the session management module addresses the scalability challenges associated with traditional monitoring of network interfaces by allowing UC&C applications to inform the ADS of active sessions on the network. This allows the ADS to limit monitoring only to those interfaces through which active sessions are flowing to prevent overloading the monitored devices or the network itself.

Detailed interactions between the UC&C infrastructure and the ADS will be illustrated using the sample network topology as shown in Figure 2 below. For simplicity sake this document assumes that this network is entirely within the domain of a single controller.

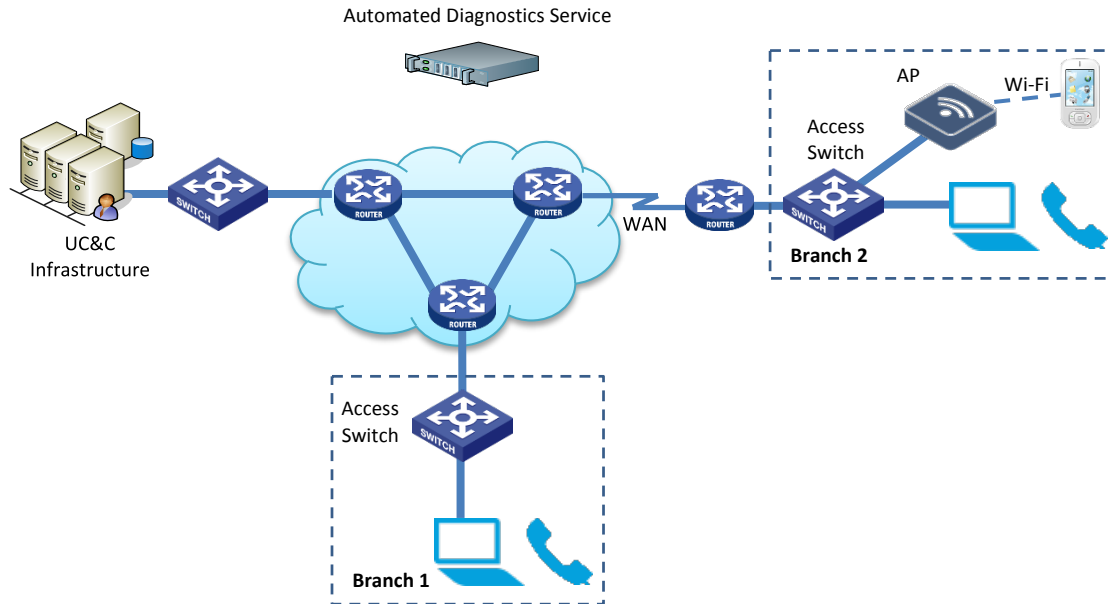


Figure 2. *Sample Topology for Automated Diagnostics Use Cases*

The following represents the flow and logic:

1. The ADS interacts with the SDN controller to gain access to the network topology for the given SDN domain. This allows the ADS to determine the path for media flows between any two given UC&C endpoints on the network.
2. When a new UC&C session starts up, the UC&C application sends a ***Session\_Start*** message to the ADS to inform it of the new session as shown in Figure 3 below. The Session Start message contains the IP addresses of the UC&C endpoints involved in the session which allows the ADS to determine the forwarding path for the media flows between the two UC&C endpoints. Note that because asymmetrical routing or load balancing can occur, the ADS will construct a separate path for each direction.

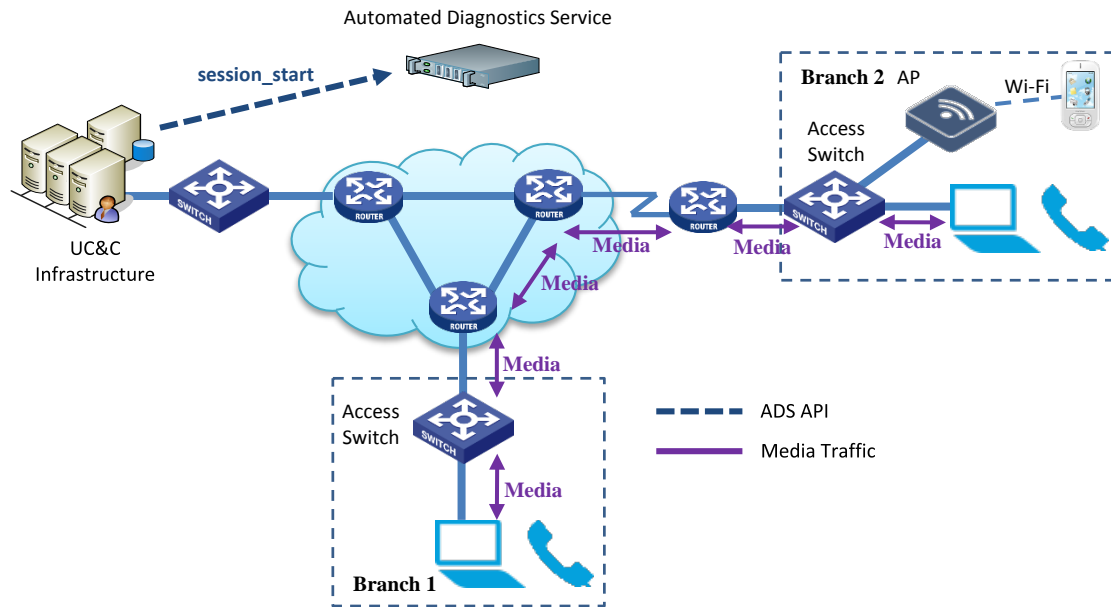


Figure 3. *UC&C Message to Inform ADS of Media Traffic*

3. The ADS then instructs the SDN controller to poll for specific network statistics for each network interface along the path for the given UC&C session as shown in Figure 4 below. The ADS does not need to poll network elements or interfaces that are not involved in any active UC&C sessions, which greatly reduces the amount of information that needs to be collected.

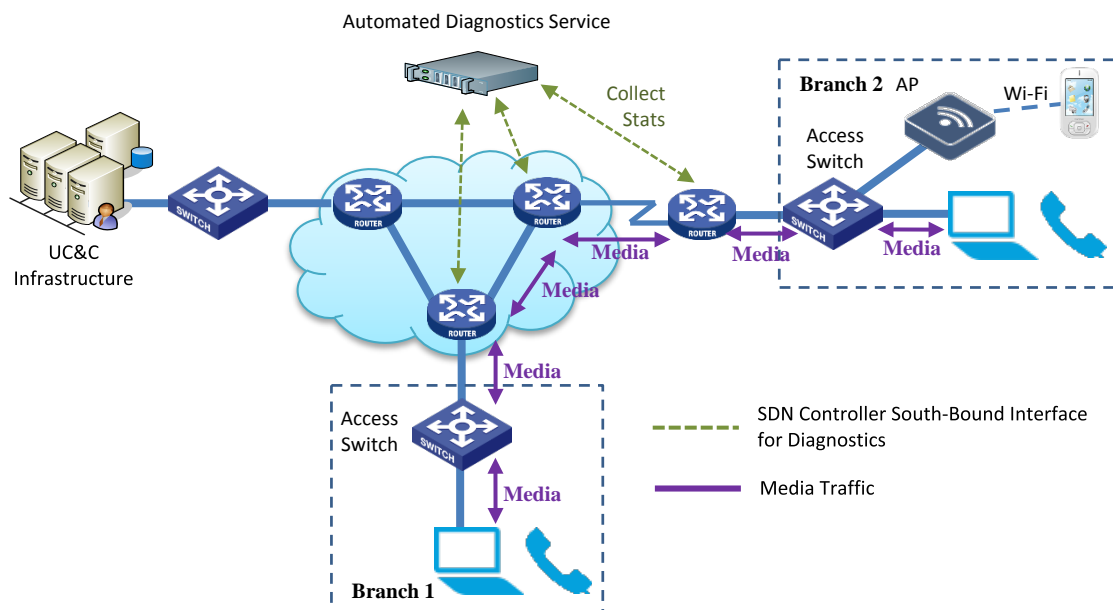


Figure 4. *Targeted Monitoring of Network Interfaces*

4. The time interval between polls can be longer to start with so as not to overwhelm the network elements or data repository. Only during times when sessions experience poor quality does the ADS need to poll with a shorter time interval and/or for more specific information. How this is handled will be described in the *Fine-Grain Network Data Collection* section below.
5. When the UC&C session is terminated, the UC&C application sends a ***Session\_End*** message to the ADS. In response to this message, the ADS stops monitoring the corresponding network interfaces involved in this session, which further reduces load on the network and the monitoring databases.

As this use case illustrates, by using session information provided by the UC&C applications the ADS can target data collection to only those network elements through which UC&C traffic is actively flowing. This provides a significantly more scalable network monitoring approach.

### UC&C Data Collection

As indicated earlier, the absence of network alerts does not automatically translate into acceptable quality for UC&C sessions. For example, quality degradation could occur as a result of intermittent network congestion problems that cannot be easily exposed through alerts. Consequently, administrators can only be assured that the system is operating properly if they receive positive confirmation from the UC&C application that session quality meets the desired SLAs.

In addition, it is important to be able to receive positive feedback as confirmation that proper changes and system adjustments have been made, when attempting to resolve any prior quality alert issues.

The ADS collects this UC&C application-centric data as follows:

1. Most UC&C applications include the ability to capture the quality experienced by the end-user. This quality information may be sent as ***Quality Summary Reports*** by the UC&C applications to the ADS at the end of every session. The quality reports includes metrics such as MOS scores, but other parameters such as packet loss rates, latency, jitter, echo, etc. are tracked as well.
2. While UC&C sessions are active, UC&C applications may send ***Periodic Quality Reports*** for active sessions to the ADS that include these user-focused quality metrics. As long as quality metrics are within the acceptable thresholds, these quality reports act as a positive confirmation that the system is performing as required.

Figure 5 shows the interactions between the UC&C applications and the ADS. Note that the mechanism by which the UC&C application as a whole collects information from the various UC&C endpoints is outside the scope of this document.

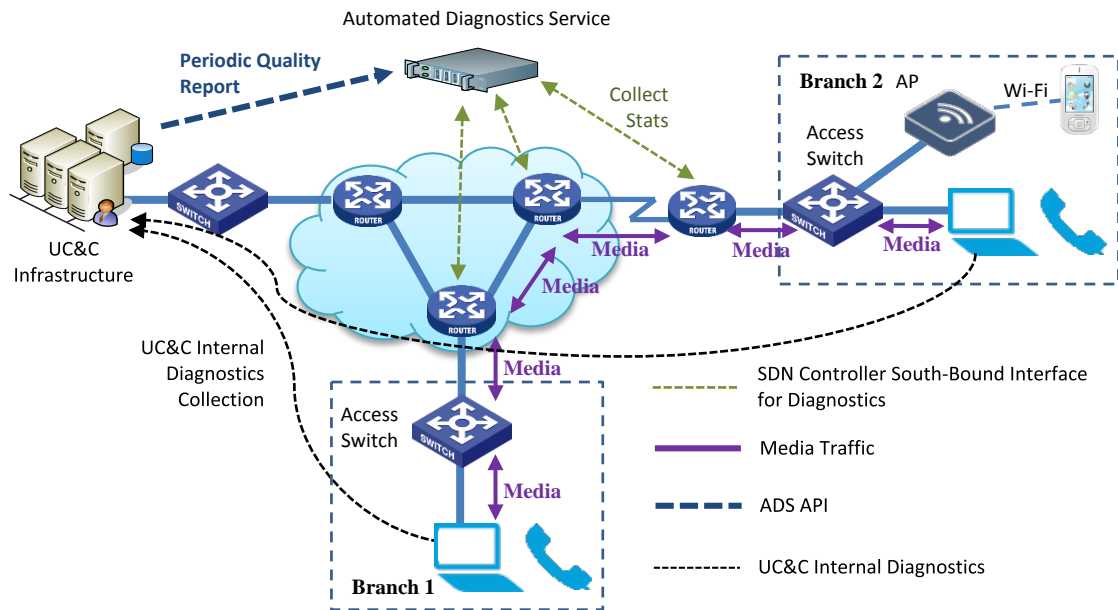


Figure 5. UC&C Data Collection

Aside from providing general health information about UC&C systems, quality reports can also be used as early warning mechanism for potential future quality problems. For example, the ADS could identify gradually degrading MOS scores, increasing packet loss rates, increasing latency, etc. that might help to anticipate network capacity problems long before users are even aware that anything is going wrong. This is especially important with modern codecs that are capable of concealing a variety of network impairments, so that users are less likely to notice these problems and as a result do not report them in a timely fashion.

### Automated Problem Reporting

As stated earlier, end-users tend to significantly under-report QoE problems, which makes it difficult for administrators to obtain timely problem reports. A third use case for the ADS is to automate problem reporting by taking end-users out of the loop:

1. As explained in the previous use case, most UC&C endpoints and services can report user-focused quality metrics. Consequently, these metrics can be used to automatically identify quality problems when acceptable thresholds are exceeded.
2. Whenever a UC&C endpoint or service identifies a quality problem, the UC&C application can send a **Quality Alert** message to the ADS to make it aware of the problem. These Quality Alert messages include quality metrics that indicate which media flows are experiencing poor quality.
3. In response to quality alert messages from the UC&C application, the ADS could use traditional mechanisms to make human operators aware of the problem.



Figure 6 shows an example of a Quality Alert message sent to the ADS when the endpoint in Branch 1 experiences a quality issue.

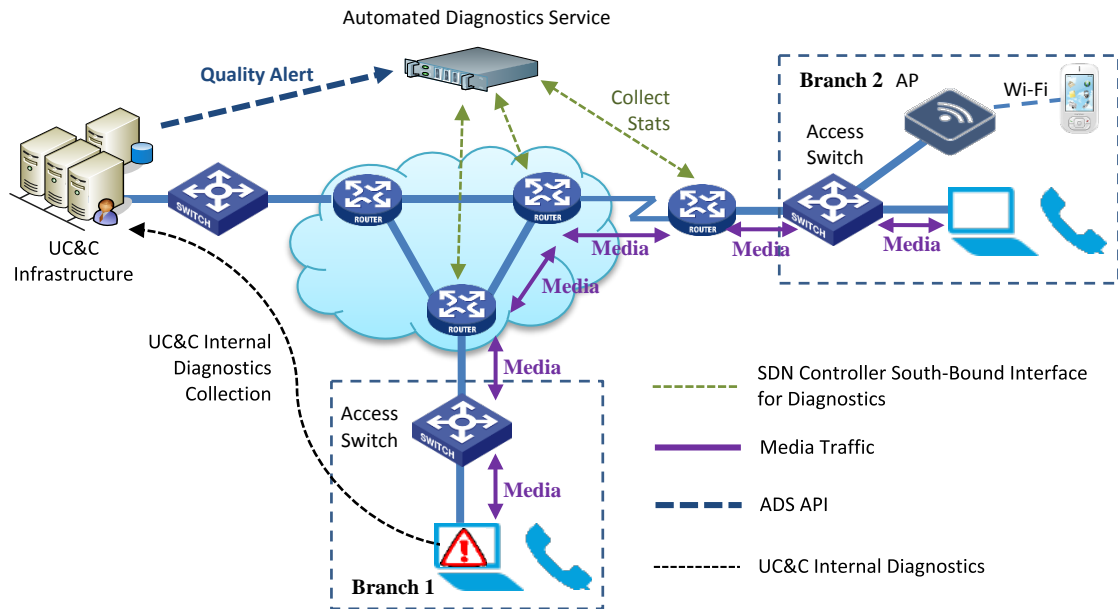


Figure 6. Automated Problem Reporting

Note that in addition to high-level quality metrics, Quality Alerts should also include any additional attributes that might help the ADS pinpoint to root cause of the problem. These attributes need not be limited to network-specific information but could include:

- “Environmental” info (e.g. Automatic Gain Control levels, level of background noise, etc.) that could explain poor user experiences.
- Device-specific information (such as device type, OS, driver versions, headset model, video camera model, etc.) could be sent as well.

### Fine-Grain Network Data Collection

Quality alerts generated by the UC&C applications help to resolve a second scalability problem associated with traditional network monitoring:

1. As stated earlier, the time interval at which information is collected from network elements must be sufficiently long so as not to overwhelm the network elements themselves or the databases that store the information.
2. However, when the ADS receives a quality alert from the UC&C application, network data collection interval times can temporarily be shortened just for those network interfaces that are involved with sessions currently experiencing quality issues. In addition, more comprehensive information can also be collected from those network elements to help determine the probable cause of the quality issue.

This approach allows for more targeted fine-grain and comprehensive monitoring of network data primarily during times when there are quality issues to reduce the risk of overloading the monitoring system or the network itself.

Figure 7 shows an example of the ADS automatically increasing the amount of network diagnostics being gathered in response to a quality alert. The shortened polling interval and the additional data being collected are illustrated in the figure below through the increased thickness of the “Diagnostics” line between the ADS and the targeted network elements.

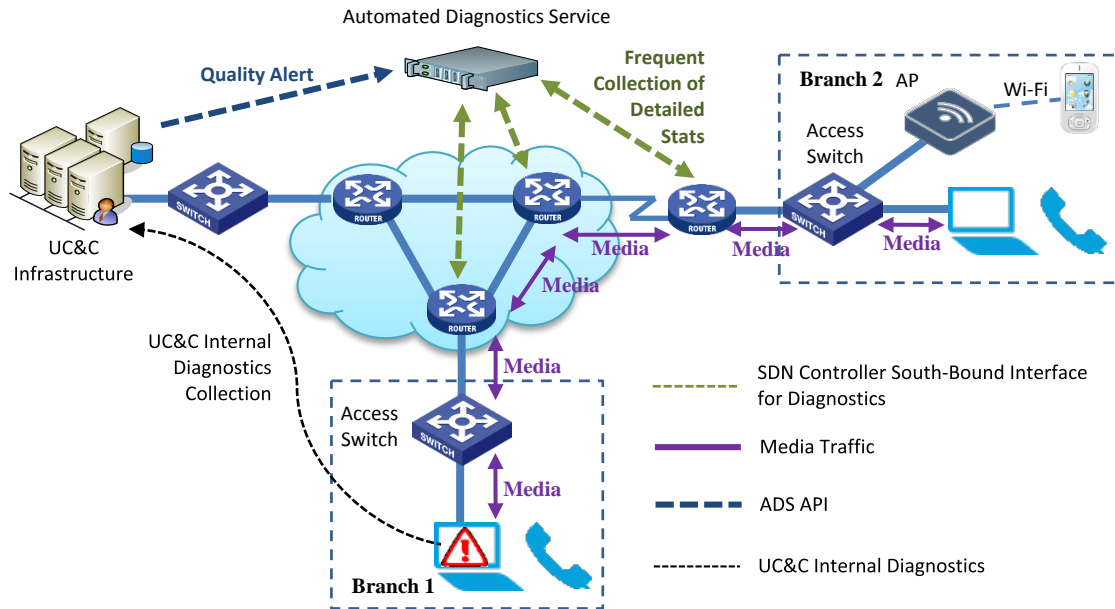


Figure 7. *Fine-Grain Network Data Collection*

## Automated Problem Resolution

By interacting not only with the network but also with the UC&C applications, the ADS is in an excellent position to not only diagnose the root cause of the problem but also to automatically correct certain types of problems. For this purpose, the ADS includes an error resolution module that provides the following functions:

1. Network error resolution
2. Endpoint error resolution

## Network Error Resolution

The ADS can automatically identify root causes or problems and correct those problems as follows:

1. The ADS can correlate quality metrics received from the UC&C application with targeted fine-grain diagnostics information from those network interfaces along the path of the affected sessions. This allows the ADS pin-point the root cause of the problem more quickly and more accurately than can be done using traditional counters or probes.

Figure 8 shows an example where the ADS uses a quality alert along with fine-grain network data collection to identify a congested link between two routers in the network.

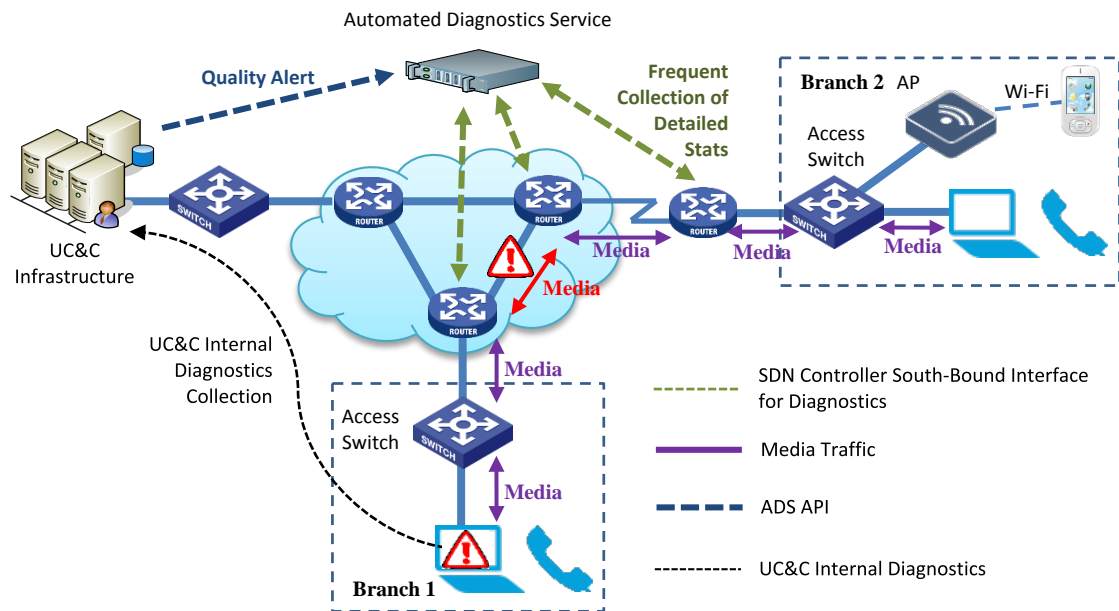


Figure 8. *ADS Identifies Congested Link*

2. Once the root cause of the problem has been identified, the ADS can attempt to automatically correct the problem. For example, it could decide to invoke other UC-SDN mechanisms to reroute sessions or to allocate additional bandwidth to voice and video queues on some network elements.

As a last resort, when the ADS has determined the root cause of a bad session, it can propagate this information to the UC&C application itself, to a human operator or an external system for further resolution.

Figure 9 shows how the ADS endpoint invokes the [Dynamic Traffic Engineering functionality of the Automated QoE Service](#) [12] to reroute the media flow that experiences quality problems around the congested link. Note that since the new path includes an additional network element, the ADS invokes targeted fine-grain monitoring on that network element as well.

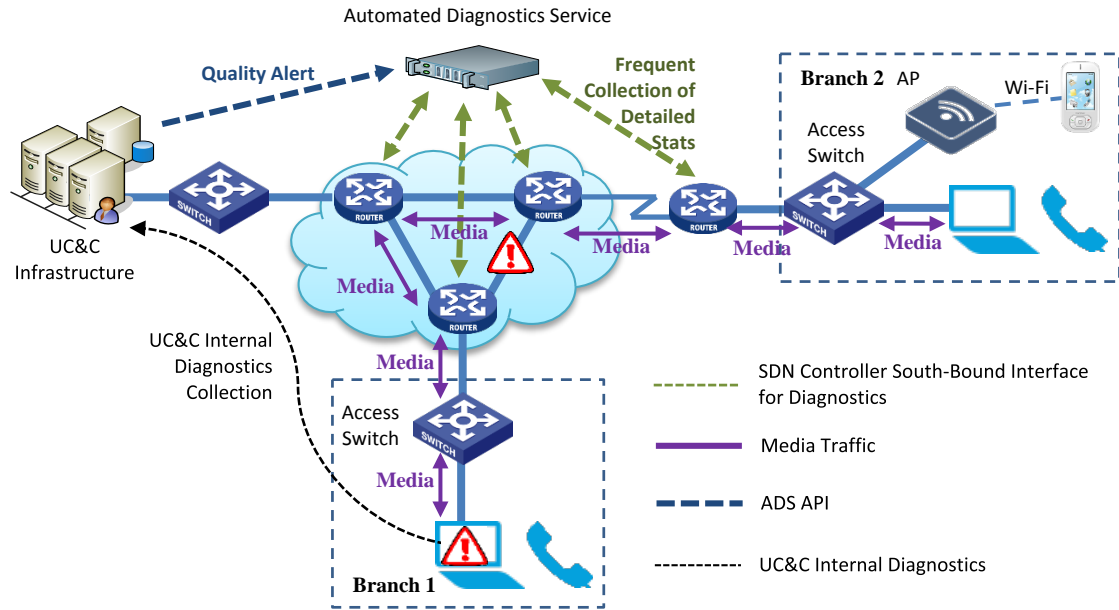


Figure 9. *ADS Reroutes Media Flow Around Congested Link*

3. If the ADS is able to resolve the problem automatically, the UC&C application will detect that the quality problem has gone away and it will send a quality alert indicating that the issue has been restored. In addition, the periodic quality reports also signal to the ADS that the quality issue has cleared up. In response, the ADS will revert back to normal polling intervals for collecting network data.

Figure 10 shows the system state after the ADS has resolved the problem. Note the network link in question may still be congested but it no longer affects the UC&C session in question.

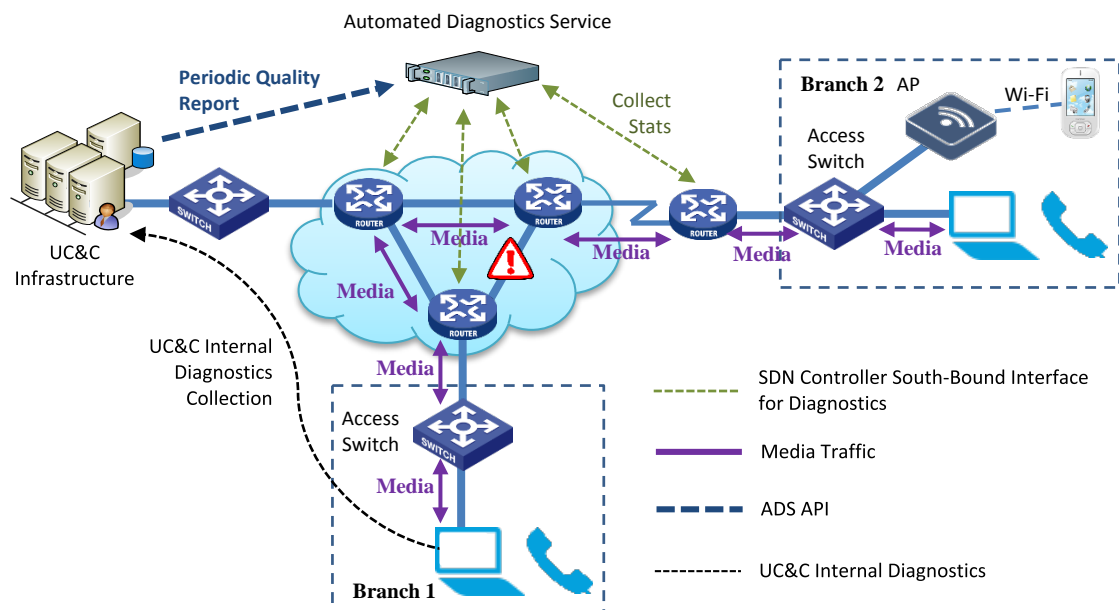


Figure 10. *System State After Problem Resolution*

## Endpoint Error Resolution

While the main focus of the ADS is on identifying network issues that are at the root of quality issues experienced by users, the ADS can also be used to help administrators when quality problems aren't caused by the network but rather are the result of configuration or performance problems with the user's endpoint. Administrators can avoid a lot of wasted time troubleshooting the network if the ADS could give them a positive indication that the issue is definitely not with the network.

The ADS supports this functionality as shown in Figure 11:

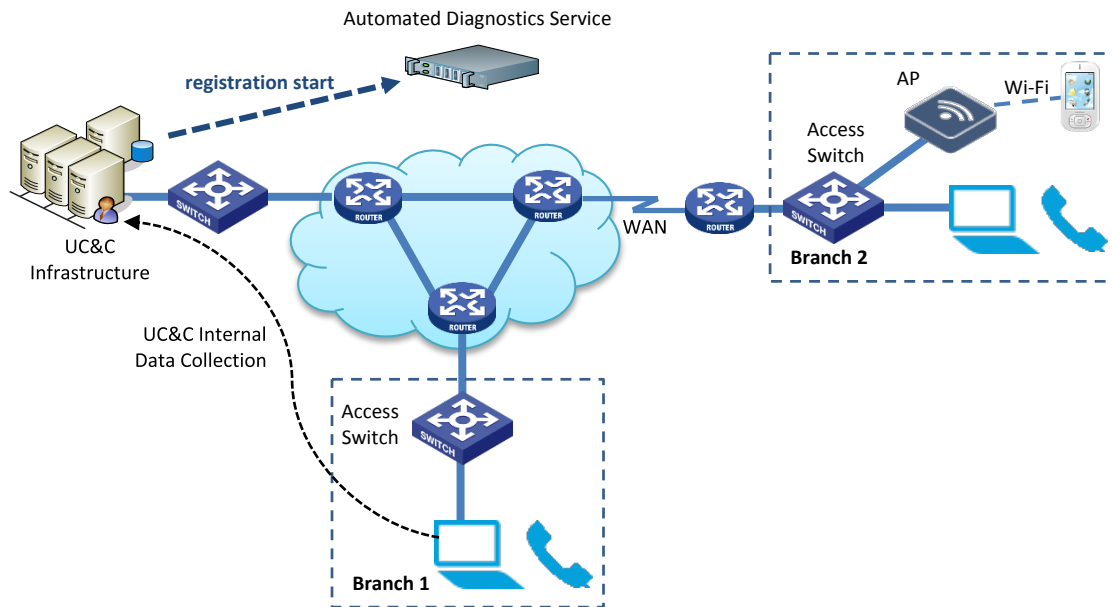


Figure 11. *Endpoint error resolution*

1. Whenever a new UC&C endpoint comes online (e.g. by issuing a SIP REGISTER message), the UC&C application infrastructure collects (through UC&C-specific mechanisms) a broad collection of information about the endpoint. For example, the UC&C application might collect information about the attached A/V devices and their associated software drivers, about the supported network interfaces and their software drivers, and about any other system information that is involved in processing audio/video streams on the endpoint
2. The UC&C application then informs the ADS about this new endpoint and its parameters using a **registration\_start** message. This message carries all the information elements that were provided by the endpoint to the UC&C application infrastructure.
3. If at some later point, the endpoint experiences a quality issue, the ADS could use endpoint information to find correlations between the type of quality problem and specific endpoint attributes. For example, the ADS might find that specific A/V devices are prone to quality problems, or that certain versions of software drivers result in frequent quality issues.
4. Using these types of correlations, the ADS will (over time) build up a knowledge based of known endpoint problems that help administrators resolve issues when these issues are not the result of network problem.

5. Once the ADS has built up this type of knowledge base, it could proactively alert administrators whenever endpoints register using a “known bad” configuration. This could help administrators resolve issues even before they occur.

## Analytics

Collecting quality-related metrics in the ADS will over time result in a large amount of quality data that can be run through an analytics engine for further analysis. Using an analytics engine exposes two types of useful information:

- Real-time data correlation to identify, categorize or exclude known issues:
  - A known bad driver causing a bad call alert.
  - Pre-categorizing and grouping issues for more efficient and focused investigations.
- Historical data that provides baseline trends and provide answers to the following questions:
  - Based on endpoint type, location, time of day, what type of experience can be expected?
  - Are there any poorly performing device types, questionable driver versions, specific network locations, etc. that are a likely source of quality issues?
  - What is the status of the network and associated resources, compared to baseline trends?

Real-time data can be used to dynamically optimize media path selection or to enforce admission control appropriately. Historical data can be used for network capacity planning and trend analysis. For example, this information could be used to predict the type of quality a user is likely to experience and set expectations accordingly, or as an early indicator to identify locations where additional network capacity may be required in the future.

The analytics engine leverages and correlates information obtained from:

1. UC Applications via the SDN API
2. Topology and path information from the Network Controller
3. Network event, counters and statistics from the Network Controller

Detailed description for how analytics can be used to “mine” ADS quality-related metrics are outside the scope of this document.

## 7. Operations

In order to support the use cases outlined above, the Automated Diagnostics Service (ADS) supports a number of operations that allow UC&C applications to exchange diagnostics-related information with the service. These operations fall in the following three categories:

1. Registration
2. Session
3. Quality report

This section describes operations in each of these categories in detail.

### Registration Operations

Registration operations inform the ADS with static information about endpoint devices that register with the UC&C service. This endpoint information is used by the ADS to assist with diagnosing and resolving any quality issues that may come up related to sessions that involve these endpoints.

Registration operations are initiated by the UC&C infrastructure and follow a standard CRUD (create/read/update/delete) model. Each of the operations takes a “registration” parameter that uniquely identifies the endpoint on the network and carries relevant diagnostics-related information about that endpoint.

Registration operations include the following requests:

`registration_start(registration)`

This UC&C infrastructure uses this operation to signal the start of a registration to the ADS. The endpoint argument includes information about the endpoint that might be relevant to help diagnose quality issues.

`registration_read(registration)`

The UC&C infrastructure uses this request to obtain information about a specific registration from the ADS.

`registration_update(registration)`

The UC&C infrastructure uses this operation to inform the ADS of updated endpoint attributes.

`registration_end(registration)`

The UC&C infrastructure uses this operation to inform the ADS that an endpoint registration has ended or is no longer active on the UC&C system. Depending on the UC&C implementation, this event may not always be provided because an endpoint device may suddenly drop off without unregistering.

### Session Operations

Session-based operations inform the ADS of each session (and their associated flows) dynamically as they are admitted on the network. These operations are initiated by the UC&C infrastructure and sent to the ADS. The ADS uses information in session operations to initiate and manage targeted monitoring of network elements.

Session-related operations follow a standard CRUD (create/read/update/delete) model where each of the operations takes a “session” parameter that uniquely identifies the session on the network. This session parameter contains the media flows for the session and the associated treatment that specifies how the UC&C infrastructure would like the SDN controller to handle these flows.

These session-related operations and associated information model are the same as specified in the [Automated QoE Service](#) [12].

Session-based operations include the following requests:

`session_start(session)`

The UC&C infrastructure uses this operation to signal the start of a session to the ADS. The session argument includes information about the media flows associated with the session.

`session_read(session)`

The UC&C infrastructure uses this request to obtain information about a specific session from the ADS.

`session_update(session)`

The UC&C infrastructure uses this operation to inform the ADS of updated session attributes.

`session_end (session)`

The UC&C infrastructure uses this operation to inform the ADS that a session has ended.

## Quality Report Operations

In addition to basic session information, UC&C applications also communicate session quality metrics to the ADS. These session quality metrics are used by the ADS to augment diagnostics information received from the network with the goal of identifying, diagnosing, and resolving any quality issues more quickly than could be done using network diagnostics alone.

Quality report operations are initiated by the UC&C infrastructure and sent to the ADS. Quality report operations include a set of quality-related metrics as well as a session parameter that uniquely identifies the session to which the quality metrics apply.

The following three requests are supported:

`session_quality_report(session, quality_report)`

This operation is used by UC&C applications to send periodic quality reports so the Automated Diagnostic Service can combine this with network diagnostics to create fine-grain trend information about session quality and early indicators of potential quality problems.

**Note:** The time span to use for computing attribute values for periodic reports is the duration between successive periodic quality reports.

`session_quality_alert(session, quality_alert)`

This operation is used by UC&C applications to alert the ADS of a degradation (or restoration) in session quality. In response to such indicators, the ADS can increase or decrease the granularity of network diagnostics to help pinpoint the root cause of the quality degradation. The UC&C application will need to implement a throttling



mechanism to prevent overloading the ADS with excessive quality alerts (for example, only once every 30 seconds).

**Note:** The time span to use for computing attribute values for quality alerts is the duration since the most recent periodic quality report, a prior quality alert, or the beginning of the session (whichever is the shortest interval).

```
session_quality_summary(session, quality_summary)
```

This operation allows UC&C endpoints to send quality summary reports to the ADS at the end of each session. These summary reports can be used by analytics engines to capture historical trends and predict future performance.

**Note:** The time span to use for computing attribute values for summary reports is the entire duration of the session.

The information model and corresponding attributes returned from the three report operations above are the same, with the primary difference being under what condition (e.g. threshold exceeded) and how frequently they are sent to the ADS.

## 8. Information Model

This section describes the various information elements and attributes that are included with the registration, session, and diagnostics operations presented in the previous section.

### Registration Information Model

Registration operations that communicate information about the start, update, and end of endpoint registrations use the endpoint information model shown in the following figure:

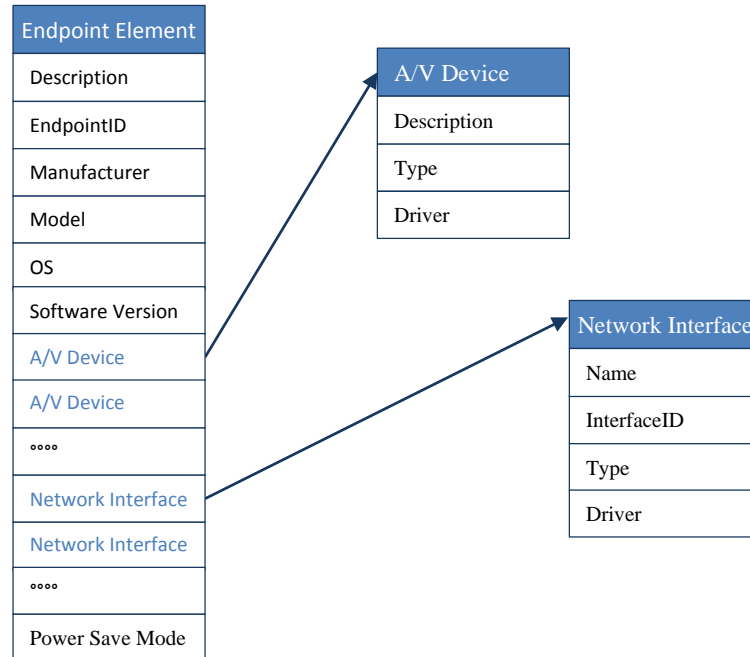


Figure 12. *Registration Information Model*

As shown in figure 12, the registration information model includes information about the endpoint itself as well as about the various network interfaces and audio/video peripherals used by the endpoint. The following describes each of these sub-elements in detail:

#### Endpoint Element

An endpoint element includes:

- Information about the manufacturer, the make and model of the endpoint
- Information about the software on the endpoint
- A list of A/V Device information elements for the various audio/video devices connected to the endpoint
- A list of Network Interface information elements for the various network interfaces connected to the endpoint

Detailed Endpoint information is as follows:

Attribute Name	Type	Cardinality	Description
Description	String	1	Friendly description of the endpoint (e.g. machine name, user name, system description or other human readable unique identifier)
EndpointID	EndpointID	1	Uniquely identifies the endpoint device. This is used for correlating what endpoints in the registration model belong to a given session.
Manufacturer	String	1	Manufacturer of the endpoint
Model	String	1	Endpoint model
OS	String	1	Name and version of the operating system running on the endpoint
Software	String	1	Name and version of the endpoint software
A/V Device	A/V Device Element	1..n	Information elements describing the various A/V devices for the endpoint
Network Interface	Network Interface Element	1..n	Information elements describing the various network interfaces for the endpoint
Power Save Mode	enum	[performance, powersave]	Device power save mode setting

### A/V Device Element

The A/V device element contains the relevant information about audio/video devices for the endpoint:

- Information about the manufacturer, the make and model of the AV device
- The type of device (microphone, speaker, camera, display)
- Information about software drivers for the device
- Type-specific info (e.g. microphone type, are devices Bluetooth-connected, etc.)

Detailed A/V Device information is as follows:

Attribute Name	Type	Cardinality	Description
Description	String	1	Friendly description of the device (e.g. device name, manufacturer and model)
Type	enum	1	Type of device. Valid values include MICROPHONE, SPEAKER, VIDEO, DISPLAY, OTHER
Driver	String	1	Driver software and version for the device

## Network Interface Element

Similarly, the Network Interface element contains the relevant information about the network interfaces used by the device to exchange audio/video media streams. Specifically, the network interface element contains:

- Information about the manufacturer, the make and model of the network interface.
- The type of network interface (Ethernet, Wi-Fi, Cellular, etc.)
- Information about software drivers for the device

In addition, these elements contain a number of network type-specific information. For example, for Wi-Fi networks, it might keep track of the following:

- What radio bands are supported?
- How many MIMO streams are supported?
- What chipset and driver version is being used?

Other network interface types track similar information.

Detailed Network Interface information is as follows:

Attribute Name	Type	Cardinality	Description
Name	String	1	Name of the network interface
InterfaceID	String	1	ID that identifies the interface and is unique for a given Endpoint Element.
Type	String	1	Type of network (e.g. Ethernet, Wi-Fi, Cellular, etc.)
Driver	String	1	Network driver software and version

## Session Information Model

Session operations that communicate information about the start, update, and end of a session use the information model shown in figure 13 below. Note that the tree representation in this figure is intended to show a hierarchical breakdown of the top-level session element (as opposed to a set of tables in a relational database). In this figure, information elements that are linked into the tree using dashed lines are optional.

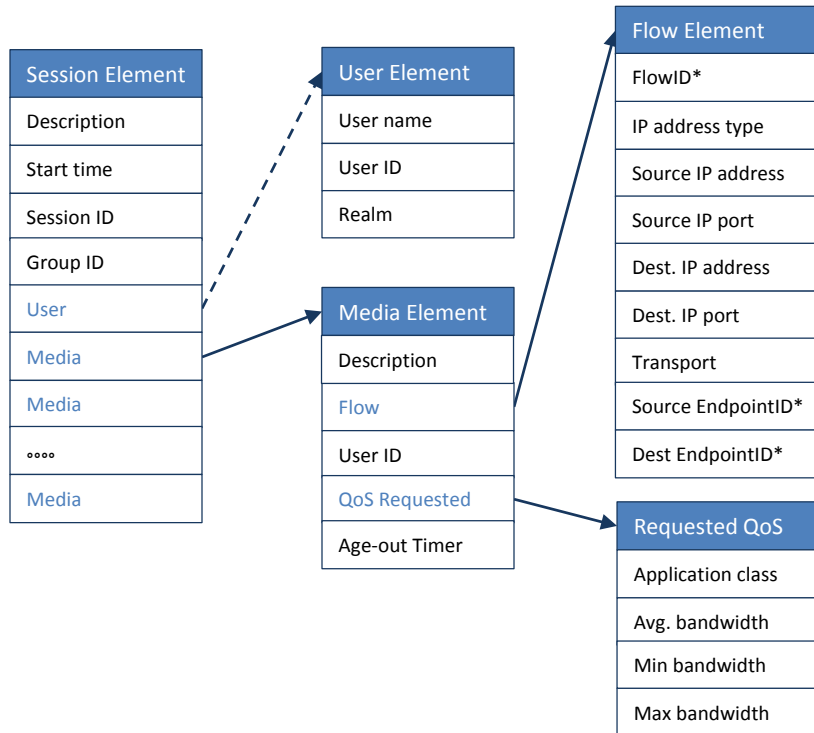


Figure 13. Session Information Model

\*The following describes the additional sub-elements in the Flow Element that are in addition to those defined in the session information model in the [Automated QoE Service](#) [12].

Attribute Name	Type	Cardinality	Description
FlowID	FlowID	1	Uniquely identifies the flow. This is used for correlating flows in the registration model with the flows in the media metrics.
Source EndpointID	EndpointID	1	Uniquely identifies the source endpoint device. This is used for correlating with the endpoints from the registration model.
Dest EndpointID	EndpointID	1	Uniquely identifies the destination endpoint device. This is used for correlating with the endpoints from the registration model.

## Diagnostics Information Model

The Diagnostics Information model contains information that is relevant to measuring media quality and identifying root cause of quality problems. Figure 14 below presents the Diagnostics Information model.

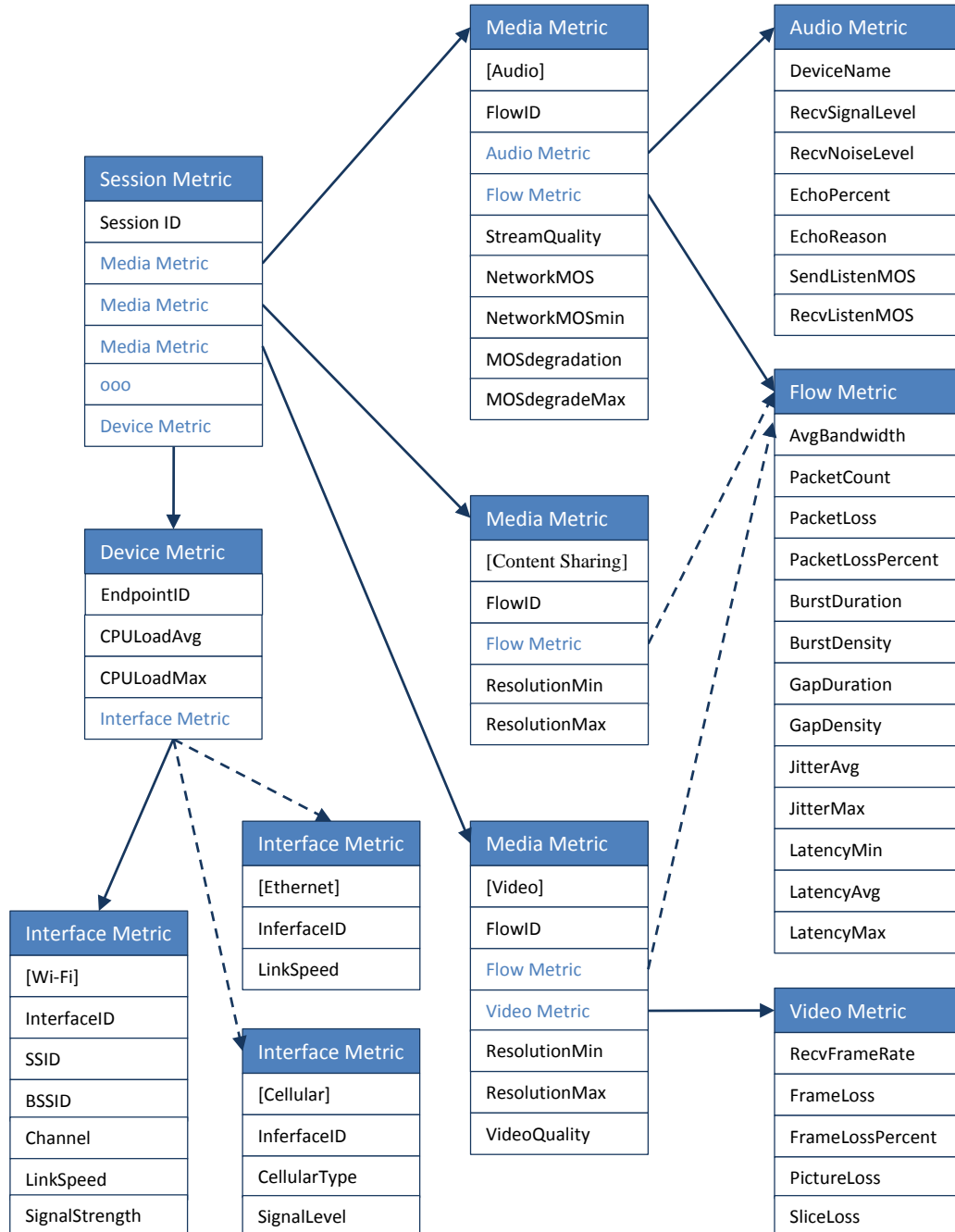


Figure 14. UC Diagnostic Information Model

Note that this information model parallels the session information model, but also extends it to provide detailed diagnostics about the various elements included in a session and also the

endpoint devices. Specifically, the UC diagnostics information model contains the quality metric relationships to the UC session and its elements.

## Session Metric

The session metric serves as a container that groups all diagnostics elements related to a session. Its main attribute is a session ID that allows the ADS to relate the diagnostics elements to the session it pertains to. As shown in the table below, session metric information attributes fall in the following categories:

1. Media Metrics
2. Endpoint Device Metrics

Session Metric element references the individual Media and Device Metric elements associated with a session:

Attribute Name	Type	Cardinality	Description
Session ID	Session ID	1	Uniquely identifies the session. This is used for correlating separate flows and device belonging to same session.
Media Metric	Media Metric Element	1..n	Information elements describing the various media metrics associated with this session.
Device Metric	Device Metric Element	1..n	Information elements describing the device metrics associated with this session.

## Media Metrics

Media metrics capture high-level quality metrics for each of the media flows involved in the session. These media quality metrics are sent periodically as part of a session quality report and provide the ADS with an up-to-date view of the overall quality of all sessions on the network.

The specific attributes included in media metric information elements depend on the type of media to which they pertain. Broadly, media types are classified into audio, video and content sharing. In turn, the video media-type itself can be further classified into SVC and AVC types of video though fundamentally the quality characteristics are represented similarly and would be denoted as a different code type. Note that other media types are also possible – such as data channels involving Instant Messaging, but are out of scope of this document.

## Audio Metric

Audio media metric elements include information that is specific to audio streams. Most importantly, it includes a variety of Mean Opinions Score (MOS) values that represents a prediction of the user perceived quality of the audio streams. These include:

- **Sending MOS:** the wideband Listening Quality Mean Opinion Score (MOS-LQ) of the audio stream before it is sent to the network. This value depends primarily on the quality of the audio capture devices and only takes into consideration acoustic factors such as codec used, echo, distortion, signal and noise levels.
- **Network MOS:** the wideband Mean Opinion Score (MOS) of the received audio stream. This value only takes into consideration network factors such as codec used, packet loss, packet reorder, packet discards, latency and jitter.
- **Listening MOS:** the wideband Listening Quality (MOS-LQ) of the received audio stream to be played to the user. This value takes into consideration all measurable impairments including network impairments and acoustic factors such as codec used, echo, distortion, signal and noise levels. Since this is an all-inclusive MOS, it will by definition always be the lowest value of the various MOS scores for a given audio stream.

The difference between the various MOS scores is that the Network MOS only considers the impact of network impairments, whereas Sending and Listening MOS also considers acoustic factors (echo, signal level, noise level, etc.). This makes Network MOS useful for identifying network conditions impacting the audio quality being delivered, while the Sending and Listening MOS are useful for identifying acoustic or performance issues on the endpoint devices.

The codec type impacts the MOS score by taking into consideration how effective techniques like packet loss concealment (PLC) and forward error correction (FEC) are in compensating for packet loss on the network.

The eventual intent is to generate notifications when UC&C system defined thresholds are exceeded to alert of possible network or media related issues for automated diagnostics and correlative analytic investigation by the ADS.

Audio media metric elements include information that is specific to audio streams:

- Audio quality based on network impairments (e.g. packet loss, jitter, latency)
- Audio quality including acoustic impairments (e.g. echo, noise, etc.)



Detailed audio-specific metric information is as follows:

Attribute Name	Type	Values	Description
FlowID	FlowID	[0-n]	To correlate this metric with the flow in the registration model.
Audio Metric	Audio Metric Element	1	Information element describing the audio peripheral metrics for this media element.
Flow Metric	Flow Metric Element	1	Information element describing the detailed flow metrics for this media element.
StreamQuality	enum	Good, Poor, Bad	Estimated quality of the duration of the stream, useful for alerting purposes (Good, Poor, Bad).
NetworkMOS	MOS	[1-5]	Average MOS as specified by [ITUP.800.1] section 2.1.2, based on the codec used and network impairments.
NetworkMOSmin	MOS	[1-5]	Minimum MOS as specified by [ITUP.800.1] section 2.1.2, based on the codec used and network impairments.
MOSDegradation	Number	[0-4] (-1 if not available)	Difference between the NetworkMOS and the maximum possible MOS for the codec used by a flow.
MOSDegradMax	Number	[0-4] (-1 if not available)	Worst degradation of NetworkMOS for the duration of a flow. This is the difference between the NetworkMOSmin and the maximum possible MOS for the codec used.

Note: some UC&C applications do not calculate a MOS score or will only provide a Network MOS, but for completeness the Automated Diagnostics API needs to support the various MOS related metrics for easier human interpretation of audio quality results.

## Video Metric

Video media metric elements include information that is specific to video streams:

- Video quality
- Video resolution
- Frames received and loss rates
- Slice and picture loss indication

The parameters referenced here are consistent with the package parameters referenced in [5], Extended Reports parameters referenced in [6] and base parameters referenced in [4]. In the first reference, the parameters are delivered from endpoints to the registered UC&C server as event packages. In the latter two references, the parameters are reported in the media path (to the bridge, gateway or its peer endpoint).

The eventual intent is to generate notifications when UC&C system defined thresholds are exceeded to alert of possible network or media related issues for automated diagnostics and correlative analytic investigation by the ADS.

[9, 10] extends the latency metrics reporting applicability to a range of RTP types. Also, RTCP XR support for Explicit Congestion Notification [11] are important inputs for distinguishing between congestion situations and signaling/media packet loss/damage situation.

Video-specific metric information is as follows:

Attribute Name	Type	Values	Description
FlowID	FlowID	[0-n]	To correlate this metric with the flow in the registration model.
Flow Metric	Flow Metric Element	1	Information element describing the detailed flow metrics for this media element.
Video Metric	Video Metric Element	1	Information element describing the detailed video specific metrics for this media element.
ResolutionMin	Integer, Integer	[0-n],[0-n]	Minimum video resolution negotiated for this session, in X-Pixels by Y-Pixels (e.g. Standard Definition SD video would be '640, 480').
ResolutionMax	Integer, Integer	[0-n],[0-n]	Maximum video resolution negotiated for this session, in X-Pixels by Y-Pixels.
VideoQuality	Number	[0-n]	Video quality score – such as PEVQ.

Detailed video-specific metric information is as follows:

Attribute Name	Type	Values	Description
RecvFrameRate	Integer	[0-n]	Average frames per second received for all video streams and computed over the duration of a flow. (frames/s)
FrameLoss	Integer	[0-n]	Total number of frames lost on the video receiver side for a given flow, including frames recovered from network losses.
FrameLossPercent	Percent	[0-100]	Percent of frames lost on the video receiver side as computed over the duration of a flow, including frames recovered from network loss. (percent)
PictureLoss	Integer	[0-n]	The number of Picture Loss Indication events detected by a receiver (typically sent via RTCP feedback) to inform the sender that inter-picture prediction chain may be broken. This typically will trigger sending several full intra-pictures to achieve resynchronization.
SliceLoss	Integer	[0-n]	The number of lost or corrupted macroblocks detected by a receiver (typically sent via RTCP feedback) to inform the sender about the need for intra macroblock retransmissions.

## Content Sharing Metric

Content sharing-specific metric information is as follows:

Attribute Name	Type	Values	Description
FlowID	FlowID	[0-n]	To correlate this metric with the flow in the registration model.
ResolutionMin	Integer, Integer	[0-n],[0-n]	Minimum resolution negotiated for this session, in X-Pixels by Y-Pixels.
ResolutionMax	Integer, Integer	[0-n],[0-n]	Maximum resolution negotiated for this session, in X-Pixels by Y-Pixels.

## Flow Metric

Flow metrics reference the information model from the [Automated QoE Service](#) [12] that is used to describe the network segments along a flow-path. They would be used as the basis for mapping the network-level metrics monitored by ADS to the flows associated with a given session and the ensuing correlation of network events to anticipated or detected UC events on the flow(s). This applies for all media types (e.g. audio, video and content sharing).

Flow metrics in each direction and of different media types are represented separately. This is because:

- Asymmetric networks (e.g. up and downstream characteristics are different, such as with ADSL) may result in different media metrics in each direction.
- Different media flows may be routed across different network paths, due to load balancing or network policy.

One exception is that RTP multiplexing becomes a special case of a union of audio, video and content sharing media running over a single RTP stream – represented by a single FlowID. In this case the different media type metrics would still be reported individually, but all referencing the same set of Flow Metrics.

Flow metrics should include the following information:

- Estimated bandwidth and number of packets in the stream
- Packet loss rate
- Information about packet loss bursts: A burst period is a period in which a high proportion of packets are either lost or discarded due to late arrival. This is represented using burst and gap density metrics.
- Jitter
- Round-trip latency

Where relevant, quality metrics include both an average value and as well the maximum for the time period over which the metrics are collected.

The parameters referenced here are consistent with the package parameters referenced in [6], Extended Reports parameters referenced in [5] and base parameters referenced in [4] using Sender Reports and Receiver Reports. In the first reference, the parameters are delivered from

endpoints to the registered UC&C server as event packages. In the latter two references, the parameters are reported in the media path (to the bridge, gateway or its peer endpoint).

These flow metrics (or any of the session metrics) may be used by the ADS to detect imminent issues that can result in QoE degradation (for example excessive packet loss or poor Wi-Fi SignalStrength). As allowed by the administrative policy, the ADS could then invoke the Automated QoE module to initiate appropriate corrective action. For example, it could invoke the Dynamic Traffic Engineering functionality [12] to reroute the affected media flows around a congested link.

The eventual intent is to generate notifications when UC&C system defined thresholds are exceeded to alert of possible network or media related issues for automated diagnostics and correlative analytic investigation by the ADS.

Detailed network-related flow metric information is as follows:

Attribute Name	Type	Values	Description
AvgBandwidth	Kbps	[0-n]	The average bandwidth received for a given RTP flow. (Kbps)
PacketCount	Integer	[0-n]	Number of RTP packets received for a flow. (packets)
PacketLoss	Integer	[0-n]	Number of RTP packets lost over the duration of a flow. (packets)
PacketLossPercent	Percent	[0-100]	Average percent of RTP packets lost, as specified in [RFC3550] section 6.4.1, computed over the duration of a flow. (percent)
BurstDuration	Integer	[0-n]	The average burst <sup>1</sup> duration, as specified in [RFC3611] section 4.7.2, is computed with a Gmin=16 for the received RTP packets. This metric is reported for audio streams when available. (ms)
BurstDensity	Integer	[0-n]	Average burst density, as specified in [RFC3611] section 4.7.2, is computed with a Gmin <sup>2</sup> =16 for the received RTP packets. This measures the average density of packet loss during bursts of losses. This field must be set to zero if no packets have been received.

<sup>1</sup> A burst [4] is a period during which a high proportion of packets are either lost or discarded due to late arrival. A burst is defined, in terms of a value Gmin, as the longest sequence that (a) starts with a lost or discarded packet, (b) does not contain any occurrences of Gmin or more consecutively received (and not discarded) packets, and (c) ends with a lost or discarded packet.

<sup>2</sup> The gap threshold. This field contains the value used for this report block to determine if a gap exists. The recommended value of 16 corresponds to a burst period having a minimum density of 6.25% of lost or discarded packets

GapDuration	Integer	[0-n]	Average burst gap <sup>3</sup> duration, as specified in [RFC3611] section 4.7.2, computed with a Gmin=16 for the received RTP packets. (ms)
GapDensity			Average burst gap density, as specified in [RFC3611] section 4.7.2, computed with a Gmin=16 for the received RTP packets.
JitterAvg	Integer	[0-n]	Average inter-arrival jitter, as specified in [RFC3550] section 6.4.1. (ms)
JitterMax	Integer	[0-n]	Maximum inter-arrival jitter, as specified in [RFC3550] section 6.4.1. (ms)
LatencyMin	Integer	[0-n]	Minimum network propagation round-trip time as specified in [RFC3550] section 6.4.1. (ms)
LatencyAvg	Integer	[0-n]	Average network propagation round-trip time as specified in [RFC3550] section 6.4.1. (ms)
LatencyMax	Integer	[0-n]	Maximum network propagation round-trip time as specified in [RFC3550] section 6.4.1. (ms)

### Endpoint Device Metric

The endpoint device metric contains information about the operational state of the endpoint itself that may have an impact on or provide insight into the quality of the sessions involving this endpoint.

These metrics should include:

- CPU load
- Local network interface metrics

Device related metric information is as follows:

Attribute Name	Type	Values	Description
EndpointID	EndpointID	[0-n]	Uniquely identifies the endpoint device. This is used for correlating with the endpoint from the registration model.
CPULoadAvg	Percent	[0-100]	Average CPU load during the session
CPULoadMax	Percent	[0-100]	Max CPU load during the session
Interface Metric	Interface Metric Element	1..n	Information elements describing the various network interfaces on this device

<sup>3</sup> A gap [4], informally, is a period of low packet losses and/or discards. Formally, a gap is defined as any of the following: (a) the period from the start of an RTP session to the receipt time of the last received packet before the first burst, (b) the period from the end of the last burst to either the time of the report or the end of the RTP session, whichever comes first, or (c) the period of time between two bursts.

## Network Interface Metric

The Network Interface metric contains information about the operational state of the local interface on the endpoint that may have an impact on or provide insight into the quality of the sessions involving this endpoint. The specific attributes included in network interface metric information elements depend on the interface type (e.g. Ethernet, Wi-Fi, Cellular, etc.).

Ethernet interface metric information is as follows:

Attribute Name	Type	Values	Description
InterfaceID	InterfaceID	[0-n]	To correlate this metric with the interface in the registration model.
LinkSpeed	Mbps	[0-n]	Link speed in Mbps.

Wi-Fi interface metric information is as follows:

Attribute Name	Type	Values	Description
InterfaceID	InterfaceID	[0-n]	To correlate this metric with the interface in the registration model.
SSID	String	ASCII	Service Set Identifier of the wireless network.
BSSID	String	ASCII	Equivalent to over-the-air MAC address of the AP radio.
Channel	Integer	[0-n]	Channel number or frequency in MHz of the active channel.
LinkSpeed	Mbps	[0-n]	Current link speed in Mbps.
SignalStrength	Integer	[0-n]	An indication of the Wi-Fi signal strength. Typically represented in -dBm format as a value from 0 to -100. The closer it is to zero, the stronger the signal is.

Cellular interface metric information is as follows:

Attribute Name	Type	Values	Description
InterfaceID	InterfaceID	[0-n]	To correlate this metric with the interface in the registration model.
CellularType	String	ASCII	Type of Cellular interface (e.g. CDMA, GSM, LTE, WCDMA, etc.)
SignalLevel	Integer	[0-4]	An indication of the cellular signal strength. Typically a value from 0 to 4.

## Audio Peripheral Metric

Audio Peripheral Device-related metric information includes the following:

- Information about performance of the capture and rendering devices
- Information about signal to noise ratios
- Information about echo and Acoustic Echo Cancellation operation

Detailed audio device-related metric information is as follows:

Attribute Name	Type	Values	Description
DeviceName	String	ASCII	Name of Audio Peripheral Device.
RecvSignalLevel	Integer	[0-n]	Received signal level in units of dB. This metric is reported for audio streams when available. Average energy level of received audio is classified as mono speech, or left channel of stereo speech. (dB)
RecvNoiseLevel	Integer	[0-n]	Received noise level in units of dB that is reported for audio streams when available. Average energy level of received audio is classified as noise, mono signal or the left channel of stereo signal. (dB)
EchoPercent	Percent	[0-100]	Percentage of time when echo is detected in the audio after echo cancellation.
EchoReason	String	1	Reasons of device echo detection and reported for audio streams when available. (E.g. High level of echo remained after echo cancellation, Signal from capture device had significant instances of maximum signal level).
SendListenMOS	MOS	[1-5]	MOS as specified by [ITUP.800.1] section 2.1.2, for the pre-encoded audio for a given flow before it is sent to the network. Includes acoustic impairments like noise and echo introduced on the sending device.
RecvListenMOS	MOS	[1-5]	MOS as specified by [ITUP.800.1] section 2.1.2, for the decoded audio received for a given flow. Includes all measurable impairments (e.g. echo, noise, network, codec compression, etc.).

## Quality Alerts

When a session experiences poor quality, the UC&C application may send the following event reason for a periodic quality report update to the ADS to notify the service of major quality related problems:

Event Reason	Description
PeriodicUpdateEvent	A periodic quality report, with no major quality related issue.
ThresholdEvent	One or more of the session metrics has been exceeded or restored. See the detailed session quality metrics for more information.
CPUInsufficientEvent	CPU cycles are insufficient for processing with the current modalities and applications, causing distortions in the audio channel.
DeviceCaptureNotFunctioningEvent	Capture device currently being used for the session is not functioning correctly and, possibly, preventing one-way audio from working correctly.
DeviceRenderNotFunctioningEvent	Render device currently being used for the session is not functioning correctly and, possibly, causing one-way audio issues.
DeviceClippingEvent	Speaker clips the microphone, causing the remote listener to receive clipping-induced distortions.
DeviceHowlingEvent	Experiencing audio feedback loop, caused by multiple endpoints sharing the audio path.
NetworkDelayEvent	Network latency is severe and impacting the experience by preventing interactive communication
DeviceNearEndToEchoRatioEvent	User speech is too low compared to the echo which impacts the user's experience. The situation may be improved by reducing speaker volume or moving the microphone closer to the speaker.
DeviceEchoEvent	A device or setup is causing echo beyond the compensatory ability of the system.



## 9. Authors

Name	Company	Role
Chris Lauwers	Ubicity Corp.	Vice Chair and Editor
Manfred Arndt	Hewlett Packard Enterprise	Co-Editor and Contributor
Pascal Menezes	Microsoft Skype for Business	Chair and Contributor
Gunter Leeb	Microsoft Skype for Business	Contributor
Mahalingam Mani	Polycom	Contributor
Shambhu Rai	Sonus	Contributor
Jon Snyder	Cisco	Contributor
Peter Thornycroft	Aruba, a Hewlett Packard Enterprise Company	Contributor
Russell Wiant	Nectar Corp.	Contributor

## 10. References

1. [RFC 7206](#): Requirement for an end-end session identifier in IP-based Multimedia Communication Networks (3PCC example)
2. [RTP Topologies \(draft\)](#)
3. [RFC 3550](#): RTP - A Transport Protocol for Real-Time Applications
4. [RFC 3611](#): RTP Control Protocol Extended Reports (RTCP XR)
5. [RFC 6035](#): Session Initiation Protocol Event Package for Voice Quality Reporting
6. [RFC 4585](#): Extended RTP Profile for Real-time Transport Control Protocol (RTCP)-Based Feedback (RTP/AVPF)
7. [RFC 5506](#): Support for Reduced-Size Real-Time Transport Control Protocol (RTCP)
8. [RFC 6642](#): RTP Control Protocol (RTCP) Extension for a Third-Party Loss Report
9. [RFC 6843](#): RTP Control Protocol (RTCP) Extended Report (XR) Block for Delay Metric Reporting
10. [RFC 6798](#): RTCP Extended Report (XR) Block for Packet Delay Variation Metric Reporting
11. [RFC 6679](#): Explicit Congestion Notification (ECN) for RTP over UDP
12. [IMTC Automating UC QoE using SDN](#) (Version 2.02, July 28, 2014)
13. [ONF-CIM Core Model base document 1.0](#) and [Model 1.0](#) (March 2015 | TR-512)

## 11. About the [UC SDN Activity Group](#)

Today many enterprises worldwide are retooling their voice environments to Unified Communications (UC) as it provides many end-user productivity advantages over traditional TDM voice or VoIP. Unfortunately, anecdotal evidence suggests that many UC deployments suffer from a variety of quality and reliability issues: users may have problems establishing voice or video calls, and when calls are established they occasionally suffer from poor audio quality, from pixelated, intermittent, and low-quality video, or from poor interactivity. These quality and reliability challenges prevent customers from realizing the full value of their UC deployments.

Information from UC systems that include Quality of Service (QoS) monitoring capabilities suggest that 60% to 80% of (QoS) problems are caused by issues with the underlying network. In practice, troubleshooting UC network issues is a non-trivial task and when issues have been identified, addressing them often requires infrastructure upgrades or network reconfigurations, all of which have a significant negative impact on total cost of ownership.

The IMTC UC SDN program investigates the use of Software-Defined Networking (SDN) as a solution to these quality challenges. By allowing UC infrastructure to dynamically interact with the network we aim to ensure that application-level quality and performance requirements can be met by the underlying network infrastructure.

The UC SDN program engages in the following tasks:

- Define use cases
- Analyze SDN capabilities
- Define a UC SDN framework
- Define APIs along with information model
- Define a certification program