Cisco Smart Care Service Voice Quality Monitor

Contents

1. Introduction ..............................................................................................................2
2. Scope .........................................................................................................................2
3. Voice Quality Measurement ....................................................................................2
   3.1 Business Case ............................................................................................................... 2
   3.2 Customer and Partner Challenges ................................................................................. 3
      3.2.1 Voice Quality Assessment ................................................................................................. 3
      3.2.2 Voice Quality Monitoring ........................................................................................................ 4
   3.3 Measuring Voice Quality with VQM ........................................................................... 5
   3.4 Solution Benefits ............................................................................................................ 5
   3.5 VQM Feature Design ..................................................................................................... 6
      3.5.1 Core Components ....................................................................................................................... 6
      3.5.2 Control and Bearer Connections ................................................................................................. 7
      3.5.3 DDNS .......................................................................................................................................... 7
   3.6 Voice Quality Monitor versus Voice Assessment ....................................................... 8
   3.7 Infrastructure Setup ........................................................................................................ 8
      3.7.1 Classification and Marking at the Network Edge ................................................................. 8
      3.7.2 Policing ...................................................................................................................................... 11
         3.7.2.1 Switchport with the Cisco Smart Care Network Appliance ..................................................... 11
         3.7.2.2 Switchport with the Reflector PC (with or without an IP phone) .................................................... 11
      3.7.3 Honoring the DSCP Marking in the Infrastructure ......................................................... 12
      3.7.4 Queuing and Scheduling ................................................................................................. 12
      3.7.5 Admission Control ........................................................................................................ 12
      3.7.6 Provisioning Required Bandwidth .................................................................................. 12
   4. Use Cases and Reports .............................................................................................. 13
      4.1 Voice Quality Assessment ............................................................................................ 13
      4.2 Voice Quality Monitoring ............................................................................................ 17
      4.3 Immediate Runs for Verifications and Troubleshooting .............................................. 17
   5. Specifications .............................................................................................................. 22
   6. Glossary of Terms ........................................................................................................ 23
1. **Introduction**

Voice Quality Monitor (VQM) is a new feature of Cisco® Smart Care Release 1.1 that allows partners to assess their customer infrastructure for its readiness to support a converged voice and data network. It also allows them to monitor the infrastructure for adherence to voice quality metrics on an ongoing basis. This feature evaluates the infrastructure against the three foundation parameters for voice quality: delay, jitter, and packet loss.

This paper discusses the business case for this feature, customer and partner challenges, solution design, infrastructure requirements, and finally sample use cases with reports. The technical specifications of this feature are also included.

2. **Scope**

The scope of this feature is limited to the assessment and monitoring of the network infrastructure for voice quality. It neither assesses nor monitors data applications or other interactive applications such as video.

This feature injects voice bearer traffic into the network and assesses the quality of that traffic, but neither injects nor assesses the quality of voice signaling traffic. It also does not assess the quality of any of the existing bearer or signaling traffic generated by other endpoints in the network.

3. **Voice Quality Measurement**

3.1 **Business Case**

Networks engineered to transport voice traffic in a converged environment must adhere to strict quality-of-service (QoS) guidelines in order to guarantee voice conversational quality. In a converged network transporting a multitude of traffic flows, such a guarantee requires the presence of several critical design criteria. The Solutions Reference Network Design (SRND) guide for Enterprise QoS ([http://www.cisco.com/go/srnd](http://www.cisco.com/go/srnd)) addresses these criteria in detail. Because of the dynamic nature of traffic flows and the use of bandwidth on links, there is a need to assess voice quality prior to deploying voice traffic and monitor voice quality after its deployment.

In a typical workflow leading up to the deployment of a converged network, you consult with your customer to identify the applications in the network, associate a business priority, assess the bandwidth requirement on links for these applications, and determine how they could be apportioned by priority such that resource allocation is based on business priority. This methodology attempts to ensure a service level that is a compromise between the available bandwidth and expected end-user experience, especially during times of link congestion. Although such methodology is an essential step, you do not gain an understanding of the user experience of voice quality or its projected effect on the mission-critical data applications prior to voice deployment. A toolset to simulate voice traffic in the midst of the existing applications and measure the quality offers an opportunity to assess the network for voice traffic and fine-tune the QoS policies. Without this tool, you would have to postpone this assessment until after a voice system is deployed and multiple users would have to make test calls to measure voice quality.

After deployment of voice traffic in a converged environment, ongoing monitoring is necessary to confirm that voice packets are continuously being allocated the required resources. This monitoring is particularly critical when existing QoS policies are modified to accommodate new applications on a voice-enabled network or to detect inadvertent configuration errors in the network infrastructure as part of an operational maintenance process that could cause intermittent voice quality problems.
3.2 Customer and Partner Challenges

3.2.1 Voice Quality Assessment

Assessment of the ability of an infrastructure to provide the desired voice quality typically occurs when an existing infrastructure supporting existing applications is being provisioned to also cater to the additional voice traffic. Because of the stringent requirements for traffic, partners and customers experience some of the following apprehensions prior to voice deployment:

- What would my end-user experience with my business-critical application be like if some of the existing bandwidth is taken away by voice when deployed?
- Will my QoS configuration in the infrastructure achieve the goal of provisioning appropriate bandwidths to both voice and data applications, such that they can all coexist successfully and continue to offer acceptable service levels?
- In the absence of real voice traffic with endpoints, how can I know what the voice quality will be like on my network? Will the delay, jitter, or packet loss in the network exceed the published best-practice guidelines or will they be within those guidelines?

Figure 1 shows a typical scenario that necessitates a Voice Quality Assessment.

Figure 1. Challenges Prior to Voice Deployment
3.2.2 Voice Quality Monitoring

In the case where a converged voice and data network is already in place, network managers and partners wish to seek reassurance that the infrastructure is continuing to provide and meet the voice quality best-practice guidelines—particularly when the customer is paying a premium charge to a service provider for priority handling of voice traffic over the enterprise WAN. Figure 2 shows the scenario for Voice Quality Monitoring.

Figure 2. Challenges After Voice Deployment

Some of the questions that customers ask after deploying the voice traffic follow:

- My network traffic is dynamic and supports many applications. I can also run new applications temporarily, without a formal approval process. Is there any symptom of voice quality degradation in these cases? How can I detect that on an ongoing basis?

- I have subscribed to a premium service plan from my service provider in order to prioritize voice traffic over their network. I would like to monitor and get a report on call quality from end to end for a sample call.
3.3 Measuring Voice Quality with VQM

The Voice Quality Monitor (VQM) feature of Cisco Smart Care 1.1 can help you answer these challenges before and after voice deployment (Figure 3).

Figure 3. VQM Solution to the Challenges

By injecting synthetic voice traffic into the network from the Cisco Smart Care Network Appliance to the Reflector software on a client PC at the chosen destination sites, you can determine the quality of these voice calls as well as the effect of such voice traffic on existing applications before deployment. This scenario gives you an opportunity to address the problems prior to production cutover. The appropriate course of action could be one of numerous action items, including the fine-tuning of QoS policies.

Also, you can answer the challenges after voice deployment by injecting one call worth of synthetic voice traffic into the network to a given destination site. The infrastructure devices will direct this call into its priority queues, and any degradation experienced by this call is likely to be experienced by other calls going through the links from end to end.

Note: Synthetic voice traffic injected on a production network generates the same amount of traffic as a real call. It is critical to ensure that extra bandwidth is made available in the priority queues of the infrastructure. Please refer to the “QoS Requirements of VoIP” section in the Enterprise QoS SRND document at: http://www.cisco.com/go/srnd to determine the bandwidth requirements by codec and link type.

3.4 Solution Benefits

In summary, the benefits of the Voice Quality Monitor feature include the following:

- By injecting Real-Time Transport Protocol (RTP) bearer traffic identical to that from an IP phone, VQM simulates the condition of production voice traffic in its exact form, so the results will be identical to those of production traffic.
- VQM proactively detects and reports voice quality problems in the infrastructure, regardless of the root cause within the infrastructure.
By displaying the values of the individual parameters that affect voice quality—delay, jitter, and packet loss—the tool guides you in further troubleshooting. A network with high delay but no packet losses points to a different problem than a network with low delay but numerous packet losses.

- VQM removes the need for subjective call quality assessment by end users.
- By simulating up to 20 concurrent calls, VQM removes the need to have 40 concurrent users (20 at each end) making simultaneous calls and making subjective assessments.
- By assessing the network prior to voice deployment, you can determine the effect of voice on existing data applications and apply corrective action.
- You can load the Reflector software on a PC and so, move it around to narrow the source of a problem.
- VQM provides a level of reassurance that the QoS policies in place provide a service level that will be acceptable to end users for both voice and data.
- Without such a tool, you will not know the effect and value of the QoS policies or the presence of any other infrastructure problems until after "production cutover". You suffer the risk of severely affecting business productivity for your customer, not to mention the high stress levels for your engineers and your credibility at stake if you cannot determine the root cause of the problem in a reasonable timeframe.

### 3.5 VQM Feature Design

#### 3.5.1 Core Components

The feature works by initiating a connection from the Cisco Smart Care Network Appliance as the source to a PC with the Reflector software as the destination. The Reflector software is available to partners for download from Cisco. Before bearer traffic flows between the Network Appliance and the Reflector, a TCP connection is set up between these endpoints for control. After the TCP connection is set up and the ports negotiated, synthetic RTP bearer traffic is sent between the two. At the end of the call, the TCP connection is torn down.

After the Reflector negotiates the port usage with the Network Appliance for the bearer traffic, it waits for the bearer traffic from the appliance. Upon receipt of the bearer traffic on the negotiated port, it simply “reflects” or sends the traffic back to the appliance. The Reflector software sets the IP and MAC headers in the return packet to the appropriate values in order to get the traffic back to the appliance.
3.5.2 Control and Bearer Connections

Figure 4 illustrates the design of the feature in terms of the control and bearer connections.

**Figure 4. VQM Feature Design**

When a VQM service is initiated from the dashboard, as either an immediate or a scheduled run to one or more reflectors using either the G.711 or G.729 codecs, the Network Appliance communicates with the Reflector over the TCP control connection to inform about the impending bearer stream and the port that the stream will be sent on. When acknowledged by the Reflector, the appliance initiates the streaming of the RTP bearer traffic for the period of time specified in the portal. When this time expires, the TCP control informs the client of the completion of the bearer streaming and tears down the TCP connection.

As noted in the figure, all TCP control traffic is marked Best Effort, because this traffic is not call signaling traffic such as Skinny Client Control Protocol (SCCP) or Media Gateway Control Protocol (MGCP). All RTP bearer traffic is marked Expedited Forwarding. This design helps ensure that no traffic other than the bearer traffic is directed into the priority queue of the infrastructure whose bandwidth is provisioned solely for bearer traffic.

The default TCP port for control is 17000, but it can be changed at the time of Reflector software installation. The default bearer ports range from 17001 to 17200, and they can be changed through the portal under “Reflector Management”.

3.5.3 DDNS

The Cisco Smart Care Network Appliance implements a Dynamic Domain Name System (DDNS) Server service and the Reflector software implements the client service. The Reflector client notifies the appliance of changes to its IP address, whenever it occurs. This feature allows you to assess and monitor the infrastructure by using Reflector names rather than the underlying IP address. The initial Reflector names and the associated IP addresses are assigned under “Reflector Management” on the partner portal. After the names are assigned, the DDNS service takes care of ongoing management of the binding.
3.6 Voice Quality Monitor versus Voice Assessment
Cisco Smart Care already offers a “Voice Assessment” feature, so why do we need this new feature?

The Voice Assessment feature provides a recommendation for the maximum number of G.711 and G.729 calls for a given link based on the link bandwidth and theoretical best-practice recommendations.

Voice Quality Monitor, on the other hand, reports on the quality of voice calls by injecting G.711 or G.729 traffic into the network and measuring the critical parameters.

Both Voice Assessment and Voice Quality Monitor are toolsets that provide unique perspectives to help you determine the number of calls that can be provisioned over a given link. Provision of QoS and the determination of the number of calls over a link is a consultative process between you and your customer. These toolsets can help in the decision-making process.

3.7 Infrastructure Setup
This section covers the relevant QoS detail pertinent to VQM services.

**Note:** You must be conversant with the QoS setup in your customer network infrastructure prior to initiating the service through the portal.

**Note:** All configuration statements provided in this document are based on the Cisco Catalyst 3560 Series Switch running Cisco IOS® Software. Please refer to the “Campus QoS Design” section of the Enterprise QoS SRND document (http://www.cisco.com/go/srnd) for equivalent configurations in other platforms.

3.7.1 Classification and Marking at the Network Edge
Figure 5 illustrates the configuration requirement on the switch port that connects the Smart Care Network Appliance to the network

**Figure 5.** Switchport with the Network Appliance

As stated earlier, all bearer RTP traffic from the Network Appliance is marked Expedited Forwarding, which is a standard for marking real-time voice packets. The appliance communicates with the Reflector software over a TCP connection for control. Because this traffic is not call signaling traffic such as SCCP or MGCP, used for call control, this traffic is marked Best Effort.
It is important for the switchport connecting the appliance to not remark or reset these markings. If mls qos is enabled globally on the switch, the switchport connecting to the appliance must be set to trust the DSCP marking. A sample configuration for a Cisco Catalyst 3560 Series Switch follows:

```
interface <interface number of switch port with the Network Appliance>
  mls qos trust dscp
```

If mls qos is enabled, it is important to ensure that the switch trusts the DSCP marking. Otherwise the switch will reset the marking to Best Effort, subsequently causing the RTP traffic to be queued inappropriately. This situation can lead to inaccurate results.

You can check the status of mls qos on a Cisco Catalyst 3560 with the sh mls qos command.

**Note:** If mls qos is disabled globally on any switch, the packet marking will not be rewritten by the switch and there is no need for any configuration on the ingress port.

Figure 6 illustrates the recommended configuration on the switch port that connects the Reflector PC to the network.

**Figure 6.** Switchport with the Reflector PC

The Reflector software marks the bearer traffic with a DSCP setting of Expedited Forwarding. For a switchport directly connecting the Reflector PC, this DSCP can be set to be trusted if the incoming packet is a User Datagram Protocol (UDP) packet within a certain port range. You can tighten the granularity of the access list, if required. For all other traffic, the packets must be reset to a Best Effort marking. This marking avoids any potential misuse of the priority treatment of Expedited Forwarding-marked packets in the infrastructure by any other application in that PC setting packets with this marking. The following shows a sample configuration for a Cisco Catalyst 3560 Switch with the Reflector PC. The requirement and the parameter detail for policing the Reflector traffic referenced in the configuration is given in section 3.7.2.2.

```
ip access-list extended REFLECTOR-Bearer
  permit udp <Data VLAN Subnet> host <IP Address of Network Appliance>
  range 16384 32767
class-map match-any REFLECTOR-Bearer
  match access-group name REFLECTOR-Bearer
```
policy-map REFLECTOR-PORT
  class REFLECTOR-Bearer
    police 128000 8000 exceed-action drop
    trust dscp
  class class-default
    set dscp default

interface <Interface id with the Reflector PC>
  service-policy input REFLECTOR-PORT ! Applies policy to interface

**Note:** For the above configuration to reset the DSCP marking for the default class, mls qos must be enabled globally on the switch.

If a QoS configuration is applied to the switchport already using the service-policy command, you must decide if this configuration is still applicable to that environment and integrate it as appropriate.

Figure 7 illustrates the recommended configuration on the switch port that connects the IP phone and the Reflector PC to the network

**Figure 7.** Switchport with an IP Phone and the Reflector PC

A sample configuration for a Cisco Catalyst 3560 Switch follows for the case of a switchport with an IP phone installed. In this case, the configuration also includes trusting of the IP phone signaling and bearer traffic. You can tighten the granularity of the access lists, if required. The requirement and the parameter detail for policing the Reflector traffic is given in Section 3.7.2.2. In this example, this policing logic also applies to the Voice VLAN-Bearer class from an IP phone to provision up to 320 kbps for the RTP stream of a G.722 codec, and up to 32 kbps for the Voice VLAN-Signal class for call signaling from an IP phone.

```bash
mls qos map policed-dscp 0 24 46 to 8

ip access-list extended REFLECTOR-Bearer
  permit udp <Data VLAN Subnet> host <IP Address of Network Appliance> range 16384 32767
ip access-list extended VVLAN-Bearer
  permit udp <Voice VLAN Subnet> any range 16384 32767 dscp ef
ip access-list extended VVLAN-Signal
```
permit tcp <Voice VLAN Subnet> any dscp cs3
permit tcp <Voice VLAN Subnet> any dscp af31

class-map match-any VVLAN-Bearer
match access-group name VVLAN-Bearer

class-map match-any VVLAN-Signal
match access-group name VVLAN-Signal

class-map match-any REFLECTOR-Bearer
match access-group name REFLECTOR-Bearer

policy-map REFLECTOR-PORT

class VVLAN-Bearer
  police 320000 10000 exceed-action drop
  trust dscp

class VVLAN-Signal
  police 32000 8000 exceed-action policed-dscp-transmit
  trust dscp

class REFLECTOR-Bearer
  police 128000 8000 exceed-action drop
  trust dscp

class class-default
  set dscp default

set dscp default

interface <Interface id of the IP Phone>

service-policy input REFLECTOR-PORT ! Applies policy to interface

Note: For the above configuration to reset the DSCP marking for the default class, mls qos must be enabled globally on the switch.

If a QoS configuration is applied to the switchport already using the service-policy command, you must decide if this configuration is still applicable to that environment and integrate it as appropriate.

3.7.2 Policing

3.7.2.1 Switchport with the Cisco Smart Care Network Appliance
No policing configuration must be applied on the switchport connecting the Cisco Smart Care Network Appliance.

3.7.2.2 Switchport with the Reflector PC (with or without an IP phone)
If the rate of packets that is expected for the VQM traffic is within bounds, it is deemed to conform to the policy and the packet is transmitted. However, if the rate of packets is beyond the expected bounds, it is deemed to exceed, so the packet must be dropped. Again, this control places a check on the anomalous rate of traffic beyond the expected normal flow for a single voice call of a given codec under any circumstance. For a single G.711 call factoring possible Layer 2 overheads and a safety buffer above the Layer 2 overheads, we set it to 128000 bits per second as the rate. The burst size allows for a burst of up to 250 milliseconds, with a minimum configurable burst size of 8000 bytes. This level of policing is achieved through the following configuration for the case of a Cisco Catalyst 3560 Switch.
class REFLECTOR-Bearer
police 128000 8000 exceed-action drop

Note: If a QoS configuration is applied to the switchport already with a policer, you must decide if this configuration is still applicable to that environment and integrate it as appropriate.

3.7.3 Honoring the DSCP Marking in the Infrastructure
It is important for the infrastructure to honor the DSCP marking set at the edge from both the Network Appliance and the Reflector "end to end", and not remark or reset it. If mls qos is enabled globally on any switch in the path between the Cisco Smart Care Network Appliance and the client PC with Reflector software, the ingress port on those switches for this path must be set to trust the DSCP marking. Likewise, if service policies are applied to interfaces on the path, these policies must preserve the marking. This setup helps ensure that this setting is not remarked or reset, and that the RTP packets are queued appropriately for accurate results.

3.7.4 Queuing and Scheduling
Synthetic voice traffic from the VQM session must be directed to the same queue in both switches and routers as the real voice traffic. Best-practice design guidelines advocate matching such real-time packets to be directed into the priority queue on both routers and switches.


3.7.5 Admission Control
This feature does not integrate with locations- or gatekeeper-based Call Admission Control (CAC). Hence it is important to provision the required bandwidth needed for the measurement in the infrastructure devices.

3.7.6 Provisioning Required Bandwidth

Note: Regardless of whether or not QoS is configured in the network and regardless of the types of traffic in the existing network, it is mandatory that you ensure that the required bandwidth for assessment or monitoring has been provisioned in the infrastructure between the Network Appliance and the Reflector(s), at all times during the voice quality measurement. If not, the infrastructure device will not have sufficient bandwidth in its queues during times of congestion and will cause packets to be dropped. Provisioning the additional bandwidth is especially critical if the network is QoS enabled with voice deployed through IP phones. Because the synthetic packets are marked Expedited Forwarding, the infrastructure devices will honor the marking and direct it to the priority queue. In the absence of bandwidth in this queue and with no mechanism to discriminate the measurement packets from those from an IP phone, both the synthetic and the IP phone voice packets will be dropped. As to be expected, if this occurs in a converged network, the quality of all voice calls will be affected, including that of end-user voice conversations.

Please refer to the “QoS Requirements of VoIP” section in the Enterprise QoS SRND document located at: http://www.cisco.com/go/srnd to determine the bandwidths that need to be provisioned on links. The bandwidth provisioned must include the Layer 2 overheads for a call generated at a rate of 50 packets per second.
4. **Use Cases and Reports**

These use cases assume that the Reflector software has already been installed in PCs in the customer network. After the software is installed, each Reflector must be added through the portal by clicking on “Add Reflector” in “Reflector Management” under the Administration section of that customer, specifying an identifier and the IP address of the PC. The identifier can be any name that helps easy identification. Default port assignments can also be changed here. Once the Reflector is registered, assessments can begin between the Network Appliance and the Reflector.

4.1 **Voice Quality Assessment**

Assessing the voice readiness of an infrastructure has three objectives:

- Assess the quality of voice calls prior to voice traffic deployment
- Assess the effect of voice traffic on existing applications
- Implicitly, the first two assess the effectiveness of the QoS policies

These assessments are typically run for a period of time that covers the peaks of network usage to ensure that an acceptable voice quality will always be obtained over a given link for a given number of calls and for a particular codec type, regardless of the use by other applications. The VQM feature allows you to schedule a voice assessment every 10 minutes, with each assessment lasting up to 590 seconds, when the synthetic traffic is injected into the network. This setup provides an almost continuous assessment of voice quality.

At the end of the assessment, you can look at the summary graph showing the averaged values of round-trip delay, round-trip jitter, round-trip packet loss, and the MOS calculated based on these parameters. You can also look at the individual data points that were averaged to display the graph. The individual data points give you access to the granular detail.

**Sample Case:** Symptoms of non-voice packets intermittently entering the priority queue are causing high delay, high jitter, and some packet losses.

The following screenshots describe the process of executing the assessment.

**Step 1. Initiating Voice Quality Assessment**

Figure 8 shows the section of the portal that performs this function; it is available under the “Schedule” option.

**Figure 8. Initiating Scheduled Runs to Measure Voice Quality**
Step 2. Entering the parameters

The assessment is based on a scheduled run to a single Reflector, using the G.729 codec every 10 minutes for a total of 2 hours, where each run lasted 590 seconds (Figure 9).

**Note:** Although the example uses a single Reflector, you can use multiple Reflectors for the assessment.

Figure 9. Parameters for the Scheduled Run (test executed for 590 seconds every 10 minutes)

Step 3. Click an action for the Notification Message

The portal notifies you about the provisioning of bandwidth requirements and the infrastructure requirement to not reset or remark the DSCP (Figure 10).

Figure 10. Message About Ensuring Bandwidth Provisioning and DSCP Markings Prior to the Run
Step 4. Viewing report

When the assessment is complete, the Quality Monitor tab of the portal under Voice (Figure 11) will display the results. By default, it displays the results for the last 24 hours for both codecs. By selecting the date and time range and the codec and then clicking “Get Report”, you can narrow the results down to the particular assessment run.

Figure 11. Clicking the Quality Monitor Tab to View the Report

The assessment report is shown in Figure 12. The report indicates minimal packet losses, but a good overall score. It is important to note that these graphs are based on average values. It is strongly recommended that you select View Details. The granular information, illustrated in Figure 13, can expose other problems.
Step 5. Viewing detailed report

Clicking View Details gives the report shown in Figure 13.

**Figure 13. Scheduled Run Report Showing Granular Detail**

**Observation:** This report clearly indicates infrastructure problems causing intermittent high delay and jitter and, to a certain extent, packet losses too. Although the average values are within best-practice limits, the highlighted areas indicate that there were times when delay and jitter were outside of the limits and thus require further investigation into the QoS setup.

**Note:** We strongly recommend that you select View Details to look for results that could point to intermittent problems, as demonstrated in this example.
**Note:** The out-of-bound values are highlighted in Figure 13 to help you. The actual report does not show them with these highlighted red circles.

**Summary:** This case demonstrates the need and utility of the Assessment function of the VQM that can help you find “intermittent” infrastructure problems before production cut-over. Your customers also can gain an understanding of how the voice traffic affects the data applications. However, if voice over IP traffic had been cut-over to production, voice quality would either be degraded or unacceptable and productivity will be affected until the root cause is identified and fixed.

4.2 **Voice Quality Monitoring**

You and your customers can continually monitor the network for voice quality to try to detect symptoms of deviations of best-practice voice quality parameters in a converged network. In fact, you should continually monitor a voice-operational network in order to detect any symptoms of problems for the voice traffic.

Typically, monitoring and assessment are different in two respects:

- The length of time specified for monitoring is generally much shorter.
- Only one voice call is simulated to each remote site when monitoring.

VQM allows a monitoring time period as low as 10 seconds for each run, and you can schedule each run at a frequency of 10 minutes or more. The result is low network usage for monitoring purposes.

Apart from the parameters stated previously that you will choose prior to scheduling the service, the type and number of reports generated for assessment and monitoring are identical. The required steps to initiate either assessment or monitoring on the portal are also identical. They were covered in the previous section.

4.3 **Immediate Runs for Verifications and Troubleshooting**

VQM also allows you to perform an immediate assessment for voice quality, rather than as a scheduled job, so you can quickly detect failure points. Some cases for the use of the quick, immediate run is when you have implemented a QoS policy and want a quick test for its effectiveness or you are fine-tuning the QoS policy to troubleshoot a problem and want to have a quick assessment to determine if the changes were effective.
Sample case: A configuration problem has caused packet losses.

The following screenshots describe the process of executing the assessment.

Step 1. Initiating Voice Quality Assessment

Figure 14 shows the section of the portal that performs this assessment; it is available as the Run Now option.

Figure 14. Initiating Immediate Runs to Measure Voice Quality

Step 2. Entering the parameters

The assessment is based on an immediate run to a single Reflector, using the G.711 codec for 20 seconds. Figure 15 illustrates this assessment.

Note: Although this example selects a single Reflector, you can also use multiple Reflectors.

Figure 15. Parameters for the Immediate Run (test executed for 20 seconds)
Step 3. Click an action for the Notification Message

The portal notifies you about the provisioning of bandwidth requirements and the infrastructure requirement to not reset or remark the DSCP (Figure 16).

Figure 16. Message About Ensuring Bandwidth Provisioning and DSCP Markings Prior to the Run

Step 4. Viewing report

When the assessment is complete, the link to the “Last run report” (Figure 17) shows the details of the assessment.

Figure 17. Clicking to View the Last Run Report
Figure 18 shows the assessment report.

**Figure 18.** Last Run Report Showing Packet Losses and a Bad MOS

![Last Run Report](image)

**Observation:** The report clearly indicates numerous packet losses, resulting in a very low MOS.
Step 5. Viewing detailed report

Selecting View Details displays the values for individual data points. Although the graph shows the average values, the details include the minimum and maximum values, as well as the number of packets that were lost. Figure 19 shows the results.

Figure 19. Show Details Report for Granular Information

<table>
<thead>
<tr>
<th>Site</th>
<th>Reflect</th>
<th>Codec</th>
<th>Start Time</th>
<th>Duration (Seconds)</th>
<th>Result</th>
<th>Delay Min</th>
<th>Delay Max</th>
<th>Delay Avg</th>
<th>Jitter Min</th>
<th>Jitter Max</th>
<th>Jitter Avg</th>
<th>Lost Packets (%)</th>
<th>Packet Loss (%)</th>
<th>MOS</th>
</tr>
</thead>
<tbody>
<tr>
<td>North Sydney</td>
<td>10.6.1.2.25</td>
<td>711</td>
<td>06/01/08</td>
<td>20</td>
<td>Success</td>
<td>15</td>
<td>27</td>
<td>17</td>
<td>0</td>
<td>19</td>
<td>0</td>
<td>199</td>
<td>20.01</td>
<td>2.14</td>
</tr>
<tr>
<td>Close</td>
<td></td>
<td></td>
<td>12:10:20</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Problem analysis: On further investigation, it was determined that an incorrect fragment size over a Frame Relay link was causing packet losses. When this problem was fixed, the test was executed again to confirm that it was fixed. Figure 20 shows these results as a graph and Figure 21 provides additional detail. Note that without such a tool, we would not have even known that there was a failure point in the configuration. Most likely it would have surfaced after the production cutover.

Figure 20. Last Run Report Without Packet Losses and a Good MOS
Summary: This case demonstrates the need and utility of the Assessment function of the VQM that can help you proactively identify the presence of permanent infrastructure problems very quickly. However, if voice had just been put into production, the problem would have surfaced after cutover and affected productivity for the length of time it took to troubleshoot the problem.

Although you can use the Immediate Run as a quick assessment to verify and troubleshoot configurations, a thorough assessment as given in Voice Quality Assessment is necessary to identify intermittent problems.

5. Specifications

Table 1. Voice Quality Monitor

<table>
<thead>
<tr>
<th>Device</th>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Smart Care Network Appliance</td>
<td>Maximum number of concurrent calls from the Appliance</td>
<td>20</td>
</tr>
<tr>
<td></td>
<td>Minimum duration for Immediate runs</td>
<td>10 seconds</td>
</tr>
<tr>
<td></td>
<td>Maximum duration for Immediate runs</td>
<td>30 minutes</td>
</tr>
<tr>
<td></td>
<td>Minimum duration for Scheduled runs</td>
<td>10 seconds</td>
</tr>
<tr>
<td></td>
<td>Maximum duration for Scheduled runs</td>
<td>590 seconds</td>
</tr>
<tr>
<td></td>
<td>Intervals for Scheduled runs</td>
<td>Minimum 10 minutes; no maximum limit</td>
</tr>
<tr>
<td></td>
<td>Supported codecs</td>
<td>G.711 and G.729</td>
</tr>
<tr>
<td></td>
<td>Traffic injection rate per call</td>
<td>50 packets per second</td>
</tr>
<tr>
<td></td>
<td>Bandwidth used at Layer 3</td>
<td>80 kbps in each direction for G.711</td>
</tr>
<tr>
<td></td>
<td></td>
<td>24 kbps in each direction for G.729</td>
</tr>
<tr>
<td></td>
<td>Bandwidth used at Layer 2</td>
<td>Refer to the “QoS Requirements of VoIP” section in the Enterprise QoS SRND document located at <a href="http://www.cisco.com/qo/srnd">http://www.cisco.com/qo/srnd</a>.</td>
</tr>
<tr>
<td></td>
<td>Packet marking</td>
<td>Expedited Forwarding or DSCP 46 for RTP streams, Best Effort or DSCP 0 for TCP connections</td>
</tr>
<tr>
<td>Reflector</td>
<td>Platform support for Reflectors</td>
<td>Windows XP SP2, Windows 2000</td>
</tr>
<tr>
<td></td>
<td>Recommended CPU</td>
<td>1.6-GHz Pentium 4</td>
</tr>
<tr>
<td></td>
<td>Recommended memory</td>
<td>1-GB RAM</td>
</tr>
<tr>
<td></td>
<td>Minimum disk space</td>
<td>10 MB</td>
</tr>
<tr>
<td></td>
<td>Windows software component</td>
<td>QoS Packet Scheduler</td>
</tr>
<tr>
<td></td>
<td>Maximum number of concurrent calls per Reflector</td>
<td>1</td>
</tr>
</tbody>
</table>
6. **Glossary of Terms**

**DSCP:** Differentiated services code point: A field in the IP packet that provides a mechanism for the infrastructure devices to offer differentiated treatment to application traffic, based on the value of this field.

**Codec:** Coder/decoder: A piece of hardware or software that takes an audio or video signal and converts it to a digital format, and conversely.

**Converged network:** A network that transports more than just data applications over an IP network. Other applications include real-time applications such as voice and video.

**Delay:** The time elapsed between the time a packet was sent from the source and the time it was received at the destination.

In the case of VQM, all delay measurements are round-trip from the Network Appliance to the Reflector and back.

**Jitter:** The variation in delay between consecutive packets measured at the receiver.

In the case of VQM, all jitter measurements are round-trip from the Network Appliance to the Reflector and back.

**MGCP:** Media Gateway Control Protocol: A protocol used for call signaling in a VoIP infrastructure.

**MOS:** Mean opinion score: A common benchmark used to determine the quality of sound produced by specific codecs.

**Packet loss:** The number of packets lost in transit between the source and destination.

In the case of VQM, all packet-loss measurements are round-trip from the Network Appliance to the Reflector and back.

**QoS:** Quality of service: Refers to the ability of a network to provide improved service to selected network traffic over various underlying technologies.

**Reflector:** Software supplied by Cisco Systems, Inc. as part of the VQM feature that can be installed on desktops or laptops meeting minimal requirements on complying operating systems. The software returns the traffic received from the Network Appliance back to the appliance.

**SCCP:** Skinny Call Control Protocol: A protocol used for call signaling in a VoIP infrastructure.

**SRND:** Solutions Reference Network Design: A design containing best-practice recommendations on numerous technology areas and published by Cisco Systems, Inc. The recommendations are available at: [http://www.cisco.com/go/srnd](http://www.cisco.com/go/srnd). This document specifically refers to the one on Enterprise QoS.

**VQM:** Voice Quality Monitor: A new feature with Cisco Smart Care 1.1 that includes both Assessment and Monitoring of voice traffic.