The Power of We™

TECHNICAL WHITE PAPER

Audio Quality issue with Communication Server 1000 Network

Objectives and Overview

The Audio/Voice forms the very basis for every voice call. If there is a deterioration of the same, there will be no satisfaction to either party. The problem can increase if there are more people added to the call and conferences are the ones that are badly affected.

This whitepaper deals with Key factors which drive voice quality on CS1000 Network and possible steps that will help in reducing or isolating Audio quality issue quickly.

This document is applicable to all CS1000 Processor Types and Releases.

Terminologies

SBWM---- Shared Bandwidth Management
CS1000 ---Communication Server 1000
MGC ------ Media Gateway Controller
LAN ------Local Area Network
WAN --- Wide Area Network
ELAN ------Embedded LAN
TLAN ------ Telephony LAN
SS ---------- Signaling Server
VoIP -------Voice Over IP
QoS ------ Quality of Service
BQ ------ Best Quality
BB ------ Best Bandwidth
VAD ----- Voice Activity Detection
SM ----- Session manager
PNI ---- Private Network Identifier

Abstract

This whitepaper gives insights on the various kinds of systems that we find around the globe, the voice quality problems associated with each of the call setup and how to achieve the best quality. We will detail the best practices to be followed.

There are two major types of networks as far as we can categorise namely the TDM networks that have been since time immemorial and the VoIP networks.

Let us consider first the VoIP networks that are recent and most used networks at many customer sites or at least are getting migrated from the TDM networks. Please note that the below recommendations are mostly for the VoIP networks but some of them apply for the TDM networks as well.

To achieve excellence in voice quality, we need to consider the following elements that form the performance criteria.

- A properly engineered network
- Good network equipment and redundancy
- Adequate bandwidth for peak usage
- Use of QoS mechanisms
- Ongoing monitoring and maintenance

If these elements are not present, voice quality will suffer.

The network should also meet the following specifications:

1. End-to-end packet delay: Packet delay is the point-to-point, one-way delay between the time a packet is sent to the time it is received at the remote end. It is comprised of delays at the Voice Gateway Media Card, Internet Telephone, and the IP network. To minimize delays, the IP Telephony node and Internet Telephone must be located to minimize the number of hops to the network backbone or WAN.

Important:
Avaya recommends an end-to-end delay of <= 50 ms on the IP network to ensure good voice quality. The 50 ms does not include the built-in delay of the Voice Gateway Media Card and IP Phone.

2. End-to-end packet loss: Packet loss is the percentage of packets sent that do not arrive at their destination. Transmission equipment problems, packet delay, and network congestion cause packet loss. In voice conversation, packet loss appears as gaps in the conversation. Sporadic loss of a few packets can be more tolerable than infrequent loss of a large number of packets clustered together.

Important:

- For high-quality voice transmission, the long term average packet loss between the IP Phones and the MGC/Voice Gateway Media Card TLAN network interface must be < 1%, and the short term packet loss must not exceed 5% in any 10-second interval.

- Avaya strongly recommends that you use the G.711 codec with the following configuration:
  - end-to end delay less than 150 ms one way (network delay + packetization delay + jitter buffer delay < 150)
  - packet loss less than 0.5% (approaching 0%)
  - maximum jitter buffer setting for IP Phone as low as possible (maximum 100 ms)

- Packet loss on the ELAN network interface can cause
  - communication problems between the Call Server and the Voice Gateway Media Cards
  - lost SNMP alarms
  - other signaling related problems

- Because the ELAN network is a Layer 2 Switched LAN, the packet loss must be zero. If packet loss is experienced, its source must be investigated and eliminated. For reliable signaling communication on the ELAN network interface, the packet loss must be < 1%.

Estimate voice quality

The E-Model Transmission Planning Tool produces a quantifiable measure of voice quality based on relevant factors. For more information about the E-Model and its application, see the ITU-T recommendations E.107 and E.108.

A simplified version of the E-Model is applied to provide an estimate of the voice quality that the user can expect, based on various configuration choices and network performance metrics.

The simplified E-Model is as follows: $R = 94 – Ic – Id – Ip$

- Ic = Codec Impairment (see Table 1: Impairment factors of codecs)
- Id = delay impairment (see Table 2: Impairment factors due to network delay)
- Ip = packet loss impairment (see Table 3: Impairment factors due to packet loss)

Note: This model takes into account some characteristics of the IP Phone and; therefore, the impairment factors are not identical to those shown in the ITU-T standards.

See Table 4: R value translation for the translation of R values into user satisfaction levels.

Table 1 : Impairment factors of codecs

Codec	Codec impairment (lc) (ms frames)
G.711	0
G.711 a-law	8
G.711 mu-law	0
G.723.1	4
G.729A G.729AB	18
G.729A/AB	11 - 20 or 30
G.729A/AB	16 - 40 or 50
G.723.1 (5.3 kbit/s)	19
G.723.1 (6.3 kbit/s)	15

Table 2 : Impairment factors due to network delay

Network delay* (ms)	Delay impairment (ld)
0–49	0
50–99	5
100–149	10
150–199	15
200–249	20
250–299	25

* Network delay is the average one-way network delay plus packetization and jitter buffer delay.

Table 3: Impairment factors due to packet loss

Packet loss (%)	Packet Loss Impairment (lp)
0	0
1	4
2	8
4	15
8	25

Table 4 : R value translation

R Value (lower limit)	MOS	User Satisfaction
90	4.5	Very satisfied
80	4.0	Satisfied
70	3.5	Some users dissatisfied
60	3.0	Many users dissatisfied
50	2.5	Nearly all users dissatisfied
0	1	Not recommended

Use Table 5: QoS levels to estimate the voice quality level based on performance measurements of the intranet. To limit the size of this table, the packet loss and one-way delay values are tabulated in increments of 1% and 10 ms, respectively. The techniques used to determine and apply the information in this table are proprietary to Avaya.

Table 5 : QoS levels

Network Delay (ms)	Packet Loss (%)	Voice quality level		
		G.711 20	G.729A/AB 30	G.723.1 (6.3 kbit/s) 30
49	0	excellent	good	fair
49	1	excellent	fair	fair
49	2	good	fair	Fair
49	4	fair	poor	poor
49	8	poor	Not recommended	Not recommended
50 - 99	0	excellent	fair	fair
99	1	good	fair	fair
99	2	good	fair	poor
99	4	fair	poor	poor
99	8	poor	Not recommended	Not recommended
100 - 149	0	good	fair	poor
149	1	good	fair	poor
149	2	fair	poor	poor
149	4	fair	poor	not recommended
149	8	poor	not recommended	not recommended
150 – 199	0	fair	Poor	poor
199	1	Fair	Poor	Good
199	2	Fair	Poor	Fair
199	4	Poor	not recommended	not recommended
199	8	not recommended	not recommended	not recommended

200 – 249	0	Poor	not recommended	not recommended
249	1	Poor	not recommended	not recommended
249	2	Poor	not recommended	not recommended
249	4	not recommended	not recommended	not recommended
249	8	not recommended	not recommended	not recommended
250 - 299	0	Poor	not recommended	not recommended
299	1	Poor	not recommended	not recommended
299	2	Poor	not recommended	not recommended
299	4	not recommended	not recommended	not recommended
299	8	not recommended	not recommended	not recommended

Note: The QoS levels are equivalent to the following MOS values: excellent = 4.5, good = 4, fair = 3, poor = 2, and not recommended = less than 2.

Quality of Service

To ensure consistent voice quality, QoS must be supported on the platforms that transport VoIP. Consider the following list to provide QoS:
- Bandwidth Management
- packet classification
- DiffServ
- fragmentation
- traffic shaping
- queueing mechanisms provided by the platform

If appropriate QoS mechanisms are not supported by the platform, an upgrade can be required.

QoS mechanism

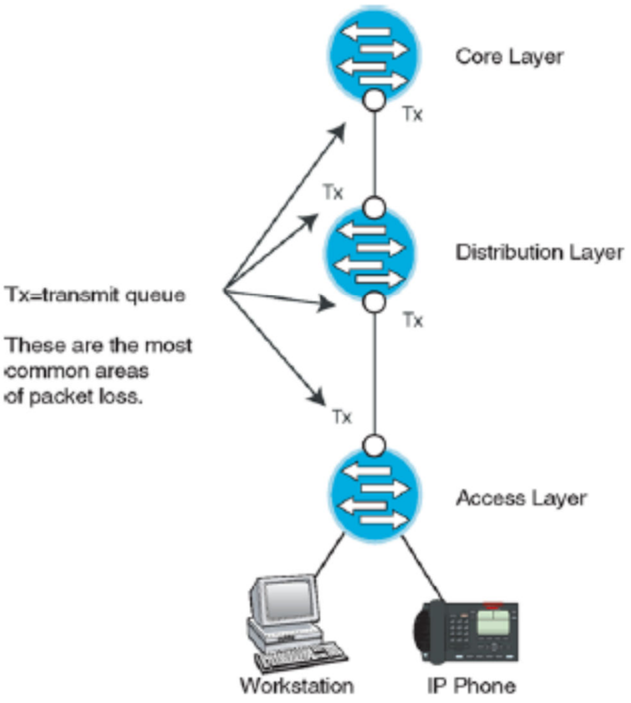
An IP network must be properly engineered and provisioned to achieve high voice quality performance. The network administrator should implement QoS policies network-wide, so voice packets receive consistent and proper treatment as they travel the network. IP networks that treat all packets the same are called best-effort networks. In such a network, traffic can experience different amounts of delay, jitter, and loss at any given time. This can produce the following problems:
- speech breakup
- speech clipping
- pops and clicks
- echo

A best-effort network does not guarantee bandwidth at any given time. The best way to guarantee bandwidth for voice applications is to use QoS mechanisms in the intranet when the intranet is carrying mixed traffic types. QoS mechanisms ensure bandwidth is 100% available at most times, and maintain consistent, acceptable levels of loss, delay, and jitter, even under heavy traffic loads. QoS mechanisms are extremely important to ensure satisfactory voice quality. If QoS mechanisms are not used, there is no guarantee that the bandwidth required for voice traffic is available. For example, a data file downloaded from the intranet could use most of the WAN bandwidth unless voice traffic has been configured to have higher priority. If the data file download uses most of the available bandwidth, it causes voice packet loss and; therefore, poor voice quality.

Apply QoS mechanisms to the following VoIP media and signaling paths:
- TLAN connections
- VoIP traffic between IP Deskphones
- VoIP traffic between IP Deskphones and Voice Gateway Media Cards on the TLAN subnet

Important:
Avaya strongly recommends that you implement suitable QoS mechanisms on any IP network that carries VoIP traffic.

QoS problem locations:



Potential Uplink Problem areas

The QoS process

Packet handling on a QoS-enabled network consists of three stages:
1. Classification
2. Marking
3. Queueing, also known as Forwarding

To implement QoS on an IP network, all packets entering the IP network must be classified and marked. The packets are then placed into transmission queues of a certain priority. Packets in high-priority queues are transmitted before packets in best-effort lower priority queues. VoIP packets no longer have to compete with best-effort data packets for IP network resources. Typical QoS implementations protect call quality by minimizing loss, delay, and jitter. Bandwidth cannot be assured without the use of some type of reservation protocol, such as Resource Reservation Setup Protocol (RSVP).

Codec selection

Codec refers to the voice coding and compression algorithm used by DSPs. Each codec has different QoS and compression properties.

Codec	Payload size
G.711 A/mu-law	10 millisecond (ms), 20 ms, and 30 ms
G.711 Clear Channel	Supported on the MC32S and DSP d/bs (Mindspeed) and not on the MC32 Cards
G.722	10 ms, 20 ms, 30 ms, and 40 ms
G.723.1	30 ms, although it can limit the number of DSP channels available
G.729 A	10 ms, 20 ms, 30 ms, 40 ms, and 50 ms
T.38 for fax	Supported for fax calls on gateway channels

Table 6 : Supported Codecs

To ensure optimal voice quality, minimize the number of compression and decompression stages use a G.711 codec wherever bandwidth permits.

The Call Server considers BQ codec as G.711 and BB as either G.729 or G.723 (assuming that both parties support it).

Each codec has specific parameters that must be configured, such as packetization delay and voice activity detect. These parameters are configured on the Signaling Server using Element Manager.

Ensure the voice codec images on all sites match by using the same software version at each site. Use the same codecs, packetization, and jitter buffer settings on each system. There is a potential to degrade the voice quality if codecs are cascaded. This can occur when there are multiple compression and decompression stages on a voice call. The more IP links used in a call, the more delay is added, and the greater the impact on voice quality.

The following applications and devices can impact voice quality if you use a compression codec, such as G.729A:

- Voice mail, such as Avaya CallPilot, introduces another stage of compression and decompression.
- Conferences can double the number of IP links.
- IP Trunks can add additional stages of compression and decompression.

Important:

Avaya recommends that all cards in a system have the same image. If multiple codec images are used in a VoIP network, the calls default to the G.711 group when the originating and destination codecs differ.

If there are multiple nodes on a system and the same codec is selected on more than one node, ensure that each node has the same voice payload size configured for the codec.

Note:

The G.711 codec does not support VAD if the bandwidth policy is configured as BQ. VAD is only supported if you configure the bandwidth policy as BB.

For more information about codecs, see Avaya Signaling Server IP Line Applications Fundamentals, NN43001-125.

Bandwidth demand

VoIP can use an existing WAN data network to save on interoffice toll calls. However, offices often connect over low-bandwidth WAN connections, so special considerations must be made when you add VoIP over a bandwidth-limited connection.

When VoIP calls are active, routers configured with QoS (which prioritizes voice traffic over data traffic) reduce the data traffic throughput by the amount of bandwidth used for the VoIP call. This reduces the data traffic throughput to a possibly unacceptable level. Adding VoIP to the existing WAN data network might require an increase in the WAN bandwidth.

VoIP bandwidth depends on the following:

- type of codec used
- Voice Activity Detection (VAD), if used; also known as Silence Suppression
- packetization rate (voice sample size)
- IP/UDP/RTP encapsulations

- RTP Header Compression, if used
- Layer 2 (link layer) protocol overhead for the specific link the voice traffic is traversing.

Depending on the link protocol used and the options invoked, the link protocol adds the following to each VoIP packet:
- 5 to 6 octets (FR)
- 7 to 8 octets (PPP)
- 18/22:26/30:38/42 octets (802.3 LAN – with or without 802.1Q/802.1p 8-octet preamble and 12-octet interframe gap)

The extra octets create an additional overhead of 2 kbit/s (5-octet FR) to 16.8 kbit/s (42-octet 802.3 LAN) for each VoIP call.

ATM has its own overhead requirements. Due to the fixed cell size of 53 octets, the additional overhead varies widely, depending on the codec and packetization rate used.

VoIP Bandwidth Management zones

Bandwidth Management zones divide IP Phones and Voice Gateway Media Cards into logical groups (zones) to determine codec selection and Bandwidth Management. Zones are configured after the QoS managed IP network has been designed.

As calls are made, the Call Server software chooses a codec to be used for the call based on the zone configuration (inter or intra). The software also tracks bandwidth usage within each zone and between zones. When making an interzone call, the codec is selected according to interzone policy. This policy is a configurable value and can be configured to BQ or BB.

Each IP Phone and Voice Gateway Media Card port is assigned a zone number in which it resides. Place all IP Phones and Voice Gateway Media Cards at a site in the same zone (for example, configure IP Phones and Voice Gateway Media Cards at the same Branch office in the same Media Gateway 1000B [MG 1000B] zone).

Virtual Trunk routes also allow configuration of a zone. A single Call Server considers calls sent from a Virtual Trunk as terminated on that Virtual Trunk. Therefore, Virtual Trunks should not be in the same zones as any IP Phones or Voice Gateway Media Cards.

Place all virtual trunk routes in the same zone for all main office and MG 1000B systems. Virtual trunk zones are not for Bandwidth Management except when they connect to a third-party gateway. Configure virtual trunk intrazone and interzone policy to Best Quality (BQ) and intrazone and interzone bandwidth to the maximum value of 1 Gbit/s (1 000 000 kbit/s).

Bandwidth is already managed within the IP Phone zone.

Bandwidth management zones can be network-wide but this is dependent on your VPNI setting and zone number. If the VPNI setting and zone number match on the originating system and terminating system the call servers will treat the call as INTRAZONE, even though its traversing between those two systems. The following table captures the different cases of VPNI settings and zone numbering.

Originating VPNI	Originating Zone	Terminating VPNI	Terminating Zone	Choose policy
1	100	1	100	Intrazone
1	100	1	150	Interzone
1	100	5	100	Interzone
1	100	5	200	Interzone

Table 7 : VPNI Settings and Zone numbering

Interzone versus Intrazone

For Bandwidth Management, a network of Call Servers is divided into zones, typically one Zone for each Call Server. Calls between zones are interzone calls and calls within a Zone are intrazone calls. Typically, intrazone calls travel over LANs on which bandwidth is widely available. Conversely, interzone calls travel over WANs on which bandwidth can be limited and expensive. Distinguish between intrazone and interzone VoIP calls for increased control over VoIP traffic.
The following call scenarios describe how each call type works.

Intrazone call
- An intrazone call is made between two endpoints on the same Call Server.
- The intrazone treatment is consulted to determine whether it is Best Bandwidth or Best Quality.
- Based on the intrazone treatment, the correct codec is selected.
- The intrazone bandwidth table is also consulted to determine if there is enough intrazone bandwidth to support the call. If there is not enough bandwidth, the call is blocked.

Interzone call
- An interzone call is made between two Call Servers.
- An interzone call is made between an endpoint in one Zone to another endpoint in a different Zone. The Zone of the endpoints are compared to the Virtual Trunk Zone as the two zones are different; the call is an interzone call.

- The interzone treatment is consulted to determine whether it is Best Bandwidth or Best Quality.
- Based on the interzone treatment, the correct codec list is selected for the call setup.
- The interzone bandwidth table and the virtual trunk bandwidth limit are also consulted to determine if there is enough intrazone bandwidth to support the call. If there is not enough bandwidth, the call is blocked, or alternate treatment is provided.

Shared Bandwidth Management

The SBWM feature allows sharing of bandwidth between multiple servers and/or bandwidth consumers in a single location. Bandwidth is dynamically allocated between video and voice by Avaya Aura Session Manager (SM), which shares the bandwidth management responsibilities with all SIP entities using a common interface PUBLISH API. This interface allows Aura SM to share bandwidth management responsibilities with the SIP entities and to inform SIP entities when the overall audio or multimedia thresholds are crossed.

On the Call Server, the calculation of bandwidth and Call Admission Control (CAC) is split between the originating and terminating sides of a call; the terminating Call Server performs bandwidth management for both the originating and terminating sides of the call. The originating Call Server does not perform any CAC or bandwidth management for outgoing SIP calls. The terminating Call Server performs CAC for both the originating and terminating locations.

Avaya Aura SM uses a bandwidth publish request mechanism to account for calls. The publish request mechanism allows the Call Server to pre-allocate a small pool of bandwidth from the Avaya Aura SM. In order to minimize the number of bandwidth publish requests, the Call Server pre-allocates bandwidth a block of bandwidth at time, and not on a per call basis. The Call Server uses this block of bandwidth to perform CAC and bandwidth accounting locally.
A key to managing and implementing the Shared Bandwidth Management feature is the amount of bandwidth that the Call Server pre-allocates from the Avaya Aura SM, and determining when the Call Server should return the bandwidth to the Session Manager. The amount of bandwidth that the Call Server pre-allocates is called the Reserved Bandwidth Block Size.

The Call Server pre-allocates and de-allocates bandwidth in blocks equal to the Reserved Bandwidth Block Size. When the Call Server detects that the available bandwidth in the local pool is less than the Reserved Bandwidth Block Size, it sends a publish request for another block of bandwidth, which is equal in size to the Reserved Bandwidth Block Size. If the Call Server detects that the available bandwidth is greater than two block sizes, the Call Server gives a block of bandwidth back to the Avaya Aura SM, equal in size to the Reserved Bandwidth Block Size. The objective is to maintain the amount of available bandwidth between one and two block sizes. The maximum pre-allocated bandwidth on the Call Server is twice the Reserved Bandwidth Block Size.

The Avaya Aura SM manages bandwidth using the concept of locations. The location concept is analogous to bandwidth zones on the Call Server. In order to comply with the Avaya Aura SM location scheme, the Call Server uses zone names. A zone name corresponds to a location on the Session Manager.

SBWM on CS 1000 requires the following configuration:

- You must add zone names that correspond to Avaya Aura SM location names.
- You must enable SBWM on outgoing SIP routes.
- You must determine the Reserved Bandwidth Block Size.

Note:

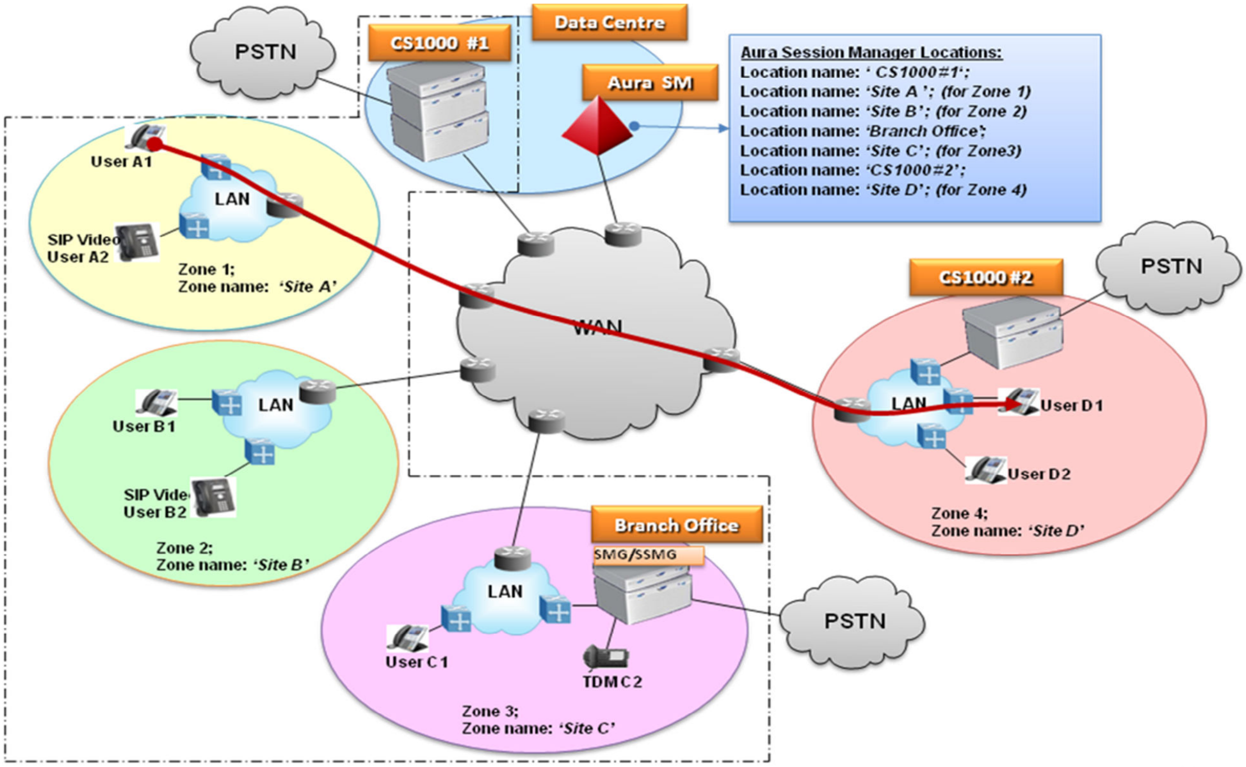
In order for SBWM to work correctly, all zone data must be replicated in all the Call Servers in a peer group. Use the export zone data feature to transfer the zone data from one Call Server to all the other Call Servers in the peer group. All Call Servers in a peer group must enable SBWM for the feature to work properly.

Avaya Aura SM requires the following configuration:

- Configure a SIP entity with the Call Admission Control option. This configuration tells Avaya Aura SM not to perform bandwidth calculations and not to make call blocking decisions for calls terminated to that SIP Entity, because the SIP Entity calculates bandwidth.
- Configure the SIP entity as a shared bandwidth manager, which tells the Avaya Aura SM that this SIP entity supports the Publish API interface.

For more information about configuring Avaya Aura Session Manager, see Administering Avaya Aura ® Session Manager.

Sample Call Flow:


PSTN
CS1000 #1
Data Centre
Aura SM
Aura Session Manager Locations:
Location name: ' CS1000#1';
Location name: 'Site A '; (for Zone 1)
Location name: 'Site B'; (for Zone 2)
Location name: 'Branch Office';
Location name: 'Site C'; (for Zone3)
Location name: 'CS1000#2';
Location name: 'Site D'; (for Zone 4)
User A1
LAN
SIP Video User A2
Zone 1; Zone name: 'Site A'
WAN
CS1000 #2
PSTN
LAN
User D1
User D2
Zone 4; Zone name: 'Site D'
User B1
LAN
SIP Video User B2
Zone 2; Zone name: 'Site B'
Branch Office
SMG/SSMG
LAN
User C1
TDM C2
PSTN
Zone 3; Zone name: 'Site C'
14

- Scenario
  - User A1 on site A makes a call to User D1 on site D.
- Analysis
  - CS1000 #1 allows the outgoing trunk call to be sent out without applying CAC & zone update.
  - CS1000 #1 sends SIP INVITE message to Aura SM
  - Aura SM routes the call to CS1000 #2 adding a plocation header describing the location where the media has originated from
  - CS1000 #2 detects terminating zone 4
  - CS1000 #2 updates zone 4 and zone 1 intra & inter bandwidth usages
  - CS1000 #2 provides CAC for both zone 4 and zone 1
  - If CS1000 #2 detects insufficient bandwidth in either zone 1 or zone 4 the call is to be blocked
  - CS1000 #2 sends both 'Site D' and 'Site A' statistics as a part of Publish Update to Aura SM, after 5 minute time interval is elapsed

Network design assessment

Ensure you fully understand the design of an existing data network before you implement a VoIP network.

For example, assess the network for such things as:
- the distribution of protocols in the network
- the level of QoS on the network
- the link speeds, link types, and link utilization
- the traffic flows in the network

Warning:
Before a Communication Server 1000 system can be installed, a network assessment must be performed and the network must be VoIP ready. If the minimum VoIP network requirements are not met, the system does not operate properly.

Network planning for Bandwidth Management

Perform the following actions before you configure Bandwidth Management in a Communication Server 1000 network:

- Main Office and Branch Office need to have the same VPNI setting to ensure correct bandwidth management control by the Main Office. Another reason to have the same VPNI setting across call servers is to support bandwidth management for Network Wide Virtual Office (NWVO). Also, two systems within the same LAN would require the same VPNI setting to ensure INTRAZONE call treatment.
- Choose unique Bandwidth zone numbers for all Call Servers in the network to use when configuring the endpoints (telephones and gateways) on the Call Server.
- Choose the same zone number for Virtual trunk resources for all Call servers within the same network (for example, Main Office and Branch Office configuration or MG 1000B groups or call servers within one LAN).
- Choose the codecs to enable on each Call Server.
- Identify the interzone codec strategy (BB or BQ) for each zone in the network.
- Identify the intrazone codec strategy (BB or BQ) for each zone in the network.
- Calculate the bandwidth available for intrazone calls for each zone in the network.
- Calculate the available bandwidth for interzone calls for each zone in the network.
- Calculate the available bandwidth for intrazone calls.

Caution:
Service Interruption
If the network is planned so IP Phones use a different route to the main office than the MG 1000B Terminal Proxy Server (TPS), a fault condition can occur. When the MG 1000B TPS can ping the main office but the IP Phone cannot ping the main office due to a network outage, an IP Phone registration can force the telephone into a cycle of registering locally, being redirected to the main office, rebooting and then registering locally again. When this cycle occurs, further diagnose the network outage.

Proactive Voice Quality management

Proactive Voice Quality management (PVQ) allows the user to monitor the voice quality of Voice over Internet Protocol (VoIP) calls on an ongoing basis and detect specific problems when they occur. Alarms and traffic reports are used to implement this.

Four metrics on voice quality are collected on every call: packet loss, latency, jitter, and Rvalue. The metrics are analyzed to determine if an alarm should be generated. The metrics are also aggregated and reported, along with other information, in Traffic Report 16.
The R-level metric is calculated only for those IP Phones equipped with a firmware version of 2.0 or higher.
A PVQ alarm is generated whenever a metric exceeds a given threshold. The thresholds are user defined in LD 117 at a Call Server and propagate throughout the system. Listed in order of increasing severity, the threshold levels include: good, warning, and unacceptable.
The following types of PVQ alarms exist:

- Alarms generated on a per zone basis (zone based) — generated if the aggregate metrics for a particular zone, such as a branch office, exceeds a warning or unacceptable threshold. These alarms are generated by the Call Server.
- Alarms generated on a per call basis — each call is monitored and an alarm generated if any metric meets or exceeds a warning or unacceptable threshold. These alarms are generated by the Signaling Server.

The user can configure a Notification Level to control when and how often an alarm is generated. This capability is useful when many alarms are generated, but most are minor and relate to potential system capacity issues rather than voice quality. It is also useful when a user wants to monitor a particular area of a network, such as a branch office. Notification levels are defined in LD 117.

Network performance measurement tools

Ping and traceroute are standard IP tools that are usually included with a network host TCP/IP stack. QoS measurement tools and packages are commonly available that include delay monitoring tools, which include features like timestamping, plotting, and computation of standard deviation. For information about network performance measurement tools, refer to

- QoS monitoring and reporting tools from NN43001-260
- Proactive Voice Quality management on Page 17
- Avaya IP Phones Fundamentals, NN43001-368

The following measuring tools are based on the Internet Control Messaging Protocol (ICMP):

- Ping — sends ICMP echo requests
- Traceroute — sends packets to unequipped port numbers and processes to create ICMP destination unavailable messages

Both ping and traceroute are basic measuring tools that can be used to assess the IP Line network and are standard utilities that come with most commercial operating systems. Ping is used to measure the round trip delay of a packet and the percentage of packet loss. Traceroute breaks down delay segments of a source destination pair and any hops in between to accumulate measurements.

There are several third-party applications that perform data collection similar to ping and traceroute, but also analyze data and plot performance charts. The use of ping and traceroute to collect data for manual analysis is labor intensive; however, they provide information as useful as the more sophisticated applications.

The following network performance evaluation overview assumes that the ping program is available on a PC, or a network management tool is available to collect delay and loss data and to access the LAN that connects to the router to the intranet.

Evaluating network performance

1. Use ping or an equivalent tool to collect round-trip delay (in ms) and loss (in %) data.
2. Divide the delay by 2 to approximate one-way delay and add 93 ms to adjust for ITG processing and buffering time.
3. Use a QoS chart (Table 5) to predict the QoS categories: Excellent, Good, Fair or Poor.
4. If a customer wants to manage the QoS in a more detailed fashion, rebalance the values of delay compared to loss by adjusting system parameters, such as preferred codec, payload size, and routing algorithm, to move the resulting QoS among different categories.
5. If the QoS objective is met, repeat the process periodically to make sure the required QoS is maintained.

Network availability

Network availability has the most significant effect on QoS. If the network is unavailable, even for brief periods of time, the user or application can achieve unpredictable or undesirable performance levels.

Network availability is dependent on the availability of a survivable, redundant network. A redundant network should include the following elements to ensure survivability:

- redundant devices, such as
  - interfaces
  - processor cards
  - power supplies in routers and switches
- resilient networking protocols
- multiple physical connections, such as copper or fiber
- backup power sources

Media Security

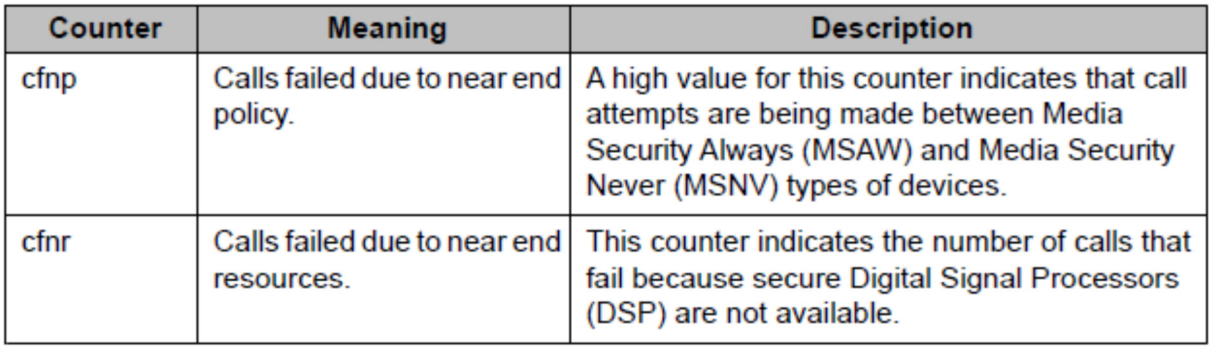
Media Security enables two endpoints capable of Secure Real-Time Transport Protocol (SRTP) connections to engage in secure media exchanges. For calls that pass over IP systems only, Media Security can provide end-to-end encryption of the call if both endpoints can support

SRTP connections. If you configure Media Security to use the Media Security Always CoS, it blocks any calls that cannot be encrypted.

When you assess the reliability of the network, be aware that the Media Security feature, if configured to use the Media Security Always CoS, can block a call if any of the following conditions is valid:

- One of the telephones in the call is an IP Phone registered on the same Call Server as the other endpoint, but does not support Media Security.
- One of the telephones in the call is a nonIP phone on the same Call Server as the other endpoint, but a Voice Gateway TN resource that supports SRTP is not available.
- One of the telephones in the call is configured to use the Media Security Always CoS, and the trunk is an H.323 trunk or a SIP trunk configured to use the Media Security Never CoS.
- One of the telephones in the call is configured to use the Media Security Always CoS, and the far end is an IP Phone, media gateway, or media server that does not support Media Security or is incompatible with the SRTP key exchange protocol used by Avaya Communication Server 1000 SIP Virtual Trunk (VTRK) Gateway.

You can use the Traffic Reports available in LD 2 to determine the cause of a call failure if you suspect Media Security is blocking calls, as shown in Table 8: Traffic reports for blocked calls as below:



Counter	Meaning	Description
cfnp	Calls failed due to near end policy.	A high value for this counter indicates that call attempts are being made between Media Security Always (MSAW) and Media Security Never (MSNV) types of devices.
cfnr	Calls failed due to near end resources.	This counter indicates the number of calls that fail because secure Digital Signal Processors (DSP) are not available.

Table 8: Traffic reports for blocked calls

For more information about Traffic Reports in LD 2, see Avaya Traffic Measurement Formats and Output Reference, NN43001-750. If you suspect calls are being blocked because of Media Security policy restrictions imposed by your system security administrator, contact the security administrator responsible for Media Security configuration policies on your system.
For more information about Media Security, including further recommendations about configuration, see Avaya Security Management Fundamentals, NN43001-604.

DSP and voice quality troubleshooting

General troubleshooting suggestions

Audio problems can be difficult to troubleshoot because often they are affected by user perception. A card that reboots in a certain situation is perceived as a rebooting card; however, a call with slight distortion or echo may be tolerated by some users while considered intolerable by others. The following suggestions can help you with troubleshooting.

Echo

Echo is the most frequently reported audio complaint on the MGC/VGMC product. The first task is to isolate the scenario in which echo is the experienced.

Echo is typically not reported on IP Phone to IP Phone calls. Experience indicates echo usually occurs for calls through the MGC gateway or the VGMC card. One indication that the DSP echo canceller is not working optimally is to try to make a similar call with no MGC/VGMC involved and check if the echo disappears.

If the echo occurs only as a short burst at the beginning of the call, this is caused by the DSP echo canceller converging on the echo, a normal function. This process typically takes a couple of seconds. It is usually not annoying enough to report, but may be reported with a more severe symptom.

Second, if the echo is occurs only on trunk calls, determine with a non-IP Phone (for example, a 3904 digital telephone) if the same calls have echo. The echo may be caused by trunking, CO, or long-distance carrier problems. If the problem occurs mainly with long distance calls, make a call using a calling card for a different carrier and see if the problem occurs. Analog trunks can cause a complex echo that the DSP echo canceller has difficulty converging on. Majority of echo problems on analog trunks are caused by the loss plan and/or balance impedance settings not matching country specific.

Please refer to Transmission Parameters Reference NN43001-282 for more details.

Signal limiter

Echo represents the major impairment in VoIP. Although Avaya Communication Server 1000 has a carrier-grade echo canceller (ECAN) that complies with the G.168 recommendation from the ITU-T, cases still occur where the existing PSTN network involves nonlinear hybrids. In these cases, the ECAN experiences difficulties eliminating echoes generated when the voice signal is at loud levels.

To solve the problem, Avaya CS 1000 uses a signal limiter. The signal limiter (SL) deals intelligently with the voice signal going from CS 1000 system to the PSTN. While preserving the quiet voice signal levels, the signal limiter (SL) adds some attenuation to loud signal levels. Extra attenuation is added when the voice signals become louder.

For versatility, the signal limiter is granular. Several modes of operation exist with only one parameter called SLim. The SLim parameter uses any integer value from 1 to 5. A value of 1 is the most aggressive, while a value of 5 is the least aggressive. A value of 0 means the functionality is disabled, which is the default value when the CS 1000 is installed.

IP Network Troubleshooting Suggestions

Because the IP Phone depends on the IP network to communicate with other IP Phones, problems on the LAN or WAN can cause a variety of voice quality and usage issues. The following are some suggestions to determine if the network is causing problems:

- Make sure the ELAN, TLAN, and node IP addresses are properly configured on the VGMC or Signaling Server. Every card has unique ELAN and TLAN interface IP addresses. The node IP is shared among the cards and is programmed on the TLAN interface of the current Master.

Note:
Use separate subnets for the ELAN and TLAN interfaces.

- ELAN (Embedded LAN): carries maintenance, administration, and alarm data between EM and the VGMC/Signaling Servers. It also carries RUDP/TCP signaling traffic between the Call Server and the VGMC/Signaling Servers. All ELAN addresses for all nodes must be on the same subnet and must be the same as the Call Server CPU subnet.

- TLAN (Telephony LAN): carries RUDP and RTP packet data between VGMC/ Signaling Server and IP Phones. The TLAN addresses in all devices in a node must be on the same subnet.

- CLAN (Customer LAN): regular customer LAN for PCs. Protect the VGMC/Signaling Server TLAN from the broadcast traffic that can regularly occur on the CLAN by isolating it to its own VLAN. Turn off Spanning Tree, or configure ports as fast port enable, fast learning.

- Node IP (on the TLAN subnet): used by IP Phones to register with the node. This address is shared by the devices; it is assigned to the TLAN interface of the current Master.

TLAN packet loss errors

The VGMC/Signaling Server software contains detection mechanisms for RTP packet loss. The impact of packet loss varies, but even single lost packets can cause audible clicks, while high packet loss sounds like choppy speech or periods of silence. Packet loss is usually due to a router discarding the RTP packets when the network is busy.

Perform the following tasks:
- Verify the ports of the router/switch the TLAN and IP Phone are connected to are configured as one of the following (in highest to least desirable order):
- Autonegotiation: this is the recommended setting. The VGMC/Signaling Server TLAN interface and the IP Phone autosense the speed and autonegotiate the half or full duplex setting. Setting the switch or router port to do the same means the fastest possible connection negotiate without intervention.

- Manual setting: 100BaseT, half duplex
- Manual setting: 10BaseT, half duplex

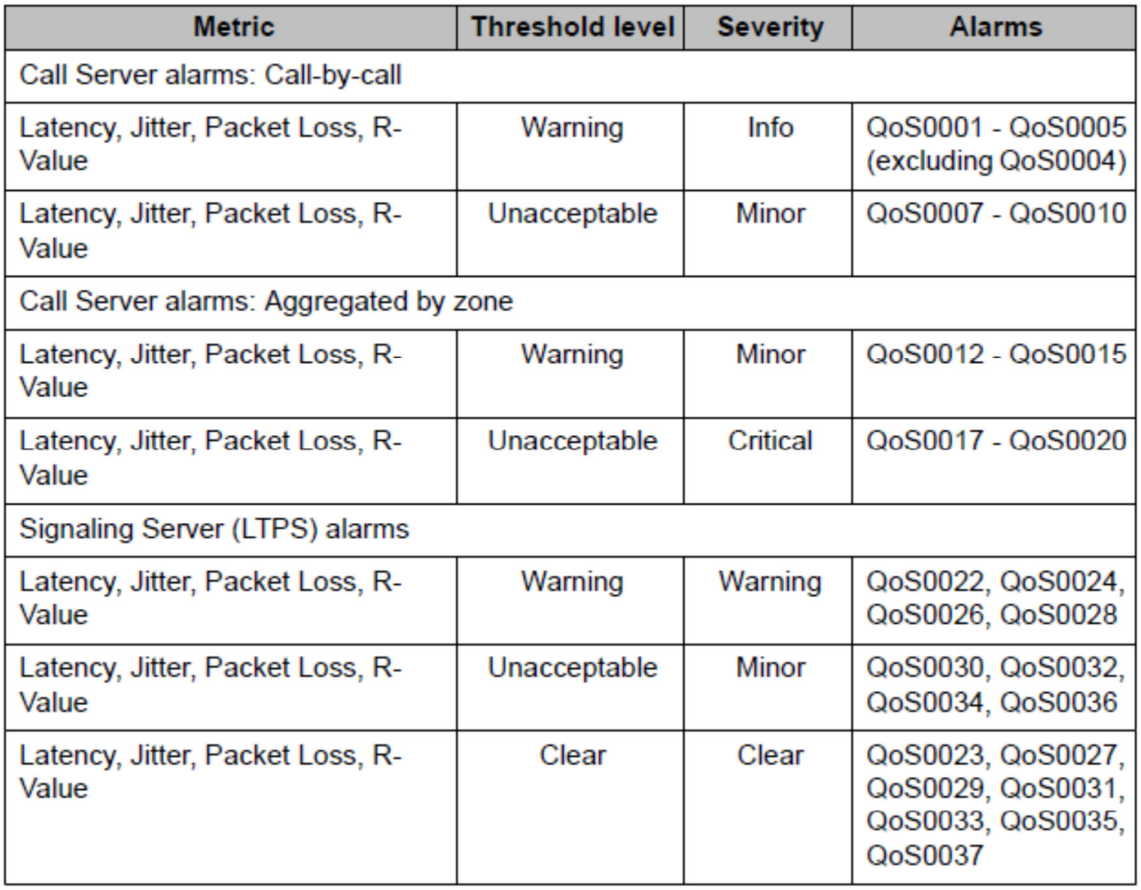
Note:
The SMC card TLAN interface supports 10BaseT and 100BaseT half and full duplex, while the ELAN supports only 10BaseT half-duplex. The IP Phones support 10BaseT or 100BaseT half-duplex and 10BaseT full duplex.
MGC Supports either Auto-negotiate or 100BaseT full duplex for both ELAN and TLAN.
You cannot manually configure a port on the switch or router to 10BaseT or 100BaseT full duplex and have an error-free connection to the IP Phones or VGMC/Signaling Server.

Manual configuration turns off autonegotiation in nearly every product on the market. By definition of the standards, without autonegotiation, the VGMC, Signaling Server and IP Phones revert to half duplex operation. This means the switch or router will be in a full duplex mode while the VGMC device is in a half-duplex mode, a situation guaranteed to cause packet loss. If the switch port is set to half duplex and sees lots of late collisions and duplicate collisions or if it is in full duplex mode and sees lots of CRC Errors or runt frames then odds are there is a mismatch.

- Check the router statistics to see the amount of network traffic on each subnet and the number of discarded packets.
- Check for differences in subnet configurations (that is, full versus half duplex or 10BaseT vs 100BaseT) if the problem occurs only for some IP Phones and not others.
- Check which QoS mechanism is enabled on the router to give priority to the packet traffic from the IP Phones.
- To eliminate packet loss messages, configure the switch or router for 10BaseT half-duplex operation and check if that eliminates the packet loss messages. If the messages stop, check the wiring and ensure the site has CAT-5 cable.

The below are the various QoS errors that are seen on the Call Server related to the Voice Quality. QoS001, Qos0007 and Qos0014 are alarms specific for Packet loss as an example for Info, Minor and Critical levels respectively.

Please refer to the Table 9 : Call Server alarms: Call-by-call



Metric	Threshold level	Severity	Alarms
Call Server alarms: Call-by-call			
Latency, Jitter, Packet Loss, R-Value	Warning	Info	QoS0001 - QoS0005 (excluding QoS0004)
Latency, Jitter, Packet Loss, R-Value	Unacceptable	Minor	QoS0007 - QoS0010
Call Server alarms: Aggregated by zone			
Latency, Jitter, Packet Loss, R-Value	Warning	Minor	QoS0012 - QoS0015
Latency, Jitter, Packet Loss, R-Value	Unacceptable	Critical	QoS0017 - QoS0020
Signaling Server (LTPS) alarms			
Latency, Jitter, Packet Loss, R-Value	Warning	Warning	QoS0022, QoS0024, QoS0026, QoS0028
Latency, Jitter, Packet Loss, R-Value	Unacceptable	Minor	QoS0030, QoS0032, QoS0034, QoS0036
Latency, Jitter, Packet Loss, R-Value	Clear	Clear	QoS0023, QoS0027, QoS0029, QoS0031, QoS0033, QoS0035, QoS0037

Table 9 : Call Server alarms: Call-by-call

Choppy speech

Choppy speech is usually a side effect of network problems, such as packet loss. Packets are lost or arrive late and the DSP must fill in or drop packets.

Wavering voice or tones

This problem is typically reported on handsfree calls. Sometimes users report that the receive volume fluctuates during tones. Wavering voice or tones can be caused by an interaction of the telephone speaker and microphone and the handsfree algorithm. To determine the cause, mute the handsfree and press the digits again; the DTMF tones should sound without waver. A similar problem can occur during handsfree conversations when room noise, drafts, or other disturbances cause the handsfree receive volume to fluctuate. Turn down the speaker receive volume to help or eliminate the problem.

The Power of We™

FAX over IP

Fax support is a commonly used value addition feature on CS 1000. The CS 1000 provides Fax support on both Analog or PSTN and over VoIP environments.

The CS 1000 supports Standard facsimile operations in an analog or PSTN environment adhering to the ITU published T.30 specification.

More information can be obtained in the following Product Correction Notice :
https://downloads.avaya.com/css/P8/documents/100150017

References :
NN43001-730 - Troubleshooting Guide for Distributors Avaya Communication Server 1000
NN43001-368 - IP Deskphones Fundamentals Avaya Communication Server 1000
NN43001-260 - Converging the Data Network with VoIP Fundamentals Avaya Communication Server 1000