METHOD OF REGULATING THE NUMBER OF CONCURRENT PARTICIPANTS IN A VIDEO CONFERENCING SYSTEM

TECHNICAL FIELD

[001] This invention relates to video conferencing technology, including multiple conferencing feeds from diverse network formats and multimedia data streams including IP, PSTN, ISDN and 3G cellular networks. It particularly concerns regulating the number of concurrent participants of the conferencing session to conserve system resources to within predetermined amount.

PRIOR ART

[002] ISDN (Integrated Services Digital Network) has been the traditional transport for digital videoconferencing since it is able to provide dedicated channels from end to end in bandwidths that can be dynamically allocated in multiples of 64 Kbps, typically in the range of 128 – 784 Kbps. Video conferencing end-points set up on desktop PCs or dedicated room-based end-point hardware running on proprietary codec are commonly carried by ISDN. PSTN (Public Switched Telephone Network) may also be fed into a video conference, typically as a voice-only participant.

[003] With the improvement and growth in Internet networking and bandwidth, video conferencing over Internet Protocol (IP) has become a more popular transport due to ease of access, bandwidth availability and control over quality of service. Thus, IP-based end-points, which typically employs webcams and microphones on PCs, are emerging as a significant mode of video conferencing. The evolution of mobile phone cellular services from GSM's 2G and 2.5G (GPRS/EDGE) to 3G (UTMS) and 3.5G (HSDPA) has also enable video phones to be used and thus opens another category of video conferencing end points.

[004] These 4 main categories of end-points transport, namely PSTN, ISDN, IP-based and 3G needs to be moderated and integrated in a video conferencing system which are likely to use universal hosted hardware platforms using ITU standards-based codecs for each category. E.g. H.323 for the IP-based codecs, H.320 for ISDN codecs and 3G codecs. Using such ITU standards codecs enables data integration apart from other features such as data-collaboration, instant messaging (text chat), recording & archiving, etc.

[005] A large number of codec standards, applications, hardware and technologies are involved in achieving a common platform which enables video and audio communication between desktop webcam, ISDN room-based end point, 3G mobile videophone, etc. in a successful video conferencing system in an integrated and seamless connection to the hosted platform. However, most conventional video conferencing systems are able to integrate the first 2 types

of end points, i.e. ISDN-based and IP-based, but not 3G. While it is presently possible to hold video conferencing between 3G videophone handsets, there is a lack of a universal platform to allow 3G video communication be established and connected to the existing PSTN, ISDN and IP-based end points.

[006] Another concern of video conferencing systems is to allocate resources judiciously among the users requesting for conferencing sessions. The resources may be connection bandwidth, end-points volume, audio codec and video codec whether they are embedded in devices or device firmware, and software including user licenses allowed and like copyright issues.

[007] U.S. Patent No. 7,085,243-B2 (Polycom Israel Ltd.) discloses a video conferencing method which multipoint control unit (MCU) is capable of determining if there are enough resources for an end point ("terminal 114") seeking to join a conference session. There is however no teaching on accommodating 3G end points in this reservationless conference method.

[008] U.S. Patent No. 6,611,503 (Tandberg Telecom AS) discloses a method for dynamically allocating transmission bandwidth amongst video, audio and data channels in multimedia conferencing service. While PSTN, ISDN and IP-based channels are described, there is no mentioned of 3G channel integration.

SUMMARY OF DISCLOSURE

[009] It is therefore desirable to provide for a multimedia conferencing system wherein all types of end points, including PSTN, ISDN, IP and 3G feeds from a 3G video phone may be accepted as one of the conferencing end points and integrated into the system as a participant using a universal hosted platform. With such integration, specific advantages and features such as dynamically allocating of resources, including the number of participating end points, of the video conference system may then be implemented.

[010] As a general embodiment of our invention, a method is disclosed for regulating number of concurrent participating end points, including PSTN, ISDN, IP and 3G-based end points (hereinafter "**participants**") in a video conferencing system employing multimedia data streaming codec in ITU H.323 network protocol standard, said number of concurrent participants is regulated to within a predetermined maximum number at a H.323 gatekeeper, said method comprising the steps of:

(a) authenticating whether a participant attempting to login has pre-registered with the system with requisite information provided and stored as said participant's gatekeeper web account, said authenticating includes verifying one or more of participant's identity (ID), password (PIN) and conference reference code;

(b) determining from the conference reference code whether said participant has a scheduled conference reservation or is seeking *ad hoc* conferencing;

(c) if said participant has conference reservation, using said participant's login ID and PIN to identify and retrieve the participant's gatekeeper web account to be presented as an H.323 client and registering the same with the H.323 gatekeeper's server, thus inducting said participant into the video conference;

(d) if said participant is seeking *ad hoc* conferencing (hereinafter "***ad hoc* participant**"), checking for free concurrent participant available in the H.323 gatekeeper, wherein the free concurrent participant available is a pool of balance of the predetermined maximum number less the number of other concurrent participants engaged in on-going teleconferencing sessions in the teleconferencing system;

(e) upon availability of free concurrent participant, admitting said *ad hoc* participant into the sought teleconference session by identifying and retrieving said *ad hoc* participant's gatekeeper web account from said *ad hoc* participant's login ID and PIN, and presenting said *ad hoc* participant's gatekeeper web account as an H.323 client and registering the same with the H.323 gatekeeper server; and

(f) upon each participant, whether *ad hoc* or having reservation, leaving a teleconferencing session by logging off, deregistering said participant's gatekeeper web account from the H.323 gatekeeper and releasing the number of leaving participants to the pool of available free concurrent participants;

preferably executed in the order recited above.

[011] In one aspect of our method, the predetermined maximum number of concurrent participants admissible by the H.323 gatekeeper may be predetermined on the basis of resource allocation, including at least one of bandwidth capacity, traffic volume, devices or device firmware, software or codecs, including user licenses allowed and like copyright issues. Preferably, the predetermined maximum number of concurrent participants is base on the number of codec licenses allowed and each license is tracked based on the number of participants concurrently registered with the H.323 gatekeeper.

[012] In a second aspect of our method, a participant having conference reservation may seek to extend the conference session, or extend his participation in the conference session, at the end of the reserved time slot by seeking as an *ad hoc* participant as in step (d).

[013] In a third aspect of our method, the participant may pre-registers his particulars at a webpage which is retrievably stored in the form of a gatekeeper web account, wherein said account may be provided to be registered with the H.323 gatekeeper in accordance with the aforesaid method steps.

[014] In a fourth aspect of our method, at least a multipoint control unit (hereinafter "**MCU**") may be employed to integrate and/or moderate the multimedia data streams from multiple participants in various network format, including Internet Protocol (hereinafter "**IP**"), Public Services Telephone Network (hereinafter "**PSTN**"), Integrated Services Digital Network (hereinafter

"**ISDN**") and 3G cellular network. Preferably, the MCU is employed to integrate and/or moderate data streams from IP, PSTN, ISDN networks, and a 3G gateway is employed to integrate and/or moderate data streams from 3G cellular network. Preferably still, the MCU is a *Polycom* MGC-100™ whereas the 3G gateway is a *Dilithium* DTG-2000™. Product literatures relating to the *Polycom* MGC-100™ and *Dilithium* DTG-2000™ from their respective manufacturers, including those available online at:

www.polycom.com/resource_center

and

www.dilithiumnetworks.com/products/DTG2000.htm.

[015] A preferred embodiment of our method provides for the data streams from the MCU and 3G gateway are seamlessly integrated and moderated. The MCU includes any one or combination of applications, firmware or hardware including built-in H.323 gatekeeper, call manager, including video PBX with call switching, forwarding and transfer; data network management for quality of service (QoS); bandwidth management; and accounting provided in the form of components or modules of the videoconferencing system.

[016] In a fifth aspect of our video conferencing method, the number of participants ("participating end points") counted are based on the total or combined total of each of the following end points types – PC-based VoIP applications and accessories; IP end point, including room-based hardware,

accessories and codec; ISDN room-based codec; audio phone, including 2G (GSM) and PSTN networks; video phone, including 3G networks.

[017] A method of regulating a number of concurrent participants in a video conferencing system according to Claim 1 wherein the number of gatekeeper web accounts allowed provisional reservation status in the pool to be considered for video conferencing services to be double the number of predetermined maximum number of allowed concurrent participants. Preferably, the first available gatekeeper web account from the pool is picked to join the video conference session.

[018] In a sixth aspect of our invention, the participants' gatekeeper web accounts are retrievably stored in a database managed by the video conferencing system, wherein upon a participant being accepted to join a video conference session, said participant's gatekeeper web account is retrieved and sent to the H.323 gatekeeper to be registered.

[019] In a seventh aspect of our invention, all participants' (i.e. including both *ad hoc* and those having reservation) requests are channeled to an MCU entry queue wherein, the MCU entry queue preferably implements a single dial entry sequence so as to process and approve each request in turn according to the aforesaid steps to keep in count the number of concurrent participants to within the predetermined maximum number.

[020] Our method may be implemented in part or wholly in any one or more of components of a video conferencing system including a gatekeeper; an MCU (multipoint control unit); a gateway including a media gateway controller (MGC); and a participant (participating video conferencing end point, including PSTN, ISDN, IP and 3G-based end points).

LIST OF ACCOMPANYING DRAWINGS

[021] The drawings listed below, with the accompanying detailed description that follows, may provide better and further understanding of our invention as non-limiting and exemplary illustration of specific aspects or preferred embodiments, in which:

[022] FIGURE 1 shows a highly simplified diagram outlining the main components of our proposed video conferencing system as an overview;

[023] FIGURE 2 shows a highly simplified schematic diagram outlining the system architecture of our video conference system;

[024] FIGURE 3 shows a graphical representation of a multimedia gateway in integrated configuration with our video conference system;

[025] FIGURE 4 shows the client-server configuration of the H.323

gatekeeper in our video conference system;

[026] FIGURE 5 shows a logical network diagram of our video conference system;

[027] FIGURE 6 shows a physical network diagram, in limited redundancy, of our video conference system;

[028] FIGURE 7 shows a diagram of the end points connection of our video conference system in relation to a public internet provider;

[029] FIGURE 8 shows a physical network diagram of the security design of our video conference system;

[030] FIGURE 9 shows a simplified schematic diagram of the access methods of our video conference system;

[031] FIGURE 10 shows a simplified schematic diagram of our video conference's links with public IM servers;

[032] FIGURE 11 illustrates an example of an ISDN (H.320) Room Based Videoconferencing Call Flow according to our invention;

[033] FIGURE 12 illustrates an example of a PSTN Audio-only Call Flow

according to our invention;

[034] FIGURE 13 illustrates an example of a 3G Mobile End points (H.324M) Call Flow according to our invention;

[035] FIGURE 14 illustrates an example of an IP (H.323) Room-based Video Conferencing Call Flow according to our invention;

[036] FIGURE 15 illustrates an example of an IP (H.323) Integrated Desktop Conferencing (Video and audio) Call Flow according to our invention;

[037] FIGURE 16 illustrates an example of an IP (H.323) Integrated Desktop Conferencing (Video, audio and data) Call Flow according to our invention;

[038] FIGURES 17 – 20 illustrate in simplified graphic diagrams, the manner in which various end points, including 3G Mobile end points, desktop clients, audio device (PSTN line phone), and Room-based system may respectively join our video conferencing system;

[039] FIGURE 21 illustrates a flowchart generally showing the various end points i.e. 2G/ PSTN phone, ISDN Room, IP Room, 3G Video Phone and the Web based Embedded Client dialling into the system via the MCU (1) to initiate and join a conference session;

[040] FIGURE 22 illustrates a flowchart diagram detailing on the process of managing and allocating available conference resources for various end point types;

[041] FIGURE 23 illustrates a flowchart diagram on a PC-based end point's logic flow in dialing in to join a conference session based on our invention;

[042] FIGURE 24 illustrates a Web-based Embedded Client dialing into our proposed video conferencing system to establish a conference session;

[043] FIGURE 25 depicts a flowchart diagram for the logic flow of the MCU dialing out to defined participating end points;

[044] FIGURE 26 depicts a flowchart diagram for the logic flow of the MCU dialing out to undefined participating end points;

[045] FIGURE 27 depicts a simplified block diagram of the various combinations of scheduled and unscheduled conferences with dial-in and dial out options for different end points;

[046] FIGURE 28 depicts a block diagram of the end point dial in conference flow according to our invention;

[047] FIGURE 29 depicts a flowchart diagram of the Gatekeeper Web

account dynamic resource allocation algorithm;

[048] FIGURE 30 depicts a timeline diagram showing overlapping conference sessions;

[049] FIGURE 31 depicts a table and axial lines to illustrate number of participants in a given time line; and

[050] FIGURE 32 depicts a Venn diagram on the gatekeeper web accounts.

DETAILED DESCRIPTION OF SPECIFIC EMBODIMENTS

[051] An overview of our video conferencing system employing a method of our invention described herein may be outlined in FIGURE 1 while FIGURE 2 shows a highly simplified schematic diagram of the overall system architecture of our system. Generally, our proposed system may comprise of the following listed key system components, each of which we shall describe.

(i) Video/Audio Conferencing bridge in the form of an MCU;

(ii) 3G Conferencing Gateway;

(iii) H.323 Gatekeeper;

(iv) Data Collaboration Server;

(v) Instant Messaging (IM) Server;

(vi) Recording/Archiving Server;

(vii) Streaming Server; and

(viii) Application Servers for Web, Database, Billing, etc.

[052] **Video/Audio Conferencing Bridge.** We propose to use an industry-leading Video/Audio Conferencing MCU in the system to provide a high performance and reliable platform for a converged video, voice conferencing over multiple networks – IP, ISDN, PSTN, etc.

[053] **3G Conferencing Gateway**, which is a Multimedia Gateway that provides transcoding and proxy functions for call signalling, command and control, and voice and video transcoding between multimedia systems protocols including 3G-324M/H.324M, ITU-T H.323 and the IETF SIP. The 3G Conferencing Gateway provides transcoding tailored to end-terminals such as 3G-enabled mobile phones or video phones, and IP terminals. Our choice of 3G Conferencing Gateway should also support a variety of voice and video coding standards and connects end-terminals on circuit switched, packet switched networks, and wireless networks.

[054] **H.323 Gatekeeper**. This device centralizes the management of Video over IP communication within the enterprise-wide network. It provides centralized videoconferencing management services and transfers many administration and configuration tasks from the individual end points, to the network, where they belong. The videoconferencing endpoints, recording sever and MCU needs to register with the H.323 Gatekeeper in order to participate in

the multipoint calls through the MCU.

[055] **Data Collaboration Server**. We propose to deploy a carrier-grade and highly functional web conference server that allows Service Providers to deploy a robust, scalable, manageable web conferencing service to consumers, enterprises and Internet Service Providers (ISP). It provides the data collaboration service which supports all the necessary data conference features such as whiteboard, sharing application, slide show, text chat and recording. The data contents can be recorded as a windows media format into, for example, a Data Connect Live recording server.

[056] **Instant Messaging Server.** We may use, for example, the *Microsoft® Office Live Communications Server 2005* (Live Communications Server 2005) which provides a powerful, scalable, instant messaging (IM) and integrated presence awareness solution. IM is a feature enabling the transfer text messages in real time over an Internet Protocol (IP) network such as the Internet or a corporate network. Presence awareness is the feature enabling the detection of another user's availability or status on one or more devices.

[057] **Video/Audio Recording and Archiving Server**. The Recording Server enables the recording of both the video and audio streams from the videoconferencing sessions (H.323 streams) as well as the data conferencing sessions. The conference may be recorded in the *Windows Media* format and can be played back via *Windows Media* Player. The complete conference

recording functionality may include recordings into 2 separate *Windows Media* files, one is created by Data Collaboration Server, and the other one created by the H.323 Recording Server. In order to play back the recorded conference, the proposed system will create a publish point at the Windows Media Server to stream out the two *Windows Media* files simultaneously.

[058] Third party equipment or devices proposed for some of the key components of our video conferencing system are tabulated in Table 1 below:

Table 1

S/N	Equipment	Brand & Model
1	Multipoint Control Unit (MCU)	*Polycom* MGC 100
2	3G Video Gateway	*Dilithium* DTG2000
3	H.323 Gatekeeper	*VCON* MXM
4	Desktop Videoconferencing Embedded Client	*VCON* vPoint HDDK
5	Data Collaboration Server	*Dataconnection* Meeting Server
6	IM Server	*Microsoft* Live Communications Server LCS 2005
7	H.323 Recording Server	*Starbak* VCG400
8	SSL VPN	*Juniper* SA 4000

[059] SUPPORTED END POINTS. The following end points are anticipated to be supported by our proposed video conferencing system.

[060] **ISDN Room-based systems (ISDN Room).** These are the ISDN-specific, appliance-based videoconferencing systems that support the ITU-T H.320 protocol. The system normally come with specific camera, microphones

and dedicated high performance codec for the ISDN videoconferencing signals broadcast from and received at an ISDN conference room setup.

[061] **Internet Protocol or IP Room Based Systems (IP Room).** These are appliance-based videoconferencing systems that support ITU-T H.323 protocol. The system normally come with specially designed camera, microphones and dedicated high performance codec for the coding and decoding of the videoconferencing signals. These are normally used in a conference room setup.

[062] **Personal Computer-based (PC-based).** These are PC (desktop or notebook) running the custom web based embedded H.323 software client. The client works in conjunction with the PC based accessories such as USB or Bluetooth web camera and microphone to provide the highest quality video conferencing and data Collaboration experience.

[063] **Audio Phone.** These are normal telephone handsets connected to the fixed line or terrestrial telephone network (PSTN or Public Services Telephone Network) that provide for audio signal transmission only, as well as 2G mobile or cellular phone that provide audio signal and limited data services.

[064] **3G Video Phone** – These are 3G handsets which support ITU-T H.324M protocol for videoconferencing over 3G network.

[065] A brief comparison of the audio-video and data features of these various end points is provided in the following Table 2.

Table 2

End Point Type	Audio Phone (2G/PSTN)	Video Phone (3G)	ISDN Room	Computer	IP Room
AV conference Feature					
Connection Type	ISDN	IP	ISDN	IP	IP
Max Bandwidth	64K	128K	128K 256K 384K	128K	128K 256K 384K
Audio	Yes	Yes	Yes	Yes	Yes
Video	No	Yes	Yes	Yes	Yes
Dial-in	Yes	Yes	Yes	Yes	Yes
Dial-out	Yes	Yes	Yes	No	Yes
Data Conference Feature					
Data Collaboration	No	No	No	Yes	No

[066] Our proposed video conferencing system is able to support the typical 2 types of scheduling, namely, (i) scheduled and (ii) on demand or *ad hoc* conferencing. A schedule conference is reserved prior the actual conference session. The resources of the various endpoint type, connection access, conference start date and time, conference duration are defined by the conference organiser. Based on these input, the details will be stored in the system. An *ad hoc* conference does not require any reservation. A conferencing chairman or moderator and the participants may attempt to access the system to start an On-Demand or *ad hoc* conference. As there is no prior reservation, the On-demand conference's availability is subject to the availability of the resources of the system. Some of the key features supported in respect

of either types of scheduling are indicated in the following Table 3.

Table 3

End Point Access Mode	Defined Dial-in Participant	Defined Dial-out Participant	Undefined Dial-in Participant	Undefined Dial-out Participant
Scheduled Conference	Supported	Supported (except Computer)	Supported	Supported (except Computer)
On-demand conference	NA	NA	Supported	Supported (except Computer)

[067] Referring back to Table 1 above, some of the equipment or devices proposed in our video conferencing system are described in some detail below.

Dilithium Networks DTG2000 Media Transcoding Gateway.

[068] One of the key capability of the MMC system is the ability of allowing 3G users (with 3G handsets or adaptor cards) to join in the multipoint conference. This is achieved through the integration with the *Dilithium* DTG2000 Media Tanscoding Gateway. The DTG 2000™ is a Multimedia Gateway that provides transcoding and proxy functions for call signaling, command and control, and voice and video transcoding between multimedia systems protocols including 3G-324M/H.324M and ITU-T H.323. A graphical configuration of such integration is shown in FIGURE 3.

[069] The DTG performs all necessary negotiation and mediation between network entities and client devices to allow effortless communications across

network boundaries including Circuit Switch to Packet Switch Mapping, Capability Negotiation, Command Mediation and Media Transcoding. The crucial steps in configuring the DTG for the purpose of our invention are described in the following.

[070] The basic IP address configuration of the DTG2000 is performed prior to other components being configured. An example of the network IP addresses used in the configuration is shown in Table 4 below.

Table 4

Parameter	Setting	Description
Internal IP address	192.168.x.x	Host Controller Card Ethernet Interface 0 (for telnet purpose)
Internal IP address	x.x.x.x (DMZ Zone)	Transcoder Engine Module (TEM 3) (for network traffic)
gatekeeper	x.x.x.x (DMZ Zone)	VCON MXM IP address
hostname	DTG2000	For DNS registration
IP subnet	255.255.x.x	Subnet mask
IP Gateway	192.168.x.x	Default Gateway
nameserver	x.x.x.x-x	IP address of Primary and secondary network Domain Name Server
Ntp	x.x.x.x	IP address of the Simple Network Time Protocol.
Syslog	x.x.x.x	IP address of server to store system log output.

[071] Session Mediation Module (SMM) must also be configured for all components in order that the DTG2000 may operate correctly. The configuration of all components must be consistent, both internally between components, and externally with network elements in order for the DTG2000 to operate correctly. For example, the appropriate types of transcoder must be defined, assigned to a Session Mediation Module (SMM), and correspond to the

type of traffic carried on connected circuits. The configuration information may be stored on a flash memory disk and read upon system startup to configure the system. The following Table 5 below shows the SMM configuration.

Table 5

Command	Setting	Description
H223 adaptation-layer	A12	
H323 video lvfu	Enable	Fast update
H323 video max-bit rate	112	Specify maximum supported video bitrate capability sent to remote H.323 terminal.
H323 video codec	H263	
H323 audio codec	G711alaw	
Rtp video preferred-packet-size	200	Set the preferred payload size of video RTP packets transmitted over the IP network,
Rtp audio gsmamr payload-format rfc3267	Octet-aligned	

ISDN Call Signaling and H.323 Gatekeeper

[072] With reference to FIGURE 4, while our video conferencing system is configured to accept and integrate signals from disparate multiple terminals to which calls can be routed via address ranges, the H.323 Gatekeeper is nevertheless configured as a separate entity under the Call Agent. The Gatekeeper provides external call routing services. All H.323 client IP addresses must be configured in the client to match the rest of the network.

[073] Client number ranges may be assigned as listed below.

- **8xxxxxxx** H.324M client number

- 9xxxxxxxx H.324M client number
- **x.x.x.x** H.323 client IP addresses

In this scenario the H.324M client number range is 8xxxxxxx, 9xxxxxxx so that the wildcard pattern is [**8-9][0-9]<7>**. The following Table 6 may be used to configure system-wide ISDN signaling parameters:

Table 6

Config mode	Command	Setting	Description
ISDN Signaling	Sapi	0	Configure values of Service Access Point Identifier (SAPI).
ISDN Signaling	Tei	0	Configure values of Terminal Endpoint Identifier (TEI).
Interface	Signaling	Isdn	Set the interface signaling protocol to ISDN.
Interface	Line-code	Hdb3	Set line code of current interface,
Interface	line-mode	120 balanced	Layer 1 (physical) characteristics of the interface to match the connected Equipment.
interface	Polarity	user	Set protocol polarity for current interface
interface	Crc	On	Enable CRC-4 for current interface
TEM	Interface	e1 2 0	Assign the TEM to the E1 interface.
TEM	Smm	1	Assign the TEM to the SMM.
Call-Agent isdn-bearer-capability	coding-standard	ITU-T	ISDN Bearer Capability settings to match the ISDN network provider's Settings.
Call-Agent isdn-bearer-capability	Data-synchronism	synchronous	ISDN Bearer Capability settings to match the ISDN network provider's settings
Call-Agent isdn-bearer-capability	User-information-layer1-protocol	H223_and_H245	ISDN Bearer Capability settings to match the ISDN network provider's settings
Call-Agent isdn-bearer-capability	L3-polarity	user	Set Layer 3 polarity (interface direction) for ISDN stack
Resource management	isdn	interface-id 0	Define all channels of the circuit on port 0 of the interface as ISDN bearers.
Resource management	isdn	Channel_start_id 0	first channel in range
Resource management	isdn	Channel_end_id 31	last channel in range
Resource	isdn	Channel	set according to connected

Config mode	Command	Setting	Description
management		selection order increase	equipment
Number Analysis	isdn	number-id [8-9][0-9]<7>	Map the numbers of the H.324M clients (8xxxxxxx, 9xxxxxxx) to the defined ISDN interface on port 0. All incoming packet-switched calls from the H.323 client to these called party numbers are directed to this interface.
Number Analysis	Number manipulation	H323 24[8-9][0-9]<7> strip 2	
gatekeeper	Ip-address	x.x.x.x	Define the Gatekeeper IP address.
gatekeeper	terminal-alias	H323id DTG	Set up an alias by which other terminals can identify the specified terminal
gatekeeper	terminal-alias	E164 24	Set up an alias by which other terminals can identify the specified terminal
gatekeeper	Gateway-service-prefix	24	
gatekeeper	Listen-port	1721	Number of UDP port.
gatekeeper	Write-port	1721	Number of UDP port.
gatekeeper	Bandwidth	256	Maximum allowed bandwidth for a call in kbps,
gatekeeper	Lightweight-reg	yes	re-registering with the gatekeeper on

NETWORK & SECURITY DESIGN

[074] With reference to FIGURE 5, the design for Local Area Network (LAN), Wide Area Network & Network Security Design will now be described for our proposed video conferencing system. Our LAN infrastructure serves to connect the various servers and devices in a local network so as to enable all the components to talk to each other. Two units of *Cisco Catalyst* 2970 are proposed to be configured to provide high speed switching between network nodes.

[075] In order to secure critical systems, our video conferencing LAN is proposed to be segregated into three main networks. The public zone is connected to the Managed IP Networks: Meg@POP, C+ as well as Public Internet. The DMZ, as the name implies, hosts public servers. This zone will serve as the entry point of our video conferencing service to the users. In addition to network switches, a load balancer may also be installed to provide load balancing mechanism between two units of web server in DMZ.

[076] As part of network infrastructure, a firewall will be in place to segregate the sub-networks within the LAN, which will be the first line of defense to monitor the traffic flow into and out of our video conferencing systems. SSL-VPN may provide secure access method between users and our video conferencing systems. Besides security features, SSL-VPN also facilitates connectivity mechanism between our system and users through the firewall. By tunneling the multimedia (H.323) traffic into SSL session, a customer will not have to face with any firewall reconfiguration.

[077] In respect of the Wide Area Network, our video conferencing system may be connected to the rest of the world via three media: Internet, Meg@POP and C+.

[078] Redundant switches may support the LAN by providing high speed switching between network devices connected to the same VLAN. In this design, LAN switches are not configured with layer 3 (routing) configuration.

Instead, all network devices in the VLAN must point to firewall IP address as their default gateway so that security can be enforced because all traffics must go through the firewall before it can reach other network devices in other VLAN.

Ethernet interfaces on the switch operate at 10, 100, or 1000 Mbps and in either full- or half-duplex mode. In full-duplex mode, two stations can send and receive traffic at the same time. Normally, 10-Mbps ports operate in half-duplex mode, which means that stations can either receive or send traffic. The arrangement of network devices connected to LAN switches are as follow:

Table 7.1 - Switch Port Assignment – CS1

CS1					
Port	**VLAN**	**VLAN ID**	**Device**	**Speed**	**Duplex**
0/1	Public	100	MMC_FW 1	Auto	Auto
0/2	DMZ	90	MMC_FW 2	Auto	Auto
0/3	Spare	Spare	MMC_FW 3	Auto	Auto
0/4	Mgmt	70	MMC_FW 4	Auto	Auto
0/5	Private	50	MMC_FW 5	Auto	Auto
0/6	DMZ	90	SSL_VPN	Auto	Auto
0/7	Public	100	Router_1	Auto	Auto
0/8	Public	100	Spare	Auto	Auto
0/9	Mgmt	70	MCU	Auto	Auto
0/10	DMZ	90	WebServer1	Auto	Auto
0/11	DMZ	90	VconMXM1	Auto	Auto
0/12	DMZ	90	DataconSVR1	Auto	Auto
0/13	DMZ	90	BU_SVR1	Auto	Auto
0/14	DMZ	90	Streaming_SVR	Auto	Auto
0/15	DMZ	90	MCU	Auto	Auto
0/16	DMZ	90	LB_Server1	Auto	Auto
0/17	Private	50	App_Svr1	Auto	Auto
0/18	Private	50	DB_Svr1	Auto	Auto
0/19	Private	50	Archive_Svr1	Auto	Auto
0/20	Private	50	Starbak	Auto	Auto
0/21	Private	50	LCS AD	Auto	Auto
0/22	Spare	Spare	Spare	Auto	Auto
0/23	Spare	Spare	Spare	Auto	Auto
0/24	802.1Q		MMC_CS2 0/24	1000	Full

Table 7.2 - Switch Port Assignment – CS2

CS2					
Port	**VLAN**	**VLAN ID**	**Device**	**Speed**	**Duplex**
0/1	Public	100	Spare	Auto	Auto
0/2	DMZ	90	Spare	Auto	Auto
0/3	SSL	80	Spare	Auto	Auto
0/4	Mgmt	70	Spare	Auto	Auto
0/5	Private	50	Spare	Auto	Auto
0/6	Public	100	Spare	Auto	Auto
0/7	Public	100	Router_2	Auto	Auto
0/8	Public	100	Spare	Auto	Auto
0/9	Mgmt	70	Dilithium	Auto	Auto
0/10	DMZ	90	WebServer2	Auto	Auto
0/11	DMZ	90	VconMXM2	Auto	Auto
0/12	DMZ	90	DataconnSVR2	Auto	Auto
0/13	DMZ	90	LCS_XS_Proxy	Auto	Auto
0/14	DMZ	90	Dilithium	Auto	Auto
0/15	DMZ	90	Spare	Auto	Auto
0/16	Private	50	Spare	Auto	Auto
0/17	Private	50	App_Svr2	Auto	Auto
0/18	Private	50	DB_Svr2	Auto	Auto
0/19	Private	50	LiveR_Svr	Auto	Auto
0/20	Private	50	BU_SVR2	Auto	Auto
0/21	Private	50	LCS 2005	Auto	Auto
0/22	Private	50	LCS Director	Auto	Auto
0/23	Spare	Spare	Spare	Auto	Auto
0/24	802.1Q		MMC_CS2 0/24	1000	Full

[079] Switch Ports. Switch ports are Layer 2-only interfaces associated with a physical port. Switch ports belong to one or more VLANs. A switch port can be an access port or a trunk port. It can be configured as an access port or trunk port or let the Dynamic Trunking Protocol (DTP) operate on a per-port basis to set the switch port mode by negotiating with the port on the other end of the link. Switch ports are used for managing the physical interface and associated Layer 2 protocols.

[080] Access Ports. An access port belongs to a particular VLAN and carries the traffic of that VLAN only unless it is configured as a voice VLAN port. Traffic is received and sent in native formats with no VLAN tagging. Traffic arriving on an access port is therefore assumed to belong to the particular VLAN assigned to the port. If an access port receives a tagged packet (Inter-Switch Link [ISL] or IEEE 802.1Q tagged), the packet is dropped and the source address is not learned. In this design, static VLAN access port will be configured for most of the switch ports.

[081] Trunk Ports. A trunk port carries the traffic of multiple VLANs and by default is a member of all VLANs in the VLAN database. As indicated in the Tables 7 above, the last port of each network switch will be configured as 802.1q trunk. An IEEE 802.1Q trunk port supports simultaneous tagged and untagged traffic. An IEEE 802.1Q trunk port is assigned a default Port VLAN ID (PVID), and all untagged traffic travels on the port default PVID. All untagged traffic and tagged traffic with a NULL VLAN ID are assumed to belong to the port default PVID. A packet with a VLAN ID equal to the outgoing port default PVID is sent untagged. All other traffic is sent with a VLAN tag.

[082] VLAN Planning. A VLAN is a switched network that is logically segmented by function, project team, or application, without regard to the physical locations of the users. Although VLANs may have the same attributes as physical LANs, end stations may be grouped together even if they are not physically located on the same LAN segment. Any switch port can belong to a

VLAN and unicast, broadcast, and multicast packets are forwarded and flooded only to end stations in the VLAN. Each VLAN is considered a logical network, and packets destined for stations that do not belong to the VLAN must be forwarded through a router or a switch supporting fallback bridging. In this design, Firewall will be the layer 3 termination for each VLAN. The VLAN listed in the following table segregate the network devices from other network devices in other VLANs. Each VLAN represent different network and there is no direct layer two communication between those VLANs. The following Table 8 shows the mapping between IP addresses and VLAN ID.

Table 8

VLAN	VLAN ID	Network ID	Subnet Mask	Reserved IP Add	Available IP Add
Public	100	58.185.x.x	255.255.x.x	58.185.x.x – x	58.185.x.x – x
DMZPub	95	58.185.x.x	255.255.x.x	58.185.x.x – x	58.185.x.x – x
DMZ	90	192.168.x.x	255.255.x.x	192.168.x.x-x	192.168.x.x-x
Mgmt	70	192.168.x.x	255.255.x.x	192.168.x.x-x	192.168.x.x-x
Private	50	192.168.x.x	255.255.x.x	192.168.x.x-x	192.168.x.x-x

[083] VTP (VLAN Trunking Protocol) configuration is also part of the VLAN planning. VTP is a Layer 2 messaging protocol that maintains VLAN configuration consistency by managing the addition, deletion, and renaming of VLANs on a network-wide basis. VTP minimizes misconfigurations and configuration inconsistencies that can cause several problems, such as duplicate VLAN names, incorrect VLAN-type specifications, and security violations.

[084] Due to the size of the network, VTP is recommended to be configured in transparent mode. VTP transparent switches do not participate in VTP. A VTP transparent switch does not advertise its VLAN configuration and does not synchronize its VLAN configuration based on received advertisements. However, in VTP Version 2, transparent switches do forward VTP advertisements that they receive from other switches through their trunk interfaces.

[085] Below is the detail for VTP configuration:

VTP Domain : MMC

VTP Mode : Transparent

[086] Spanning Tree Configuration (STP) is a Layer 2 link management protocol that provides path redundancy while preventing loops in the network. For a Layer 2 Ethernet network to function properly, only one active path can exist between any two stations. Multiple active paths among end stations may cause loops in the network, whereupon the end stations might receive duplicate messages. Switches might also learn end-station MAC addresses on multiple Layer 2 interfaces. These conditions will result in an unstable network. Spanning-tree operation is transparent to end stations, which cannot detect whether they are connected to a single LAN segment or a switched LAN of multiple segments.

[087] With reference to FIGURE 6, our proposed video conferencing system

network infrastructure does not have issues regarding spanning tree. The main reason is that there is only a pair of switches in the network which connect to the end stations. However, a problem may occur if a server with redundant network port configured as Network Bridge. In this case, redundant path is available to reach that particular server. Configuring one of the switches as a root bridge will avoid future problem in spanning tree. PVST + (Per VLAN Spanning Tree) is recommended to be applied in our proposed video conferencing LAN configuration.

[088] The PVST+ provides Layer 2 load balancing for the VLAN on which it runs. Different logical topologies can be created by using the VLANs on the network to ensure that all of the links are used but that no one link is oversubscribed. Each instance of PVST+ on a VLAN has a single root switch. This root switch propagates the spanning-tree information associated with that VLAN to all other switches in the network. Because each switch has the same information about the network, this process ensures that the network topology is maintained. All ports in the switch must follow through blocking, listening, learning phases before finally able to forward the network traffic. These spanning tree processes are required to ensure the stability of the network, especially if the switch is connected to other network switches. For the switch port which is connected to end station, running through the whole process can cause delay to the activation of that port.

[089] Port Fast immediately brings an interface configured as an access or

trunk port to the forwarding state from a blocking state, and bypassing the listening and learning states. In addition to port fast, the BPDU guard feature is used in the network to prevent an access port from participating in the spanning tree.

[090] Various methods of accessing our proposed video conferencing system are possible. With collective reference to FIGUREs 7, 8 and 9, the first method to access the video conferencing system is via the Internet. To support this access method, one of our system's router will be connected to a Public Internet Provider.

[091] For managed network access, our video conferencing system may be connected via *Connect Plus* and *Meg@POP* to provide access for users from these managed networks. The current design allows connection to these networks via Fast Ethernet link. One of the guideline for users from managed network is that they have to create special LAN for multimedia user at their respective conferencing participant end point (CPE). By assigning this LAN with public IP address, the video conferencing system can avoid having redundant IP address between two different customers.

[092] In the event a customer has more than one video conferencing end points (Room based systems) in their network, customer is required to apply for an additional public IP address for each of the end point. It is important to know that one video conferencing end point require one public IP address. The

exception of this requirement is desktop client. When using desktop client, the user can use SSL-VPN to encapsulate multimedia traffic. Port address translation can be configured instead of NAT in this scenario.

[093] Our video conferencing system's proposed security components comprises of SSL-VPN Gateway and Perimeter Firewall which are described below.

SSL VPN Gateway

[094] Tradition firewalls are having problem supporting multimedia network traffic (H.323). The introduction of SSL-VPN Gateway allows all the multimedia network traffic to be tunneled through SSL, which is typically allowed in most organization. This eliminates the need of firewall reconfiguration as well as lack of H.323 support in the traditional firewall. The SSL-VPN Gateway provides a secure encrypted channel between users and our video conferencing system. The primary purpose of the SSL-VPN deployment is to secure the multimedia network traffic by encrypting the traffic between the individual clients and service provider.

[095] For equipment, Juniper Networks Secure Access 4000 is proposed to be used as the SSL-VPN Gateway. It provides three different access methods. These methods consist of Clientless Core Web access, Secure Application Manager (SAM) and the Network Connect (NC) adaptor. In this implementation,

only the NC adaptor access will be used. The purpose of the Network Connect is to allow the client machine to become a node on the DMZ network and access the video conferencing gateway. The SSL VPN would assign a dynamic IP based on the allocated IP pool. It would also restrict access to certain resources such as IP addresses and services. One precaution for running the Network Connect module is that it requires administrator access to be installed for the first time on the client.

[096] In respect of Access Control Policy, two separate access - one each for the two main groups, i.e. the video conferencing users and the SSL-VPN administrators, may be set. For User Access Group, the video conference system users connecting from the internet via the SSL VPN to the video conferencing gateway are regulated. This method allows traversing of possible corporate firewalls, as well as eliminates the problem reconfiguring such firewalls on the client side. To integrate and incorporate with our proposed video conferencing portal, anonymous method of accessing the VPN may be used. The users will initially establish a SSL tunnel (via the NC adaptor) to the SSL-VPN gateway and would automatically be redirected to our video conferencing web portal. The users will then be authenticated and be forwarded to the appropriate video conferencing session page.

[097] For Administrator Access Group, access is allowed for assigned Administrators to manage the SSL-VPN gateway. The administrators would only be restricted to access the SSL-VPN from the SingTel Corporate LAN

(restricted by Firewall), DMZ or the video conferencing's private LAN.

Perimeter Firewall

[098] The perimeter firewall will monitor, protect and segregate the sub-networks in the video conferencing network. Due to the limited amount of available public IP addresses as well as to cater for future expansion, the firewall will do NAT (Network Address Translation) between the public IPs and private IPs for the server in the DMZ.

[099] For equipment, Lucent Firewall Brick® will be used as the firewall for the video conferencing network. It will provide basic perimeter defense and segregate the different sub-networks in the designed network configuration. To facilitate the use of a cold-standby firewall during any possible failure of the active firewall, a distributed configuration was chosen. The firewall management modules, in which Lucent Security Management Server (LSMS) is proposed, will be placed on a Windows 2003 Server. This would allow the current firewall policies to be pushed to any firewall. Details of the firewall module are provided in the following Table 9.

Table 9

Firewall Module	Details
Firewall Management Server	AS-PE1850 with Windows 2003 Server SP1
Active Firewall	Lucent Firewall Brick® 1100
Cold Stand-by Firewall	Lucent Firewall Brick® 350

[0100] Rules – the basic security or firewall rules for our video conferencing network design are provided in the following Table 10:

Table 10

No.	Source	Destination	Services	Action	Remarks
1	*	*	NetBIOS	Drop	
2	*	Firewall	*	Drop	Stealth Rule
	*	*	*	Drop	Clean Up Rule

[0101] NAT (Network Address Translation) - In order to maintain scalability of the network due the limited number of public IP addresses, the firewall would require to do NAT between the internal and external networks.

Instant Messaging and Status Detection.

[0102] With reference to FIGURE 10, the features of Instant Messaging and Status Detection (e.g. “online”, “offline”, “away”, “not available”, “do not disturb”, etc.) may be communicated within our video conferencing as extended implementation from public IM servers such as Microsoft MSN, Yahoo Messenger & AOL. These features may be achieved via the Microsoft Live Communications Server (LCS).

[0103] Microsoft LCS server comprises of four servers. In addition, LCS requires the Active Directory server and two SQL instances as indicated in the following Table 11, i.e. one in the clustered servers and the other in the LCS Archive server.

Table 11

Server	LCS version	SQL Server
LCS Application Pool	2005 Enterprise	SQL Cluster
LCS Director	2005 Enterprise	Archive Server
LCS Access Proxy	2005 Standard	Not required
LCS Archive Server	2005 Standard	Archive Server

[0104] LCS requires the Active Directory schematics to be modified. In addition, LCS servers communicate with each other using Transport Layer Security. TLS also requires server certificates. Except for the Access Proxy server's public interface, internal certificates can be used to reduce costs. The Access Proxy requires a public certificate as it is required for connections to public IMs. The following information is required to complete the LCS installation:

SIP domains names supported:	mmclcs.corp
Enable federation and public IM connectivity:	Enabled
Network address:	lcspool2.mmclcs.corp
Port:	5061
Trusted Access Proxy:	mmlap01.mmclcs.corp
Archive all communications with internal users:	Enabled
Archive all communications with federated partners:	Enabled

[0105] LCS DNS requirements include requiring a DNS record for each

Application and Director pool installed. The record name must match the pool names. In addition, LCS requires DNS srv records to function correctly. Two service records are used are

_sip._tls.mmclcs.corp and

_sip._tcp.mmclcs.corp.

The srv records will respond with the name of the LCS Application pool.

[0106] LCS Application Pool includes the application servers that process requests, updates and retrieves information from the SQL database. LCS manages all servers in the Application Pool as a single object. Only unique server properties such as port, certificate and logging (not archiving) configuration are to be configured individually on each pool member. The Application pool servers are members of the LCS Active Directory.

[0107] The Application Pool should send all outgoing requests to the LCS Director servers. The Application Pool server requires a Transport Layer Security (TLS) certificate to communicate securely with the LCS Director servers. An internal certificate is sufficient. Before installing the Application Pool, the following tasks must be performed:

1) Prep Active Directory Schema and Forest
2) Prep Domain
3) Create Enterprise Pool
4) Activate Enterprise Edition Server

[0108] The following information is required to create the Application Pool:

Pool Name:	lcspool1
FQDN for the domain:	mmclcs.corp
Back-end Database SQL server:	prodsql
Install database to:	S:\LC Data\
Install transaction log to:	L:\LC Log\

[0109] The Application Pool requires a domain account to run its services. The account can be created when activating the server. To this end the Application Pool configuration includes:

Maximum contacts per user:	150
Request compression on outgoing server-to-server connections:	Disabled
Enable compression on client-to-server connections:	Enabled
Authentication:	NTLM

[0110] The LCS Director is optional but strongly recommended for any external connections. It directs incoming and outgoing requests in an LCS system. In addition, the Director authenticates users and directs them to the appropriate Application Pool. The Application pool sends all outgoing requests to the director and the Access Proxy sends incoming requests to the LCS Director. LCS Directors are members of the LCS Active directory and do not house any LCS accounts.

[0111] All communications between the Director and its peers are performed securely using Mutual Transport Layer Security (MTLS). An internal TLS certificate is sufficient for the LCS Director. The LCS Director Pool will be installed using LCS Enterprise edition which allows two or more directors to be

managed as one and requires SQL Server. The SQL server on the Archive server will be used for the Director Pool. Installing the LCS Director is similar to installing the Application Pool. The same service accounts for the Application Pool can be used for the Director.

[0112] The following information is required to create the Director Pool:

Pool Name:	lcspool2
FQDN for the domain:	mmclcs.corp
Back-end Database SQL server:	mmlas01
Install database to:	D:\LC Data\
Install transaction log to:	D:\LC Log\

[0113] Application Pool configuration includes:

Maximum contacts per user:	150
Request compression on outgoing server-to-server connections:	Disabled
Enable compression on client-to-server connections:	Enabled
Authentication:	NTLM
Federation Network Address:	mmlap01.mmcsys.corp
Federation Port:	5061

[0114] The LCS Access Proxy server is used to connect to public IMs and to federated LCS domains. The Access Proxy server has two network interfaces: one interface for public connections and the second interface connect to internal servers. All communications to and from the Access Proxy server are encrypted using TLS. The Access proxy public interface requires a Transport Layer Security (TLS) public certificate to connect to public IMs and to federated LCS domains. The private interface requires another TLS certificate. The private interface TLS certificate can be an internal certificate.

[0115] The Access Proxy server is the only LCS server that is not joined to the LCS Active Directory domain. It will be a member of the management domain instead. The LCS Access Proxy requires a service account. The account can be created when activating the Proxy. The LCS Global properties must be configured to trust Access Proxy servers. The Access Proxy can only be managed from the Computer Management – Services and Applications. The Access Proxy requires the following information:

Federate with other domains:	Enabled
Allow remote user access to your network:	Disabled
Public network address:	192.168.x.x
Private network address:	192.168.x.x
Internal Next hop network address:	mmldp01.mmclcs.corp
Internal SIP domains supported by Live Communications servers in your organisation:	mmclcs.corp
Internal servers authorised to connect to this Access Proxy server:	mmldp01.mmclcs.corp
Request compression on outgoing server-to-server connections:	Disabled
Enable compression on client-to-server connections:	Enabled

[0116] The LCS Archive Server archives all instant messaging conversations for all or specific users. The Archiving Server does not archive video, audio or file transfers. LCS can be configured to include IM conversations with external LCS domains.

[0117] Both LCS Application pool and Archive servers require the Microsoft Message Queuing (MSMQ) to be installed. The default message queue path name will be used. In addition, the Archive server requires SQL Server to store the archived messages. A copy of SQL Server will be installed on the Archive

Server itself. The LCS Archive server requires a service account to run. The account can be created when activating the Archive service. Other information required are:

SQL Server instance:	default
Enter database name:	LcsLog
Install database to:	D:\LC Archiving Data\
Install transaction log to:	D:\LC Archiving Log\

EXAMPLES OF CONFERENCING CALL FLOWS

[0118] Some of the types of conference call flows will now be described in some detail with reference to specific process steps.

[0119] EXAMPLE 1 - ISDN (H.320) Room Based Videoconferencing Call Flow is described in the following with reference to FIGURE 11.

Step 1 - Endpoint dials a number that is stated in the Reservation Confirmation which corresponds to the assigned ISDN dial-in number for the Entry Queue.

Step 2 – The carrier conveys the dial-in number to the MCU.

Step 3 – According to the dial-in number, the MCU searches for the appropriate Entry Queue and connects the participant to the Entry Queue. The participant is requested to enter the target conference Numeric ID.

Step 4 – According to this conference ID, the participant is routed to the appropriate conference. The participant is requested to enter the

target conference/chairperson password.

[0120] EXAMPLE 2 - Public Switched Telephone Network (PSTN) Audio Only Call Flow is described in the following with reference to FIGURE 12.

Step 1 – The endpoint dials a number that is stated in the Reservation Confirmation which corresponds to the assigned ISDN dial-in number for the Entry Queue.

Step 2 – The carrier conveys the dial-in number to the MCU.

Step 3 – According to the dial-in number, the MCU searches for the appropriate Entry Queue and connects the participant to the Entry Queue. The participant is requested to enter the target conference Numeric ID.

Step 4 – According to this conference ID, the participant is routed to the appropriate conference. The participant is requested to enter the target conference/chairperson password.

[0121] EXAMPLE 3 – 3G Mobile End points (H.324M) Call Flow is described in the following with reference to FIGURE 13.

Step 1 – Endpoint dials a number that is stated in the Reservation Confirmation which corresponds to the H.323 service prefix (64) and the Entry Queue Numeric ID. This number is also fall inside the range of DDI numbers assigned by the 3G mobile network for

MMC usage.

Step 2 – The MSC in the 3G carrier conveys the dial-in number to the ISDN exchange.

Step 3 – The ISDN carrier conveys the dial-in number to the Dilithium Gateway.

Step 4 – The Gateway sends the dial-in number to the active gatekeeper where, using the prefix, the gatekeeper identifies the MCU.

Step 5 – The gatekeeper returns the IP alias of the MCU IP-48 card to the Gateway.

Step 6 – The Gateway in turn transfers the call to the MCU with the numeric ID of the dial string.

Step 7 – According to the numeric ID, the MCU searches for the appropriate Entry Queue and connects the participant to the Entry Queue. The participant is requested to enter the target conference Numeric ID.

Step 8 – According to this conference ID, the participant is routed to the appropriate conference. The participant is requested to enter the target conference/chairperson password.

[0122] EXAMPLE 4 – IP (H.323) Room-based Video Conferencing Call Flow is described in the following with reference to FIGURE 14.

Step 1 – Endpoint dials a number that is stated in the Reservation Confirmation which corresponds to the H.323 service prefix (64)

and the Entry Queue Numeric ID. Prior to that, the endpoint must register to the gatekeeper.

Step 2 – The call arrives at the firewall which has been configured to permit calls leaving the MMC network to be placed and for the media from the known endpoint to return to the caller on the LAN.

Step 3 – The number is sent to the active gatekeeper where, using the prefix, the gatekeeper identifies the MCU.

Step 4 – The gatekeeper translates the prefix to the IP alias of the MCU IP-48 card.

Step 5 – The call is transferred to the MCU with the numeric ID of the dial string.

Step 6 – According to the numeric ID, the MCU searches for the appropriate Entry Queue and connects the participant to the Entry Queue. The participant is requested to enter the target conference Numeric ID.

Step 7 – According to this conference ID, the participant is routed to the appropriate conference. The participant is requested to enter the target conference/chairperson password.

[0123] EXAMPLE 5 – IP (H.323) Integrated Desktop Conferencing (Audio & Video) Call Flow is described in the following with reference to FIGURE 15.

Step 1 – Desktop User clicks Join Conference button from MMC portal. System proceeds to establish a VPN tunnel (for security

purposes) using anonymous SSL login.

Step 2 – Desktop User submits conference details specified on the Reservation Confirmation. The call is made by the customized application and arrives at the firewall which has been configured to permit calls leaving the MMC network to be placed and for the media from the known endpoint to return to the caller.

Step 3 – The dial string which comprises the Network Service Prefix, EQ Numeric ID, Destination Conference Numeric ID and Password is sent to the active Gatekeeper where, using the prefix, the gatekeeper identifies the MCU.

Step 4 – The gatekeeper translates the prefix to the IP alias of the MCU IP-48 card.

Step 5 – The call is transferred to the MCU with the EQ numeric ID of the dial string.

Step 6 – According to the EQ numeric ID, the MCU searches for the appropriate Entry Queue and connects the participant to the Entry Queue.

Step 7 – According to the conference ID of the dial string, the participant is routed to the appropriate conference. And lastly, based on the target conference/chairperson password of the dial string, the endpoint is connected to the conference.

[0124] EXAMPLE 6 – IP (H.323) Integrated Desktop Conferencing (Audio, Video and Data) Call Flow is described in the following with reference to

FIGURE 16.

Step 1 – Desktop User clicks Join Conference button from MMC portal. System proceeds to establish a VPN tunnel (for security purposes) using anonymous SSL login.

Step 2 – Desktop User submits conference details specified on the Reservation Confirmation. The Video and Data call is made by the customized application and arrives at the firewall which has been configured to permit calls leaving the MMC network to be placed and for the media from the known endpoint to return to the caller.

Video Call

Step 3 – The dial string which comprises the Network Service Prefix, EQ Numeric ID, Destination Conference Numeric ID and Password is sent to the active Gatekeeper where, using the prefix, the gatekeeper identifies the MCU.

Step 4 – The gatekeeper translates the prefix to the IP alias of the MCU IP-48 card.

Step 5 – The call is transferred to the MCU with the EQ numeric ID of the dial string.

Step 6 – According to the EQ numeric ID, the MCU searches for the appropriate Entry Queue and connects the participant to the Entry Queue.

Step 7 – According to the conference ID of the dial string, the participant is routed to the appropriate conference. And lastly, based on the target conference/chairperson password of the dial string, the

endpoint is connected to the conference.

Data Call

Step 3 – The submitted Name, Conference Ref and PIN is sent to the Load Balancer.

Step 4 – The Load Balancer routes the requests to one of the Front End Servers. Upon external authentication by the Web server, the Data conference is created by the Front End Server.

Step 5 – The Primary Master Server starts the Data conference and assigns the conference to one of the Conference Servers.

Step 6 – Conference data (presentation slides, chat transcript) are hosted on the assigned Conference Server which also handles the running of the Data conference (broadcasting the media streams, synchronizing the input etc.) until the conference ends.

JOINING A CONFERENCE FROM VARIOUS END POINTS

[0125] Joining a video conference session in our video conferencing system from various end points are graphically illustrated in FIGURES 17 to 20 wherein joining from 3G Mobile end points, desktop clients, audio device (PSTN line phone), and Room-based system are respectively shown.

[0126] The flowchart in FIGURE 21 shows generally the various end points, i.e. 2G/ PSTN phone, ISDN Room, IP Room, 3G Video Phone and the Web

based Embedded Client dialling into the system via the MCU (1) to establish a conference session. Details on how our video conferencing system manages and allocates the actual AV conference resources for various end point types are further elaborated in the next flowchart, i.e. FIGURE 22.

[0127] Basically, our system processes the conference level checking first, followed by participant resource checking. If the requested conference is already ongoing conference, the system will inform the MCU to allow the on-going participant to extend participation in the conference as long as there is sufficient resource allocation.

[0128] If the requested conference is an on-demand conference which has yet started, the system will inform the MCU to create a new conference based on predefined conference template and allow the participant to join conference as long as there is sufficient resource allocation. If the requested conference is an invalid conference, MMC will inform MCU to reject the participant.

[0129] Information on the exact end point type is important in order to make sure the resource calculation is accurate because different end point type consumes different conference resource. However, such information is not passed to the video conferencing system during MCU external authentication. The acquiring of the pertinent information is instead achieved by querying the MCU entry queue about the end point detail for those waiting participant with the same alias and conference reference.

[0130] Although there is no difference in terms of the flow logic when either 2G/PSTN, 3G, IP Room and/or ISDN room join the conference, the computer or PC end point type needs to be treated as a special case. Please look at the condition box "Is end point type a computer?" in FIGURE 22 in respect of both the ongoing conference flow and on-demand conference flow. If this condition is true, there is no need to check the resource for computer and MCU will grant conferencing access to computer directly. The reason for the computer's exemption from resource availability check is that the computer needed to login to the web portal before it could call into the MCU entry queue. Thus all the necessary resource checking has been done during the web portal authentication flow. To further explain this situation whereby a computer-based end point joins a conference session, we would refer to FIGURE 23 wherein is shown a PC-based end point in the form of a web-based embedded client dials into the system to establish a conference session.

[0131] The flowchart diagram in FIGURE 24 depicts the detail flow for the Web-based Embedded Client dialling into the system to establish a conference session. This flow further elaborates the steps in FIGURE 23 in respect of how the video conferencing system manages and allocates the actual AV conference resources for computer end point types.

[0132] Our video conferencing system processes the conference level checking first, followed by participant resource checking. If the requested

conference is already ongoing conference, the video conferencing system will inform the MCU to allow the participant to join conference as long as there is sufficient resource allocation.

[0133] If the requested conference is an on-demand conference which has yet started, the system will inform the MCU to create a new conference based on predefined conference template and allow the participant to join conference as long as there is sufficient resource allocation. If the requested conference is an invalid conference, our video conferencing system will inform MCU to reject the participant.

[0134] There is an authentication of PIN for computer participant, which need to key in the PIN at the login web page. The computer-based end point which request the system to authenticate the PIN, the PIN authentication for the rest end point types is done by MCU. Upon successful authentication, the MCU will dial out to the end points, as depicted in FIGURES 25 – 26 to establish a conference session. Specifically, FIGURE 25 shows the MCU dialling out to defined participating end points while FIGURE 26 shows the MC dialling out to undefined participating end points.

DYNAMIC RESOURCE ALLOCATION

[0135] One of the key feature of our video conferencing system is the ability to

dynamically allocate conferencing resources to the various end points. In a simplified manner, FIGURE 27 illustrates the various combinations of scheduled and unscheduled conferences with dial-in and dial out options for different types of end points including:

- IP room-based codec (IP);
- ISDN room-based codec (ISDN);
- 2G/PSTN audio phone (AP);
- 3G; and
- PC-based participant.

[0136] With reference to FIGURE 28 to FIGURE 32 collectively, the logic flow of the dynamic allocation of resources for the Gatekeeper Web Account may be described in the following.

[0137] A PC participant would typically join a conference via the video component embedded in the web page. The participant may be a scheduled or *ad hoc* participant. The video component embedded in the web page for conducting the audio/video conference is an H.323 client (hereby referred to as "**H.323 web client**") which need to register with a H.323 gatekeeper (hereby referred to as "**gatekeeper**") via the given user name and password account (hereby called gatekeeper web account) before the PC participant initiate a audio/video conference call.

[0138] The gatekeeper web account used by the video component is

provisioned or registered in gatekeeper in advance. There is no limit on the maximum number of web accounts that may be created in gatekeeper. However, since it is not feasible to provision an unlimited number of web accounts in gatekeeper, a fixed number of web accounts is preferably provisioned into gatekeeper during system setup stage. It should be noted that this kind of account is only used for the H.323 web client (PC participant) to login to the gatekeeper. A table is maintained in the video conferencing system's database to store the same account information for purposes of the dynamic account allocation during joining conference stage via web portal.

[0139] The total number of gatekeeper web account provisioned in gatekeeper is preferably double the total number of concurrent calls limited by licensing. This is a preferred quantity in terms of the searching performance on the accounts records, i.e. having too many accounts would result in slower search performance during the process of dynamically allocating resources to the accounts. Besides, the concurrent call license limit would be always be hit first before the number of gatekeeper web account total is reached. Hence, there is no point in provisioning a number of accounts far too many than the license limit.

[0140] The license limit on the maximum concurrent connections (say, for example, 100) in the H.323 gatekeeper means the total number of the connected call at any one time via the gatekeeper should not exceed the license limit. This license limit would apply to all the H.323 clients, including the combined total of H.323 web clients, 3G mobile phones and IP room based codecs.

[0141] There are two approaches to allocating the gatekeeper web account to a PC participant: (i) the conventional pre-allocation during conference reservation time, and our novel (ii) dynamic-allocation upon a PC participant joining the conference time.

[0142] For the pre-allocation approach, when the conference chairman tries to extend the conference duration, the gatekeeper web account used for the connected PC participants in this conference session might have been allocated to the participants of a second conference which is supposed to start immediately after the first conference ends. As one gatekeeper account can only be used by one PC participant, the conference extension request would be rejected due to the conflicting allocation of the gatekeeper web account.

[0143] Dynamic-allocation would solve this conflict as it guarantees only the free account would be allocated to the requesting PC participant and the allocated accounts will be valid for the whole conference duration, including the extended period. In our proposed system, the gatekeeper web account can only be dynamically allocated to the H.323 web client after the conference authentication is passed and there is still free concurrent call license available with the gatekeeper. The steps involved in the dynamic allocation process may include the following.

[0144] The scenario may begin with a PC Participant logging in to the join

conference at the login page. The system authenticates the PC participant by verifying the conference reference code and PIN. If passed, the system would check the following information in order to determine if there is any free gatekeeper concurrent call licenses available in the gatekeeper:

1. The total number of the reserved PC participants in the video conferencing system for the current time slot is determined.
2. The total number of connected *ad-hoc* PC participants in the video conferencing system for the current time slot is determined.
3. The total number of the reserved 3G participants in the video conferencing system for the current time slot is determined.
4. The total number of the connected ad-hoc 3G participants in the video conferencing system for the current time slot is determined.
5. The total number of the reserved IP room based participants in the video conferencing system for the current time slot is determined.
6. The total number of the connected *ad-hoc* IP room based participants in the video conferencing system for the current time slot is determined.

[0145] If the sum of the above participants, each of whom would take up one gatekeeper concurrent connection license, does not exceed the maximum concurrent license limit, system will look up the table and find an available gatekeeper web account from the account pool. The selected account will then be passed over to the H.323 web client for it to login to gatekeeper server.

[0146] If the PC participant is an *ad-hoc* PC participant, the gatekeeper web account will be released back to the account pool once the PC participant logoff from the conference. The released account can be then used for a new allocation.

[0147] If the PC participant is a scheduled PC participant, the gatekeeper web account will be released back to the account pool after the whole conference ends. The released account can be then used for a new allocation.

[0148] Although specific models of hardware, such as the MCU being a *Polycom* MGC-100™ and the 3G gateway being a *Dilithium* DTG-2000™, are described as specific embodiments, it will be appreciated by a person having ordinary skill in the art that many of these devices or hardware may be substituted with equivalents or comparable devices available in the market or which may be modified or adapted from suitable devices or built from components with ordinary engineering skills.

[0149] Some of the networks and systems layout and method disclosed herein may also be alternatively configured, modified or adapted accordingly for purposes of achieving specific preferred features. These substitutes, equivalents, modifications, adaptations, reconfigurations or alternative embodiments which are not specifically described herein are nevertheless to be considered as falling within the scope and intent of the following claims.

CLAIMS

What we claim are:

1. A method of regulating number of concurrent participating end points, including PSTN, ISDN, IP and 3G-based end points, (all of which are hereinafter referred to as "**participants**") in a video conferencing system employing multimedia data streaming codec in ITU H.323 network protocol standard, said number of concurrent participants is regulated to within a predetermined maximum number at a H.323 gatekeeper, said method comprising the steps of:

(a) authenticating whether a participant attempting to login has pre-registered with the system with requisite information provided and stored as said participant's gatekeeper web account, said authenticating includes verifying one or more of participant's identity (ID), password (PIN) and conference reference code;

(b) determining from the conference reference code whether said participant has a scheduled conference reservation or is seeking *ad hoc* conferencing;

(c) if said participant has conference reservation, using said participant's login ID and PIN to identify and retrieve the participant's gatekeeper web account to be presented as an H.323 client and registering the same with the H.323 gatekeeper, thus inducting said participant into the video conference;

(d) if said participant is seeking *ad hoc* conferencing (hereinafter referred to as "***ad hoc* participant**"), checking for free concurrent participant

available in the H.323 gatekeeper, wherein the free concurrent participant available is a pool of balance of the predetermined maximum number less the number of other concurrent participants engaged in on-going teleconferencing sessions in the teleconferencing system;

(e) upon availability of free concurrent participant, admitting said *ad hoc* participant into the sought teleconference session by identifying and retrieving said *ad hoc* participant's gatekeeper web account from said *ad hoc* participant's login ID and PIN, and presenting said *ad hoc* participant's gatekeeper web account as an H.323 client and registering the same with the H.323 gatekeeper server; and

(f) upon each participant, whether *ad hoc* or having reservation, leaving a teleconferencing session by logging off, deregistering said participant's gatekeeper web account from the H.323 gatekeeper and releasing the number of leaving participants to the pool of available free concurrent participants.

2. A method of regulating a number of concurrent participants in a video conferencing system according to Claim 1 wherein the predetermined maximum number of concurrent participants admissible by the H.323 gatekeeper is predetermined on the basis of resource allocation, including at least one of bandwidth capacity, traffic volume, devices or device firmware, software or codecs, including user licenses allowed and like copyright issues.

3. A method of regulating a number of concurrent participants in a video

conferencing system according to Claim 2 wherein the predetermined maximum number of concurrent participants is base on the number of codec licenses allowed and each license is tracked based on the number of participants concurrently registered with the H.323 gatekeeper.

4. A method of regulating a number of concurrent participants in a video conferencing system according to Claim 1 wherein a participant having conference reservation may seek to extend the conference session, or extend his participation in the conference session, at the end of the reserved time slot by seeking as an *ad hoc* participant as in step (d).

5. A method of regulating a number of concurrent participants in a video conferencing system according to Claim 1 wherein the participant has pre-registered his particulars at a webpage which is retrievably stored in the form of a gatekeeper web account, wherein said account may be provided to be registered with the H.323 gatekeeper in accordance with the aforesaid method steps.

6. A method of regulating a number of concurrent participants in a video conferencing system according to Claim 1 wherein at least a multipoint control unit (hereinafter referred to as "**MCU**") is employed to integrate and/or moderate the multimedia data streams from multiple participants in various network format, including Internet Protocol (hereinafter referred to as "**IP**"), Public Services Telephone Network (hereinafter referred to as "**PSTN**"), Integrated Services Digital Network (hereinafter referred to as "**ISDN**") and 3G cellular network.

7. A method of regulating a number of concurrent participants in a video conferencing system according to Claim 6 wherein a MCU is employed to integrate and/or moderate data streams from IP, PSTN, ISDN networks, and a 3G gateway is employed to integrate and/or moderate data streams from 3G cellular network.

8. A method of regulating a number of concurrent participants in a video conferencing system according to Claim 7 wherein the MCU is a *Polycom* MGC-100™.

9. A method of regulating a number of concurrent participants in a video conferencing system according to Claim 7 wherein the 3G gateway is a *Dilithium* DTG-2000™.

10. A method of regulating a number of concurrent participants in a video conferencing system according to Claim 7 wherein the data streams from the MCU and 3G gateway are seamlessly integrated and moderated.

11. A method of regulating a number of concurrent participants in a video conferencing system according to Claim 7 wherein the MCU includes any one or combination of applications, firmware or hardware including

- built-in H.323 gatekeeper,
- call manager, including video PBX with call switching, forwarding

and transfer;

- data network management for quality of service (QoS);
- bandwidth management; and
- accounting

provided in the form of components or modules of the videoconferencing system.

12. A method of regulating a number of concurrent participants in a video conferencing system according to Claim 1 wherein the number of participants ("participating end points") counted are based on the total or combined total of each of the following end points types:

- PC-based VoIP applications and accessories;
- IP end point, including room-based hardware, accessories and codec;
- ISDN room-based codec
- audio phone, including 2G (GSM) and PSTN networks;
- video phone, including 3G networks.

13. A method of regulating a number of concurrent participants in a video conferencing system according to Claim 1 wherein the number of gatekeeper web accounts allowed provisional reservation status in the pool to be considered for video conferencing services to be double the number of predetermined maximum number of allowed concurrent participants.

14. A method of regulating a number of concurrent participants in a video conferencing system according to Claim 13 wherein the first available

gatekeeper web account from the pool is picked to join the video conference session.

15. A method of regulating a number of concurrent participants in a video conferencing system according to Claim 1 wherein the participants' gatekeeper web accounts are retrievably stored in a database managed by the video conferencing system, wherein upon a participant being accepted to join a video conference session, said participant's gatekeeper web account is retrieved and sent to the H.323 gatekeeper to be registered.

16. A method of regulating a number of concurrent participants in a video conferencing system according to Claim 1 wherein all participants' (i.e. including both *ad hoc* and those having reservation) requests are channeled to an MCU entry queue.

17. A method of regulating a number of concurrent participants in a video conferencing system according to Claim 16 wherein the MCU entry queue implements a single dial entry sequence so as to process and approve each request in turn according to the aforesaid steps to keep in count the number of concurrent participants to within the predetermined maximum number.

18. A method of regulating a number of concurrent participants in a video conferencing system according to Claim 1 executed in the order recited.

19. A gatekeeper and/or a (or link to a) network proxy server, implementing at least one of steps (a) to (f) as part of implementing a video conferencing system according to a method according to one of Claims 1 – 18.

20. An MCU and/or call manager implementing at least one of steps (a) to (f) as part of implementing a video conferencing system according to a method according to one of Claims 1 – 18.

21. A gateway, including a media gateway controller (MGC), implementing at least one of steps (a) to (f) as part of implementing a video conferencing system according to a method according to one of Claims 1 – 18.

22. An end point implementing at least one of steps (a) to (f) as part of implementing a video conferencing system according to a method according to one of Claims 1 – 18.

23. A video conferencing system incorporating any one or combination of the devices according to Claims 19 – 22.

24. A video conferencing system incorporating a method according to one of Claims 1 – 18 as part of implementing a video conferencing session.

*****