

TANDBERG Endpoints and IP

TANDBERG

D12434, Rev 3.3

Table of Contents

1. INTRODUCTION	4
2. WHAT IS H.323?	4
2.1 COMPONENTS	4
2.1.1 Terminals	4
2.1.2 Gatekeepers	5
2.1.3 Gateways	5
2.1.4 Multipoint Control Units	6
2.2 STANDARDS	7
2.2.1 The Audio Standards:	8
2.2.2 The Video Standards:	8
2.2.3 The Communications Standards:	8
2.2.4 The Encryption Standards:	8
3. TANDBERG'S IP IMPLEMENTATION	9
3.1 COMMON IMPLEMENTATION FEATURES	9
3.1.1 Remote Management	9
3.2 B1 SOFTWARE	10
3.2.1 Main Features	10
3.2.2 Layer 4 Ports Used	10
3.2.3 Example of Point to Point call using B1 (IP direct dialing)	11
3.2.4 B1 Through A FireWall	12
3.2.5 Audio (IP)	12
3.2.6 Video (IP)	12
3.2.7 Latency	12
3.3 B2 SOFTWARE	13
3.3.1 Main Features	13
3.3.2 Layer 4 Ports Used	13
3.3.3 Example of Point to Point call using B2 (IP direct dialing)	14
3.3.4 B2 Through A Firewall	15
3.3.5 Audio	15
3.3.6 Video	15
3.3.7 Jitter And Latency	15
3.4 B3 SOFTWARE	16
3.4.1 Main Features	16
3.4.2 Layer 4 Ports Used	17
3.4.3 Example of Point to Point call using B3 (IP direct dialing)	19
3.4.4 B3 Through A Firewall	20
3.4.5 Audio	21
3.4.6 Video	21
3.4.7 Jitter And Latency	21
3.5 B4, B5, B6, E1 SOFTWARE	22
3.5.1 B4 Main IP Features	22
3.5.2 B5 Main IP Features	22
3.5.3 B6 Main IP Features	22
3.5.4 E1 Main IP Features	22
3.5.5 Layer 4 Ports Used	23
3.5.6 Example of Point to Point (IP direct dialing)	25
3.5.7 Conferencing Through A Firewall	26
3.5.8 Audio	27
3.5.9 Video	27
3.5.10 Jitter And Latency	28

4.	TANDBERG'S H.323 FEATURES	29
4.1	SPECIAL FEATURES	29
4.1.1	<i>H.323 MultiSite^{TF}</i>	29
4.1.2	<i>Intelligent Packet Loss Recovery (IPLR^{TF})</i>	29
4.1.3	<i>H.235 Encryption</i>	29
4.2	PRESENTATIONS	30
4.2.1	<i>H.323 Duo Video^{TF}</i>	30
4.2.2	<i>High Bandwidth Streaming</i>	31
4.3	QUALITY OF SERVICE	31
4.3.1	<i>RSVP</i>	31
4.3.2	<i>Differential Services</i>	32
4.3.3	<i>IP Precedence and Type of Service</i>	33
4.4	REMOTE MANAGEMENT	34
4.4.1	<i>Simple Network Management Protocol (SNMP)</i>	34
4.4.2	<i>HTTP Server</i>	34
4.4.3	<i>FTP Server</i>	35
4.4.4	<i>Telnet Server</i>	35
4.5	VIDEO	35
4.5.1	<i>Natural Video^{TF} 60 FPS Interlaced Video</i>	35
4.5.2	<i>H.263+ Custom Video Formats (Digital Clarity^{TF})</i>	36
4.5.3	<i>4CIF Digital Clarity^{TF}</i>	36
4.6	OTHER	36
4.6.1	<i>Network Address Translation (NAT) Support</i>	36
4.6.2	<i>Auto Gatekeeper Discovery</i>	37
4.6.3	<i>TCS-4</i>	37
4.6.4	<i>Asymmetrical Encoders and Decoders</i>	38
4.6.5	<i>Inband Switching of Video and Audio Algorithms</i>	38
4.6.6	<i>Flow Control</i>	38
4.6.7	<i>Dynamic Bandwidth Management</i>	38
4.6.8	<i>Lip Sync</i>	39
5.	H.323 COMMUNICATIONS WITH TANDBERG SYSTEMS.....	40
5.1	ONLY CALLING ENDPOINT HAS GATEKEEPER	41
5.2	ONLY CALLED ENDPOINT HAS GATEKEEPER	42
5.3	BOTH ENDPOINTS REGISTERED TO DIFFERENT GATEKEEPERS	44
6.	LIST OF TERMS.....	46
7.	APPENDIX A	48
7.1	POLYCOM H.323 LAYER 4 PORTS	48
7.2	PICTURETEL H.323 LAYER 4 PORTS	49

1. Introduction

H.323 is an International Telecommunications Union (ITU) standard that describes the protocols, services and equipment necessary for multimedia communications including audio, video and data on networks without guaranteed Quality of Service (QoS). These networks technologies may include Ethernet, Fast Ethernet, and Token Ring and protocols like Internet Protocol (IP) or Integrated Packet Exchange (IPX). Due to the need to communicate between smaller networks connected to the Internet, IP will be a more popular transport for H.323.

Today, the dominant method of Internet communications is email. However, there is a growing need to increase communications to include audio, video and data. The explosion of the Internet in the early 1990's has paved the way to higher bandwidth connections to corporate offices, universities and even to the home. Now that the bandwidth is available, the demand for multimedia communications over the Internet is growing.

2. What is H.323?

H.323 is an umbrella recommendation from the International Telecommunications Union (ITU) that sets standards for “terminals and other entities that provide multimedia communications services over Packet Based Networks (PBN) which may not provide a guaranteed Quality of Service”.

2.1 Components

H.323 specifies several new standards to allow for communications between terminals on IP networks. These standards dictate how different mandatory and optional components of the H.323 standard interoperate with each other. The major network components of H.323 include the mandatory terminal, and the optional gatekeeper, gateway and multipoint control unit (MCU).

2.1.1 Terminals

The terminal or endpoint must support a minimum of G.711 audio, H.225, H.245, Q.931 and RTP. If the terminal supports video, it must support a minimum of H.261 QCIF. The terminal may support T.120 data sharing although this support is optional. The TANDBERG 550, 880, 1000, 2500, 6000 and 8000 video conferencing systems all fit the definition of a H.323 terminal.



TANDBERG 1000



TANDBERG 880



TANDBERG 8000

2.1.2 Gatekeepers

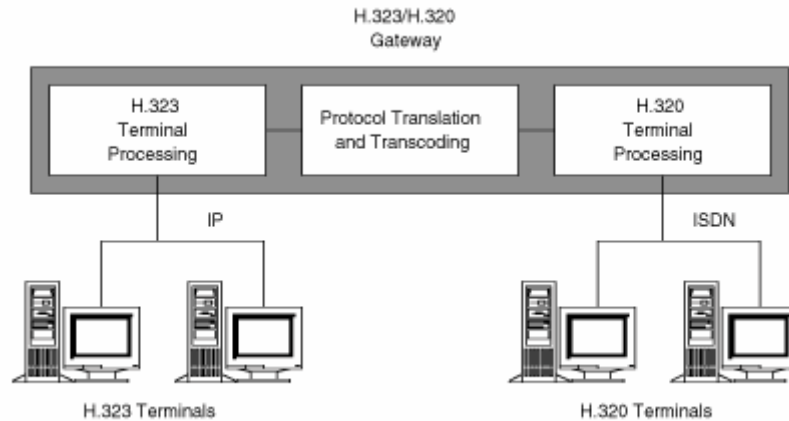
The gatekeeper is an optional component of H.323 that is responsible for managing other components of a H.323 network. It is a very important component to the managed network. The gatekeeper has several responsibilities which include: translation of E.164 aliases to IP addresses, bandwidth management of incoming or outgoing calls, call admission to accept or deny calls, and zone management. Gatekeepers can also support an optional feature that allows a call to be rerouted if there is no answer from the intended terminal. Gatekeepers also help manage different H.323 zones and help manage H.323 MCU sessions. It is important to remember that while gatekeepers are optional, the H.323 terminal must make use of the gatekeeper's services if the gatekeeper is present in the network.

Gatekeepers are typically software products that reside on a server. Although many H.323 MCUs and gateways have embedded gatekeepers, they usually offer less features than stand alone gatekeepers.

There are several gatekeepers that are readily available on the market including the Cisco MCM and the RADVision ECS.

2.1.3 Gateways

If there is a need for a H.323 terminal to communicate with another terminal on a H.320, H.324 or analog PSTN networks, a H.323 gateway is required to perform the translation. This optional component typically has ISDN and IP network connections and support the translation between these two networks. The number of simultaneous connections allowed through a gateway is not specified in any standard, so there are different options available from different manufacturers. Gateways typically have built in gatekeepers with minimal features.



There are a several manufacturers of gateways on the market today. Some good examples are the TANDBERG Gateway, Cisco 3540 gateway and the RADVision ViaIP gateway.



TANDBERG Gateway (front)



TANDBERG Gateway (rear)

2.1.4 Multipoint Control Units

The last of the major components is the MCU which controls conferences between 3 or more terminals. The H.323 MCU may be a separate component or may be incorporated into a terminal. The TANDBERG 880, 2500, 6000 and 8000 have optional software packages that enable internal H.323 MCU capabilities. The TANDBERG products are capable of providing MCU services for up to 4 sites. If support for more than 4 sites is required, TANDBERG recommends and can provide larger MCUs.

There are a several manufacturers of MCUs on the market today. Some good examples include TANDBERG, Cisco and RADVision.



TANDBERG MCU (front)



TANDBERG MCU (rear)

2.2 Standards

H.323 has its own collection of standards that are defined in the chart below. We have included the other popular communications standards as a comparison.

	H.320	H.321	H.322	H.323 V1/V2	H.324
Approval Date	1990	1995	1995	1996/1998	1996
Network	Narrowband switched digital ISDN	Broadband ISDN ATM LAN	Guaranteed bandwidth packet switched networks	Non-guaranteed bandwidth packet switched networks, (Ethernet)	PSTN or POTS, the analog phone system
Video	H.261 H.263 H.264	H.261 H.263	H.261 H.263	H.261 H.263 H.264	H.261 H.263
Audio	G.711 G.722 G.722.1 G.728	G.711 G.722 G.728	G.711 G.722 G.728	G.711 G.722 G.722.1 G.728 G.723 G.729	G.723
Multiplexing	H.221	H.221	H.221	H.225.0	H.223
Control	H.230 H.242	H.242	H.242 H.230	H.245	H.245
Multipoint	H.231 H.243	H.231 H.243	H.231 H.243	H.323	
Data	T.120	T.120	T.120	T.120	T.120
Comm. Interface	I.400	AAL I.363 AJM I.361 PHY I.400	I.400& TCP/IP	TCP/IP	V.34 Modem
Text Chat	T.140	T.140	T.140	T.140	T.140
Encryption	H.233 H.234	H.233 H.234		H.235	H.233 H.234

2.2.1 The Audio Standards:

- G.711:** 64 Kbps, 8K samples/sec, 8-bit companded PCM (A-law or μ -law), high quality, low complexity. Required for H.320 and H.323.
- G.722:** ADPCM audio encode/decode (64 kbit/s, 7 kHz).
- G.723:** Speech coder at 6.3 and 5.3 Kbps data rate. Medium complexity. Required for H.324; Optional for H.323.
- G.728:** 16 Kbps, LD-CELP, high quality speech coder, very high complexity. Optional for H.320 and H.323.
- G.729:** 8Kbps, LD-CELP, high quality speech coder, medium complexity. G.DSVD is an interoperable subset.
- GSM:** Group Special Mobile -- European telephony standard, not ITU. Used by ProShare Video Conferencing software versions 1.0-1.8. 13Kbps, medium quality for voice only, low complexity.

2.2.2 The Video Standards:

- H.261:** Supports 352x288 (CIF or FCIF) and 176x144 (QCIF). DCT-based algorithm tuned for 2B to 6B ISDN communication. Required for H.320, H.323, and H.324.
- H.263:** Much-improved derivative of H.261, tuned for POTS data rates. Mostly aimed at QCIF and Sub-QCIF (128x96 -- SQCIF), while providing better video than H.261 on QCIF and CIF. Optional for H.323.
- H.264:** Joint collaboration between the ITU and ISO. Improved video over H.263 providing similar quality at half the bandwidth.

2.2.3 The Communications Standards:

- H.221:** Frame Structure 64-1920 Kbps.
- H.223:** Multiplexing protocol for low-bit rate multimedia communication.
- H.225:** Media Stream Packetization and synchronization on non-guaranteed quality-of service LANs.
- H.230:** Frame synchronous control and indication signals for audio visual systems.
- H.242:** System for establishing audio visual terminals using digital channels up to 2Mbps.
- H.243:** Procedures for establishing communication between three or more audio visual terminals using digital channels up to 2 Mbps.
- H.245:** Control of communications between visual telephone systems and terminal equipment on non-guaranteed bandwidth LANs.

2.2.4 The Encryption Standards:

- H.233:** Confidentiality system for audiovisual services
- H.234:** Encryption key management and authentication system for audiovisual services (Diffie-Hellman key exchange)
- H.235:** Security and Encryption for H.323 multimedia terminals

3. TANDBERG's IP Implementation

TANDBERG implemented IP video in all of its products beginning with B1 in October 2000. There have been several subsequent versions of software since that have expanded the feature set of the TANDBERG products, some of which are defined in this document. For a full description of the features, please consult your user's manual.

Version	Release Date
B1	October 2000
B2	February 2001
B3	July 2001
B4	February 2002
B5	November 2002
B6/E1	January 2003
B7/E2	July 2003

Please consult the appropriate section for details on a particular version of software.

3.1 Common Implementation Features

3.1.1 Remote Management

TANDBERG systems have four methods of remote management.

1. **HTTP:** The systems have an embedded web browser for remote setup and control
2. **Telnet:** The systems have an embedded telnet server for full access to the codec's dataport functionality
3. **FTP:** The systems have an embedded FTP server for uploading software, directories and codec configuration files. In addition, the directory and codec configuration files can be downloaded using FTP.
4. **SNMP:** The systems have an embedded SNMP manager for proactive reporting of problems and systems status. The TANDBERG Management Suite (TMS) makes use of this feature.

With B5 and later software, these services can be disabled.

3.2 B1 Software

3.2.1 Main Features

The main IP features in the B1 release are:

1. H.323 point to point calls
2. H.323 max bandwidth of 2Mbps
3. Streaming (not in a call)
4. Cisco's IP Precedence
5. H.323 Version 2

3.2.2 Layer 4 Ports Used

Point to Point / MultiSite^{TF} / DuoVideo^{TF}

Function	Port	Type	Direction
Gatekeeper RAS	1719	UDP	↔
Gatekeeper Discovery	224.0.1.41:1718	UDP	↔
Q.931 Call Setup	1720	TCP*	↔
H.245	Range 1024 – 65535	TCP	↔
Video	Range 2326 – 2500	UDP	↔
Audio	Range 2326 – 2500	UDP	↔
Data/FECC	Range 2326 – 2500	UDP	↔
FTP	21	TCP*	↔
Telnet	23	TCP*	↔
HTTP	80	TCP*	↔
NTP	123	UDP*	⇐ (incoming to codec)
SNMP (Queries)	161	UDP*	↔
SNMP (Traps)	962	UDP	⇒ (outgoing from codec)
Netlog	963	TCP	↔
FTP/data	964	TCP	↔
VNC	965	TCP	↔
Streaming/RTP Video	970	UDP	⇒
Streaming/RTCP Video	971	UDP	⇒
Streaming/RTP Audio	972	UDP	⇒
Streaming/RTCP Audio	973	UDP	⇒
SAP**	974	UDP	⇒

* denotes a listening port.

** stream is directed to 224.2.127.254, port 9875

3.2.3 Example of Point to Point call using B1 (IP direct dialing)

Using two sites known as 'Site Alice' and 'Site Bob'. Alice will call Bob:

Call Connect:

1. Alice creates a TCP socket for Q.931 and connects to Bob:1720. ***The source port on Alice is dynamic and cannot be predicted (range 1024 – 65535)***
2. Bob creates a TCP socket for H.245 and binds it to port 5555
3. Bob sends Q.931 'connect' to Alice and in this message it tells Alice what port the H.245 socket is on
4. Alice creates a TCP socket for H.245 and connects it to the specified port on Bob. ***The source port on Alice is dynamic and cannot be predicted (range 1024 – 65535)***
5. Capability sets are exchanged
6. Master/slave determination
7. Call is connected

Video Media Stream:

8. Alice creates two UDP sockets, one for RTP and one for RTCP. It binds the RTP socket to an even port number and the RTCP socket to the following odd port number. ***The RTP and RTCP ports cannot be predicted (range 2326—2500)***
9. Alice sends OpenLogicalChannel to Bob which contains the address and port for the RTCP socket
10. Bob creates two UDP sockets, one for RTP and one for RTCP. It binds the RTP socket to an even port number and the RTCP socket to the following odd port number. ***The RTP and RTCP ports cannot be predicted (range 2326—2500)***
11. Bob responds with OpenLogicalChannelAck which contains the addresses and ports for the RTP/RTCP sockets.

Audio Media Stream:

12. Alice creates two UDP sockets, one for RTP and one for RTCP. It binds the RTP socket to an even port number and the RTCP socket to the following odd port number. ***The RTP and RTCP ports cannot be predicted (range 2326—2500)***
13. Alice sends OpenLogicalChannel to Bob which contains the address and port for the RTCP socket
14. Bob creates two UDP sockets, one for RTP and one for RTCP. It binds the RTP socket to an even port number and the RTCP socket to the following odd port number. ***The RTP and RTCP ports cannot be predicted (range 2326—2500)***
15. Bob responds with OpenLogicalChannelAck which contains the addresses and ports for the RTP/RTCP sockets.

Data/FECC Media Stream:

16. Alice creates two UDP sockets, one for RTP and one for RTCP. It binds the RTP socket to an even port number and the RTCP socket to the following odd port number. ***The RTP and RTCP ports cannot be predicted (range 2326—2500)***
17. Alice sends OpenLogicalChannel to Bob which contains the address and port for the RTCP socket

18. Bob creates two UDP sockets, one for RTP and one for RTCP. It binds the RTP socket to an even port number and the RTCP socket to the following odd port number. ***The RTP and RTCP ports cannot be predicted (range 2326—2500)***
19. Bob responds with OpenLogicalChannelAck which contains the addresses and ports for the RTP/RTCP sockets.

3.2.4 B1 Through A FireWall

If TANDBERG (B1) solutions are used, opening the following ports, incoming and outgoing, will enable H.323 point to point, MultiSite^{TF}, and DuoVideo^{TF} communications through a firewall:

Point to Point / MultiSite^{TF} / DuoVideo^{TF}

Function	Port	Type	Direction
Gatekeeper RAS	1719	UDP	↔
Gatekeeper Discovery	224.0.1.41:1718	UDP	↔
Q.931 Call Setup	1720	TCP*	↔
H.245	Range 1024 – 65535	TCP	↔
Video	Range 2326 – 2500	UDP	↔
Audio	Range 2326 – 2500	UDP	↔
Data/FECC	Range 2326 – 2500	UDP	↔

This port range should work for most manufacturers of video conferencing endpoints.

* denotes a listening port.

3.2.5 Audio (IP)

The B1 audio codec of the TANDBERG systems supports G.711, G.722 and G.728. TANDBERG uses 20ms packets to transmit audio.

3.2.6 Video (IP)

The B1 video codec of the TANDBERG systems supports H.261 (QCIF, CIF, annex D), and H.263 (CIF, 4CIF). TANDBERG video is variable and will only take the required bandwidth to transmit the video at a given instant.

3.2.7 Latency

Latency can be defined as the time between a node sending a message and receipt of the message by another node. The TANDBERG systems can handle any value of latency, however, the higher the latency, the longer the delay in video and audio. This may lead to conferences with undesirable delays causing participants to interrupt and speak over each other.

3.3 B2 Software

3.3.1 Main Features

The main IP features in the B2 release are:

1. MultiSite^{TF} (4 sites at 768kbps, 3 sites at 1Mbps)
2. DuoVideo^{TF}
3. Far End Camera Control
4. TCS-4 support for gateways
5. Natural Video^{TF} H.263+ 60fps interlaced video
6. Cisco's Type of Service (ToS)
7. Streaming during a call up to 384kbps

3.3.2 Layer 4 Ports Used

Point to Point / MultiSite^{TF} / DuoVideo^{TF}

Function	Port	Type	Direction
Gatekeeper RAS	1719	UDP	↔
Gatekeeper Discovery	224.0.1.41:1718	UDP	↔
Q.931 Call Setup	1720	TCP*	↔
H.245	Range 1024 – 65535	TCP	↔
Video	Range 2326 – 2500	UDP	↔
Audio	Range 2326 – 2500	UDP	↔
Data/FECC	Range 2326 – 2500	UDP	↔
FTP	21	TCP*	↔
Telnet	23	TCP*	↔
HTTP	80	TCP*	↔
NTP	123	UDP*	⇐ (incoming to codec)
SNMP (Queries)	161	UDP*	↔
SNMP (Traps)	962	UDP	⇒ (outgoing from codec)
Netlog	963	TCP	↔
FTP/data	964	TCP	↔
VNC	965	TCP	↔
Streaming/RTP Video	970	UDP	⇒
Streaming/RTCP Video	971	UDP	⇒
Streaming/RTP Audio	972	UDP	⇒
Streaming/RTCP Audio	973	UDP	⇒
SAP**	974	UDP	⇒

* denotes a listening port.

** stream is directed to 224.2.127.254, port 9875

3.3.3 Example of Point to Point call using B2 (IP direct dialing)

Using two sites known as 'Site Alice' and 'Site Bob'. Alice will call Bob:

Call Connect:

1. Alice creates a TCP socket for Q.931 and connects to Bob:1720. ***The source port on Alice is dynamic and cannot be predicted (range 1024 – 65535)***
2. B creates a TCP socket for H.245 and binds it to port 5555
3. Bob sends Q.931 'connect' to Alice and in this message it tells Alice what port the H.245 socket is on
4. Alice creates a TCP socket for H.245 and connects it to the specified port on Bob. ***The source port on Alice is dynamic and cannot be predicted (range 1024 – 65535)***
5. Capability sets are exchanged
6. Master/slave determination
7. Call is connected

Video Media Stream:

8. Alice creates two UDP sockets, one for RTP and one for RTCP. It binds the RTP socket to an even port number and the RTCP socket to the following odd port number. ***The RTP and RTCP ports cannot be predicted (range 2326—2500)***
9. Alice sends OpenLogicalChannel to Bob which contains the address and port for the RTCP socket
10. Bob creates two UDP sockets, one for RTP and one for RTCP. It binds the RTP socket to an even port number and the RTCP socket to the following odd port number. ***The RTP and RTCP ports cannot be predicted (range 2326—2500)***
11. Bob responds with OpenLogicalChannelAck which contains the addresses and ports for the RTP/RTCP sockets.

Audio Media Stream:

12. Alice creates two UDP sockets, one for RTP and one for RTCP. It binds the RTP socket to an even port number and the RTCP socket to the following odd port number. ***The RTP and RTCP ports cannot be predicted (range 2326—2500)***
13. Alice sends OpenLogicalChannel to Bob which contains the address and port for the RTCP socket
14. Bob creates two UDP sockets, one for RTP and one for RTCP. It binds the RTP socket to an even port number and the RTCP socket to the following odd port number. ***The RTP and RTCP ports cannot be predicted (range 2326—2500)***
15. Bob responds with OpenLogicalChannelAck which contains the addresses and ports for the RTP/RTCP sockets.

Data/FECC Media Stream:

16. Alice creates two UDP sockets, one for RTP and one for RTCP. It binds the RTP socket to an even port number and the RTCP socket to the following odd port number. ***The RTP and RTCP ports cannot be predicted (range 2326—2500)***
17. Alice sends OpenLogicalChannel to Bob which contains the address and port for the RTCP socket

18. Bob creates two UDP sockets, one for RTP and one for RTCP. It binds the RTP socket to an even port number and the RTCP socket to the following odd port number. ***The RTP and RTCP ports cannot be predicted (range 2326—2500)***
19. Bob responds with OpenLogicalChannelAck which contains the addresses and ports for the RTP/RTCP sockets.

3.3.4 B2 Through A Firewall

If TANDBERG (B2) solutions are used, the opening the following ports, incoming and outgoing, will enable H.323 point to point, MultiSite^{TF}, and DuoVideo^{TF} communications through a firewall:

Function	Port	Type	Direction
Gatekeeper RAS	1719	UDP	↔
Gatekeeper Discovery	224.0.1.41:1718	UDP	↔
Q.931 Call Setup	1720	TCP*	↔
H.245	Range 1024 – 65535	TCP	↔
Video	Range 2326 – 2500	UDP	↔
Audio	Range 2326 – 2500	UDP	↔
Data/FECC	Range 2326 – 2500	UDP	↔

* denotes a listening port

3.3.5 Audio

The B2 audio codec of the TANDBERG systems supports G.711, G.722 and G.728. TANDBERG uses 20ms packets to transmit audio.

3.3.6 Video

The B2 video codec of the TANDBERG systems supports H.261 (QCIF, CIF, annex D), H.263 (CIF, 4CIF) and H.263+ (Natural Video^{TF} 60fps interlaced video). TANDBERG video is variable and will only take the required bandwidth to transmit the video at any given instant.

3.3.7 Jitter And Latency

Latency can be defined as the time between a node sending a message and receipt of the message by another node. The TANDBERG systems can handle any value of latency, however, the higher the latency, the longer the delay in video and audio. This may lead to conferences with undesirable delays causing participants to interrupt and speak over each other.

Jitter can be defined as the difference in latency. Where constant latency simply produces delays in audio and video, jitter can have a more adverse effect. Jitter can cause packets to

arrive out of order or at the wrong times. TANDBERG can manage packets with jitter up to 100ms.

3.4 B3 Software

3.4.1 Main Features

The main IP features in the B3 release are:

1. H.323 and H.320 in the same conference
2. DuoVideo^{TF} in MultiSite^{TF}
3. MultiSite^{TF} Voice Switch Mode (new on IP)
4. Automatic DuoVideo^{TF}
5. Max bandwidth of 3Mbps
6. H.263+ Custom Formats (SVGA, VGA, SIF, iSIF, 4SIF)
7. H.323 Version 3
8. Network Address Translation (NAT) Support
9. Flow Control During Packet Loss
10. Virtual Network Computing (VNC) Support
11. Cisco IP/TV support (**B3.1**)

3.4.2 Layer 4 Ports Used

Point To Point + DuoVideo^{TF}

Function	Port	Type	Direction
Gatekeeper RAS	1719	UDP	↔
Gatekeeper Discovery	224.0.1.41:1718	UDP	↔
Q.931 Call Setup	1720	TCP*	↔
H.245	Range 5555—5556	TCP	↔
Video	Range 2326—2341	UDP	↔
Audio	Range 2326—2341	UDP	↔
Data/FECC	Range 2326—2341	UDP	↔
FTP	21	TCP*	↔
Telnet	23	TCP*	↔
HTTP	80	TCP*	↔
NTP	123	UDP*	⇐ (incoming to codec)
SNMP (Queries)	161	UDP*	↔
SNMP (Traps)	962	UDP	⇒ (outgoing from codec)
Netlog	963	TCP	↔
FTP/data	964	TCP	↔
VNC	965	TCP	↔
Streaming/RTP Video	970	UDP	⇒
Streaming/RTCP Video	971	UDP	⇒
Streaming/RTP Audio	972	UDP	⇒
Streaming/RTCP Audio	973	UDP	⇒
SAP**	974	UDP	⇒

MultiSite + DuoVideo^{TF}

Function	Port	Type	Direction
Gatekeeper RAS	1719	UDP	↔
Gatekeeper Discovery	224.0.1.41:1718	UDP	↔
Q.931 Call Setup	1720	TCP*	↔
H.245***	Range 5555—5560	TCP	↔
Video	Range 2326—2573	UDP	↔
Audio	Range 2326—2573	UDP	↔
Data/FECC	Range 2326—2573	UDP	↔
FTP	21	TCP*	↔
Telnet	23	TCP*	↔
HTTP	80	TCP*	↔
NTP	123	UDP*	⇐ (incoming to codec)
SNMP (Queries)	161	UDP*	↔
SNMP (Traps)	962	UDP	⇒ (outgoing from codec)
Netlog	963	TCP	↔
FTP/data	964	TCP	↔
VNC	965	TCP	↔
Streaming/RTP Video	970	UDP	⇒
Streaming/RTCP Video	971	UDP	⇒
Streaming/RTP Audio	972	UDP	⇒
Streaming/RTCP Audio	973	UDP	⇒
SAP**	974	UDP	⇒

* denotes a listening port.

** stream is directed to 224.2.127.254, port 9875

*** While using MultiSite^{TF}, if a site is disconnected and reconnected without terminating the entire conference, the next site to be connected will have a H.245 port outside of the specified range. If this functionality is required through a firewall, the range of TCP ports can be extended past 5560. However, if a site is disconnected and reconnected, without ending the conference, enough times you can quickly end up outside of this range again.

Outgoing call: First call uses port 5555 for outgoing Q.931 and port 5556 for H.245, next uses port 5557 for Q.931 and port 5558 for H.245, etc.

Incoming call: First uses port 5555 for H.245, second port 5556 etc. Disconnecting a site in a call will not free up available 55XX ports until the whole conference is down.

3.4.3 Example of Point to Point call using B3 (IP direct dialing)

Using two sites known as 'Site Alice' and 'Site Bob'. Alice will call Bob:

Call Connect:

1. Alice creates a TCP socket for Q.931 and connects to Bob:1720. ***The source port on Alice is 5555.***
2. Bob creates a TCP socket for H.245 and binds it to port 5555
3. Bob sends Q.931 'connect' to Alice and in this message it tells Alice what port the H.245 socket is on
4. Alice creates a TCP socket for H.245 and connects it to the specified port on Bob. ***The source port on Alice is dynamic and cannot be predicted (range 5556 – 5560, depending on the number of sites to be connected)***
5. Capability sets are exchanged
6. Master/slave determination
7. Call is connected

Video Media Stream:

8. Alice creates two UDP sockets, one for RTP and one for RTCP. It binds the RTP socket to an even port number and the RTCP socket to the following odd port number. ***The RTP and RTCP ports cannot be predicted (range 2326—2365)***
9. Alice sends OpenLogicalChannel to Bob which contains the address and port for the RTCP socket
10. Bob creates two UDP sockets, one for RTP and one for RTCP. It binds the RTP socket to an even port number and the RTCP socket to the following odd port number. ***The RTP and RTCP ports cannot be predicted (range 2326—2365)***
11. Bob responds with OpenLogicalChannelAck which contains the addresses and ports for the RTP/RTCP sockets.

Audio Media Stream:

12. Alice creates two UDP sockets, one for RTP and one for RTCP. It binds the RTP socket to an even port number and the RTCP socket to the following odd port number. ***The RTP and RTCP ports cannot be predicted (range 2326—2365)***
13. Alice sends OpenLogicalChannel to Bob which contains the address and port for the RTCP socket
14. Bob creates two UDP sockets, one for RTP and one for RTCP. It binds the RTP socket to an even port number and the RTCP socket to the following odd port number. ***The RTP and RTCP ports cannot be predicted (range 2326—2365)***
15. Bob responds with OpenLogicalChannelAck which contains the addresses and ports for the RTP/RTCP sockets.

Data/FECC Media Stream:

16. Alice creates two UDP sockets, one for RTP and one for RTCP. It binds the RTP socket to an even port number and the RTCP socket to the following odd port number. ***The RTP and RTCP ports cannot be predicted (range 2326—2365)***
17. Alice sends OpenLogicalChannel to Bob which contains the address and port for the RTCP socket

18. Bob creates two UDP sockets, one for RTP and one for RTCP. It binds the RTP socket to an even port number and the RTCP socket to the following odd port number. ***The RTP and RTCP ports cannot be predicted (range 2326—2326)***
19. Bob responds with OpenLogicalChannelAck which contains the addresses and ports for the RTP/RTCP sockets.

3.4.4 B3 Through A Firewall

In B3, TANDBERG has reduced the dynamic nature of the H.323 ports to a smaller range of possibilities. If TANDBERG (B3) solutions are used, the opening the following ports, incoming and outgoing, will enable H.323 point to point, MultiSite^{TF}, and DuoVideo^{TF} communications through a firewall:

Point To Point + DuoVideo^{TF}

Function	Port	Type	Direction
Gatekeeper RAS	1719	UDP	↔
Gatekeeper Discovery	224.0.1.41:1718	UDP	↔
Q.931 Call Setup	1720	TCP*	↔
H.245	Range 5555—5556	TCP	↔
Video	Range 2326—2340	UDP	↔
Audio	Range 2326—2340	UDP	↔
Data/FECC	Range 2326—2340	UDP	↔

MultiSite + DuoVideo^{TF}

Function	Port	Type	Direction
Gatekeeper RAS	1719	UDP	↔
Gatekeeper Discovery	224.0.1.41:1718	UDP	↔
Q.931 Call Setup	1720	TCP*	↔
H.245*	Range 5555—5560	TCP	↔
Video	Range 2326—2375	UDP	↔
Audio	Range 2326—2375	UDP	↔
Data/FECC	Range 2326—2375	UDP	↔

* denotes a listening port

This port range will work for TANDBERG (B3) solutions only. Because H.323 does not require a specific range of ports, other manufacturers may need to open up a larger range of ports to accommodate H.323 communications.

3.4.5 Audio

The B3 audio codec of the TANDBERG systems supports G.711, G.722 and G.728. TANDBERG uses 20ms packets to transmit audio.

3.4.6 Video

The B3 video codec of the TANDBERG systems supports H.261 (QCIF, CIF, annex D), H.263 (CIF, 4CIF) and H.263+ (Natural Video^{TF} 60fps interlaced video, custom formats SVGA, VGA, and SIF). TANDBERG video is variable and will only take the required bandwidth to transmit the video at any given instant.

3.4.7 Jitter And Latency

Latency can be defined as the time between a node sending a message and receipt of the message by another node. The TANDBERG systems can handle any value of latency, however, the higher the latency, the longer the delay in video and audio. This may lead to conferences with undesirable delays causing participants to interrupt and speak over each other.

Jitter can be defined as the difference in latency. Where constant latency simply produces delays in audio and video, jitter can have a more adverse effect. Jitter can cause packets to arrive out of order or at the wrong times. TANDBERG can manage packets with jitter up to 100ms. If excessive packet loss is detected, the TANDBERG systems will downspeed the connection until acceptable packet loss is achieved.

3.5 B4, B5, B6, E1, B7, E2 Software

3.5.1 B4 Main IP Features

The main IP features in the B4 release are:

1. RSVP
2. Cascading MultiSite^{TF} on IP

3.5.2 B5 Main IP Features

The main IP features in the B5 release are:

1. H.235 DES Encryption in point to point
2. H.235 DES Encryption in the embedded MCU
3. Differential Services QoS
4. Audio only IP participants in the embedded MCU
5. Disable FTP, Telnet, HTTP, SNMP, and H.323
6. Intelligent Packet Loss Recovery (IPLR^{TF})
7. H.323 Version 4

3.5.3 B6 Main IP Features

The main IP features in the B6 release are:

1. AES Encryption
2. SNMP Security Alert Notification
3. H.323 Empty Capabilities
4. MCU Request Floor Functionality

3.5.4 E1 Main IP Features

The main IP features in the E1 release are:

1. XGA Native Resolution
2. AES Encryption
3. SNMP Security Alert Notification
4. H.323 Empty Capabilities
5. MCU Request Floor Functionality

3.5.5 B7 Main IP Features

The main IP features in B7 release are:

1. Chair Control (H.243)
2. G722.1 Audio
3. 20 & 40ms Audio Packet Sizes
4. H323 56k Bearer Cap Support
5. H323 Port – Static\Dynamic
6. IP Conflict Warning
7. MD5 Challenge Encryption Password for Telnet

3.5.6 E2 Main IP Feature

The main IP features in E2 release are:

1. H264 Video
2. Chair Control (H.243)
3. G722.1 Audio
4. 20 & 40ms Audio packet Sizes
5. H323 56k Bearer Cap Support
6. H323 Port – Static/Dynamic
7. IP Conflict Warning
8. MD5 Challenge Encryption Password for Telnet

3.5.7 Layer 4 Ports Used

Point To Point + DuoVideo^{TF}

Function	Port	Type	Direction
Gatekeeper RAS	1719	UDP	↔
Gatekeeper Discovery	224.0.1.41:1718	UDP	↔
Q.931 Call Setup	1720	TCP*	↔
H.245	Range 5555—5556	TCP	↔
Video	Range 2326—2341	UDP	↔
Audio	Range 2326—2341	UDP	↔
Data/FECC	Range 2326—2341	UDP	↔
FTP	21	TCP*	↔
Telnet	23	TCP*	↔
HTTP	80	TCP*	↔
NTP	123	UDP*	⇐ (incoming to codec)
SNMP (Queries)	161	UDP*	↔
SNMP (Traps)	962	UDP	⇒ (outgoing from codec)
Netlog	963	TCP	↔
FTP/data	1026	TCP	↔
VNC	1027	TCP	↔
Streaming/RTP Video	970	UDP	⇒
Streaming/RTCP Video	971	UDP	⇒
Streaming/RTP Audio	972	UDP	⇒
Streaming/RTCP Audio	973	UDP	⇒
SAP**	974	UDP	⇒

MultiSite + DuoVideo^{TF}

Function	Port	Type	Direction
Gatekeeper RAS	1719	UDP	↔
Gatekeeper Discovery	224.0.1.41:1718	UDP	↔
Q.931 Call Setup	1720	TCP*	↔
H.245***	Range 5555—5560	TCP	↔
Video	Range 2326—2573	UDP	↔
Audio	Range 2326—2573	UDP	↔
Data/FECC	Range 2326—2573	UDP	↔
FTP	21	TCP*	↔
Telnet	23	TCP*	↔
HTTP	80	TCP*	↔
NTP	123	UDP*	⇐ (incoming to codec)
SNMP (Queries)	161	UDP*	↔
SNMP (Traps)	962	UDP	⇒ (outgoing from codec)
Netlog	963	TCP	↔
FTP/data	964	TCP	↔
VNC	965	TCP	↔
Streaming/RTP Video	970	UDP	⇒
Streaming/RTCP Video	971	UDP	⇒
Streaming/RTP Audio	972	UDP	⇒
Streaming/RTCP Audio	973	UDP	⇒
SAP**	974	UDP	⇒

* denotes a listening port.

** stream is directed to 224.2.127.254, port 9875

*** While using MultiSite^{TF}, if a site is disconnected and reconnected without terminating the entire conference, the next site to be connected will have a H.245 port outside of the specified range. If this functionality is required to operate through a firewall, the range of TCP ports can be extended past 5560. However, if a site is disconnected and reconnected, without ending the conference a sufficient number of times, it is possible to quickly exceed this range once more.

Outgoing call: First call uses port 5555 for outgoing Q.931 and port 5556 for H.245, next uses port 5557 for Q.931 and port 5558 for H.245, etc.

Incoming call: First uses port 5555 for H.245, second port 5556 etc. Disconnecting a site in a call will not free up available 55XX ports until the whole conference is down.

3.5.8 Example of Point to Point (IP direct dialing)

Using two sites known as 'Site Alice' and 'Site Bob'. Alice will call Bob:

Call Connect:

1. Alice creates a TCP socket for Q.931 and connects to Bob:1720. ***The source port on Alice is 5555.***
2. Bob creates a TCP socket for H.245 and binds it to port 5555
3. Bob sends Q.931 'connect' to Alice and in this message it tells Alice what port the H.245 socket is on
4. Alice creates a TCP socket for H.245 and connects it to the specified port on Bob. ***The source port on Alice is dynamic and cannot be predicted (range 5556 – 5560, depending on the number of sites to be connected)***
5. Capability sets are exchanged
6. Master/slave determination
7. Call is connected

Video Media Stream:

8. Alice creates two UDP sockets, one for RTP and one for RTCP. It binds the RTP socket to an even port number and the RTCP socket to the following odd port number. ***The RTP and RTCP ports cannot be predicted (range 2326—2365)***
9. Alice sends OpenLogicalChannel to Bob which contains the address and port for the RTCP socket
10. Bob creates two UDP sockets, one for RTP and one for RTCP. It binds the RTP socket to an even port number and the RTCP socket to the following odd port number. ***The RTP and RTCP ports cannot be predicted (range 2326—2365)***
11. Bob responds with OpenLogicalChannelAck which contains the addresses and ports for the RTP/RTCP sockets.

Audio Media Stream:

12. Alice creates two UDP sockets, one for RTP and one for RTCP. It binds the RTP socket to an even port number and the RTCP socket to the following odd port number. ***The RTP and RTCP ports cannot be predicted (range 2326—2365)***
13. Alice sends OpenLogicalChannel to Bob which contains the address and port for the RTCP socket
14. Bob creates two UDP sockets, one for RTP and one for RTCP. It binds the RTP socket to an even port number and the RTCP socket to the following odd port number. ***The RTP and RTCP ports cannot be predicted (range 2326—2365)***
15. Bob responds with OpenLogicalChannelAck which contains the addresses and ports for the RTP/RTCP sockets.

Data/FECC Media Stream:

16. Alice creates two UDP sockets, one for RTP and one for RTCP. It binds the RTP socket to an even port number and the RTCP socket to the following odd port number. ***The RTP and RTCP ports cannot be predicted (range 2326—2365)***
17. Alice sends OpenLogicalChannel to Bob which contains the address and port for the RTCP socket

18. Bob creates two UDP sockets, one for RTP and one for RTCP. It binds the RTP socket to an even port number and the RTCP socket to the following odd port number. ***The RTP and RTCP ports cannot be predicted (range 2326—2326)***
19. Bob responds with OpenLogicalChannelAck which contains the addresses and ports for the RTP/RTCP sockets.

3.5.9 Conferencing Through A Firewall

In B4 and later, TANDBERG has reduced the dynamic nature of the H.323 ports to a smaller range of possibilities. If TANDBERG B4 and later solutions are used, the opening the following ports, incoming and outgoing, will enable H.323 point to point, MultiSite^{TF}, and DuoVideo^{TF} communications through a firewall:

Point To Point + DuoVideo^{TF}

Function	Port	Type	Direction
Gatekeeper RAS	1719	UDP	↔
Gatekeeper Discovery	224.0.1.41:1718	UDP	↔
Q.931 Call Setup	1720	TCP*	↔
H.245	Range 5555—5556	TCP	↔
Video	Range 2326—2340	UDP	↔
Audio	Range 2326—2340	UDP	↔
Data/FECC	Range 2326—2340	UDP	↔

MultiSite + DuoVideo^{TF}

Function	Port	Type	Direction
Gatekeeper RAS	1719	UDP	↔
Gatekeeper Discovery	224.0.1.41:1718	UDP	↔
Q.931 Call Setup	1720	TCP*	↔
H.245*	Range 5555—5560	TCP	↔
Video	Range 2326—2375	UDP	↔
Audio	Range 2326—2375	UDP	↔
Data/FECC	Range 2326—2375	UDP	↔

* denotes a listening port

This port range will work for TANDBERG B4 and later solutions only. Because H.323 does not require a specific range of ports, other manufacturers may need to open up a larger range of ports to accommodate H.323 communications.

3.5.10 Audio

The B4, B5, B6, E1 audio codec of the TANDBERG systems supports G.711, G.722 and G.728. B7/E2 audio codec supports G.722.1 and 40ms audio packets over IP in addition.

Audio	Length (ms)	Audio size	IP Header	UDP Header	RTP Header	Total
G.711	20ms	160 bytes	20 bytes	8 bytes	12 bytes	200 bytes
G.711	40ms	320 bytes	20 bytes	8 bytes	12 bytes	360 bytes
G.722	20ms	160 bytes	20 bytes	8 bytes	12 bytes	200 bytes
G.722	40ms	320 bytes	20 bytes	8 bytes	12 bytes	360 bytes
G.722.1_24	20ms	60 bytes	20 bytes	8 bytes	12 bytes	100 bytes
G.722.1_24	40ms	120 bytes	20 bytes	8 bytes	12 bytes	160 bytes
G.722.1_32	20ms	80 bytes	20 bytes	8 bytes	12 bytes	120 bytes
G.722.1_32	40ms	160 bytes	20 bytes	8 bytes	12 bytes	200 bytes
G.728	20ms	40 bytes	20 bytes	8 bytes	12 bytes	80 bytes
G.728	40ms	80 bytes	20 bytes	8 bytes	12 bytes	120 bytes

3.5.11 Video

The B4, B5, B6, E1 video codec of the TANDBERG systems supports H.261 (QCIF, CIF, annex D), H.263 (CIF, 4CIF) and H.263+ (Natural Video^{TF} 60fps interlaced video, custom formats, XGA (E1), SVGA, VGA, and SIF). TANDBERG video is variable and will only take the required bandwidth to transmit the video at any given instant.

B4:

Video	Video size (max)	IP Header	UDP Header	RTP Header	Total (max)
H.261	1450 bytes	20 bytes	8 bytes	12 bytes	1490 bytes
H.263/+/++	1450 bytes	20 bytes	8 bytes	12 bytes	1490 bytes

B5, B6, B7, E1:

Video	Video size (max)	IP Header	UDP Header	RTP Header	Total (max)
H.261	1400 bytes*	20 bytes	8 bytes	12 bytes	1440 bytes
H.263/+/++	1400 bytes*	20 bytes	8 bytes	12 bytes	1440 bytes

E2:

Video	Video size (max)	IP Header	UDP Header	RTP Header	Total (max)
H.261	1400 bytes*	20 bytes	8 bytes	12 bytes	1440 bytes
H.263/+/++	1400 bytes*	20 bytes	8 bytes	12 bytes	1440 bytes
H.264	1400 bytes*	20 bytes	8 bytes	12 bytes	1440 bytes

* for B5, B6/E1, B7/E2 software, the dataport command 'h323mtu' can be used to change the maximum video payload size to any value between 1200-1400 bytes.

3.5.12 Jitter and Latency

Latency can be defined as the time between a node sending a message and receipt of the message by another node. The TANDBERG systems can handle any value of latency, however, the higher the latency, the longer the delay in video and audio. This may lead to conferences with undesirable delays causing participants to interrupt and speak over each other.

Jitter can be defined as the difference in latency. Where constant latency simply produces delays in audio and video, jitter can have a more adverse effect. Jitter can cause packets to arrive out of order or at the wrong times. TANDBERG can manage packets with jitter up to 100ms. If excessive packet loss is detected, the TANDBERG systems will make use of IPLR^{TF} (see document D50165 for more information) or downspeeding (flow control) to counteract the packet loss.

4. TANDBERG's H.323 Features

TANDBERG has implemented H.323 version 4 across its entire product line beginning with Version B5 of the TANDBERG software. With this release, TANDBERG has elevated the basic IP terminal to a new level, building on such features as Encryption, H.323 MultiSite^{TF}, H.323 Duo Video^{TF}, high-bandwidth streaming, IP Precedence and Type of Service (TOS), RSVP, IPLR^{TF} and Simple Network Management Protocol (SNMP).

4.1 Special Features

4.1.1 H.323 MultiSite^{TF}

Available on the TANDBERG 8000, 7000, 6000, 2500, 880, and 800
From Software Version B2.x to present

With version B3 of the TANDBERG software, TANDBERG systems can offer a maximum of 3 sites at 1Mbps or 4 sites at 768kbps at business quality 30 fps utilizing H.261 or H.263 video compression over IP. If you decide to make use of the MultiSite^{TF} feature and want to add additional sites to your call, simply dial the E.164 alias or IP address of the destination system. The embedded Multisite allows for both incoming and outgoing calls. TANDBERG uses *flow control* to automatically downspeed the current call if necessary to make room for the new connections. The user is not required to know how much bandwidth is available for the next site, just dial, sit back and let the system intelligently provide you with the best available video and audio. The MultiSite^{TF} feature also allows the additional sites to dial in or dial out allowing for the maximum flexibility of any embedded MCU on the market today.

4.1.2 Intelligent Packet Loss Recovery (IPLR^{TF})

Available on the TANDBERG 8000, 7000, 6000, 2500, 880, 800, 1000, 550, and 500
From Software Version B5.x to present

TANDBERG systems have a standards based method for improving video quality under packet loss situations. This method works with other vendor's endpoints and MCUs. Video quality is improved on both the transmit and receive video streams. Please see TANDBERG document D50165 for details on the IPLR feature.

4.1.3 H.235 Encryption

Available on the TANDBERG 8000, 7000, 6000, 2500, 1000, 880, 800, 550, and 500
From Software Version B5.x to present

TANDBERG was first to market with embedded standards based encryption. Today, all systems with B5 and later are capable of DES encryption on IP as a standard feature. In B6/E1, the option to install AES 128bit encryption on IP is also available.

4.2 Presentations

4.2.1 H.323 Duo Video^{TF}

Available on the TANDBERG 8000, 7000, 6000, 2500, 880, and 800

From Software Version B1.x to present

Duo Video^{TF} is a revolutionary new concept that TANDBERG introduced early in 2000 and is now available during a MultiSite^{TF} call. This feature uses the current ITU-T standards to allow for 2 simultaneous live video streams to be transmitted and received. Simply choose to 'Add Duo', select your second video source and the call connects automatically. If you prefer, you may set your system to 'automatic Duo' and simply pressing any peripheral source key will automatically open Duo Video^{TF}. The system supports downspeeding and upspeeding on this feature to provide bandwidth for Duo Video^{TF} and to release this bandwidth when the Duo Video^{TF} session is over. This clever use of the current standards empowers businesses to have face to face meetings and share content without losing the face to face contact that makes a successful meeting. Any live video source, including the direct XGA input of the system, document camera, DVD and VCR can be transmitted using the Duo Video^{TF} functionality.

4.2.2 High Bandwidth Streaming

Available on the TANDBERG 8000, 7000, 6000, 2500, 1000, 880, 800, 550, and 500
From Software Version B2.x present

TANDBERG has recognized the usefulness of streaming to businesses today. TANDBERG has also realized that the 64kbps of video and audio offered by other manufacturers today is not enough in some cases. Therefore, TANDBERG has expanded on this concept by allowing for selectable video rates up to 320kbps video and 64kbps audio using Multicast or Unicast. This feature allows users to customize their streaming needs for their applications. Video can be viewed using most common viewers available for free on the Internet. The video and audio are streamed using RTP and can be viewed with any RTP compatible viewer such as QuickTime (supporting unicast or multicast) or RealPlayer (supporting multicast only). Please refer to document D12408 for more details on streaming.

The user can choose to stream the local or far end video along with the mixed audio from both endpoints. A third alternative is to stream a voice switched conference where the current speaker will be seen by the streaming viewer and audio from both sides will be mixed and heard. The streaming feature has a separate streaming password to allow viewers to stream without allowing administrative rights to the system.

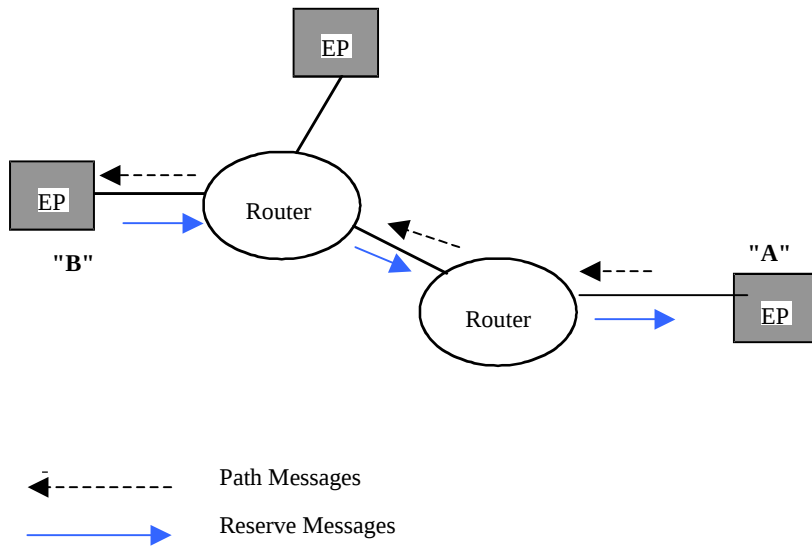
4.3 Quality of Service

4.3.1 RSVP

Available on the TANDBERG 8000, 7000, 6000, 2500, 1000, 800, 880, 550, and 500
From Software Version B4.x to present

RSVP is specified in IETF RFC 2005. The RSVP standard is used by an endpoint to request certain qualities from the network that will transport the video and audio data. This request is made at each node throughout the network and each node must comply or the reservation will fail.

The Figure below shows a possible scenario for a RSVP reservation. Endpoint A sends a reservation request (Path message). This request is processed by the routers and forwarded if the reservation is granted. If all routers along the path and endpoint B grants the reservation a Reserve message is sent back to endpoint A.

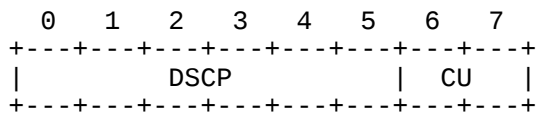


RSVP is a protocol like TCP and UDP. It has no concept of ports and hence it must be some sort of mechanism in the firewall to enable RSVP traffic. To enable RSVP you need to find the RSVP setting and turn it on. Consult the firewalls technical manual to see if there are separate settings for incoming and outgoing RSVP traffic

4.3.2 Differential Services

Available on the TANDBERG 8000, 7000, 6000, 2500, 1000, 880, 800, 550, and 500
From Software Version B5.x to present

Differential Services is another method of QoS offered by TANDBERG that utilizes 6 bits of the Type of Services Byte. This method is currently replacing IP Precedence as the preferred method for setting priority of packet traffic.



DSCP: differentiated services codepoint
CU: currently unused

In version B5 and later, the values for signaling, video, audio and data can all be set independently by the user/administrator.

4.3.3 IP Precedence and Type of Service

Available on the TANDBERG 8000, 7000, 6000, 2500, 1000, 880, 800, 550 and 500
From Software Version B1.x to present

TANDBERG has implemented IP Precedence and Type of Service (TOS). IP Precedence allows the video terminal to prioritize its video and audio above or below other IP traffic on the same network

Bits 0-2: Precedence.
Bit 3: 0 = Normal Delay, 1 = Low Delay.
Bits 4: 0 = Normal Throughput, 1 = High Throughput.
Bits 5: 0 = Normal Reliability, 1 = High Reliability.
Bit 6-7: Reserved for Future Use.

0	1	2	3	4	5	6	7
PRECEDENCE			D	T	R	0	0

Precedence

111 - Network Control
110 - Internetwork Control
101 - CRITIC/ECP
100 - Flash Override
011 - Flash
010 - Immediate
001 - Priority
000 - Routine

	B1	B2	B3	B4	B5
Signaling	n	n	n	n	User config
Video	n	n	(n-2)	(n-2)	User config
Audio	n	n	(n-2)	(n-2)	User config
Data (FECC)	n	n	(n-3)	(n-3)	User config

Where 'n' is the value set by the user in the menu system.

The TOS values available are maximum throughput, minimum monetary cost, minimum delay, maximum reliability, and normal (off). This feature is used to allow routers to make decisions on how to delay traffic if congestion occurs.

The QoS capabilities of the TANDBERG systems can be used to manage a private LAN or WAN more effectively. IP Precedence and TOS help prioritize IP traffic, control congestion, and allow for a better integration of video conferencing into an existing LAN. In times of high network stress, these features will help the routers to drop lower precedence data to increase router stability and offer higher probability that the video conferencing data will reach its destination. In some instances it may help provide a larger proportion of the link without having to configure policy. In the near future Differential

Services may be available from ISP's and ASP's that will use the TOS information to offer better services to the users.

In version B5 and later, the values for signaling, video, audio and data can all be set independently by the user/administrator.

4.4 Remote Management

4.4.1 Simple Network Management Protocol (SNMP)

Available on the TANDBERG 8000, 7000, 6000, 2500, 1000, 880, 800, 550, and 500

From Software Version A2.x to present

Simple Network Management Protocol (SNMP) is a feature available on most IP based technologies and required by IT professionals to aid in effectively managing their networks. SNMP was developed to reduce the complexities of managing IP based technologies and minimize the amount of resources required to support it. Management programs such as the TANDBERG Management Suite use this feature to provide proactive management of video networks. Currently, TANDBERG supports MIB II (RFC 1213) and its own Enterprise MIB expanded upon under MIB II. Details on MIB II can be found at <http://www.faqs.org/rfcs/rfc1213.html> .

For security reasons, the SNMP manager can be disabled by using the 'services' command available through the dataport. The SNMP manager can also be password protected using the command 'ippassword'. Disabling the SNMP manager requires B5.x software and later.

The functionality available through SNMP is always being improved with each version of software. Later versions will be more fully featured.

4.4.2 HTTP Server

Available on the TANDBERG 8000, 7000, 6000, 2500, 1000, 880, 800, 550, and 500

From Software Version A1.x to present

The TANDBERG systems have integrated web servers to allow for remote management of the systems. To connect to the web server, simply open an Internet browser and type in the IP address of the system to be managed.

For security reasons, the web server can be disabled by using the 'services' command available through the dataport. The webserver can also be password protected using the command 'ippassword'. Disabling the HTTP server requires B5.x software and later.

4.4.3 FTP Server

Available on the TANDBERG 8000, 7000, 6000, 2500, 1000, 880, 800, 550, and 500
From Software Version A1.x to present

The TANDBERG systems have integrated FTP servers to allow for software updates and configuration changes to the systems. To connect to the FTP server, simply open a FTP client and type in the IP address of the system to be managed.

For security reasons, the FTP server can be disabled by using the ‘services’ command available through the dataport. The FTP server can also be password protected using the command ‘ippassword’. Disabling the FTP server requires B5.x software and later.

4.4.4 Telnet Server

Available on the TANDBERG 8000, 7000, 6000, 2500, 1000, 880, 800, 550, and 500
From Software Version A1.x to present

The TANDBERG systems have integrated telnet servers to allow for system control and configuration changes to the systems. To connect to the telnet server, simply open a telnet client and type in the IP address of the system to be managed.

For security reasons, the telnet server can be disabled by using the ‘services’ command available through the dataport. The telnet server can also be password protected using the command ‘ippassword’. Disabling the telnet server requires B5.x software and later.

4.5 Video

4.5.1 H.264 Video

Available on the TANDBERG 8000, 7000, 6000, 2500, 1000, 880, and 550,
Software Version E2.x to present

H.264 is the new video codec from the ITU that delivers comparable quality video to H.263 at half the bandwidth. It is optimized to provide better quality video at lower bandwidths.

4.5.2 Natural Video^{TF} 60 FPS Interlaced Video

Available on the TANDBERG 8000, 7000, 6000, 2500, 880, and 800
From Software Version B1.x (IP) to present

Natural Video^{TF} is the new interlaced H.263 video format from the ITU. TANDBERG has had this feature since July 2000 (A2 software). This annex to the H.263 standard provides the means to encode, transmit, and decode an interlaced video image for more lifelike motion. This feature is now available over IP (B2 software and later).

4.5.3 H.263+ Custom Video Formats (Digital Clarity^{TF})

**Available on the TANDBERG 8000, 7000, 6000, 2500, 1000, 880, 800, 550, and 500
Software Version B3.x to present (XGA is available in Version E1 and later)**

TANDBERG supports encoding of a true XGA (E1), SVGA, VGA and NTSC (SIF) resolutions. This allows the TANDBERG to send all video signals in their true 'native resolution'. If the source is sending SVGA or VGA, the receiving system will decode and display the same quality image as was sent by the transmitting side. This feature is available over IP and ISDN

Also supported under the H.263+ custom formats is TANDBERG's use of SIF (Source Input Format) that allows for an improved NTSC image over traditional CIF based systems. This feature is available over IP and ISDN.

4.5.4 4CIF Digital Clarity^{TF}

**Available on the TANDBERG 8000, 7000, 6000, 2500, 1000, 880, 800, 550, and 500
From Software Version B1.x (IP) to present**

TANDBERG was first to market with live 4CIF in February 2000. This feature allows for H.263 4CIF live video images to be sent to the far end allowing 4 times higher resolution than traditional videoconferencing systems for displaying document cameras and other high resolution images. This feature is available over IP and ISDN

4.6 Other

4.6.1 Network Address Translation (NAT) Support

**Available on the TANDBERG 8000, 7000, 6000, 2500, 1000, 880, 800, 550, and 500
From Software Version B3.x to present**

Network Address Translation (RFC 1631) is important because of the limitations of the IP v4 addressing scheme. This feature also plays into the Small Office/Home Office (SOHO) using commercially available Internet accesses such as cable modems or xDSL. Most Internet Service Providers (ISPs) will provide a subscriber with 1 public IP address, however quite often it is important to provide multiple IP address for an office. At a minimum, a home office will need an IP address for a PC as well as the video conferencing unit.

For the port range required by the TANDBERG systems, please see the section on Firewalls in this document.

When a packet from a system behind the NAT arrives at the NAT, the router will de-encapsulate the packet and rewrite the packet with its own IP address and port

information. The NAT will remember the original information and send this packet on to its destination. When information returns to the NAT, it will again de-encapsulate the packet again and put the original information back in and send it on to the originating system. For a more detailed explanation on how a NAT works, please look at <http://www.howstuffworks.com/nat.htm> .

4.6.2 Auto Gatekeeper Discovery

Available on the TANDBERG 8000, 7000, 6000, 2500, 1000, 880, 800, 550, and 500
From Software Version B1.x to present

TANDBERG supports automatic gatekeeper discovery using RAS. This feature allows the TANDBERG system to find an available gatekeeper and register to that gatekeeper using its E.164 alias or H.323 ID. The user is not required to know the gatekeeper's IP address, simply plug in the system to the IP LAN and it will auto-detect the gatekeeper by using the **224.0.1.41** Multicast address on **port 1718**.

4.6.3 TCS-4

Available on the TANDBERG 8000, 7000, 6000, 2500, 1000, 880, 800, 550, and 500
From Software version B2.x to present

TCS-4 allows the user to specify the H.323 alias, in the dial string, of the party being called when calling inbound through a gatekeeper. Currently, if TCS-4 is not supported, the user must use DTMF tones after connection to the gateway to specify the E.164 alias of the site to be reached on the LAN. With TANDBERG's implementation of TCS-4, the user can now specify the E.164 alias at the time of the initial call allowing a seamless connection between a H.320 site and H.323 site.

Example: TANDBERG 6000 E.164 alias is 56774
 H.323/H.320 gateway ISDN number is 703-555-1212

To dial from an ISDN based TANDBERG directly to the TANDBERG 6000; simply type 7035551212*56774 and the call will automatically connect without have to use the IVR.

4.6.4 Asymmetrical Encoders and Decoders

Available on the TANDBERG 8000, 7000, 6000, 2500, 1000, 880, 800, 550, and 500

From Software Version B1.x (IP) to present

Realizing there are many different types of videoconferencing units in the world that do not support the same video and audio algorithms, TANDBERG has implemented asymmetrical encoders and decoders. This feature allows different systems with different video and audio algorithms to communicate to TANDBERG without having to settle on the lowest common denominator. The asymmetrical nature of the system really shines when using the embedded H.320/H.323 Multisite as TANDBERG can accept *any* of its supported algorithms in any combination from any site and always transmit the best video and audio to the far end.

4.6.5 Inband Switching of Video and Audio Algorithms

Available on the TANDBERG 8000, 7000, 6000, 2500, 1000, 880, 800, 550, and 500

From Software version B1.x (IP) to present

TANDBERG has the ability to change its video and audio algorithms ‘on the fly’ during a conference. This is valuable when switching between the live user image (CIF) and the live PC (SVGA, VGA) or Document Camera (4CIF) image. This feature ensures the best possible picture for each source is displayed.

4.6.6 Flow Control

Available on the TANDBERG 8000, 7000, 6000, 2500, 1000, 880, 800, 550, and 500

From Software version B2.x to present

The TANDBERG systems use Flow Control to control the amount of information being received from each endpoint. If the TANDBERG system requires bandwidth to be freed up, such as making a MultiSite^{TF} call, the TANDBERG system will use Flow Control to request the other endpoint to drop the bandwidth.

This feature comes in handy when using H.323 over networks with poor QoS such as the Internet. If the TANDBERG system detects excessive packet loss, it will use Flow Control to ‘downspeed’ the far end overcoming the packet loss problem. Packet loss can occur when routers become overloaded and discard packets or when the receiving video system cannot keep up with the transmitting video system.

4.6.7 Dynamic Bandwidth Management

Available on the TANDBERG 8000, 7000, 6000, 2500, 1000, 880, 800, 550 and 500

From Software version B1.x to present

In addition, TANDBERG understands how valuable the IP network is to the user and how valuable the bandwidth is to the processes that take place on that network. TANDBERG systems will dynamically change the bandwidth used based on bandwidth needed during a call. If the full bandwidth is not required, i.e. low motion video, the used bandwidth by the system will be decreased, freeing up this bandwidth for other process such as Internet, email, VoIP and other applications currently sharing the corporate network.

4.6.8 Lip Sync

**Available on the TANDBERG 8000, 7000, 6000, 2500, 1000, 880, 800, 550 and 500
From Software version B2.x to present**

Synchronizing audio to video on synchronous networks such as ISDN is a task most video conferencing units today are capable of doing very well. However, IP is an asynchronous network that sends audio and video separately. It is easy to see that these two streams may not arrive at their destination at the same time. Lip sync problems are a certainty if precautions are not taken in the implementation of the codec.

TANDBERG supports sequencing of the video and audio IP packets and the reassembly of these packets at the destination if they are received out of order. If the video stream is received before the audio stream, the TANDBERG codec will buffer this data until the necessary audio is received and reassemble the data the codec will use to reproduce a clear image with exceptional sound quality and lip sync at the destination site.

5. H.323 Communications with TANDBERG Systems

It is important to understand exactly how H.323 communications take place. Without this understanding, it is near impossible to create a solution that will be flexible enough to compete with ISDN technology in ease of use. To begin, we must examine the elements of session establishment, handshaking and exchange of audio, video and data.

It is also important to remember a gatekeeper is mandatory if using a gateway or MCU in your network design.

There are 3 types of gatekeepers available: direct signalling and direct media, routed signalling and direct media, and routed signalling and routed media. The most common in use today is the routed signalling and direct media gatekeeper. The next few examples will describe calls using routed signalling and direct media gatekeepers.

5.1 Only Calling Endpoint Has Gatekeeper

Endpoint 1 (EP1) is registered to a local Gatekeeper 1 (GK1). Endpoint 2 (EP2) is not registered to a gatekeeper. Gatekeeper is using routed signalling and direct media.

Step	Function	Translation
1	EP1 issues Admissions Request (ARQ) to GK1 using RAS	EP1 asks permission from GK1 to call EP2
2	GK1 issues Admission Confirm (ACF) to EP1 using RAS	GK1 gives EP1 permission to call EP2
3	EP1 sends Q.931 'setup' message to GK1	EP1 dials the IP address of EP2 and sends it to GK1
4	GK1 sends Q.931 'setup' message to EP2	GK1 dials the IP address of EP2
5	GK1 sends Q.931 'call proceeding' message to EP1, EP2 sends Q.931 'call proceeding' message to GK1	GK1 tells EP1 the call is in process. EP2 tells GK1 the call is in process
6	EP2 sends Q.931 'alerting' message to GK1, GK1 sends Q.931 'alerting' message to EP1	EP2 tells the GK1 it is ringing. GK1 tells EP1 that EP2 is ringing
7	EP2 sends Q.931 'connect' message to GK1	EP2 tells GK1 that it has connected.
8	GK1 sends Q.931 'connect' message to EP1	GK1 tells EP1 that EP2 has connected.

Video, Audio, and FECC media is passed directly between EP1 and EP2.

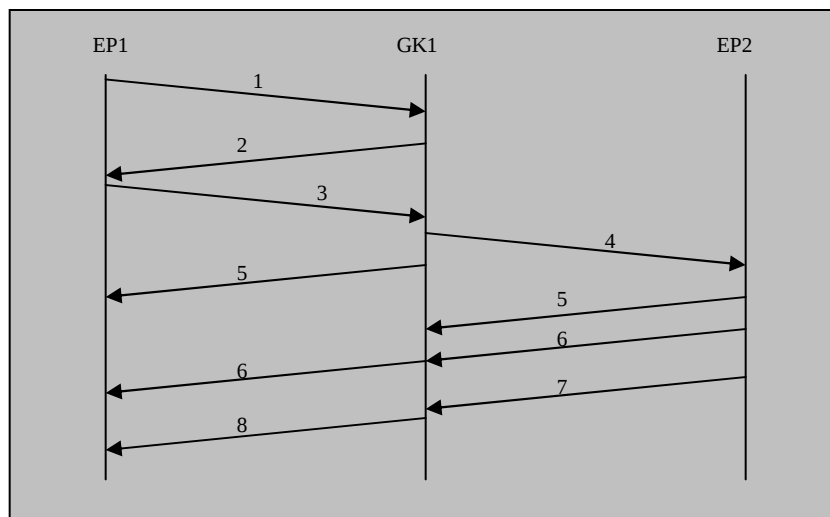


FIGURE 1

5.2 Only Called Endpoint Has Gatekeeper

Endpoint 1 is not registered to a gatekeeper. Endpoint 2 is registered to GK2 and is using routed signalling and direct media.

Step	Function	Translation
1	EP1 sends Q.931 'setup' message to EP2	EP1 dials EP2
2	EP2 sends Q.931 'call proceeding' message to EP1	EP2 tells EP1 the call is proceeding
3	EP2 sends Admissions Request (ARQ) to GK2 using RAS	EP2 asks permission to accept the call from GK2
4	GK2 sends Admissions Confirm (ACF) to EP2	GK2 denies call and requests to route call through gatekeeper
5	EP2 responds to EP1 with Call Signalling Transport Address of GK2	EP2 tells EP1 where to send the call signalling info
6	EP1 issues Q.931 'release complete' message to EP2	EP2 hangs up the current call
7	EP1 sends Q.931 'setup' message to GK2	EP1 dials GK2 Call Signalling Transport Address
8	GK2 sends Q.931 'setup' message to EP2	GK2 dials EP2
9	EP2 issues Admissions Request (ARQ) to GK2	EP2 asks for permission to answer call from GK2
10	GK2 issues Admissions Confirm (ACF) to EP2	GK2 gives permission to answer call to EP2
11	EP2 sends Q.931 'alerting' message to GK2, GK2 sends Q.931 'alerting' message to EP1	EP2 tells GK2/EP1 it is ringing
12	EP2 sends Q.931 'connect' message to GK2	EP2 tells GK2 it is connected
13	GK2 sends Q.931 'connect' message to EP1	GK2 tells EP1 it is connected

Video, Audio, and FECC media is passed directly between EP1 and EP2.

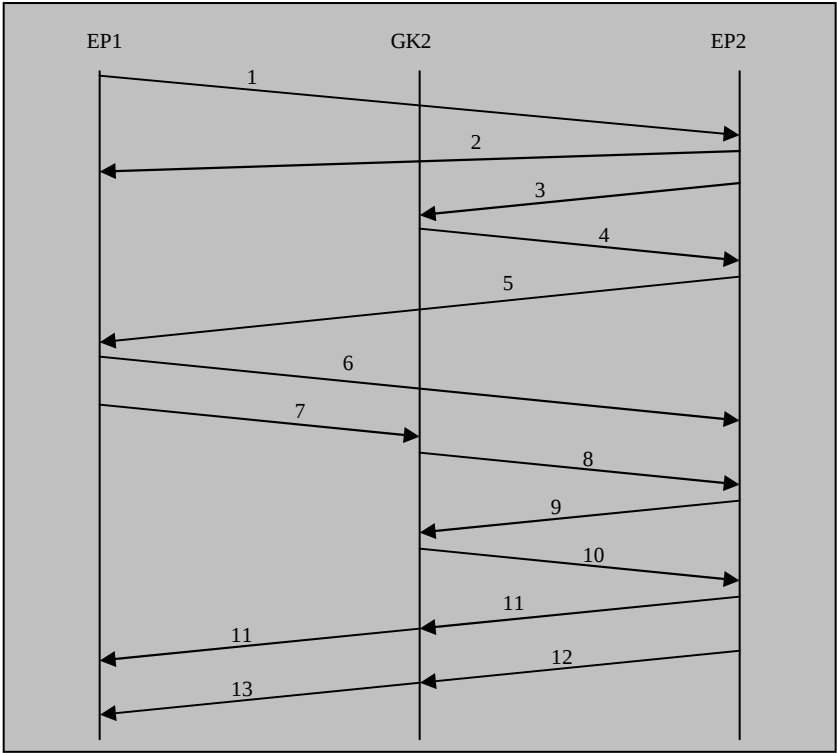


FIGURE 2

5.3 Both Endpoints Registered To Different Gatekeepers

Endpoint 1 is registered to GK1 and Endpoint 2 is registered to GK2. Both are using routed signalling and direct media.

Step	Function	Translation
1	EP1 issues Admissions Request (ARQ) to GK1	EP1 asks permission to call from GK1
2	GK1 issues Admissions Confirm (ACF) to EP1	GK1 gives permission to call to EP1
3	EP1 sends Q.931 'setup' message to GK1	EP1 dials EP2 through GK1
4	GK1 sends Q.931 'setup' message to EP2	GK1 dials EP2
5	EP2 sends Q.931 'call proceeding' to GK1, GK1 sends Q.931 'call proceeding' to EP1	EP2 notifies GK1/EP1 that the call is proceeding
6	EP2 issues Admissions Request (ARQ) to GK2	EP2 asks for permission to answer call from GK2
7	GK2 issues Admissions Confirm (ACF) to EP2	GK2 will deny and ask to route call to gatekeeper
8	EP2 sends GK1 Call Signalling Transport Address of GK2	EP2 tells GK1 where to call GK2
9	GK1 issues Q.931 'release complete' to EP2	GK1 hangs up the current call
10	GK1 issues Q.931 'setup' message to GK2	GK1 calls GK2
11	GK2 issues Q.931 'setup' message to EP2	GK2 calls EP2
12	EP2 issues Admissions Request (ARW) to GK2	EP2 asks for permission to answer call from GK2
13	GK2 issues Admissions Confirm (ACF) to EP2	GK2 gives permission to answer call to EP2
14	EP2 sends Q.931 'alerting' message to GK2, GK2 sends Q.931 'alerting' message to GK1, GK1 sends Q.931 'alerting' to EP1	EP2 tells GK2/GK1/EP1 it is ringing
15	EP2 sends Q.931 'connect' message to GK2	EP2 tells GK2 it is connected
16	GK2 sends Q.931 'connect' message to GK1	GK2 tells GK1 that EP2 is connected
17	GK1 sends Q.931 'connect' message to EP1	GK1 tells EP1 that EP2 is connected

Video, Audio, and FECC media is passed directly between EP1 and EP2.

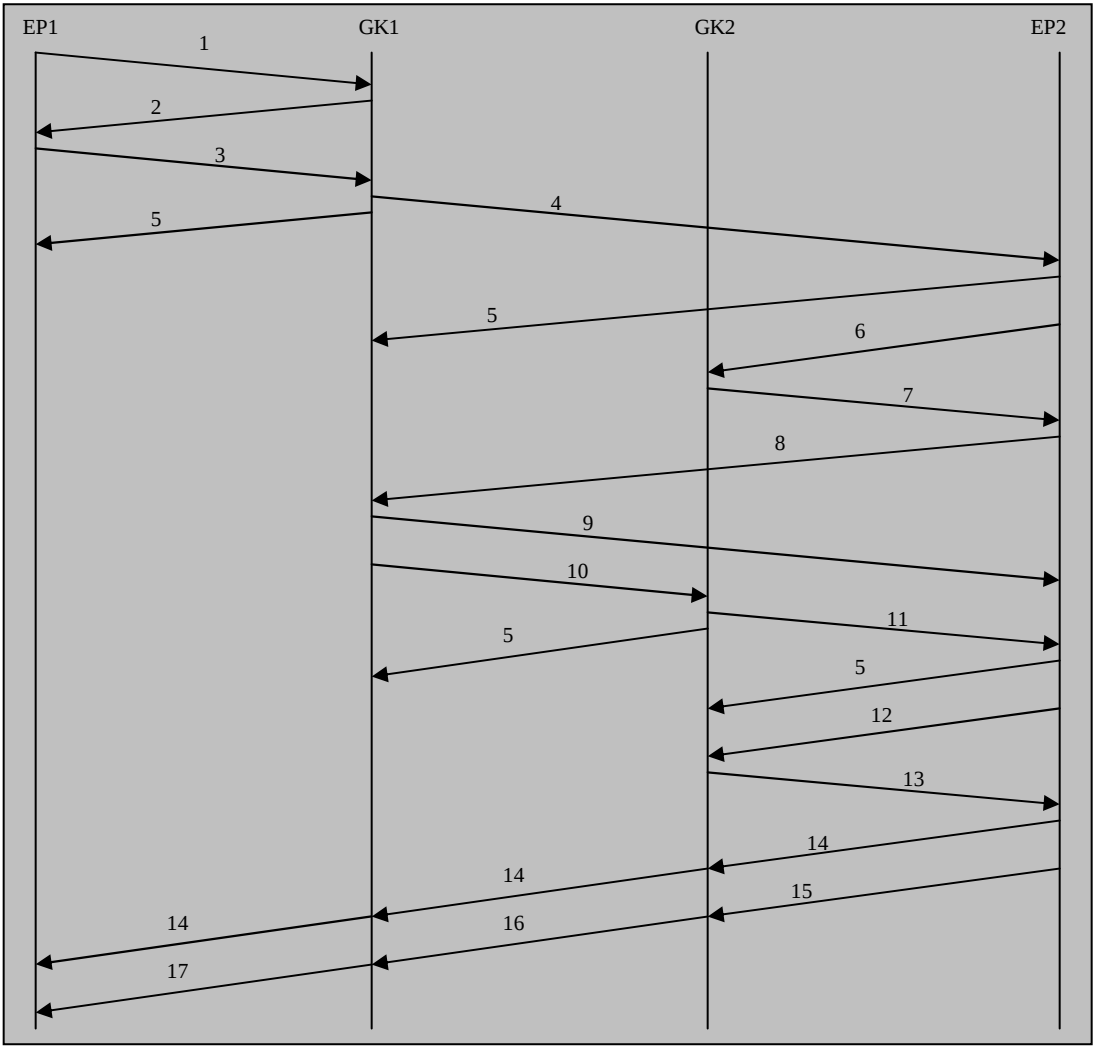


FIGURE 3

6. List of Terms

ASP – Application Service Provider

Ethernet – A local-area network (LAN) protocol developed by Xerox Corporation, DEC and Intel in 1976. Ethernet uses a bus or star topology and supports data transfer rates of 10 or 100 Mbps. It is one of the most widely implemented LAN standards.

H.225 – ITU Standard that describes H.323 call establishment and packetization. This standard also describes the use of RAS, Q.931 and RTP.

H.245 – ITU Standard that describes H.323 syntax and semantics of terminal information messages as well as procedures to use them for in-band negotiation at the start of or during communication.

H.323 – ITU Standard that describes packet based video, audio and data conferencing on networks with non guaranteed Quality of Service (QoS).

ISP – Internet Service Provider

Jitter – Jitter is the variation in network latency. Typically, video systems should be able to accommodate jitter up to at least 100ms.

LAN – Local Area Network.

Latency – The time between a node sending a message and receipt of the message by another node. Typically any latency is supportable, providing it is constant, but large latencies may result in a poor videoconference.

Packet Loss – Occurs when data is lost from the bit-stream, typically on public networks such as the Internet. Packet Loss can occur when passing through a router and has a higher chance of occurring as the hop count is increased. Packet loss can also occur at the receiver end when the transmitter sends data too quick.

Port – In TCP/IP and UDP networks, an endpoint to a logical connection. The port number identifies what type of port it is. For example, port 80 is used for HTTP traffic.

Q.931 – Used to signal call setup on ISDN. Also used by H.225 to establish and disconnect H.323 calls.

RAS – Registration, Admission and Status Protocol. Used by endpoints and gatekeepers to communicate.

RSVP – Resource Reservation Protocol for reserving bandwidth through a RSVP enabled IP network.

RTCP – Real Time Control Protocol. RTCP provides a mechanism for session control and has four main functions: quality feedback, participant identification, RTCP packet transmission rate control and session control information transmission. The primary function of RTCP is to provide feedback

RTP – Real Time Protocol. Described by H.225 on how to handle packetization of audio and video data for H.323. RTP does provide information to reconstruct real time data such as: payload type identification, sequence numbering and timestamping. RTP does not address resource reservation and does not guarantee quality-of-service for real-time services

TCP – Transport Control Protocol. A connection oriented Layer 4 protocol used in H.323 to connect Q.931 and H.245 streams.

UDP – User Datagram Protocol. A connectionless protocol used in transmission of data over IP. While it does not require as much overhead as TCP, it is not as reliable in delivering data. UDP is used to transmit audio and video data in H.323

7. Appendix A

7.1 Polycom H.323 Layer 4 ports

This information is provided ‘as is’ and is not guaranteed to be accurate as it is based on information provided by Polycom. If the version of Polycom software allows for fixed port specification, the following ports should be opened:

Function	Port	Type	Direction
Gatekeeper (RAS)	1719	UDP	↔
Gatekeeper Discovery	224.0.1.41:1718	UDP	↔
Q.931 Call Setup	1720	TCP*	↔
H.245*	Range xxxx—3231**	TCP	↔
Video	Range xxxx—3235**	UDP	↔
Audio	Range xxxx—3235**	UDP	↔
Data (Far End Camera Control)	Range xxxx—3235**	UDP	↔

** The lower limit of these port ranges are user specified.

If the version of software from Polycom does not support user specified ports then the following ports should be opened:

Function	Port	Type	Direction
Gatekeeper (RAS)	1719	UDP	↔
Gatekeeper Discovery	224.0.1.41:1718	UDP	↔
Q.931 Call Setup	1720	TCP*	↔
H.245*	Range 1024—65535	TCP	↔
Video	Range 1024—65535	UDP	↔
Audio	Range 1024—65535	UDP	↔
Data (Far End Camera Control)	Range 1024—65535	UDP	↔

7.2 PictureTel H.323 Layer 4 ports

This information is provided 'as is' and is not guaranteed to be accurate as it is based on information provided by PictureTel.

Function	Port	Type	Direction
Gatekeeper RAS	1719	UDP	↔
Gatekeeper Discovery	224.0.1.41:1718	UDP	↔
Q.931 Call Setup	1720	TCP*	↔
H.245	Range 1700-1750	TCP	↔
Video	Range 17000-17050	UDP	↔
Audio	Range 17000-17050	UDP	↔
Other UDP	Range 1700-1750	UDP	↔