TANDBERG

H.323

D50305 revision 7

March 2010

Disclaimers and notices

The objective of this documentation is to provide the reader with assistance in using and configuring the product. The capabilities of TANDBERG products and other manufacturers' products change over time and so the required configuration may be different from that indicated here. If you have any suggestions for changes to this document, please feed them back to TANDBERG through your TANDBERG Authorized Service Representative. If you need technical support, please contact your TANDBERG Authorized Service Representative.

The specifications for the product and the information in this Guide are subject to change at any time, without notice, by TANDBERG. Every effort has been made to supply complete and accurate information in this Guide; however, TANDBERG assumes no responsibility or liability for any errors or inaccuracies that may appear in this document.

TANDBERG® is a registered trademark belonging to Tandberg ASA. Other trademarks used in this document are the property of their respective holders.

TANDBERG
Philip Pedersens vei 20
1366 Lysaker
Norway
Telephone: +47 67 125 125
www.tandberg.com

TABLE OF CONTENTS

DOCUMENT REVISION HISTORY

Rev 7	Added Disclaimers and notices Corrected errors in the port definitions for the VCS Corrected errors in the source port definition for the traversal call mappings Corrected errors in the port definitions for the TANDBERG Gateway
Rev 6	Addition of the TANDBERG C-series endpoints Addition of Dual Interfaces and Static NAT to VCS section Updates to the TANDBERG MXP endpoints Updates to the TANDBERG VCS Updates to the TANDBERG Codian MSE 8050 Supervisor Blade Updates to the TANDBERG Codian 4200 MCU Updates to the TANDBERG Codian 4500 MCU Updates to the TANDBERG Codian 3200 Series ISDN Gateway Updates to the TANDBERG Codian 3500 Series IP Gateway Updates to the TANDBERG Codian 2200 Series IPVCR Corrected port range used for the TCP allocation of the H.225/Q.931 and H.245 channels for the TANDBERG Video Communication Server Corrected the software versions for the TANDBERG Codian 3200 Series ISDN Gateway and 3500 Series IP Gateway Corrected the random port range allocated to the TANDBERG Codian products. Removed „Netlog" from active ports on the TANDBERG products
Rev 5	Updates to the TANDBERG MXP Endpoints (F6 software) Updates to the TANDBERG MXP Personal Series Endpoints (L5 software) Updates to the TANDBERG MPS (J4 software) Addition of the TANDBERG Codian MSE 8000 (2.2(1.0) software) Addition of the TANDBERG Codian 4200 MCU (2.2(1.0) software) Addition of the TANDBERG Codian 4500 MCU (2.2(1.0) software) Updates to the TANDBERG MPS Gateway (J4 software) Addition of the TANDBERG Codian 3200 Series ISDN Gateway (2.2(1.0) software) Addition of the TANDBERG Codian 3500 Series IP Gateway (2.2(1.0) software) Addition of the TANDBERG Entrypoint (EP1 software) Updates to 3G Gateway (R3 software) and TANDBERG Video Portal (V3 software) Addition of the TANDBERG VCS (X1 software) Updates to the TANDBERG Content Server (S3 software) Addition of the TANDBERG Codian 2200 Series IPVCR (2.2(1.0) software) Updates to the Firewall Traversal diagrams to include the TANDBERG VCS. Updates to the List of Terms
Rev 4	Updates to the TANDBERG MXP Endpoints (F5 software) Updates to the TANDBERG Gatekeeper (N5 software) and TANDBERG Border Controller (Q5 software) Updates to the TANDBERG 3G Gateway (R2 software) Addition of the TANDBERG Video Portal (V2 software) Updates to the List of Terms

Rev 3	Updates to the TANDBERG MXP Endpoints (F4 software) Updates to the TANDBERG MXP Personal Series Endpoints (L4 software) Updates to the TANDBERG MPS (J3 software) Addition of the TANDBERG 3G Gateway (R1 software) Updates to the TANDBERG Gatekeeper (N4 software) and TANDBERG Border Controller (Q3 software) Updates to the List of Terms
Rev 2	Updates to the TANDBERG MXP Endpoints (F3 software) Updates to the TANDBERG MXP Personal Series Endpoints (L3 software) Updates to the TANDBERG MPS (J2 software) Updates to the TANDBERG Gatekeeper (N3 software) and TANDBERG Border Controller (Q2 software) Updates to the List of Terms
Rev 1	Initial Version

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 network technologies may include Ethernet, Fast Ethernet, 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 tends to be the 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.

This document is intended to discuss H.323 from both a general and TANDBERG-specific point of view. Varying levels of depth will be included within the document in order to provide a complete view of the technology and how it is implemented. In addition, deployment scenarios will be discussed, such as firewall traversal, and how those deployments will interact with other IP network components (e.g. firewalls).

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.”

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).

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 (with a minimum resolution of QCIF). If the terminal does not support these minimum standards, the endpoint is not considered an H.323 standards-compliant endpoint as the umbrella standard of H.323 dictates minimum audio and video standards that must be supported to ensure compatibility with other devices. The terminal may also support optional protocols such as T.120 data sharing; this support is not required to be H.323 compliant. All TANDBERG endpoints (including Codecs, Gateways and MCUs) fit the definition of an H.323 terminal and are fully standards-compliant.

TANDBERG Endpoint	*Minimum Software for H.323 support*
TANDBERG MXP endpoints	F1.0 / L1.0
TANDBERG Classic endpoints*	B1.0 / E1.0

* TANDBERG Classic endpoints will not be discussed further in this document.

Gatekeepers

The gatekeeper is responsible for managing other components of an H.323 network. It is a very important component of the managed network. The gatekeeper has several responsibilities which include:

- Translation of E.164 aliases to IP addresses
- Call admission to accept or deny calls
- H.323 zone management.

Optionally, a gatekeeper can also provide other functionality that is not considered required functionality. Optional services include:

- Bandwidth Management
- Call forwarding
- H.225/H.245/Media routing

By implementing H.323 to H.320 Gateways as well as H.323 MCUs within a video network deployment, gatekeepers may be required for inclusion into the network to ensure proper functionality of those particular devices.

Gatekeepers are typically software products that reside on a server, however they can also be found in appliance form factors, such as the TANDBERG Gatekeeper. Although many H.323 MCUs and gateways have embedded gatekeepers, they usually offer lower functionality and lower concurrent call density than stand alone gatekeepers.

There are several gatekeepers that are readily available on the market including the TANDBERG Video Communication Server, TANDBERG Gatekeeper, Cisco IOS (MCM) Gatekeeper, RADVISION ECS, VCON MXM and Polycom Path Navigator. Each employ different approaches to the concepts outlined above.

Gateways

If there is a need for an H.323 terminal to communicate with another terminal on an H.320, H.324 or analog PSTN networks, an H.323 gateway will be required to perform the network translation. While gateways can support the bridging of any two unlike networks, they typically are used to connect an IP and ISDN network together. They are typically deployed in IP only networks to provide the ability for IP only endpoints to connect to others over the ISDN network. The number of simultaneous connections allowed through a gateway is not specified in any standard; therefore each gateway may have different variations of their call capacity. Optionally, gateways may also have embedded gatekeepers that typically offer limited functionality.

There are several manufacturers of gateways on the market today. Most prevalent are the TANDBERG Gateway (See Figure 2.1), Cisco 3540 gateway, RADVISION ViaIP gateway and the Polycom Accord MGC.

Some gateway products are designed to double as both a gateway and an MCU within the same physical box and sharing resources. This solution has advantages by allowing the resources for the MCU to be used in a Gateway scenario, when the ports are free. However, as more users transition from scheduled to ad-hoc video calls, it is quite possible that an ad-hoc call could steal resources from a scheduled call, thereby causing the scheduled call to fail. In addition, quite often different resources are needed for gateway functionality rather than needed for MCU functionality. In other words, the highest concentration of resources needed for MCU calls are not always the ISDN resources needed for gateway calling.

TANDBERG Gateway

The TANDBERG Gateway is a 1 rack unit high (1U), 19" rack mountable Gateway that can connect up to 8 simultaneous H.323-H.320 videoconference gateway sessions and 8 simultaneous VoIP-PSTN telephone sessions. Supporting features such as H.264, H.235, H.239/DuoVideo, and audio transcoding, the TANDBERG Gateway is ideal for small enterprises or large deployments where a distributed Gateway model is needed.

TANDBERG Gateway

TANDBERG MPS Gateway

The TANDBERG MPS Gateway is an add-on option to the TANDBERG MPS system, optioned out in 10-site increments; a 10-site option will allow a total of 10 concurrent H.323-H.320 calls. Supporting all of the features of the TANDBERG Gateway as well as AAC-LD, the scalability of the MPS Gateway makes the system ideal for a centralized architecture.

TANDBERG 3G Gateway

The TANDBERG 3G Gateway will provide mobile users of standards-based H.324M (3G) endpoints the ability to connect to an internal H.323 infrastructure seamlessly. Depending on the options purchased with the system, the gateway will support up to 30 simultaneous H.323-to-H.324M calls.

TANDBERG 3G Gateway

TANDBERG Gateway	*Minimum Software for H.323 support*
TANDBERG Gateway	G1.0
TANDBERG MPS Gateway	J3.0
TANDBERG 3G Gateway	R1.0

Multipoint Control Units (MCU)

The last of the major components is the MCU which controls conferences between 3 or more terminals. The H.323 MCU can take many different forms, including a stand-alone device or it may be incorporated into a video endpoint itself.

MultiSite

Many of the TANDBERG endpoints have the ability to bridge multiple sites together into the same call. The latest TANDBERG MXP endpoints allow for all of the features of the TANDBERG MCU and MPS units while mixing H.323, SIP and H.320/ISDN calls. MultiSite within the TANDBERG endpoints is an optional feature.

TANDBERG MCU

The TANDBERG MCU is a 1 rack unit high (1U), 19" rack mountable MCU that can connect up to 16 sites of videoconference and 16 sites of telephone simultaneously. Supporting features such as H.264, H.235, DuoVideo, transcoding and speed matching, the TANDBERG MCU is ideal for small enterprises or large deployments where a distributed model is needed.

TANDBERG MCU

TANDBERG MPS

The TANDBERG MPS is a 9 rack unit high (9U), 19" rack mountable MCU that can connect up to 16 sites of videoconferencing and 20 sites of telephone per Media Blade. The TANDBERG MPS can support up to 8 Media Blades, providing for a total of 160 simultaneously connected video sites and 48 sites of telephone participants. Similar to the MCU, the MPS supports a wide range of features, including H.264, H.235 AES encryption, H.239, transcoding, speed matching, continuous presence and other features that allow the system to scale to the needs of any enterprise.

TANDBERG MPS 800

TANDBERG Codian 4500 MCU

The TANDBERG Codian 4500 series MCUs are a 2 rack unit high (2U), 19" rack mountable MCU that can connect up to 40 sites of videoconferencing and 40 sites of telephone per chassis. Similar to the other MCUs within the TANDBERG product line the Codian 4500 is a fully featured MCU that supports a wide range of features, including H.264, H.235 AES encryption, H.239, full port-by-port transcoding, full port-by-port speed matching, continuous presence and other features that allow the system to provide the highest level of user experience.

Codian 4500 MCU

TANDBERG MCU technology	*Minimum Software for H.323 support*
TANDBERG MXP endpoints MultiSite[TF]	F1.0
TANDBERG MCU	D2.0
TANDBERG MPS	J1.0
TANDBERG Codian 4500 MCU	2.0(1.0)

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	H.324	H.234M
Approval Date	1990	1995	1995	1996	1996	1998
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	Wireless (UMTS)
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	H.263
Audio	G.711 G.722 G.722.1 G.728 AAC AAC-LD	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 AAC AAC-LD	G.723	G.722.2 G.723.1
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	H.223 A/B H.245
Multipoint	H.231 H.243	H.231 H.243	H.231 H.243	H.323 H.243		
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	

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.722.1	ADPCM audio encode/decode (24 or 32 kbit/s, 7 kHz)
G.722.2	Adaptive Multirate – Wideband (AMR-WB), 16 bit uniform PCM encode/decode, 7kHz; five mandatory modes: 6.60, 8.85, 12.65, 15.85 and 23.85 kbit/s
G.723	Speech coder at 6.3 and 5.3 Kbps data rate. Medium complexity. Optional for H.324; Optional for H.323, H.324M.
G.723.1	3.4 kHz dual rate speech codec at 5.3 and 6.4 kbit/s
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.
AAC	Advanced Audio Coding, variations include AAC-LD (low delay) (TANDBERG endpoints: 64 or 128 kbit/s, 20kHz).

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 both H.320 and H.323.
H.264	Joint collaboration between the ITU and ISO. Improved video over H.263 providing similar quality at half the bandwidth.

The Communications Standards

H.221	Frame Structure 64-1920 Kbps.
H.223	Multiplexing protocol for low-bit rate multimedia communication; Annexes A & B handles light and medium error prone channels.
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.241	Extended video procedures and control signals for H.300-series terminals, signaling for H.264.
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.
H.460.18	Traversal of H.323 signalling across network address translators and firewalls
H.460.19	Traversal of H.323 media across network address translators and firewalls

The Encryption Standards

H.221	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

The Collaboration Standards

H.239	Role Management and Additional Media Channels for H.300-series Terminals
T.120	Data protocols for multimedia conferencing

TANDBERG H.323 TERMINALS

TANDBERG provides a wide variety of form factors based upon the same software and hardware platform. The products range from the personal space, to set tops, up to the executive boardroom plasma-based systems. There are even form factors available for the healthcare industry, distance education, judicial market and first responders. While these form factors may look quite different, they all share the same core technology that makes TANDBERG endpoints the most feature rich in the world.

C-series Platform

Software Version	Released	Release Notes	H.323 Stack
TC1	November 2008	D14359	
TC2	July 2009	D14502	

MXP Platform

Software Version	Released	Release Notes	H.323 Stack
F1	July 2004	D50303	Version 4
F2	February 2005	D50327	Version 4
F3	July 2005	D50359	Version 5
F4	January 2006	D50402	Version 5
F5	July 2006	D50443	Version 5
F6	May 2007	D50476	Version 5
F7	May 2008	D50519	
F8	April 2009	D14578	

Personal Series

Software Version	Released	Release Notes	H.323 Stack
L1	November 2004	D50310	Version 4
L2	April 2005	D50343	Version 4
L3	October 2005	D50388	Version 5
L4	April 2006	D50433	Version 5
L5	November 2007	D50505	Version 5

Key
TANDBERG H.323 Stack

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

TANDBERG C-series Endpoints

C-Series Layer 4 Miscellaneous Ports

The TANDBERG C-series endpoints have a central data store that can be accessed by several methods.

- ***HTTP:*** System management and setup.
- ***HTTPS:*** Secure system management and setup.
- ***Telnet:*** Provides access to the API based upon the XML engine for control, setup and status monitoring.
- ***Secure Shell (SSH):*** Secure access to the API based upon the XML engine.
- ***Secure Copy Protocol (SCP):*** SCP provides secure access to the file system of the C-series endpoint through an SSH session.
- ***SNMP:*** Provides SNMP support for TMS and other SNMP Management Applications.
- ***XML:*** Provides full control, setup and status monitoring ability. Can also be used in conjunction with HTTPS for secure control, setup and status monitoring.

Function	Port	Type	Direction
SSH/SCP	22*	TCP	Host → Endpoint
Telnet	23*	TCP	Host → Endpoint
HTTP / XML	80*	TCP	Host → Endpoint
NTP	123*	UDP	Endpoint → NTP Server
SNMP (Queries)	161*	UDP	Host → Endpoint
SNMP (Traps)	162	UDP	Endpoint → SNMP Trap Host
HTTPS / XML	443*	TCP	Host → Endpoint

* denotes a listening port. ↔ (bi-directional)

C-Series Gatekeeper Interaction

Function	Port	Type	Direction
Gatekeeper RAS	1719	UDP	Endpoint → GK
Gatekeeper Discovery	224.0.1.41:1718	UDP	Endpoint → Multicast

* RND stands for random port used. This reference will be used to signify source ports in many different applications as, depending on the endpoint, the ports could vary.

C-Series Call Flow (Site A calls Site B)

Site A outgoing	Protocol	Type	Site B incoming
5555	H.225/Q.931	TCP	1720
5556:6555	H.245	TCP	5555:6555
2326	Media (Audio)	UDP/RTP	2326
2327	Media (Audio)	UDP/RTCP	2327
2328	Media (Video)	UDP/RTP	2328
2329	Media (Video)	UDP/RTCP	2329
2330	Media (Dual Streams)	UDP/RTP	2330
2331	Media (Dual Streams)	UDP/RTCP	2331
2332	Media (FECC)	UDP/RTP	2332
2333	Media (FECC)	UDP/RTCP	2333

TANDBERG TC1-TC2 software uses a pool of 1001 TCP ports (5555:6555) for Q.931 and H.245. The ports will increment every time a new TCP connection is required. When the port number reaches the top of the port numbers allocated to the call setup messages, the port number will reset and begin using 5555 again.

TANDBERG TC1-TC2 software uses a pool of 160 UDP ports (2326:2487) for all media (both RTP and RTCP). When connecting to far end systems that support symmetrical RTP, the ports are used in increments of 8 per call (e.g. the first call will use either ports 2326-2333 or 2334-2341, depending on call direction). The port range will continue to increment once all active calls are disconnected. Only when the top of the range is reached will the ports to be allocated for the next call reset to the beginning of the range. For example, upon startup, the MXP will allocate ports 2326-2333 for the first call. Whether or not that call disconnects prior to the next call being connected, call 2 will utilize ports 2334-2341. This incremental allocation will continue until port 2487 is reached, at which time the ports will reset to the beginning of the range.

The TANDBERG C-series endpoint uses symmetrical RTP ports, thereby reducing the number of ports needed per call. Symmetrical RTP functionality allows the same port to be used for both incoming and outgoing audio streams. However, when the logical channels are opened, the start range for the UDP ports could begin at 2326 or 2334, depending on who initializes the open logical channel commands.

C-Series Audio

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.722	20ms	160 bytes	20 bytes	8 bytes	12 bytes	200 bytes
G.722.1_24	20ms	60 bytes	20 bytes	8 bytes	12 bytes	100 bytes
G.722.1_32	20ms	80 bytes	20 bytes	8 bytes	12 bytes	120 bytes
G.728	20ms	40 bytes	20 bytes	8 bytes	12 bytes	80 bytes
AAC-LD	20ms	160 bytes	20 bytes	8 bytes	12 bytes	200 bytes

C-Series Video

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

* The dataport command „xConfiguration Network [1..1] MTU: <400..1500>" can be used to change the maximum video payload size to any value between 400 and 1400 bytes.

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 systems can manage packets with jitter up to 100ms; packets not received within this timeframe will be considered lost packets. If excessive packet loss is detected, the TANDBERG systems will make use of IPLR[TF] (see document D50165, TANDBERG and IPLR, for more information) or downspeeding (flow control) to counteract the packet loss.

The C-series endpoint utilizes a dynamic jitter buffer that can increase in value depending on the performance of the network. To minimize introduced latency, this buffer will begin at 20ms and continue to 100ms if sufficient packet loss or jitter is occurring. Additionally, the C-series endpoints supports RTP time stamping into the audio packets in order to help reduce lip sync issues that may occur over an H.323 call.

To further improve lip sync with high resolution images (including XGA, w720p and other high resolution video formats), the C-series endpoints support dynamic buffering of video packets in an attempt to place information on the wire as fast as possible. Without this functionality, the endpoint would attempt to maintain a consistent packet size when placing the information on the wire, which would result in video being buffered internally to ensure that the entire packet could be filled prior to transmission. This potential buffering created a potential lip sync issue at the far end of the H.323 call as the time between the actual capture of the visual image and placing the information on the wire was not a constant and, therefore, the far end system cannot adjust for any time differences between the arrival of the video information and the arrival of the audio information.

The endpoint will now, by default, not buffer the high resolution images prior to transmission, which will ensure a constant time delta between the arrival of the video and audio information to the far end, allowing for an adjustment as necessary and improved lip sync. This change in behavior, though, can cause the endpoint to send out consecutive packets that have a relatively large difference in size. For example, one packet can come out at 1400 bytes while the packet behind that can be sent out at 800 bytes followed by a 1200 byte packet and so on. Some QoS configurations improperly handle the large adjustments in packet size, thereby dropping packets within the QoS buffer and causing packet loss in the call. If, for any reason, it is necessary to reduce the impact of this behavior, it can be done through the API command „`xConfiguration Network [1..1] TrafficControl Mode: <On/Off>`". When this setting is „`On`," the endpoint will buffer the traffic in order to provide more consistent packet sizing; „`Off`" (default) will not buffer any video internally.

TANDBERG MXP Endpoints

MXP Layer 4 Miscellaneous Ports

The TANDBERG MXP has a central data store that can be accessed by several methods.

- ***AMX Device Discovery:*** The MXP can send out a device discovery multicast packet at a random time between 30 and 60 seconds, when enabled. This protocol is disabled by default.
- ***HTTP:*** System management and setup.
- ***HTTPS:*** Secure system management and setup.
- ***FTP:*** Install software, upload configurations.
- ***Telnet:*** Provides access to the API based upon the XML engine for control, setup and status monitoring.
- ***Telnet Challenge:*** Provides secure password transmission between the telnet client and the endpoint.
- ***Secure Shell (SSH):*** Secure access to the API based upon the XML engine.
- ***SNMP:*** Provides SNMP support for TMS and other SNMP Management Applications.
- ***XML:*** Provides full control, setup and status monitoring ability. Can also be used in conjunction with HTTPS for secure control, setup and status monitoring.

Function	*Port*	*Type*	*Direction*
FTP	21*	TCP	Host → Endpoint
SSH	22*	TCP	Host → Endpoint
Telnet	23*	TCP	Host → Endpoint
Telnet Challenge	57*	TCP	Host → Endpoint
HTTP / XML	80*	TCP	Host → Endpoint
NTP	123*	UDP	Endpoint → NTP Server
SNMP (Queries)	161*	UDP	Host → Endpoint
SNMP (Traps)	162	UDP	Endpoint → SNMP Trap Host
HTTPS / XML	443*	TCP	Host → Endpoint
FTP/data	1026	TCP	Host → Endpoint
VNC	1027	TCP	Endpoint → VNC Server
AMX Device Discovery	239.255.250.250:9131	UDP	Endpoint → AMX Broadcast

* denotes a listening port. ↔ (bi-directional)

MXP Gatekeeper Interaction

Function	Port	Type	Direction
Gatekeeper RAS	1719	UDP	Endpoint → GK
Gatekeeper Discovery	224.0.1.41:1718	UDP	Endpoint → Multicast

* RND stands for random port used. This reference will be used to signify source ports in many different applications as, depending on the endpoint, the ports could vary.

MXP Streaming

The TANDBERG MXP Endpoints support a single unicast or multicast streaming session. To ensure the multicast IP address is unique for multiple TANDBERG systems on the same multicast network, TANDBERG uses a technique based upon the hardware serial number of the system to calculate a unique multicast IP address at the factory. This address can be changed by the user. TANDBERG also supports Session Announcement Protocol for identifying multicast sessions.

Function	Port	Type	Direction
Streaming/RTP Video	970	UDP	Endpoint → Host
Streaming/RTCP Video	971	UDP	Endpoint → Host
Streaming/RTP Audio	972	UDP	Endpoint → Host
Streaming/RTCP Audio	973	UDP	Endpoint → Host
SAP**	974	UDP	Endpoint → Host

** stream is directed to 224.2.127.254, port 9875

MXP (F1) Call Flow (Site A calls Site B)

Site A outgoing	Protocol	Type	Site B incoming
5555	H.225/Q.931	TCP	1720
5556	H.245	TCP	5555
2326	Media	UDP/RTP	2334
2327	Media	UDP/RTCP	2335
2328	Media	UDP/RTP	2336
2329	Media	UDP/RTCP	2337
2332	Media	UDP/RTP	2340
2333	Media	UDP/RTCP	2341
2334	Media	UDP/RTP	2326
2335	Media	UDP/RTCP	2327
2336	Media	UDP/RTP	2328
2337	Media	UDP/RTCP	2329
2340	Media	UDP/RTP	2332
2341	Media	UDP/RTP	2333

The TCP/UDP ports will continue to increment while the conference is ongoing (i.e. adding and dropping sites). Once the conference is terminated, all ports are reset to the initial values. If the firewall is adjusted to allow these ports through, take into consideration that the port range could be exceeded if sites are continually added and dropped during a conference.

MXP (F2-F8) Call Flow (Site A calls Site B)

Site A outgoing	Protocol	Type	Site B incoming
5555	H.225/Q.931	TCP	1720
5556:5574	H.245	TCP	5555:5565
2326	Media (Audio)	UDP/RTP	2326
2327	Media (Audio)	UDP/RTCP	2327
2328	Media (Video)	UDP/RTP	2328
2329	Media (Video)	UDP/RTCP	2329
2330	Media (Dual Streams)	UDP/RTP	2330
2331	Media (Dual Streams)	UDP/RTCP	2331
2332	Media (FECC)	UDP/RTP	2332
2333	Media (FECC)	UDP/RTCP	2333

TANDBERG F2-F3 software uses a pool of 11 TCP ports (5555:5565) for Q.931 and H.245. As of F4 software, however, the TCP pool has been increased from the original 11 ports to a total of 20 ports (5555:5574) for the H.225/Q.931 and H.245 connections. The ports will increment every time a new TCP connection is required. When the port number reaches the top of the port numbers allocated to the call setup messages, the port number will reset and begin using 5555 again.

TANDBERG F2-F5 software uses a pool of 160 UDP ports (2326:2487) for all media (both RTP and RTCP). When connecting to far end systems that support symmetrical RTP, the ports are used in increments of 8 per call (e.g. the first call will use either ports 2326-2333 or 2334-2341, depending on call direction). All calls with systems that do not support symmetrical RTP, however, will require 16 ports per call. After the first call is connected, the endpoint will use the next consecutive 8 ports for the subsequent call and so on until all calls are disconnected. Once all calls are disconnected, the ports will reset to the beginning.

The port allocation behavior has changed a bit in F6. While the same port range is used (UDP ports 2326:2487 inclusive), the port range will continue to increment once all active calls are disconnected. Only when the top of the range is reached will the ports to be allocated for the next call reset to the beginning of the range. For example, upon startup, the MXP will allocate ports 2326-2333 for the first call. Whether or not that call disconnects prior to the next call being connected, call 2 will utilize ports 2334-2341. This incremental allocation will continue until port 2487 is reached, at which time the ports will reset to the beginning of the range.

Beginning with software version F2, the TANDBERG endpoint also now uses symmetrical RTP ports, thereby reducing the number of ports needed per call when compared to F1 software. Symmetrical RTP functionality allows the same port to be used for both incoming and outgoing audio streams. However, when the logical channels are opened, the start range for the UDP ports could begin at 2326 or 2334, depending on who initializes the open logical channel commands.

If the H.323 ports of the endpoint are set to dynamic rather than static, the system will use random ports for both the H.225 and H.245 TCP connections. With software versions F1-F3, the MXP will use random ports within the range of 2048 and 65000; beginning with software version F4, however, the random port range is inclusive of ports between 11000 and 65000.

MXP Audio

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.722	20ms	160 bytes	20 bytes	8 bytes	12 bytes	200 bytes
G.722.1_24	20ms	60 bytes	20 bytes	8 bytes	12 bytes	100 bytes
G.722.1_32	20ms	80 bytes	20 bytes	8 bytes	12 bytes	120 bytes
G.728	20ms	40 bytes	20 bytes	8 bytes	12 bytes	80 bytes
AAC-LD	20ms	160 bytes	20 bytes	8 bytes	12 bytes	200 bytes

MXP Video

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

* The dataport command „h323mtu <500…1400>" can be used to change the maximum video payload size to any value between 500 and 1400 bytes.

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 systems can manage packets with jitter up to 100ms; packets not received within this timeframe will be considered lost packets. If excessive packet loss is detected, the TANDBERG systems will make use of IPLR^{TF} (see document D50165, TANDBERG and IPLR, for more information) or downspeeding (flow control) to counteract the packet loss.

F2 software introduced a new dynamic jitter buffer that can increase in value depending on the performance of the network. To minimize introduced latency, this buffer will begin at 20ms and continue to 100ms if sufficient packet loss is occurring.

F3 software introduced RTP time stamping into the audio packets in order to help reduce lip sync issues that may occur over an H.323 call. This operation has also been slightly modified to improve as much as possible within the F4, F5 and F6 software releases.

To further improve lip sync with high resolution images (including XGA, w720p and other high resolution video formats), F3 software has changed the behavior of image buffering prior in order to attempt to place information on the wire as fast as possible. Prior to this adjustment in behavior, the MXP endpoint would attempt to maintain a consistent packet size when placing the information on the wire, which would result in video being buffered internally to ensure that the entire packet could be filled prior to transmission. This potential buffering created a potential lip sync issue at the far end of the H.323 call as the time between the actual capture of the visual image and placing the information on the wire was not a constant and, therefore, the far end system cannot adjust for any time differences between the arrival of the video information and the arrival of the audio information.

The endpoint will now, by default, not buffer the high resolution images prior to transmission, which will ensure a constant time delta between the arrival of the video and audio information to the far end, allowing for an adjustment as necessary and improved lip sync. This change in behavior, though, can cause the MXP to send out consecutive packets that have a relatively large difference in size. For

example, one packet can come out at 1400 bytes while the packet behind that can be sent out at 800 bytes followed by a 1200 byte packet and so on. Some QoS configurations improperly handle the large adjustments in packet size, thereby dropping packets within the QoS buffer and causing packet loss in the call. If, for any reason, it is necessary to disable this behavior, it can be done through the API command „xConfiguration AllowLatency: <On/Off>" (requires the latest minor release of F4 software, at a minimum). When this setting is „On," the MXP will buffer the traffic prior to placing it on the wire; „Off" (default) will not buffer any video internally.

TANDBERG MXP Personal Series Endpoints

MXP Personal Series Layer 4 Miscellaneous Ports

TANDBERG systems have several methods of remote management.

- ***HTTP:*** Used with XML for control, setup, status monitoring and software upgrades. Can be used as a web interface for software upgrades and file manipulation (e.g. welcome screen/logo, system parameters and directories).
- ***HTTPS:*** Used with XML for control, setup, status monitoring and software upgrades.
- ***FTP:*** Install software, upload configurations.
- ***Telnet:*** Provides access to the API based upon the XML engine for control, setup and status monitoring.
- ***SNMP:*** Provides SNMP support for TMS and other SNMP Management Applications.
- ***XML:*** Provides full control, setup and status monitoring ability. Can also be used with HTTPS for secure control, setup and status monitoring.

Function	Port	Type	Direction
FTP	21*	TCP	Host → Endpoint
Telnet	23*	TCP	Host → Endpoint
HTTP / XML	80*	TCP	Host → Endpoint
NTP	123*	UDP	Endpoint → NTP Server
SNMP (Queries)	161*	UDP	Host → Endpoint
SNMP (Traps)	162	UDP	Endpoint → SNMP Trap Host
FTP/data	1026	TCP	Host → Endpoint

* denotes a listening port. ↔ (bi-directional)

MXP Personal Series Gatekeeper Interaction

Function	Port	Type	Direction
Gatekeeper RAS	1719	UDP	Endpoint → GK
Gatekeeper Discovery	224.0.1.41:1718	UDP	↔

↔ (bi-directional)

MXP Personal Series Call Flow (Site A calls Site B)

Site A outgoing	Protocol	Type	Site B incoming
5555	H.225/Q.931	TCP	1720
5556:5565	H.245	TCP	5555:5565
2326	Media (Audio)	UDP/RTP	2326
2327	Media (Audio)	UDP/RTCP	2327
2328	Media (Video)	UDP/RTP	2328
2329	Media (Video)	UDP/RTCP	2329
2330	Media (Dual Streams)	UDP/RTP	2330
2331	Media (Dual Streams)	UDP/RTCP	2331
2332	Media (FECC)	UDP/RTP	2332
2333	Media (FECC)	UDP/RTCP	2333

TANDBERG L1-L5 software uses a pool of 11 TCP ports (5555:5565) for H.225/Q.931 and H.245. The ports will increment every time a new logical connection is required on Q.931 or H.245. When the port number reaches 5565, the port number will reset and begin using 5555 again.

TANDBERG L1-L4 software uses a pool of 32 UDP ports (2326:2357) for all media (both RTP and RTCP). When connecting to far end systems that support symmetrical RTP, the ports are used in increments of 8 per call (e.g. the first call will use either ports 2326-2333 or 2334-2341, depending on call direction). All calls with systems that do not support symmetrical RTP, however, will require 16 ports per call. After the first call is connected, the endpoint will use the next consecutive 8 ports for the subsequent call and so on until all calls are disconnected. Once all calls are disconnected, the ports will reset to the beginning.

The port allocation behavior has changed a bit in L5. While the same port range is used (UDP ports 2326:2487 inclusive), the port range will continue to increment once all active calls are disconnected. Only when the top of the range is reached will the ports to be allocated for the next call reset to the beginning of the range. For example, upon startup, the MXP will allocate ports 2326-2333 for the first call. Whether or not that call disconnects prior to the next call being connected, call 2 will utilize ports 2334-2341. This incremental allocation will continue until port 2487 is reached, at which time the ports will reset to the beginning of the range.

All versions of L software use bi-directional UDP ports, thereby reducing the number of ports required to connect an H.323 call.

MXP Personal Series Audio

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.722	20ms	160 bytes	20 bytes	8 bytes	12 bytes	200 bytes
G.722.1_24	20ms	60 bytes	20 bytes	8 bytes	12 bytes	100 bytes
G.722.1_32	20ms	80 bytes	20 bytes	8 bytes	12 bytes	120 bytes

MXP Personal Series Video

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 L1 – L5 software, the API command „xconfig rtp mtu: <400…1400>" can be used to change the maximum video payload size to any value between 400 and 1400 bytes.

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 systems can manage packets with jitter up to 100ms; packets not received within this timeframe will be considered lost packets. 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.

Introduced in L2, the 150MXP software supports a dynamic jitter buffer that can increase in value depending on the performance of the network. To minimize introduced latency, this buffer will begin at 20ms and continue to 100ms if sufficient packets are arriving outside the current jitter buffer range.

L3 software introduced RTP time stamping into the audio packets in order to help reduce lip sync issues that may occur over an H.323 call.

TANDBERG H.323 INFRASTRUCTURE

TANDBERG provides several infrastructure products aimed at addressing different needs. These products include a distributed MCU, centralized MCU, gateway, gatekeeper and firewall traversal technology. While these form factors may look quite different, they all share the same core technology that makes TANDBERG infrastructure the most feature-rich solution available on the market today.

TANDBERG MCU

Software Version	Released	Release Notes	H.323 Stack
D1	July 2002	D50178	N/A
D2	January 2003	D50188	Version 4
D3	October 2003	D50238	Version 4

TANDBERG MPS

Software Version	Released	Release Notes	H.323 Stack
J1	July 2004	D50301	Version 4
J2	February 2005	D50337	Version 4
J3	January 2006	D50414	Version 5
J4	July 2007	D50489	Version 5

TANDBERG Codian 4500 MCU

Software Version	Released	Release Notes	H.323 Stack
2.2	December 2007	N/A	Version 5
2.4	September 2008	D14287	Version 5
3.0	May 2009	D14467	Version 5
3.1	July 2009	D14514	Version 5
4.0	February 2010	D14580	Version 5

TANDBERG Codian 4200 MCU

Software Version	Released	Release Notes	H.323 Stack
2.2	December 2007	N/A	Version 5
2.4	September 2008	D14287	Version 5
3.0	May 2009	D14467	Version 5
3.1	July 2009	D14514	Version 5
4.0	February 2010	D14580	Version 5

TANDBERG Gateway

Software Version	Released	Release Notes	H.323 Stack
G1	July 2003	D50207	Version 4
G2	October 2003	D50241	Version 4
G3	July 2005	D50369	Version 5

TANDBERG MPS Gateway

Software Version	Released	Release Notes	H.323 Stack
J3	January 2006	D50414	Version 5
J4	July 2007	D50489	Version 5

TANDBERG Codian ISDN Gateway 3200

Software Version	Released	Release Notes	H.323 Stack
1.3	December 2007	N/A	Version 5
1.4	July 2008	N/A	Version 5
1.5	May 2009	D14463	Version 5
2.0	December 2009	D14565	Version 5

TANDBERG Codian IP Gateway 3500

Software Version	Released	Release Notes	H.323 Stack
1.1	December 2007	N/A	Version 5
2.0	December 2008	D14535	Version 5

TANDBERG Entrypoint

Software Version	Released	Release Notes	H.323 Stack
EP1	March 2007	D50477	Version 4

TANDBERG 3G Gateway

Software Version	Released	Release Notes	H.323 Stack
R1	January 2006	D50406	Version 4
R2	April 2006	D50436	Version 4
R3	June 2007	D50495	Version 4

TANDBERG Video Portal

Software Version	Released	Release Notes	H.323 Stack
V2	April 2006	D50437	Version 4
V3	June 2007	D50496	Version 4

TANDBERG Content Server

Software Version	Released	Release Notes	H.323 Stack
S1	January 2006	D50411	Version 4[1]
S2	November 2006	D50460	Version 5
S3	January 2008	D50510	Version 5
S4	December 2009	D14589	Version 6

TANDBERG Codian IPVCR 2200

Software Version	Released	Release Notes	H.323 Stack
2.2	December 2007	N/A	Version 5
2.3	August 2008	D14241	Version 5

TANDBERG Video Communication Server

Software Version	Released	Release Notes	H.323 Stack
X1	August 2007	D50491	Version 5
X2	February 2008	D50518	Version 5
X3	June 2008	D50538	Version 6
X4	January 2009	D50559	Version 6
X5	December 2009	D50582	Version 6

TANDBERG Gatekeeper

Software Version	Released	Release Notes	H.323 Stack
N1	July 2004	D50300	Version 4
N2	February 2005	D50338	Version 4
N3	July 2005	D50360	Version 5
N4	January 2006	D50404	Version 5
N5	July 2006	D50441	Version 5

[1] The TANDBERG Content Server uses some components of version 3 of the H.323 stack, but is primarily version 4.

TANDBERG Border Controller

Software Version	Released	Release Notes	H.323 Stack
Q1	February 2005	D50339	Version 4
Q2	July 2005	D50361	Version 5
Q3	January 2006	D50405	Version 5
Q5	July 2006	D50442	Version 5

Key
Agora H.323 Stack
OpenH323 Stack
RADVISION H.323 Stack
TANDBERG H.323 Stack
Codian H.323 Stack

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

TANDBERG MCU

The TANDBERG MCU is a stand alone appliance ideal for the small enterprise needs or in larger distributed architectures.

MCU Layer 4 Miscellaneous Ports

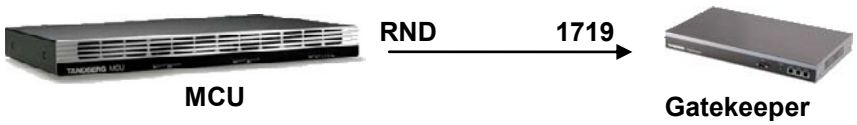
The TANDBERG MCU takes advantage of several different methods of remote management.

- ***HTTP:*** System management and setup.
- ***HTTPS:*** Secure system management and setup.
- ***Telnet:*** Provides access to the API based upon the XML engine for control, setup and status monitoring.
- ***FTP:*** Install software, upload configurations.
- ***SNMP:*** Provides SNMP support for TMS and other SNMP Management Applications.

Function	Port	Type	Direction
FTP	21*	TCP	Host → MCU
Telnet	23*	TCP	Host → MCU
HTTP	80*	TCP	Host → MCU
NTP	123*	UDP	MCU → NTP Server
SNMP (Queries)	161*	UDP	Host → MCU
SNMP (Traps)	162	UDP	MCU → SNMP Trap Host
HTTPS	443*	TCP	Host → MCU
FTP/data	1026	TCP	Host → MCU

* denotes a listening port. ↔ (bi-directional)

MCU Gatekeeper Interaction



Function	Port	Type	Direction
Gatekeeper RAS	1719	UDP	MCU → GK
Gatekeeper Discovery	224.0.1.41:1718	UDP	MCU → Multicast

MCU Call Flow (MCU calls Site A)

MCU outgoing	Protocol	Type	Site B incoming
5555	Q.931	TCP	1720
5556:5587	H.245	TCP	5555:5565
2326*	Media (Audio)	UDP/RTP	2326
2327*	Media (Audio)	UDP/RTCP	2327
2328*	Media (Video)	UDP/RTP	2328
2329*	Media (Video)	UDP/RTCP	2329
2330*	Media (Duo)	UDP/RTP	2330
2331*	Media (Duo)	UDP/RTCP	2331

* The chart above is an example of the ports used during call connectivity. The TANDBERG MCU uses a random association of ports in the range of 2326-2333 (for the first call). While the ports above are the example of one call, the exact port numbers could vary from call to call.

Beginning with software version D2, the TANDBERG MCU uses a pool of 33 TCP ports (5555:5587) for Q.931 and H.245. The ports will increment every time a new logical connection is required on Q.931 or H.245. When the port number reaches 5587, the port number will reset and begin using 5555 again.

All TANDBERG MCU software uses a pool of 512 UDP ports (2326:2837) for all media (both RTP and RTCP). The ports are used in increments of 8 per call (e.g. the first call will use ports 2326-2333). After the first call is connected, the MCU will use the next consecutive 8 ports for the subsequent call and so on until all calls are disconnected. Once all calls are disconnected, the ports will reset to the beginning.

MCU Audio

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.722	20ms	160 bytes	20 bytes	8 bytes	12 bytes	200 bytes
G.722.1_24	20ms	60 bytes	20 bytes	8 bytes	12 bytes	100 bytes
G.722.1_32	20ms	80 bytes	20 bytes	8 bytes	12 bytes	120 bytes
G.728	20ms	40 bytes	20 bytes	8 bytes	12 bytes	80 bytes

MCU Video

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

* with D2-D3 software, the dataport command „ipmtu <1200…1400>" can be used to adjust the maximum video payload size to any value between 1200 and 1400 bytes.

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 systems can manage packets with jitter up to 200ms; packets not received within this timeframe will be considered lost packets. 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.

TANDBERG MPS 200/800

The TANDBERG MPS is a card-based chassis ideal for medium to large enterprise needs or centralized deployment architecture.

MPS Layer 4 Miscellaneous Ports

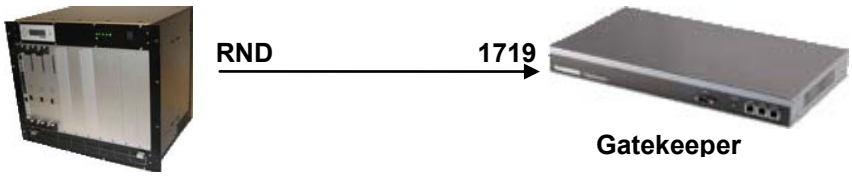
The TANDBERG MPS has a central data store that can be accessed by several methods.

- ***HTTP:*** System management and setup.
- ***HTTPS:*** Secure system management and setup.
- ***Telnet:*** Provides access to the API based upon the XML engine for control, setup and status monitoring.
- ***Secure Shell (SSH):*** Secure access to the API based upon the XML engine.
- ***SNMP:*** Provides SNMP support for TMS and other SNMP Management Applications.
- ***XML:*** Provides full control, setup and status monitoring ability. Can also be used with HTTPS for secure control, setup and status monitoring.

Function	Port	Type	Direction
FTP	21*	TCP	Host → MPS
SSH	22*	TCP	Host → MPS
Telnet	23*	TCP	Host → MPS
HTTP / XML	80*	TCP	Host → MPS
NTP	123*	UDP	MPS → NTP Server
SNMP (Queries)	161*	UDP	Host → MPS
SNMP (Traps)	162	UDP	MPS → SNMP Trap Host
HTTPS / XML	443*	TCP	Host → MPS
FTP/data	1026	TCP	Host → MPS

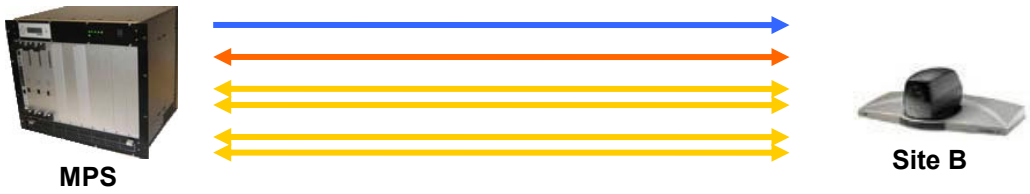
* denotes a listening port. ↔ (bi-directional)

MPS Gatekeeper Interaction



Function	Port	Type	Direction
Gatekeeper RAS	1719	UDP	MPS → GK
Gatekeeper Discovery	224.0.1.41:1718	UDP	MPS → Multicast

MPS Call Flow (MPS calls Site A)



MPS outgoing	Protocol	Type	Site B incoming
5555	Q.931	TCP	1720
5556:6555	H.245	TCP	5555:5565
2326	Media (Video)	UDP/RTP	2328
2327	Media (Video)	UDP/RTCP	2329
2328	Media (Dual Streams)	UDP/RTP	2330
2329	Media (Dual Streams)	UDP/RTCP	2331
2330	Media (Audio)	UDP/RTP	2326
2331	Media (Audio)	UDP/RTCP	2327

Beginning with software version J2, the MPS uses a pool of 1001 TCP ports for all H.225/Q.931 and H.245 messages (5555:6555). The ports will increment every time a new logical connection is required on Q.931 or H.245. When the port number reaches 6555, the port number will reset and begin using 5555 again. All H.225 and H.245 TCP traffic will flow between the System Controller card on the MPS and the far end system.

The MPS uses a pool of 4626 UDP ports (2326:6951) for all media (both RTP and RTCP). The ports are used in increments of 8 per call (e.g. the first call will use ports 2326-2333). After the first call is connected, the MPS will use the next consecutive 8 ports for the subsequent call and so on until all calls are disconnected. Once all calls are disconnected, the ports will reset to the beginning. All UDP Media content will flow directly between the specific media blade on the MPS and the endpoint connected.

The port allocation behavior has changed a bit in J4. While the same port range is used (UDP ports 2326:6951 inclusive), the port range will continue to increment once all active calls are disconnected. Only when the top of the range is reached will the ports to be allocated for the next call reset to the beginning of the range. For example, upon startup, the MPS will allocate ports 2326-2333 for the first call. Whether or not that call disconnects prior to the next call being connected, call 2 will utilize ports 2334-2341. This incremental allocation will continue until port 6951 is reached, at which time the ports will reset to the beginning of the range.

Similar to the MXP endpoints running F2 or later, the TANDBERG MPS (all versions of software) uses bi-directional UDP ports, so the number of ports required is reduced in comparison to older versions of the TANDBERG endpoints software.

MPS Audio

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.722	20ms	160 bytes	20 bytes	8 bytes	12 bytes	200 bytes
G.722.1_24	20ms	60 bytes	20 bytes	8 bytes	12 bytes	100 bytes
G.722.1_32	20ms	80 bytes	20 bytes	8 bytes	12 bytes	120 bytes
G.728	20ms	40 bytes	20 bytes	8 bytes	12 bytes	80 bytes
AAC-LD	20 ms	160 bytes	20 bytes	8 bytes	12 bytes	200 bytes

MPS Video

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

* with all versions of the MPS software, the dataport command „xconfig RTP MTU: <1200…1400>" can be used to change the maximum video payload size to any value between 1200 and 1400 bytes.

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 systems can manage packets with jitter up to 200ms; packets not received within this timeframe will be considered lost packets. 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.

To further improve lip sync with high resolution images (including XGA, w720p and other high resolution video formats), J3 software has changed the behavior of image buffering prior in order to attempt to place information on the wire as fast as possible. Prior to this adjustment in behavior, the MPS would attempt to maintain a consistent packet size when placing the information on the wire, which would result in video being buffered internally to ensure that the entire packet could be filled prior to transmission. This potential buffering created a potential lip sync issue at the far end of the H.323 call as the time between the actual capture of the visual image and placing the information on the wire was not a constant and, therefore, the far end system cannot adjust for any time differences between the arrival of the video information and the arrival of the audio information.

The MPS will now, by default, not buffer the high resolution images prior to transmission, which will ensure a constant time delta between the arrival of the video and audio information to the far end, allowing for an adjustment as necessary and improved lip sync. This change in behavior, though, can cause the MPS to send out consecutive packets that have a relatively large difference in size. For example, one packet can come out at 1400 bytes while the packet behind that can be sent out at 800 bytes followed by a 1200 byte packet and so on. Some QoS configurations improperly handle the large adjustments in packet size, thereby dropping packets within the QoS buffer and causing packet loss in the call. If, for any reason, it is necessary to disable this behavior, it can be done through the API command „`xConfiguration SystemUnit TrafficShaping: <On/Off>`" (requires the latest minor release of J3 software, at a minimum). When this setting is „On," the MPS will buffer the traffic prior to placing it on the wire; „Off" (default) will not buffer any video internally.

TANDBERG Codian MSE 8050 Supervisor Blade

The MSE 8000 is a carrier-class, card-based chassis that allows for up to 360 ports of videoconferencing in a single, fault tolerant solution.

MSE 8050 Layer 4 Miscellaneous Ports

The Codian MSE 8000 has a central data store that can be accessed by several methods.

- ***FTP:*** File transfer.
- ***HTTP:*** System management and setup.
- ***Telnet:*** Provides access to the API based upon the XML engine for control, setup and status monitoring.
- ***Secure Shell (SSH):*** Secure access to the API based upon the XML engine.
- ***SNMP:*** Provides SNMP support for TMS and other SNMP Management Applications.

Note: The Codian products allocate random ports in the range of 49152 to 65535. It is possible to change the fixed ports on which the Codian products receive and establish connections under the „Network" > „Services" portion of the management interface.

Function	Port	Type	Direction
FTP	21*	TCP	Host → MSE 8000
HTTP	80*	TCP	Host → MSE 8000
SNMP (Queries)	161*	UDP	Host → MSE 8000
SNMP (Traps)	162	UDP	MSE 8000 → Host
RTSP	554	TCP	MSE 8000 → Host
Windows Media Streaming	1755	TCP	MSE 8000 → Host
FTP/data	Random/Dynamic	TCP	Host → MSE 8000

* denotes a listening port. ↔ (bi-directional)

Note: The MSE 8000 does not participate in any H.323 communications itself, but rather relies on the installed media blades for this functionality. The behaviors of the media blades are discussed below within their particular sections.

TANDBERG Codian 4500/8500 Series MCU

The TANDBERG Codian 4500 series of MCUs are stand alone appliances supporting up to 40 ports per chassis. Multiple chassis can be combined through cascading either in a distributed or centralized architecture if an increase in capacity is required.

4500/8500 MCU Layer 4 Miscellaneous Ports

The Codian 4500 has a central data store that can be accessed by several methods.

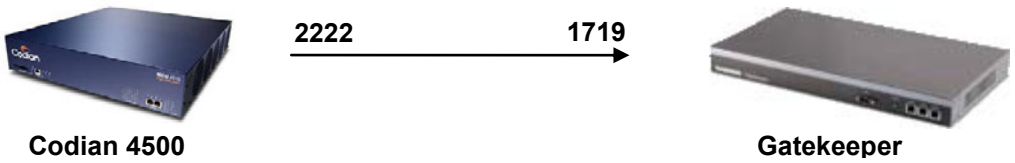
- ***FTP:*** File transfer.
- ***HTTP:*** System management and setup.
- ***SNMP:*** Provides SNMP support for TMS and other SNMP Management Applications.
- ***XML:*** Provides full control, setup and status monitoring ability.

Note: The Codian products allocate random ports in the range of 49152 to 65535. It is possible to change the fixed ports on which the Codian products receive and establish connections under the „Network" > „Services" portion of the management interface.

Function	Port	Type	Direction
FTP	21*	TCP	Host → 4500
HTTP	80*	TCP	Host → 4500
SNMP (Queries)	161*	UDP	Host → 4500
SNMP (Traps)	162	UDP	4500 → Host
RTSP	554	TCP	4500 → Host
Windows Media Streaming	1755	TCP	4500 → Host
FTP/data	Random/Dynamic	TCP	Host → 4500

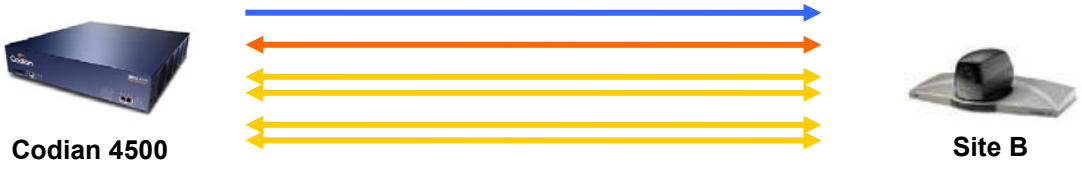
* denotes a listening port. ↔ (bi-directional)

4500/8500 MCU Gatekeeper Interaction



Function	Port	Type	Direction
Gatekeeper RAS	1719	UDP	4500 → GK

4500/8500 MCU Call Flow



4500 Outgoing	Protocol	Type	Site B incoming
49152:65535	Q.931	TCP	1720
49152:65535	H.245	TCP	Endpt Defined
49152:65535	Media (Video)	UDP/RTP	Endpt Defined
49152:65535	Media (Video)	UDP/RTCP	Endpt Defined
49152:65535	Media (Dual Streams)	UDP/RTP	Endpt Defined
49152:65535	Media (Dual Streams)	UDP/RTCP	Endpt Defined
49152:65535	Media (Audio)	UDP/RTP	Endpt Defined
49152:65535	Media (Audio)	UDP/RTCP	Endpt Defined

For all outbound and inbound H.323 connections (except the inbound Q.931 connection which uses port 1720 TCP), the Codian 4500 will use a random port within the range of 49152 to 65535. Because the same port range is shared by multiple services (i.e. FTP data, H.323 media/call signaling/control and SIP media/call signaling/control), ports are allocated at the time they are needed for each particular service; ports used for logical channels are only allocated when necessary. Logical channels and signaling channels are opened up at different times of an H.323 call; ports may or may not be consecutive within a single call. For example, a standard H.323 call (i.e. audio and video only) may occupy ports 49172/49173 TCP and 49166/49167 and 49160/49161 UDP due to the number of connections that are opened up around the same time. All random ports are allocated from the top of range down, beginning with the ports in the 65xxx grouping.

4500/8500 MCU Audio

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.722	20ms	160 bytes	20 bytes	8 bytes	12 bytes	200 bytes
G.723.1	30ms	48 bytes	20 bytes	8 bytes	12 bytes	88 bytes
G.729	20ms	20 bytes	20 bytes	8 bytes	12 bytes	60 bytes
AAC-LC_48	20ms	180 bytes	20 bytes	8 bytes	12 bytes	220 bytes
AAC-LC_56	20ms	210 bytes	20 bytes	8 bytes	12 bytes	250 bytes
AAC-LC_64	20ms	240 bytes	20 bytes	8 bytes	12 bytes	280 bytes
AAC-LC_96	20ms	400 bytes	20 bytes	8 bytes	12 bytes	440 bytes
AAC-LD_48	20ms	120 bytes	20 bytes	8 bytes	12 bytes	160 bytes
AAC-LD_56	20ms	140 bytes	20 bytes	8 bytes	12 bytes	180 bytes
AAC-LD_64	20ms	160 bytes	20 bytes	8 bytes	12 bytes	200 bytes
AAC-LD_96	20ms	240 bytes	20 bytes	8 bytes	12 bytes	280 bytes
Siren14	20ms	120 bytes	20 bytes	8 bytes	12 bytes	160 bytes
G.722.1 Annex C	20ms	120 bytes	20 bytes	8 bytes	12 bytes	160 bytes

4500/8500 MCU Video

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

* with 2.2(1.0) software, the maximum mtu used for video payload can be adjusted between 400 and 1400 bytes through the web interface control under „Settings" > „Conferences" > „Maximum transmitted video packet size."

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. The TANDBERG Codian 4500 MCU incorporates variable, independent jitter buffers for the audio and video streams of the call. The audio stream has a dynamic jitter buffer of 40ms up to and including 240ms, while the dynamic jitter buffer used for the video stream begins at 30ms and can increase when deemed necessary by an increase in jitter for the active H.323 call. The maximum size of the jitter buffer is determined by the bandwidth of the call in question; for a call connected at 384kbps, the jitter buffer can equate to a full 2 seconds, while a 2Mbps call will equate to a jitter buffer of approximately 350ms.

The Codian 4500 MCU utilizes RTP time stamping between the audio and video streams to ensure they remain synchronized throughout the call.

TANDBERG Codian 4200/8400 Series MCU

The TANDBERG Codian 4200 series of MCUs are stand alone appliances supporting up to 40 ports per chassis. Multiple chassis can be combined through cascading either in a distributed or centralized architecture if an increase in capacity is required.

4200/8400 MCU Layer 4 Miscellaneous Ports

The Codian 4200 has a central data store that can be accessed by several methods.

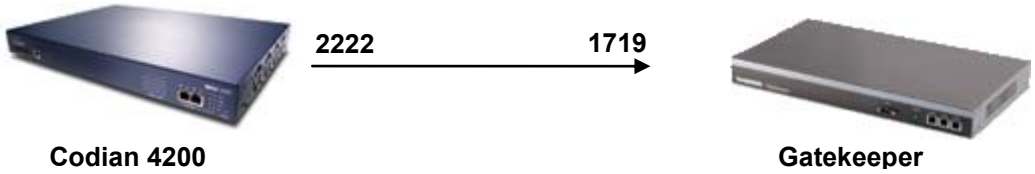
- ***FTP:*** File transfer.
- ***HTTP:*** System management and setup.
- ***SNMP:*** Provides SNMP support for TMS and other SNMP Management Applications.
- ***XML:*** Provides full control, setup and status monitoring ability.

Note: The Codian products allocate random ports in the range of 49152 to 65535. It is possible to change the fixed ports on which the Codian products receive and establish connections under the „Network" > „Services" portion of the management interface.

Function	Port	Type	Direction
FTP	21*	TCP	Host → 4200
HTTP	80*	TCP	Host → 4200
SNMP (Queries)	161*	UDP	Host → 4200
SNMP (Traps)	162	UDP	4200 → Host
RTSP	554	TCP	4200 → Host
Windows Media Streaming	1755	TCP	4200 → Host
FTP/data	Random/Dynamic	TCP	Host → 4200

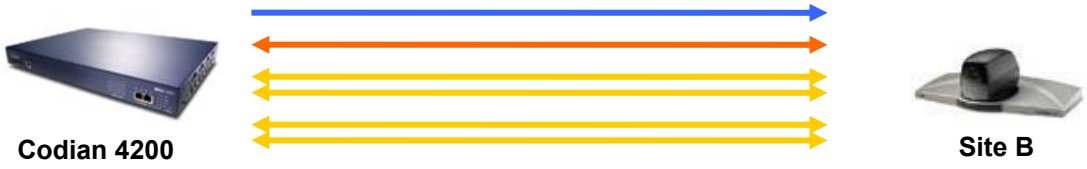
* denotes a listening port. ↔ (bi-directional)

4200/8400 MCU Gatekeeper Interaction



Function	Port	Type	Direction
Gatekeeper RAS	1719	UDP	4200 → GK

4200/8400 MCU Call Flow



4200 Outgoing	Protocol	Type	Site B incoming
49152:65535	Q.931	TCP	1720
49152:65535	H.245	TCP	Endpt Defined
49152:65535	Media (Video)	UDP/RTP	Endpt Defined
49152:65535	Media (Video)	UDP/RTCP	Endpt Defined
49152:65535	Media (Dual Streams)	UDP/RTP	Endpt Defined
49152:65535	Media (Dual Streams)	UDP/RTCP	Endpt Defined
49152:65535	Media (Audio)	UDP/RTP	Endpt Defined
49152:65535	Media (Audio)	UDP/RTCP	Endpt Defined

For all outbound and inbound H.323 connections (except the inbound Q.931 connection which uses port 1720 TCP), the Codian 4200 will use a random port within the range of 49152 to 65535. Because the same port range is shared by multiple services (i.e. FTP data, H.323 media/call signaling/control and SIP media/call signaling/control), ports are allocated at the time they are needed for each particular service; ports used for logical channels are only allocated when necessary. Logical channels and signaling channels are opened up at different times of an H.323 call, ports may or may not be consecutive within a single call. For example, a standard H.323 call (i.e. audio and video only) may occupy ports 49172/49173 TCP and 49166/49167 and 49160/49161 UDP due to the number of connections that are opened up around the same time. All random ports are allocated from the top of range down, beginning with the ports in the 65xxx grouping.

4200/8400 MCU Audio

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.722	20ms	160 bytes	20 bytes	8 bytes	12 bytes	200 bytes
G.723.1	30ms	48 bytes	20 bytes	8 bytes	12 bytes	88 bytes
G.728	20ms	40 bytes	20 bytes	8 bytes	12 bytes	80 bytes
G.729	20ms	20 bytes	20 bytes	8 bytes	12 bytes	60 bytes
AAC-LC_48	20ms	180 bytes	20 bytes	8 bytes	12 bytes	220 bytes
AAC-LC_56	20ms	210 bytes	20 bytes	8 bytes	12 bytes	250 bytes
AAC-LC_64	20ms	240 bytes	20 bytes	8 bytes	12 bytes	280 bytes
AAC-LC_96	20ms	400 bytes	20 bytes	8 bytes	12 bytes	440 bytes
AAC-LD_48	20ms	120 bytes	20 bytes	8 bytes	12 bytes	160 bytes
AAC-LD_56	20ms	140 bytes	20 bytes	8 bytes	12 bytes	180 bytes
AAC-LD_64	20ms	160 bytes	20 bytes	8 bytes	12 bytes	200 bytes
AAC-LD_96	20ms	240 bytes	20 bytes	8 bytes	12 bytes	280 bytes
Siren14	20ms	120 bytes	20 bytes	8 bytes	12 bytes	160 bytes
G.722.1 Annex C	20ms	120 bytes	20 bytes	8 bytes	12 bytes	160 bytes

4200/8400 MCU Video

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

* with 2.2(1.0) software, the maximum mtu used for video payload can be adjusted between 400 and 1400 bytes through the web interface control under „Settings" > „Conferences" > „Maximum transmitted video packet size."

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. The TANDBERG Codian 4200 MCU incorporates variable, independent jitter buffers for the audio and video streams of the call. The audio stream has a dynamic jitter buffer of 40ms up to and including 240ms, while the dynamic jitter buffer for the video stream begins at 30ms and can increase when deemed necessary by an increase in jitter for the active H.323 call. The maximum size of the jitter buffer is determined by the bandwidth of the call in question; for a call connected at 384kbps, the jitter buffer can equate to a full 2 seconds, while a 2Mbps call will equate to a jitter buffer of approximately 350ms.

The Codian 4200 MCU utilizes RTP time stamping between the audio and video streams to ensure they remain synchronized throughout the call.

TANDBERG Gateway

The TANDBERG Gateway is a stand alone appliance ideal for the small enterprise needs or in larger distributed architectures.

Gateway Layer 4 Miscellaneous Ports

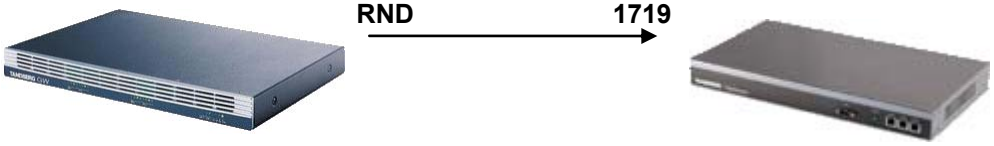
The TANDBERG Gateway has a central data store that can be accessed by several methods.

- ***HTTP:*** System management and setup.
- ***HTTPS:*** Secure system management and setup.
- ***Telnet:*** Provides access to the API based upon the XML engine for control, setup and status monitoring.
- ***Secure Shell (SSH):*** Secure access to the API based upon the XML engine.
- ***SNMP:*** Provides SNMP support for TMS and other SNMP Management Applications.
- ***XML:*** Provides full control, setup and status monitoring ability. Can also be used with HTTPS for secure control, setup and status monitoring.

Function	Port	Type	Direction
FTP	21*	TCP	Host → GW
SSH	22*	TCP	Host → GW
Telnet	23*	TCP	Host → GW
HTTP / XML	80*	TCP	Host → GW
NTP	123*	UDP	GW → NTP Server
SNMP (Queries)	161*	UDP	Host → GW
SNMP (Traps)	162	UDP	GW → SNMP Trap Host
HTTPS / XML	443*	TCP	Host → GW
FTP/data	1026	TCP	Host → GW

* denotes a listening port. ↔ (bi-directional)

Gateway Gatekeeper Interaction



Function	Port	Type	Direction
Gatekeeper RAS	1719	UDP	Gateway → GK
Gatekeeper Discovery	224.0.1.41:1718	UDP	Gateway → Multicast

Gateway G1 – G2 Call Flow (Gateway calls Site A – call initiated from ISDN side)

Gateway outgoing	Protocol	Type	Site B incoming
5555	Q.931	TCP	1720
5556:5587	H.245	TCP	5555:5565
2326	Media (Audio)	UDP/RTP	2326
2327	Media (Audio)	UDP/RTCP	2327
2328	Media (Video)	UDP/RTP	2328
2329	Media (Video)	UDP/RTCP	2329
2330	Media (Duo)	UDP/RTP	2330
2331	Media (Duo)	UDP/RTCP	2331
2332	Media (FECC)	UDP/RTP	2332
2333	Media (FECC)	UDP/RTCP	2333

Beginning with software version G1, the TANDBERG Gateway uses a pool of 33 TCP ports (5555:5587) for Q.931 and H.245. The ports will increment every time a new logical connection is required on Q.931 or H.245. When the port number reaches 5587, the port number will reset and begin using 5555 again.

All TANDBERG Gateway software uses a pool of 512 UDP ports (2326:2837) for all media (both RTP and RTCP). The ports are used in increments of 8 per call (e.g. the first call will use ports 2326-2333). After the first call is connected, the Gateway will use the next consecutive 8 ports for the subsequent call and so on until all calls are disconnected. Once all calls are disconnected, the ports will reset to the beginning.

Gateway G1 – G2 Call Flow (Gateway calls Site A – call initiated from ISDN side)

Gateway outgoing	Protocol	Type	Site B incoming
5555	Q.931	TCP	1720
5556:6555	H.245	TCP	5555:5565
2326	Media (Audio)	UDP/RTP	2326
2327	Media (Audio)	UDP/RTCP	2327
2328	Media (Video)	UDP/RTP	2328
2329	Media (Video)	UDP/RTCP	2329
2330	Media (Duo)	UDP/RTP	2330
2331	Media (Duo)	UDP/RTCP	2331
2332	Media (FECC)	UDP/RTP	2332
2333	Media (FECC)	UDP/RTCP	2333

With the upgrade to G3 software, the TANDBERG Gateway increased its TCP pool to a total of 1001 ports (5555:6555) for Q.931 and H.245. The ports will increment every time a new logical connection is required on Q.931 or H.245. When the port number reaches 6555, the port number will reset and begin using 5555 again.

The range used for UDP media was also increased to 4626 ports (2326:6951) for all media (both RTP and RTCP). The ports are used in increments of 8 per call (e.g. the first call will use ports 2326-2333). After the first call is connected, the Gateway will use the next consecutive 8 ports for the subsequent call and so on until all calls are disconnected. Once all calls are disconnected, the ports will reset to the beginning.

Gateway Audio

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.722	20ms	160 bytes	20 bytes	8 bytes	12 bytes	200 bytes
G.722.1_24	20ms	60 bytes	20 bytes	8 bytes	12 bytes	100 bytes
G.722.1_32	20ms	80 bytes	20 bytes	8 bytes	12 bytes	120 bytes
G.728	20ms	40 bytes	20 bytes	8 bytes	12 bytes	80 bytes

Gateway Video

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

* with G1-G3 software, the dataport command „ipmtu <1200…1400>" can be used to adjust the maximum video payload size to any value between 1200 and 1400 bytes.

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 systems can manage packets with jitter up to 100ms; packets not received within this timeframe will be considered lost packets. 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.

TANDBERG MPS 200/800 Gateway

The TANDBERG MPS is a card-based chassis ideal for medium to large enterprise needs or centralized deployment architecture.

MPS Gateway Layer 4 Miscellaneous Ports

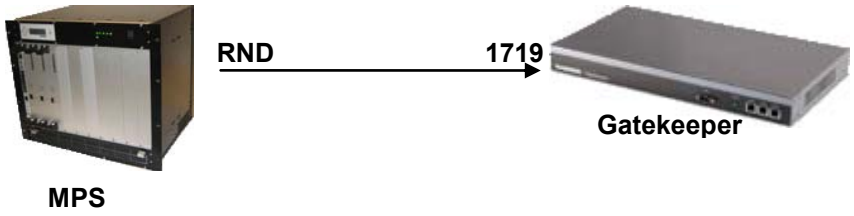
The TANDBERG MPS has a central data store that can be accessed by several methods.

- ***HTTP:*** System management and setup.
- ***HTTPS:*** Secure system management and setup.
- ***Telnet:*** Provides access to the API based upon the XML engine for control, setup and status monitoring.
- ***Secure Shell (SSH):*** Secure access to the API based upon the XML engine.
- ***SNMP:*** Provides SNMP support for TMS and other SNMP Management Applications.
- ***XML:*** Provides full control, setup and status monitoring ability. Can also be used with HTTPS for secure control, setup and status monitoring.

Function	Port	Type	Direction
FTP	21*	TCP	Host → MPS
SSH	22*	TCP	Host → MPS
Telnet	23*	TCP	Host → MPS
HTTP / XML	80*	TCP	Host → MPS
NTP	123*	UDP	MPS → NTP Server
SNMP (Queries)	161*	UDP	Host → MPS
SNMP (Traps)	162	UDP	MPS → SNMP Trap Host
HTTPS / XML	443*	TCP	Host → MPS
FTP/data	1026	TCP	Host → MPS

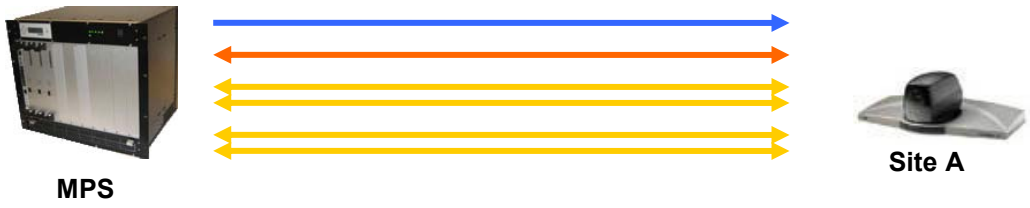
* denotes a listening port. ↔ (bi-directional)

MPS Gateway Gatekeeper Interaction



Function	Port	Type	Direction
Gatekeeper RAS	1719	UDP	MPS → GK
Gatekeeper Discovery	224.0.1.41:1718	UDP	MPS → Multicast

MPS Gateway Call Flow (MPS Calls Site A – call initiated from ISDN side)



Site A outgoing	Protocol	Type	Site B incoming
5555	Q.931	TCP	1720
5556:6555	H.245	TCP	5555:5565
2326	Media (Video)	UDP/RTP	2328
2327	Media (Video)	UDP/RTCP	2329
2328	Media (Dual Streams)	UDP/RTP	2330
2329	Media (Dual Streams)	UDP/RTCP	2331
2330	Media (Audio)	UDP/RTP	2326
2331	Media (Audio)	UDP/RTCP	2327

TANDBERG J3 software uses a pool of 1001 TCP ports (5555:6555) for H.225/Q.931 and H.245. The ports will increment every time a new logical connection is required on Q.931 or H.245. When the port number reaches 6555, the port number will reset and begin using 5555 again. All H.225 and H.245 TCP traffic will flow between the Service Controller card on the MPS and the far end system.

The MPS uses a pool of 4608 UDP ports (2326:6933) for all media (both RTP and RTCP). The ports are used in increments of 8 per call (e.g. the first call will use ports 2326-2333). After the first call is connected, the MPS will use the next consecutive 8 ports for the subsequent call and so on until all calls are disconnected. Once all calls are disconnected, the ports will reset to the beginning. All UDP Media content will flow directly between the specific media blade on the MPS and the endpoint connected.

The port allocation behavior has changed a bit in J4. While the same port range is used (UDP ports 2326:6951 inclusive), the port range will continue to increment once all active calls are disconnected. Only when the top of the range is reached will the ports to be allocated for the next call reset to the beginning of the range. For example, upon startup, the MPS will allocate ports 2326-2333 for the first call. Whether or not that call disconnects prior to the next call being connected, call 2 will utilize ports 2334-2341. This incremental allocation will continue until port 6951 is reached, at which time the ports will reset to the beginning of the range.

Similar to the MXP endpoints running F2 or later, the TANDBERG MPS uses bi-directional UDP ports, so the number of ports required is reduced in comparison to older versions of the TANDBERG endpoints software.

MPS Gateway Audio

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.722	20ms	160 bytes	20 bytes	8 bytes	12 bytes	200 bytes
G.722.1_24	20ms	60 bytes	20 bytes	8 bytes	12 bytes	100 bytes
G.722.1_32	20ms	80 bytes	20 bytes	8 bytes	12 bytes	120 bytes
G.728	20ms	40 bytes	20 bytes	8 bytes	12 bytes	80 bytes
AAC-LD	20 ms	160 bytes	20 bytes	8 bytes	12 bytes	200 bytes

MPS Gateway Video

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

* the dataport command „xconfig RTP MTU: <1200…1400>" can be used to change the maximum video payload size to any value between 1200 and 1400 bytes.

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 systems can manage packets with jitter up to 200ms; packets not received within this timeframe will be considered lost packets. 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.

To further improve lip sync with high resolution images (including XGA, w720p and other high resolution video formats), J3 software has changed the behavior of image buffering prior in order to attempt to place information on the wire as fast as possible. Prior to this adjustment in behavior, the MPS would attempt to maintain a consistent packet size when placing the information on the wire, which would result in video being buffered internally to ensure that the entire packet could be filled prior to transmission. This potential buffering created a potential lip sync issue at the far end of the H.323 call as the time between the actual capture of the visual image and placing the information on the wire was not a constant and, therefore, the far end system cannot adjust for any time differences between the arrival of the video information and the arrival of the audio information.

The MPS will now, by default, not buffer the high resolution images prior to transmission, which will ensure a constant time delta between the arrival of the video and audio information to the far end, allowing for an adjustment as necessary and improved lip sync. This change in behavior, though, can cause the MPS to send out consecutive packets that have a relatively large difference in size. For example, one packet can come out at 1400 bytes while the packet behind that can be sent out at 800 bytes followed by a 1200 byte packet and so on. Some QoS configurations improperly handle the large adjustments in packet size, thereby dropping packets within the QoS buffer and causing packet loss in the call. If, for any reason, it is necessary to disable this behavior, it can be done through the API command „`xConfiguration SystemUnit TrafficShaping: <On/Off>`" (requires the latest minor release of J3 software, at a minimum). When this setting is „`On`," the MPS will buffer the traffic prior to placing it on the wire; „`Off`" (default) will not buffer any video internally.

TANDBERG Codian 3200 Series ISDN Gateway

The TANDBERG Codian 3200 series of ISDN Gateways are stand alone appliances supporting up to 4 PRIs per chassis. Multiple chassis can be combined throughout a network to provide a full H.323-to-H.320 solution.

ISDN Gateway Layer 4 Miscellaneous Ports

The Codian 3200 has a central data store that can be accessed by several methods.

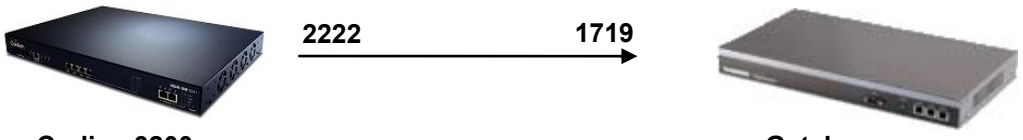
- ***FTP:*** File transfer
- ***HTTP:*** System management and setup.
- ***SNMP:*** Provides SNMP support for TMS and other SNMP Management Applications.
- ***XML:*** Provides full control, setup and status monitoring ability.

Note: The Codian products allocate random ports in the range of 49152 to 65535. It is possible to change the fixed ports on which the Codian products receive and establish connections under the „Network" > „Services" portion of the management interface.

Function	Port	Type	Direction
FTP	21*	TCP	Host → 3200
HTTP	80*	TCP	Host → 3200
SNMP (Queries)	161*	UDP	Host → 3200
SNMP (Traps)	162	UDP	3200 → Host
FTP/data	Random/Dynamic	TCP	Host → 3200

* denotes a listening port. ↔ (bi-directional)

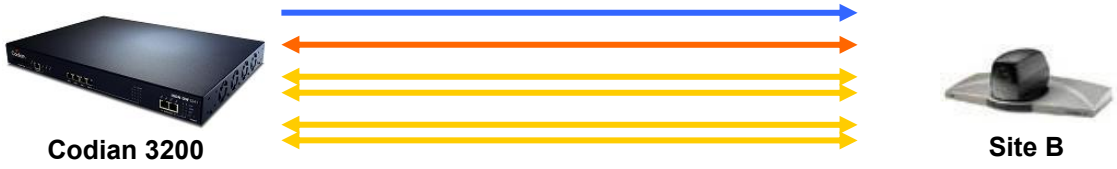
ISDN Gateway Gatekeeper Interaction



Codian 3200 **Gatekeeper**

Function	Port	Type	Direction
Gatekeeper RAS	1719	UDP	3200 → GK

ISDN Gateway Call Flow



3200 Outgoing	Protocol	Type	Site B incoming
49152:65535	Q.931	TCP	1720
49152:65535	H.245	TCP	Endpt Defined
49152:65535	Media (Video)	UDP/RTP	Endpt Defined
49152:65535	Media (Video)	UDP/RTCP	Endpt Defined
49152:65535	Media (Dual Streams)	UDP/RTP	Endpt Defined
49152:65535	Media (Dual Streams)	UDP/RTCP	Endpt Defined
49152:65535	Media (Audio)	UDP/RTP	Endpt Defined
49152:65535	Media (Audio)	UDP/RTCP	Endpt Defined

For all outbound and inbound H.323 connections (except the inbound Q.931 connection which uses port 1720 TCP), the Codian 3200 will use a random port within the range of 49152 to 65535. Because the same port range is shared by multiple services (i.e. FTP data, H.323 media/call signaling/control and SIP media/call signaling/control), ports are allocated at the time they are needed for each particular service; ports used for logical channels are only allocated when necessary. Logical channels and signaling channels are opened up at different times of an H.323 call, ports may or may not be consecutive within a single call. For example, a standard H.323 call (i.e. audio and video only) may occupy ports 49172/49173 TCP and 49166/49167 and 49160/49161 UDP due to the number of connections that are opened up around the same time. All random ports are allocated from the top of range down, beginning with the ports in the 65xxx grouping.

ISDN Gateway Audio

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.722	20ms	160 bytes	20 bytes	8 bytes	12 bytes	200 bytes
G.722.1 Annex C	20ms	120 bytes	20 bytes	8 bytes	12 bytes	160 bytes

ISDN Gateway Video

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

* with 2.2(1.0) software, the maximum mtu used for video payload can be adjusted between 400 and 1400 bytes through the web interface control under „Settings" > „Conferences" > „Maximum transmitted video packet size."

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. The TANDBERG Codian 3200 Gateway incorporates variable, independent jitter buffers for the audio and video streams of the call. The audio stream has a dynamic jitter buffer of 40ms up to and including 240ms, while the dynamic jitter buffer for the video stream begins at 30ms and can increase when deemed necessary by an increase in jitter for the active H.323 call. The maximum size of the jitter buffer is determined by the bandwidth of the call in question; for a call connected at 384kbps, the jitter buffer can equate to a full 2 seconds, while a 2Mbps call will equate to a jitter buffer of approximately 350ms.

The Codian 3200 Gateway utilizes RTP time stamping between the audio and video streams to ensure they remain synchronized throughout the call.

TANDBERG Codian 3500 Series IP Gateway

The TANDBERG Codian 3500 Series of IP Gateways are stand alone appliances supporting up to 40 calls per chassis. Multiple chassis can be combined either in a distributed or centralized architecture if an increase in capacity is required.

IP Gateway Layer 4 Miscellaneous Ports

The Codian 3500 has a central data store that can be accessed by several methods.

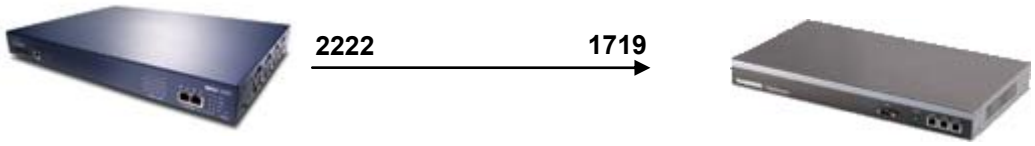
- ***FTP:*** File transfer.
- ***HTTP:*** System management and setup.
- ***XML:*** Provides full control, setup and status monitoring ability.

Note: The Codian products allocate random ports in the range of 49152 to 65535. It is possible to change the fixed ports on which the Codian products receive and establish connections under the „Network" > „Services" portion of the management interface.

Function	Port	Type	Direction
FTP	21*	TCP	Host → 3500
HTTP	80*	TCP	Host → 3500
SNMP (Queries)	161*	UDP	Host → 3500
SNMP (Traps)	162	UDP	3500 → Host
FTP/data	Random/Dynamic	TCP	Host → 3500

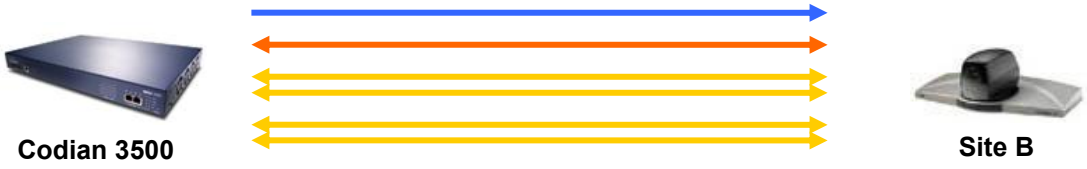
* denotes a listening port. ↔ (bi-directional)

IP Gateway Gatekeeper Interaction



Function	Port	Type	Direction
Gatekeeper RAS	1719	UDP	3500 → GK

IP Gateway Call Flow



3500 Outgoing	Protocol	Type	Site B incoming
49152:65535	Q.931	TCP	1720
49152:65535	H.245	TCP	Endpt Defined
49152:65535	Media (Video)	UDP/RTP	Endpt Defined
49152:65535	Media (Video)	UDP/RTCP	Endpt Defined
49152:65535	Media (Dual Streams)	UDP/RTP	Endpt Defined
49152:65535	Media (Dual Streams)	UDP/RTCP	Endpt Defined
49152:65535	Media (Audio)	UDP/RTP	Endpt Defined
49152:65535	Media (Audio)	UDP/RTCP	Endpt Defined

For all outbound and inbound H.323 connections (except the inbound Q.931 connection which uses port 1720 TCP), the Codian 3500 will use a random port within the range of 49152 to 65535. Because the same port range is shared by multiple services (i.e. FTP data, H.323 media/call signaling/control and SIP media/call signaling/control), ports are allocated at the time they are needed for each particular service; ports used for logical channels are only allocated when necessary. Logical channels and signaling channels are opened up at different times of an H.323 call, ports may or may not be consecutive within a single call. For example, a standard H.323 call (i.e. audio and video only) may occupy ports 49172/49173 TCP and 49166/49167 and 49160/49161 UDP due to the number of connections that are opened up around the same time. All random ports are allocated from the top of range down, beginning with the ports in the 65xxx grouping.

IP Gateway Audio

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.722	20ms	160 bytes	20 bytes	8 bytes	12 bytes	200 bytes
G.723.1	30ms	48 bytes	20 bytes	8 bytes	12 bytes	88 bytes
G.729	20ms	20 bytes	20 bytes	8 bytes	12 bytes	60 bytes
AAC-LC_48	20ms	180 bytes	20 bytes	8 bytes	12 bytes	220 bytes
AAC-LC_56	20ms	210 bytes	20 bytes	8 bytes	12 bytes	250 bytes
AAC-LC_64	20ms	240 bytes	20 bytes	8 bytes	12 bytes	280 bytes
AAC-LC_96	20ms	400 bytes	20 bytes	8 bytes	12 bytes	440 bytes
AAC-LD_48	20ms	120 bytes	20 bytes	8 bytes	12 bytes	160 bytes
AAC-LD_56	20ms	140 bytes	20 bytes	8 bytes	12 bytes	180 bytes
AAC-LD_64	20ms	160 bytes	20 bytes	8 bytes	12 bytes	200 bytes
AAC-LD_96	20ms	240 bytes	20 bytes	8 bytes	12 bytes	280 bytes
Siren14	20ms	120 bytes	20 bytes	8 bytes	12 bytes	160 bytes
G.722.1 Annex C	20ms	120 bytes	20 bytes	8 bytes	12 bytes	160 bytes

IP Gateway Video

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

* with 2.2(1.0) software, the maximum mtu used for video payload can be adjusted between 400 and 1400 bytes through the web interface control under „Settings" > „Conferences" > „Maximum transmitted video packet size."

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. The TANDBERG Codian 3500 Gateway incorporates variable, independent jitter buffers for the audio and video streams of the call. The audio stream has a dynamic jitter buffer of 40ms up to and including 240ms, while the dynamic jitter buffer for the video stream begins at 30ms and can increase when deemed necessary by an increase in jitter for the active H.323 call. The maximum size of the jitter buffer is determined by the bandwidth of the call in question; for a call connected at 384kbps, the jitter buffer can equate to a full 2 seconds, while a 2Mbps call will equate to a jitter buffer of approximately 350ms.

The Codian 3500 Gateway utilizes RTP time stamping between the audio and video streams to ensure they remain synchronized throughout the call.

TANDBERG 3G Gateway

The TANDBERG 3G Gateway is designed to be a service-provider grade H.324M to H.323/SIP gateway.

3G Gateway Layer 4 Miscellaneous Ports

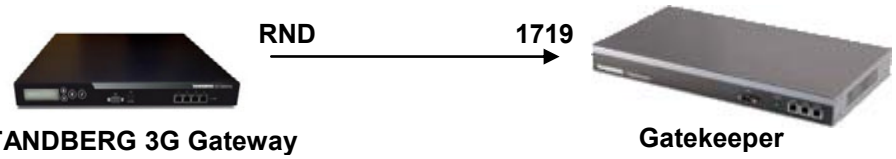
The TANDBERG 3G Gateway has several methods of remote management.

- ***HTTP:*** System management and setup.
- ***HTTPS:*** Secure system management and setup.
- ***Telnet:*** Provides access to the API based upon the XML engine for control, setup and status monitoring.
- ***Secure Shell (SSH):*** Secure access to the API based upon the XML engine.
- ***SNMP:*** Provides SNMP support for TMS and other SNMP Management Applications.
- ***XML:*** Provides full control, setup and status monitoring ability. Can also be used with HTTPS for secure control, setup and status monitoring.

Function	Port	Type	Direction
SSH	22*	TCP	Host → 3G GW
Telnet	23*	TCP	Host → 3G GW
HTTP / XML	80*	TCP	Host → 3G GW
NTP	123*	UDP	3G GW → NTP Server
SNMP (Queries)	161*	UDP	Host → 3G GW
SNMP (Traps)	162	UDP	3G GW → SNMP Trap Host
HTTPS / XML	443*	TCP	Host → 3G GW
FTP/data	1026	TCP	Host → 3G GW

* denotes a listening port. ↔ (bi-directional)

3G Gateway Gatekeeper Interaction



Function	Port	Type	Direction
Gatekeeper RAS	1719	UDP	Gateway → GK
Gatekeeper Discovery	224.0.1.41:1718	UDP	Gateway → Multicast

3G Gateway Call Flow (Gateway calls Site A – call initiated from 3G side)

Site A outgoing	Protocol	Type	Site B incoming
32767	Q.931	TCP	1720
32768:65535	H.245	TCP	5555:5565
25000	Media (Audio)	UDP/RTP	2326
25001	Media (Audio)	UDP/RTCP	2327
25002	Media (Video)	UDP/RTP	2328
25003	Media (Video)	UDP/RTCP	2329
25004	Media (Duo)	UDP/RTP	2330
25005	Media (Duo)	UDP/RTCP	2331
25006	Media (FECC)	UDP/RTP	2332
25007	Media (FECC)	UDP/RTCP	2333

Beginning with software version R1, the TANDBERG 3G Gateway uses a TCP port range from 32800:65535 for Q.931 and H.245. The ports will increment every time a new logical connection is required on Q.931 or H.245. When the port number reaches the top of the range, the port number will reset and begin using 32800 again.

All TANDBERG 3G Gateway software uses a pool of 2001 UDP ports (25000:27000) for all media (both RTP and RTCP). The ports are used in increments of 8 per call (e.g. the first call will use ports 25000-25007). After the first call is connected, the 3G Gateway will use the next consecutive 8 ports for the subsequent call and so on until all calls are disconnected. Once all calls are disconnected, the ports will reset to the beginning.

3G Gateway Audio

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

R1-R3 Video

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

* the dataport command „xConfiguration RTP MTU: <1200-1400>“ can be used to adjust the maximum video payload size to any value between 1200 and 1400 bytes.

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 systems can manage packets with jitter up to 100ms; packets not received within this timeframe will be considered lost packets. 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.

TANDBERG Video Portal

Paired with the TANDBERG 3G Gateway, the TANDBERG Video Portal is designed to provide advanced services to an H.324m to H.323/SIP service provider.

Video Portal Layer 4 Miscellaneous Ports

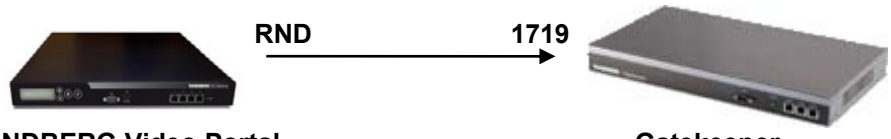
The TANDBERG Video Portal has several methods of remote management.

- ***HTTP:*** System management and setup.
- ***HTTPS:*** Secure system management and setup.
- ***Telnet:*** Provides access to the API based upon the XML engine for control, setup and status monitoring.
- ***Secure Shell (SSH):*** Secure access to the API based upon the XML engine.
- ***SNMP:*** Provides SNMP support for TMS and other SNMP Management Applications.
- ***XML:*** Provides full control, setup and status monitoring ability. Can also be used with HTTPS for secure control, setup and status monitoring.

Function	Port	Type	Direction
SSH	22*	TCP	Host → Video Portal
Telnet	23*	TCP	Host → Video Portal
HTTP / XML	80*	TCP	Host → Video Portal
NTP	123*	UDP	Video Portal → NTP Server
SNMP (Queries)	161*	UDP	Host → Video Portal
SNMP (Traps)	162	UDP	Video Portal → SNMP Trap Host
HTTPS / XML	443*	TCP	Host → Video Portal
FTP/data	1026	TCP	Host → Video Portal

* denotes a listening port. ↔ (bi-directional)

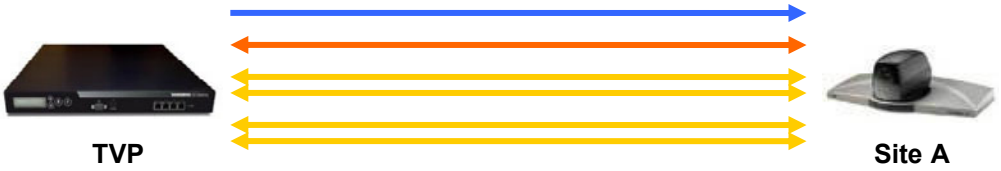
Video Portal Gatekeeper Interaction



TANDBERG Video Portal **Gatekeeper**

Function	Port	Type	Direction
Gatekeeper RAS	1719	UDP	Video Portal → GK
Gatekeeper Discovery	224.0.1.41:1718	UDP	Video Portal → Multicast

Video Portal Call Flow (Video Portal calls Site A – call initiated from 3G side)



Site A outgoing	Protocol	Type	Site B incoming
32767	Q.931	TCP	1720
32768:65535	H.245	TCP	5555:5565
25000	Media (Audio)	UDP/RTP	2326
25001	Media (Audio)	UDP/RTCP	2327
25002	Media (Video)	UDP/RTP	2328
25003	Media (Video)	UDP/RTCP	2329
25004	Media (Duo)	UDP/RTP	2330
25005	Media (Duo)	UDP/RTCP	2331
25006	Media (FECC)	UDP/RTP	2332
25007	Media (FECC)	UDP/RTCP	2333

Beginning with software version V2, the TANDBERG Video Portal uses a TCP port range from 32800:65535 for Q.931 and H.245. The ports will increment every time a new logical connection is required on Q.931 or H.245. When the port number reaches the top of the range, the port number will reset and begin using 32800 again.

All TANDBERG Video Portal software uses a pool of 2001 UDP ports (25000:27000) for all media (both RTP and RTCP). The ports are used in increments of 8 per call (e.g. the first call will use ports 25000-25007). After the first call is connected, the Video Portal will use the next consecutive 8 ports for the subsequent call and so on until all calls are disconnected. Once all calls are disconnected, the ports will reset to the beginning.

Video Portal Audio

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

Video Portal Video

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

* the dataport command „xConfiguration RTP MTU: <1200-1400>" can be used to adjust the maximum video payload size to any value between 1200 and 1400 bytes.

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 systems can manage packets with jitter up to 100ms; packets not received within this timeframe will be considered lost packets. 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.

TANDBERG Content Server

The TANDBERG Content Server is an appliance-based streaming and archiving server for use within any enterprise or educational deployment.

TCS Layer 4 Miscellaneous Ports

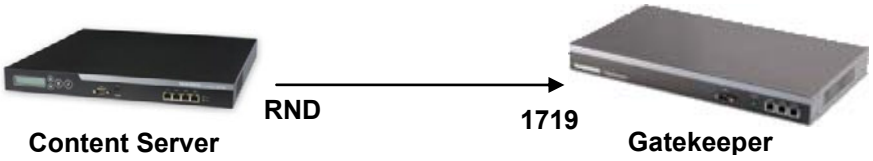
The TANDBERG Video Portal has several methods of remote management.

- ***HTTP:*** System management and setup.
- ***HTTPS:*** Secure system management and setup.
- ***XML:*** Provides full control, setup and status monitoring ability. Can also be used with HTTPS for secure control, setup and status monitoring.
- ***Microsoft Terminal Services:*** Provides full control of the Windows 2003 Server Operating System via a remote connection for management of the box itself.

Function	Port	Type	Direction
HTTP / XML	80*	TCP	Host → TCS
NTP	123*	UDP	TCS → NTP Server
HTTPS / XML	443*	TCP	Host → TCS
Terminal Services	3389*	TCP	Host → TCS

* denotes a listening port. ↔ (bi-directional)

TCS Gatekeeper Interaction



Function	Port	Type	Direction
Gatekeeper RAS	1719	UDP	TCS → GK
Gatekeeper Discovery	224.0.1.41:1718	UDP	TCS → Multicast

TCS (S1-S2) Call Flow (Content Server calls Site A)

TCS outgoing[2]	Protocol	Type	Site B incoming
3230	Q.931	TCP	1720
3231:3235	H.245	TCP	5555:5565
3230	Media (Audio)	UDP/RTP	2326
3231	Media (Audio)	UDP/RTCP	2327
3232	Media (Video)	UDP/RTP	2328
3233	Media (Video)	UDP/RTCP	2329
3234	Media (Dual Streams)	UDP/RTP	2330
3235	Media (Dual Streams)	UDP/RTCP	2331

When fixed ports are enabled, the TANDBERG Content Server with the S1 and S2 versions of software uses a pool of 6 TCP ports (3230:3235) for all H.225/Q.931 and H.245 messages. The ports will increment every time a new logical connection is required on Q.931 or H.245. When the port number reaches 3235, the port number will reset and begin using 3230 again.

The TANDBERG Content Server uses a pool of 30 UDP ports (3230:3259) for all media connections (both RTP and RTCP). The ports are divided up in increments of 6 for each of the specific lines on the Content Server. For example, Line 1 on the content server will occupy the first 6 ports in the range (e.g. 3230-3235), Line 2 will then occupy the next 6 (e.g. 3236-3241) and so on.

Similar to the MXP endpoints running F2 or later, the TANDBERG Content Server uses bi-directional UDP ports, so the number of ports required is reduced in comparison to older versions of the TANDBERG endpoints software.

Note: If fixed ports are disabled, the Content Server will use a random allocation of both TCP and UDP ports for the H.323 calls.

[2] Fixed ports are not enabled on the Content Server by default. When this is not enabled, the Content Server will used a random range of ports for both TCP and UDP connections.

TCS (S3-S4) Call Flow (Content Server calls Site A)

TCS outgoing[3]	Protocol	Type	Site B incoming
3230	Q.931	TCP	1720
3231:3239	H.245	TCP	5555:5565
3230	Media (Audio)	UDP/RTP	2326
3231	Media (Audio)	UDP/RTCP	2327
3232	Media (Video)	UDP/RTP	2328
3233	Media (Video)	UDP/RTCP	2329
3234	Media (Dual Streams)	UDP/RTP	2330
3235	Media (Dual Streams)	UDP/RTCP	2331
3236	Media (FECC)	UDP/RTP	2332
3237	Media (FECC)	UDP/RTCP	2333

As of S3 and later software, the TCS has modified the port allocation behavior on both the TCP and UDP connections. Beginning with S3, a TCP pool of 10 ports (3230:3239) is now used for the H.225/Q.931 and H.245 messages. The UDP pool has also increased to a total of 40 ports (3230:3269) as 8 total ports are allocated for each of the 5 possible calls.

The ports are allocated upon call connection. For example, the first call to connect to the Content Server will allocate the first two TCP ports for the H.225/Q.931 and H.245 connections (e.g. 3230 and 3231) and the first eight ports within the UDP pool for the media connections (e.g. 3230 – 3237). The second call will then occupy the next two TCP ports (e.g. 3232 and 3233) and the next eight UDP ports (e.g. 3238 – 3245) and so on.

Similar to the MXP endpoints running F2 or later, the TANDBERG Content Server uses bi-directional UDP ports, so the number of ports required is reduced in comparison to older versions of the TANDBERG endpoints software.

Note: If fixed ports are disabled, the Content Server will use a random allocation of both TCP and UDP ports for the H.323 calls.

[3] Fixed ports are not enabled on the Content Server by default. When this is not enabled, the Content Server will used a random range of ports for both TCP and UDP connections.

TCS (S1-S2) Audio

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.711	60ms	480 bytes	20 bytes	8 bytes	12 bytes	520 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	60ms	480 bytes	20 bytes	8 bytes	12 bytes	520 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_24	60ms	180 bytes	20 bytes	8 bytes	12 bytes	280 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.722.1_32	60ms	240 bytes	20 bytes	8 bytes	12 bytes	280 bytes

TCS (S3-S4) Audio

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.722	20ms	160 bytes	20 bytes	8 bytes	12 bytes	200 bytes
G.722.1_24	20ms	60 bytes	20 bytes	8 bytes	12 bytes	100 bytes
G.722.1_32	20ms	80 bytes	20 bytes	8 bytes	12 bytes	120 bytes
AAC-LD_64	20ms	160 bytes	20 bytes	8 bytes	12 bytes	200 bytes

TCS (S1-S2) Video

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

TCS (S3-S4) Video

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

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. However, since the Content Server serves primarily as a streaming and archiving device, latency does not have a detrimental effect on the quality of either the archived or streamed content.

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. The TANDBERG Content Server implements a dynamic jitter buffer that will automatically vary between 250ms and 750ms in order to adjust properly to the incoming video stream. Any packets not received within this timeframe will be considered lost packets.

TANDBERG Codian 2200 Series IPVCR

The TANDBERG Codian 3500 Series of IP video conference recorders are stand alone appliances supporting up to 10 recording ports and 20 playback ports per chassis. Multiple chassis can be combined throughout the network, either in a distributed or centralized architecture if an increase in capacity is required.

IPVCR Layer 4 Miscellaneous Ports

The Codian 2200 has a central data store that can be accessed by several methods.

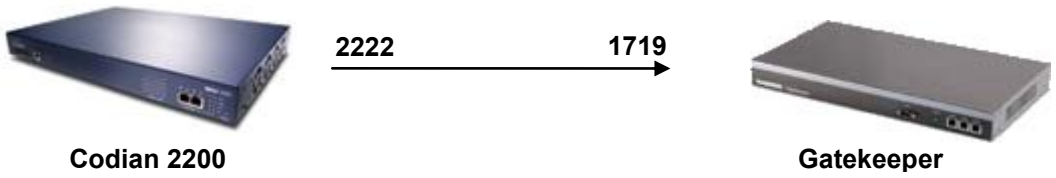
- ***FTP:*** File transfer.
- ***HTTP:*** System management and setup.
- ***SNMP:*** Provides SNMP support for TMS and other SNMP Management Applications.

Note: The Codian products allocate random ports in the range of 49152 to 65535. It is possible to change the fixed ports on which the Codian products receive and establish connections under the „Network" > „Services" portion of the management interface.

Function	Port	Type	Direction
FTP	21*	TCP	Host → 2200
HTTP	80*	TCP	Host → 2200
SNMP (Queries)	161*	UDP	Host → 2200
SNMP (Traps)	162	UDP	2200 → Host
RTSP	554	TCP	2200 → Host
Windows Media Streaming	1755	TCP	2200 → Host
FTP/data	Random/Dynamic	TCP	Host → 2200

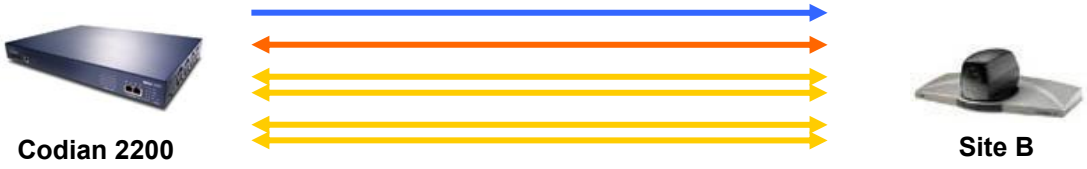
* denotes a listening port. ↔ (bi-directional)

IPVCR Gatekeeper Interaction



Function	Port	Type	Direction
Gatekeeper RAS	1719	UDP	2200 → GK

IPVCR Call Flow



2200 Outgoing	Protocol	Type	Site B incoming
49152:65535	Q.931	TCP	1720
49152:65535	H.245	TCP	Endpt Defined
49152:65535	Media (Video)	UDP/RTP	Endpt Defined
49152:65535	Media (Video)	UDP/RTCP	Endpt Defined
49152:65535	Media (Dual Streams)	UDP/RTP	Endpt Defined
49152:65535	Media (Dual Streams)	UDP/RTCP	Endpt Defined
49152:65535	Media (Audio)	UDP/RTP	Endpt Defined
49152:65535	Media (Audio)	UDP/RTCP	Endpt Defined

For all outbound and inbound H.323 connections (except the inbound Q.931 connection which uses port 1720 TCP), the Codian 2200 will use a random port within the range of 49152 to 65535. Because the same port range is shared by multiple services (i.e. FTP data, H.323 media/call signaling/control and SIP media/call signaling/control), ports are allocated at the time they are needed for each particular service; ports used for logical channels are only allocated when necessary. Logical channels and signaling channels are opened up at different times of an H.323 call; ports may or may not be consecutive within a single call. For example, a standard H.323 call (i.e. audio and video only) may occupy ports 49172/49173 TCP and 49166/49167 and 49160/49161 UDP due to the number of connections that are opened up around the same time. All random ports are allocated from the top of range down, beginning with the ports in the 65xxx grouping.

IPVCR Audio

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.722	20ms	160 bytes	20 bytes	8 bytes	12 bytes	200 bytes
G.723.1	30ms	48 bytes	20 bytes	8 bytes	12 bytes	88 bytes
G.729	20ms	20 bytes	20 bytes	8 bytes	12 bytes	60 bytes
AAC-LC_48	20ms	180 bytes	20 bytes	8 bytes	12 bytes	220 bytes
AAC-LC_56	20ms	210 bytes	20 bytes	8 bytes	12 bytes	250 bytes
AAC-LC_64	20ms	240 bytes	20 bytes	8 bytes	12 bytes	280 bytes
AAC-LC_96	20ms	400 bytes	20 bytes	8 bytes	12 bytes	440 bytes
AAC-LD_48	20ms	120 bytes	20 bytes	8 bytes	12 bytes	160 bytes
AAC-LD_56	20ms	140 bytes	20 bytes	8 bytes	12 bytes	180 bytes
AAC-LD_64	20ms	160 bytes	20 bytes	8 bytes	12 bytes	200 bytes
AAC-LD_96	20ms	240 bytes	20 bytes	8 bytes	12 bytes	280 bytes
Siren14	20ms	120 bytes	20 bytes	8 bytes	12 bytes	160 bytes
G.722.1 Annex C	20ms	120 bytes	20 bytes	8 bytes	12 bytes	160 bytes

IPVCR Video

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

* with 2.2(1.0) software, the maximum mtu used for video payload can be adjusted between 400 and 1400 bytes through the web interface control under „Settings" > „Conferences" > „Maximum transmitted video packet size."

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. The TANDBERG Codian 2200 IPVCR incorporates variable, independent jitter buffers for the audio and video streams of the call. The audio stream has a dynamic jitter buffer of 40ms up to and including 240ms, while the dynamic jitter buffer for the video stream begins at 30ms and can increase when deemed necessary by an increase in jitter for the active H.323 call. The maximum size of the jitter buffer is determined by the bandwidth of the call in question; for a call connected at 384kbps, the jitter buffer can equate to a full 2 seconds, while a 2Mbps call will equate to a jitter buffer of approximately 350ms.

The Codian 2200 IPVCR utilizes RTP time stamping between the audio and video streams to ensure they remain synchronized throughout the call.

TANDBERG Gatekeeper

The TANDBERG Gatekeeper is a high-performance, reliable, secure, and easy-to-use gatekeeper designed to complement TANDBERG's infrastructure solutions.

Gatekeeper Layer 4 Miscellaneous Ports

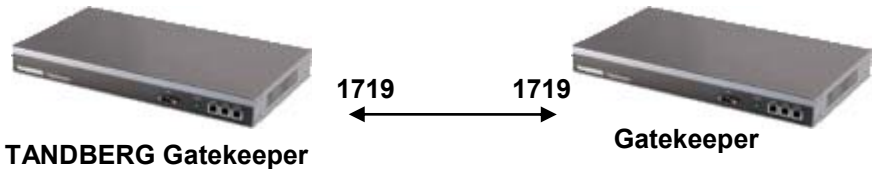
The TANDBERG Gatekeeper has a central data store that can be accessed by several methods.

- ***HTTP:*** System management and setup.
- ***HTTPS:*** Secure system management and setup.
- ***Telnet:*** Provides access to the API based upon the XML engine for control, setup and status monitoring.
- ***Secure Shell (SSH):*** Secure access to the API based upon the XML engine.
- ***SNMP:*** Provides SNMP support for TMS and other SNMP Management Applications.
- ***XML:*** Provides full control, setup and status monitoring ability. Can also be used with HTTPS for secure control, setup and status monitoring.
- ***Remote Syslog Server:*** Provides for a means of remote logging of gatekeeper actions, including administrative changes and RAS call routing.

Function	Port	Type	Direction
SSH	22*	TCP*	Host → GK
Telnet	23*	TCP*	Host → GK
HTTP / XML	80*	TCP*	Host → GK
NTP	123*	UDP	GK → NTP Server
SNMP (Queries)	161*	UDP*	Host → GK
HTTPS / XML	443*	TCP*	Host → GK
Remote Syslog Server	514	UDP	GK → Syslog Server

* denotes listening port.

Gatekeeper-to-Gatekeeper Neighbor Interaction



Function	Port	Type	Direction
Gatekeeper RAS	1719	UDP	GK ↔ GK

Gatekeeper Messaging

Registration Messages

Message	Description	Purpose
GRQ	Gatekeeper Request	Used for auto-discovery of a gatekeeper as well as gatekeeper authentication confirmation upon registration. Message can be sent to either the 224.0.1.41:1718 UDP multicast address or to the specific IP address of the Gatekeeper via a UDP unicast message.
GCF	Gatekeeper Confirm	Response by gatekeeper when GRQ is accepted. Typically includes GK IP address and RAS port (1719 UDP).
GRJ	Gatekeeper Reject	Response by gatekeeper when a GRQ is rejected. Typically includes GK IP address, terminal IP address and reject reason.
LWRRQ	Lightweight Registration Request	Sent from terminal to GK when TTL is about to expire. Used to refresh the registration of a terminal.
RRQ	Registration Request	Used by an endpoint, MCU or gateway to request a registration to the gatekeeper. Typically contains the endpoint IP address, RAS port (1719 UDP), Q.931 port (1720 TCP), H323-ID, E.164 and type of terminal (endpoint, MCU, gateway).
RCF	Registration Confirm	Response by gatekeeper when a RRQ is accepted. Typically includes GK identifier, endpoint identifier, terminal IP address, E.164, H.323-ID, RAS port, Q.931 port, TTL for registration expiration and an endpoint identifier used for all future RAS communication.
RRJ	Registration Reject	Response by gatekeeper when a RRQ is rejected. Typically includes GK IP address, terminal IP address and reject reason.
URQ	Unregistration Request	Used by an endpoint requesting to be unregistered from the gatekeeper. It is possible for the GK to send URQ as well. Calls will be accepted until registration expires
UCF	Unregistration Confirm	Response by gatekeeper when URQ is accepted.
URJ	Unregistration Reject	Response by gatekeeper when URQ is rejected. Typically includes GK IP address, terminal IP address and reject reason.

Placing and Receiving a Call Messages

Message	Description	Purpose
ARQ	Admission Request	Used by an endpoint to request permission to make or receive a call. Typically contains endpoint identifier, direction of call, bandwidth of call, far end system info (IP address, E.164, etc).
ACF	Admission Confirm	Response by gatekeeper when ARQ is accepted. Typically includes call identifier and bandwidth allowed for the call (**Note:** this can be different than the bandwidth specified in ARQ).
ARJ	Admission Reject	Response by gatekeeper when ARQ is rejected. Typically includes endpoint identifier, GK identifier and reject reason.
LRQ	Location Request	Used by a gatekeeper to query a neighboring gatekeeper as to the location of an endpoint. This message is only sent if the called system is not registered to that gatekeeper. Typically contains originating GK IP address, RAS port (1719 UDP), and called system's E.164 or H.323-ID.
LCF	Location Confirm	Response by gatekeeper that can process the call or knows where the terminal resides. Typically includes called systems IP address and Q.931 port.
LRJ	Location Reject	Response by gatekeeper when LRQ is rejected. Typically includes source gatekeeper address, destination gatekeeper address and reject reason. A possible reason for LRJ could be "called party not registered".
BRQ	Bandwidth Request	Used by a terminal to request to change the bandwidth of an ongoing call, either increasing or decreasing the bandwidth.
BCF	Bandwidth Confirm	Response by gatekeeper when BRQ is accepted. Typically includes call identifier and bandwidth allowed for call.
BRJ	Bandwidth Reject	Used by gatekeeper when BRQ is rejected. Typically includes call identifier and reject reason. A possible reason for BRJ could be the maximum bandwidths defined by the gatekeeper have been or will be exceeded by the BRQ.
DRQ	Disengage Request	Used by either a terminal or gatekeeper requesting the disconnection of an ongoing call. Typically includes endpoint identifier, call identifier and reason for disconnection.
DCF	Disengage Confirm	Used by either a terminal or gatekeeper when DRQ is accepted.
DRJ	Disengage Reject	Used by either a terminal or gatekeeper when DRQ is rejected.
IRQ	Information Request	Used by gatekeeper to request call status from a terminal. Typically terminal responds with "in call", "not in call", "available" or "unavailable."
IRR	Information Response	Used by a terminal to respond to the gatekeeper IRQ. Typically terminal responds with "in call", "not in call", "available" or "unavailable."
RIP	Request in Progress	Used by gatekeeper to indicate to a terminal that the previous request is being processed and a response is coming.
RAI	Resource Available Indicator	Used by a terminal to indicate to the gatekeeper whether or not the terminal has sufficient resources. Typical messages include "available" or "unavailable."
SCI	Service Control Indication	Used in H.460.18 by the traversal server to signal an incoming call to the H.460.18 client.

TANDBERG Gatekeeper Routed Mode

Software version N5.0 supports the ability to route all call control through the gatekeeper to provide advanced services, such as call detail records. Call routing provides administrators the ability to gather accurate Call Detail Records (CDR) and consistent call routing. Additionally, advanced services such as Multiway and H.343 call transfer functionality are available when the call signaling is routed through the gatekeeper.

EndptA	Gatekeeper	Protocol	Type	Gatekeeper	EndptB
Endpt Defined	1719	RAS	UDP	1719	Endpt Defined
Endpt Defined	15000:16800	Q.931	TCP	15000:16800	1720
Endpt Defined	19000:20800	H.245	TCP	19000:20800	Endpt Defined
Endpt Defined	N/A	Media (Audio)	UDP/RTP	N/A	Endpt Defined
Endpt Defined	N/A	Media (Audio)	UDP/RTCP	N/A	Endpt Defined
Endpt Defined	N/A	Media (Video)	UDP/RTP	N/A	Endpt Defined
Endpt Defined	N/A	Media (Video)	UDP/RTCP	N/A	Endpt Defined
Endpt Defined	N/A	Media (Dual Streams)	UDP/RTP	N/A	Endpt Defined
Endpt Defined	N/A	Media (Dual Streams)	UDP/RTCP	N/A	Endpt Defined
Endpt Defined	N/A	Media (FECC)	UDP/RTP	N/A	Endpt Defined
Endpt Defined	N/A	Media (FECC)	UDP/RTCP	N/A	Endpt Defined

Beginning with software version N2, the TANDBERG Gatekeeper uses a TCP port range from 15000:16800 for H.225/Q.931[4] and 19000:20800 for H.245. The ports will increment every time a new logical connection is required on H.225/Q.931 or H.245. When the port number reaches the top of the range, the port number will begin again from the start of the range.

Because the gatekeeper only routes the control traffic between the endpoints, it does not involve itself at all with the media. As such, no media ports are allocated by the gatekeeper to this particular call.

[4] Note: Incoming calls from systems not registered directly or through a proxy server will connect on port 1720 TCP for all H.225/Q.931 signaling.

TANDBERG Border Controller

The TANDBERG Border Controller provides Firewall Traversal and Simplified Dialing services for all H.323 devices enabling visual communication with partners, vendors, supply chains and remote workers.

Border Controller Layer 4 Miscellaneous Ports

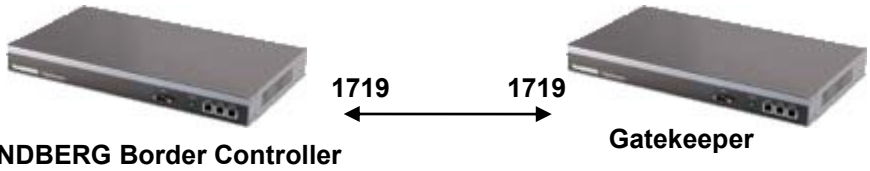
The TANDBERG Border Controller has a central data store that can be accessed by several methods.

- ***HTTP:*** System management and setup.
- ***HTTPS:*** Secure system management and setup.
- ***Telnet:*** Provides access to the API based upon the XML engine for control, setup and status monitoring.
- ***Secure Shell (SSH):*** Secure access to the API based upon the XML engine.
- ***SNMP:*** Provides SNMP support for TMS and other SNMP Management Applications.
- ***XML:*** Provides full control, setup and status monitoring ability. Can also be used with HTTPS for secure control, setup and status monitoring.
- ***Remote Syslog Server:*** Provides for a means of remote logging of gatekeeper actions, including administrative changes and RAS call routing.

Function	Port	Type	Direction
SSH	22*	TCP*	Host → BC
Telnet	23*	TCP*	Host → BC
HTTP / XML	80*	TCP*	Host → BC
NTP	123*	UDP	BC → NTP Server
SNMP (Queries)	161*	UDP*	Host → BC
HTTPS / XML	443*	TCP*	Host → BC
Remote Syslog Server	514	UDP	BC → Syslog Server

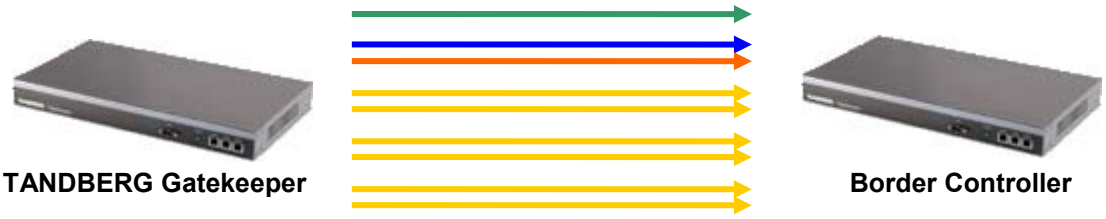
* denotes listening port.

TANDBERG Border Controller-to-Gatekeeper Neighbor Interaction



Border Controller	Protocol	Type	Gatekeeper
1719	Gatekeeper RAS	UDP	1719

TANDBERG Gatekeeper-to-TANDBERG Border Controller Traversal Interaction[5]



Gatekeeper	Protocol	Type	Border Controller
Gatekeeper Defined	Gatekeeper RAS	UDP	1719
Gatekeeper Defined	Q.931	TCP	2776
Gatekeeper Defined	H.245	TCP	2776
Gatekeeper Defined	Media (Audio)	UDP/RTP	2776
Gatekeeper Defined	Media (Audio)	UDP/RTCP	2777
Gatekeeper Defined	Media (Video)	UDP/RTP	2776
Gatekeeper Defined	Media (Video)	UDP/RTCP	2777
Gatekeeper Defined	Media (Dual Streams)	UDP/RTP	2776
Gatekeeper Defined	Media (Dual Streams)	UDP/RTCP	2777
Gatekeeper Defined	Media (FECC)	UDP/RTP	2776
Gatekeeper Defined	Media (FECC)	UDP/RTCP	2777

[5] Any traversal link established between a TANDBERG Traversal Client (e.g. TANDBERG MXP, TANDBERG Gatekeeper) will use the TANDBERG proprietary traversal technology, not H.460.18/.19

Gatekeeper Messaging

While the primary purpose of the Border Controller is to aid in firewall traversal with the registered Traversal Clients, it also does serve as the local Gatekeeper to those registered clients.

Registration Messages

Message	Description	Purpose
GRQ	Gatekeeper Request	Used for auto-discovery of a gatekeeper as well as gatekeeper authentication confirmation upon registration. Message can be sent to either the 224.0.1.41:1718 UDP multicast address or to the specific IP address of the Gatekeeper via a UDP unicast message.
GCF	Gatekeeper Confirm	Response by gatekeeper when GRQ is accepted. Typically includes GK IP address and RAS port (1719 UDP).
GRJ	Gatekeeper Reject	Response by gatekeeper when a GRQ is rejected. Typically includes GK IP address, terminal IP address and reject reason.
LWRRQ	Lightweight Registration Request	Sent from terminal to GK when TTL is about to expire. Used to refresh the registration of a terminal.
RRQ	Registration Request	Used by an endpoint, MCU or gateway to request a registration to the gatekeeper. Typically contains the endpoint IP address, RAS port (1719 UDP), Q.931 port (1720 TCP), H323-ID, E.164 and type of terminal (endpoint, MCU, gateway).
RCF	Registration Confirm	Response by gatekeeper when a RRQ is accepted. Typically includes GK identifier, endpoint identifier, terminal IP address, E.164, H.323-ID, RAS port, Q.931 port, TTL for registration expiration and an endpoint identifier used for all future RAS communication.
RRJ	Registration Reject	Response by gatekeeper when a RRQ is rejected. Typically includes GK IP address, terminal IP address and reject reason.
URQ	Unregistration Request	Used by an endpoint requesting to be unregistered from the gatekeeper. It is possible for the GK to send URQ as well. Calls will be accepted until registration expires
UCF	Unregistration Confirm	Response by gatekeeper when URQ is accepted.
URJ	Unregistration Reject	Response by gatekeeper when URQ is rejected. Typically includes GK IP address, terminal IP address and reject reason.

Placing and Receiving a Call Messages

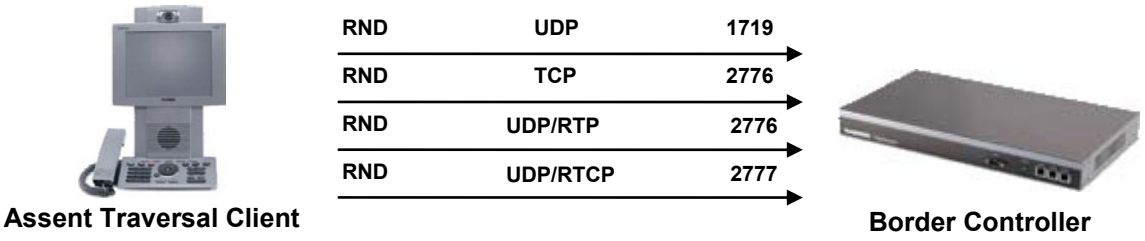
Message	Description	Purpose
ARQ	Admission Request	Used by an endpoint to request permission to make or receive a call. Typically contains endpoint identifier, direction of call, bandwidth of call, far end system info (IP address, E.164, etc).
ACF	Admission Confirm	Response by gatekeeper when ARQ is accepted. Typically includes call identifier and bandwidth allowed for the call (**Note:** this can be different than the bandwidth specified in ARQ).
ARJ	Admission Reject	Response by gatekeeper when ARQ is rejected. Typically includes endpoint identifier, GK identifier and reject reason.
LRQ	Location Request	Used by a gatekeeper to query a neighboring gatekeeper as to the location of an endpoint. This message is only sent if the called system is not registered to that gatekeeper. Typically contains originating GK IP address, RAS port (1719 UDP), and called system's E.164 or H.323-ID.
LCF	Location Confirm	Response by gatekeeper that can process the call or knows where the terminal resides. Typically includes called systems IP address and Q.931 port.
LRJ	Location Reject	Response by gatekeeper when LRQ is rejected. Typically includes source gatekeeper address, destination gatekeeper address and reject reason. A possible reason for LRJ could be "called party not registered".
BRQ	Bandwidth Request	Used by a terminal to request to change the bandwidth of an ongoing call, either increasing or decreasing the bandwidth.
BCF	Bandwidth Confirm	Response by gatekeeper when BRQ is accepted. Typically includes call identifier and bandwidth allowed for call.
BRJ	Bandwidth Reject	Used by gatekeeper when BRQ is rejected. Typically includes call identifier and reject reason. A possible reason for BRJ could be the maximum bandwidths defined by the gatekeeper have been or will be exceeded by the BRQ.
DRQ	Disengage Request	Used by either a terminal or gatekeeper requesting the disconnection of an ongoing call. Typically includes endpoint identifier, call identifier and reason for disconnection.
DCF	Disengage Confirm	Used by either a terminal or gatekeeper when DRQ is accepted.
DRJ	Disengage Reject	Used by either a terminal or gatekeeper when DRQ is rejected.
IRQ	Information Request	Used by gatekeeper to request call status from a terminal. Typically terminal responds with "in call", "not in call", "available" or "unavailable."
IRR	Information Response	Used by a terminal to respond to the gatekeeper IRQ. Typically terminal responds with "in call", "not in call", "available" or "unavailable."
RIP	Request in Progress	Used by gatekeeper to indicate to a terminal that the previous request is being processed and a response is coming.
RAI	Resource Available Indicator	Used by a terminal to indicate to the gatekeeper whether or not the terminal has sufficient resources. Typical messages include "available" or "unavailable."
SCI	Service Control Indication	Used in H.460.18 by the traversal server to signal an incoming call to the H.460.18 client.

Traversal Client-to-Border Controller Interaction

The TANDBERG Border Controller supports multiple versions of traversal technology: both Assent and H.460.18/.19. The standards-based H.460.18/.19 traversal technology is highly based off of the Assent technology, originally released by TANDBERG in January 2005. This section of the document will discuss how the Border Controller interacts with clients of both forms of technology, regardless of whether the client is embedded within an endpoint or through a traversal proxy (e.g. the TANDBERG Gatekeeper).

Assent Client-to-Border Controller Interaction

The Assent traversal client is embedded both in the TANDBERG MXP endpoints (beginning with software version F2.0 and L2.0). This technology works based on establishing outbound connections from the client to the server (the Border Controller) to ensure a secure connection between the client and the Border Controller while enabling video communications through the firewall.

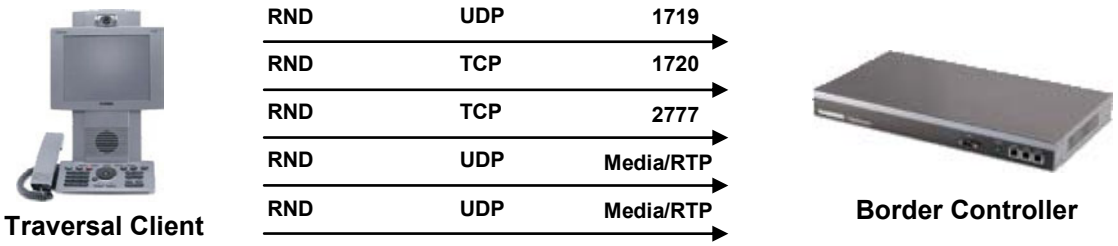


Function	*Port*	*Type*	*Direction*
Gatekeeper RAS	1719	UDP	Client → BC
H.225 Call Signaling	2776	TCP	Client → BC
H.245	2776	TCP	Client → BC
RTP Media	2776	UDP	Client → BC
RTP Media	2777	UDP	Client → BC

H.460.18/.19 Client-to-Border Controller Interaction[6]

Beginning with software version Q2.2, the TANDBERG Border Controller supported H.460.18/.19 standards-based firewall traversal. Very similar to the TANDBERG Assent technology, H.460.18/.19 works based on establishing outbound connections from the client to the server (the Border Controller) to ensure a secure connection between the client and the Border Controller while enabling video communications through the firewall.

H.460.18 governs the traversal of all call setup for an H.323 call, while H.460.19 controls the traversal of the media within the call. Optional within the H.460.19 standard is multiplexed media, a process by which the media connections between the client and the traversal server can be reduced down to a minimum number of ports – in the TANDBERG solution, multiplexed media narrows all connections down to 2776 and 2777.



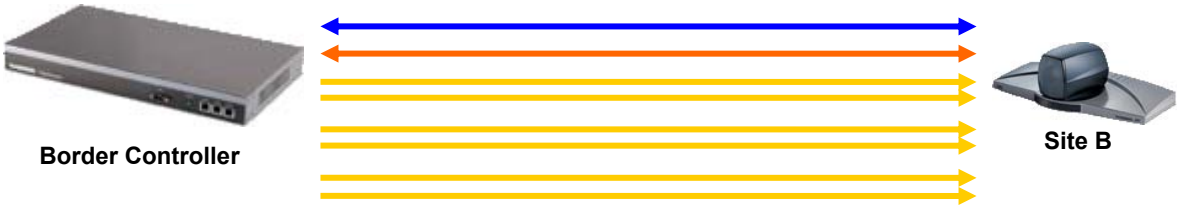
Function	Port	Type	Direction
Gatekeeper RAS	1719	UDP	Client → BC
H.225 Call Signaling	1720	TCP	Client → BC
H.245	2777	TCP	Client → BC
RTP Media	50000-52400	UDP	Client → BC
RTP Media	50000-52400	UDP	Client → BC
RTP Media (Multiplexed)	2776	UDP	Client → BC
RTCP Media (Multiplexed)	2777	UDP	Client → BC

[6] H.460.18/.19 traversal communication was first implemented in Q2.2 in the TANDBERG Border Controller)

Border Controller Unregistered System Interaction

When connecting to an unregistered system (e.g. an endpoint on a public IP address), the Border Controller will use a random association of ports within a specified range in order to complete the call. A reduced number of ports like those seen in either an Assent or H.460.18/.19 connection cannot be used for connecting to unregistered endpoints as the call must emulate a normal point-to-point H.323 call to be successful.

The below diagram and port chart discusses the ports the Border Controller will use when connecting to a public endpoint that is either not registered directly to the Border Controller or through a traversal proxy.



BC outgoing	Protocol	Type	Site B incoming
15000:16800	Q.931	TCP	1720
19000:20800	H.245	TCP	Endpoint Defined
50000	Media (Audio)	UDP/RTP	Endpoint Defined
50001	Media (Audio)	UDP/RTCP	Endpoint Defined
50002	Media (Video)	UDP/RTP	Endpoint Defined
50003	Media (Video)	UDP/RTCP	Endpoint Defined
50004	Media (Dual Streams)	UDP/RTP	Endpoint Defined
50005	Media (Dual Streams)	UDP/RTCP	Endpoint Defined
50006	Media (FECC)	UDP/RTP	Endpoint Defined
50007	Media (FECC)	UDP/RTCP	Endpoint Defined

Beginning with software version Q1, the TANDBERG Border uses a TCP port range from 15000:16800 for H.225/Q.931[7] and 19000:20800 for H.245. The ports will increment every time a new logical connection is required on H.225/Q.931 or H.245. When the port number reaches the top of the range, the port number will begin again from the start of the range.

All TANDBERG Border Controller software uses a pool of 2401 UDP ports (50000:52400) for all media (both RTP and RTCP). The ports are used in increments of 8 per call (e.g. the first call will use ports 50000-50007). After the first call is connected, the Border Controller will use the next consecutive 8 ports for the subsequent call and so on until all calls are disconnected. Once all calls are disconnected, the ports will reset to the beginning.

[7] Note: Incoming calls from systems not registered directly or through a proxy server will connect on port 1720 TCP for all H.225/Q.931 signaling.

TANDBERG Video Communication Server

The TANDBERG Video Communication Server (VCS) bridges the gap between SIP and H.323 and delivers three unique applications in one centralized device. It features innovative video call forwarding capabilities through TANDBERG FindMe™ and extends SIP support to network administration and firewall traversal.

VCS Layer 4 Miscellaneous Ports

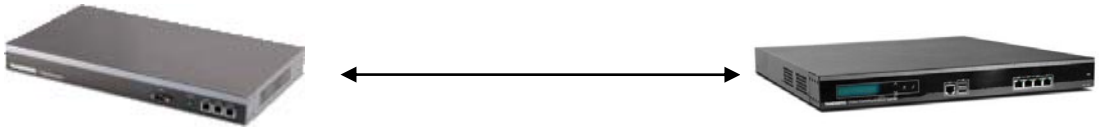
The TANDBERG VCS has a central data store that can be accessed by several methods.

- ***HTTP:*** System management and setup. For security reasons, HTTP cannot be used alone to manage the VCS, but only as a re-direct to HTTPS. If the HTTPS management of the system is disabled, HTTP will also be disabled.
- ***HTTPS:*** Secure system management and setup.
- ***Telnet:*** Provides access to the API based upon the XML engine for control, setup and status monitoring.
- ***Secure Shell (SSH):*** Secure access to the API based upon the XML engine.
- ***SNMP:*** Provides SNMP support for TMS and other SNMP Management Applications.
- ***XML:*** Provides full control, setup and status monitoring ability. Can also be used with HTTPS for secure control, setup and status monitoring.
- ***Remote Syslog Server:*** Provides for a means of remote logging of gatekeeper actions, including administrative changes and RAS call routing.

Function	Port	Type	Direction
SSH	22*	TCP*	Host → VCS
Telnet	23*	TCP*	Host → VCS
HTTP / XML	80*	TCP*	Host → VCS
NTP	123*	UDP	VCS → NTP Server
SNMP (Queries)	161*	UDP*	Host → VCS
HTTPS / XML	443*	TCP*	Host → VCS
Remote Syslog Server	514	UDP	VCS → Syslog Server

* denotes listening port.

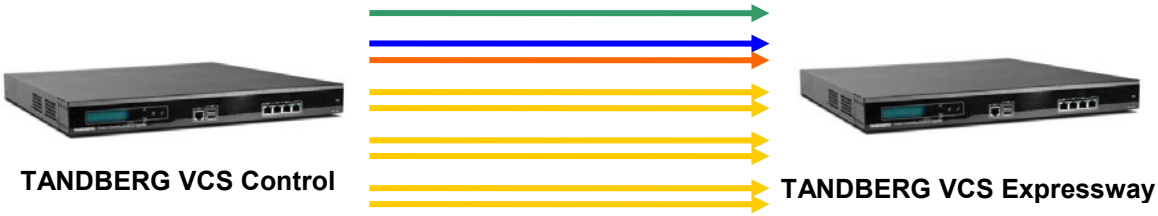
VCS Neighbor Gatekeeper Interaction



Gatekeeper **TANDBERG VCS**

Gatekeeper	Protocol	Type	Border Controller
1719	Gatekeeper RAS	UDP	1719

VCS Control-to-VCS Expressway Traversal Interaction



VCS Control	Protocol	Type	VCS Expressway
1719	Gatekeeper RAS	UDP	6001
15000:19999	Q.931	TCP	2776
15000:19999	H.245	TCP	2776
50000:52399	Media (Audio)	UDP/RTP	2776
50000:52399	Media (Audio)	UDP/RTCP	2777
50000:52399	Media (Video)	UDP/RTP	2776
50000:52399	Media (Video)	UDP/RTCP	2777
50000:52399	Media (Dual Streams)	UDP/RTP	2776
50000:52399	Media (Dual Streams)	UDP/RTCP	2777
50000:52399	Media (FECC)	UDP/RTP	2776
50000:52399	Media (FECC)	UDP/RTCP	2777

Note: all ports illustrated in the above example can be administratively configured.

To increase the security of the traversal connection, the RAS connection between the traversal proxy (e.g. TANDBERG VCS Control) will now require the manual configuration of the port used for connectivity in addition to the previous methods used for authentication. This change in the functionality does not increase the ports required for a traversal connection through a firewall, but does modify the requirements. Instead of using port 1719 UDP, as previously in the TANDBERG Border Controller, a user-configurable port is now used for the RAS traffic.

Gatekeeper Messaging

The TANDBERG VCS serves as both an H.323 gatekeeper and SIP proxy in addition to providing traversal client and server capabilities. As an H.323 gatekeeper, it provides all of the same functionality as the TANDBERG Gatekeeper, including the messaging listed within the below tables.

Registration Messages

Message	*Description*	*Purpose*
GRQ	Gatekeeper Request	Used for auto-discovery of a gatekeeper as well as gatekeeper authentication confirmation upon registration. Message can be sent to either the 224.0.1.41:1718 UDP multicast address or to the specific IP address of the Gatekeeper via a UDP unicast message.
GCF	Gatekeeper Confirm	Response by gatekeeper when GRQ is accepted. Typically includes GK IP address and RAS port (1719 UDP).
GRJ	Gatekeeper Reject	Response by gatekeeper when a GRQ is rejected. Typically includes GK IP address, terminal IP address and reject reason.
LWRRQ	Lightweight Registration Request	Sent from terminal to GK when TTL is about to expire. Used to refresh the registration of a terminal.
RRQ	Registration Request	Used by an endpoint, MCU or gateway to request a registration to the gatekeeper. Typically contains the endpoint IP address, RAS port (1719 UDP), Q.931 port (1720 TCP), H323-ID, E.164 and type of terminal (endpoint, MCU, gateway).
RCF	Registration Confirm	Response by gatekeeper when a RRQ is accepted. Typically includes GK identifier, endpoint identifier, terminal IP address, E.164, H.323-ID, RAS port, Q.931 port, TTL for registration expiration and an endpoint identifier used for all future RAS communication.
RRJ	Registration Reject	Response by gatekeeper when a RRQ is rejected. Typically includes GK IP address, terminal IP address and reject reason.
URQ	Unregistration Request	Used by an endpoint requesting to be unregistered from the gatekeeper. It is possible for the GK to send URQ as well. Calls will be accepted until registration expires
UCF	Unregistration Confirm	Response by gatekeeper when URQ is accepted.
URJ	Unregistration Reject	Response by gatekeeper when URQ is rejected. Typically includes GK IP address, terminal IP address and reject reason.

Placing and Receiving a Call Messages

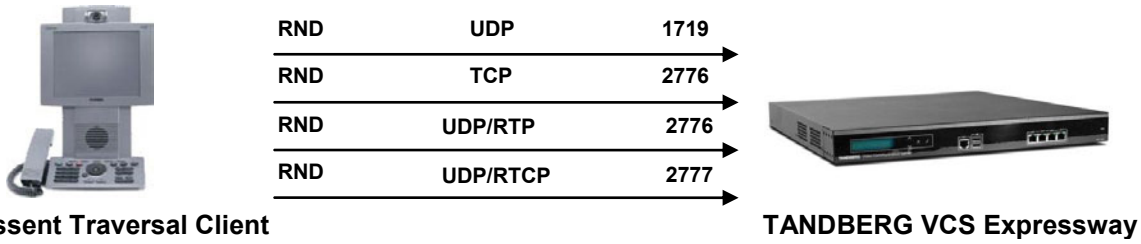
Message	Description	Purpose
ARQ	Admission Request	Used by an endpoint to request permission to make or receive a call. Typically contains endpoint identifier, direction of call, bandwidth of call, far end system info (IP address, E.164, etc).
ACF	Admission Confirm	Response by gatekeeper when ARQ is accepted. Typically includes call identifier and bandwidth allowed for the call (**Note:** this can be different than the bandwidth specified in ARQ).
ARJ	Admission Reject	Response by gatekeeper when ARQ is rejected. Typically includes endpoint identifier, GK identifier and reject reason.
LRQ	Location Request	Used by a gatekeeper to query a neighboring gatekeeper as to the location of an endpoint. This message is only sent if the called system is not registered to that gatekeeper. Typically contains originating GK IP address, RAS port (1719 UDP), and called system's E.164 or H.323-ID.
LCF	Location Confirm	Response by gatekeeper that can process the call or knows where the terminal resides. Typically includes called systems IP address and Q.931 port.
LRJ	Location Reject	Response by gatekeeper when LRQ is rejected. Typically includes source gatekeeper address, destination gatekeeper address and reject reason. A possible reason for LRJ could be "called party not registered".
BRQ	Bandwidth Request	Used by a terminal to request to change the bandwidth of an ongoing call, either increasing or decreasing the bandwidth.
BCF	Bandwidth Confirm	Response by gatekeeper when BRQ is accepted. Typically includes call identifier and bandwidth allowed for call.
BRJ	Bandwidth Reject	Used by gatekeeper when BRQ is rejected. Typically includes call identifier and reject reason. A possible reason for BRJ could be the maximum bandwidths defined by the gatekeeper have been or will be exceeded by the BRQ.
DRQ	Disengage Request	Used by either a terminal or gatekeeper requesting the disconnection of an ongoing call. Typically includes endpoint identifier, call identifier and reason for disconnection.
DCF	Disengage Confirm	Used by either a terminal or gatekeeper when DRQ is accepted.
DRJ	Disengage Reject	Used by either a terminal or gatekeeper when DRQ is rejected.
IRQ	Information Request	Used by gatekeeper to request call status from a terminal. Typically terminal responds with "in call", "not in call", "available" or "unavailable."
IRR	Information Response	Used by a terminal to respond to the gatekeeper IRQ. Typically terminal responds with "in call", "not in call", "available" or "unavailable."
RIP	Request in Progress	Used by gatekeeper to indicate to a terminal that the previous request is being processed and a response is coming.
RAI	Resource Available Indicator	Used by a terminal to indicate to the gatekeeper whether or not the terminal has sufficient resources. Typical messages include "available" or "unavailable."
SCI	Service Control Indication	Used in H.460.18 by the traversal server to signal an incoming call to the H.460.18 client.

Traversal Client-to-VCS Expressway Interaction

The TANDBERG VCS Expressway supports multiple versions of traversal technology: both Assent and H.460.18/.19. The standards-based H.460.18/.19 traversal technology is highly based off of the Assent technology, originally released by TANDBERG in January 2005. This section of the document will discuss how the VCS Expressway interacts with clients of both forms of technology, regardless of whether the client is embedded within an endpoint or through a traversal proxy (e.g. the TANDBERG VCS Control or the TANDBERG Gatekeeper).

Assent Client-to-VCS Expressway Interaction

The Assent traversal client is embedded both in the TANDBERG MXP endpoints (beginning with software version F2.0 and L2.0). This technology works based on establishing outbound connections from the client to the server (the VCS Expressway) to ensure a secure connection between the client and the VCS Expressway while enabling video communications through the firewall.



Function	Port	Type	Direction
Gatekeeper RAS	1719	UDP	Client → VCS Expressway
H.225 Call Signaling	2776	TCP	Client → VCS Expressway
H.245	2776	TCP	Client → VCS Expressway
RTP Media	2776	UDP	Client → VCS Expressway
RTCP Media	2777	UDP	Client → VCS Expressway

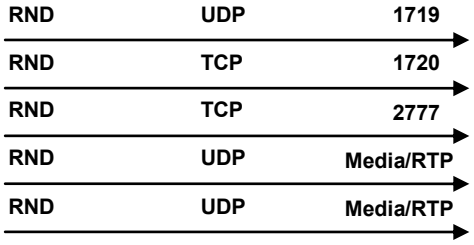
Note: all ports illustrated in the above example can be administratively configured.

H.460.18/.19 Client-to-VCS Expressway Interaction

The TANDBERG VCS Expressway also supports H.460.18/.19 standards-based firewall traversal. Very similar to the TANDBERG Assent technology, H.460.18/.19 works based on establishing outbound connections from the client to the server (the VCS Expressway) to ensure a secure connection between the client and the VCS Expressway while enabling video communications through the firewall.

H.460.18 governs the traversal of all call setup for an H.323 call, while H.460.19 controls the traversal of the media within the call. Optional within the H.460.19 standard is multiplexed media, a process by which the media connections between the client and the traversal server can be reduced down to a minimum number of ports – in the TANDBERG solution, multiplexed media narrows all connections down to 2776 and 2777.

H.460.18/.19 Traversal Client



TANDBERG VCS Expressway

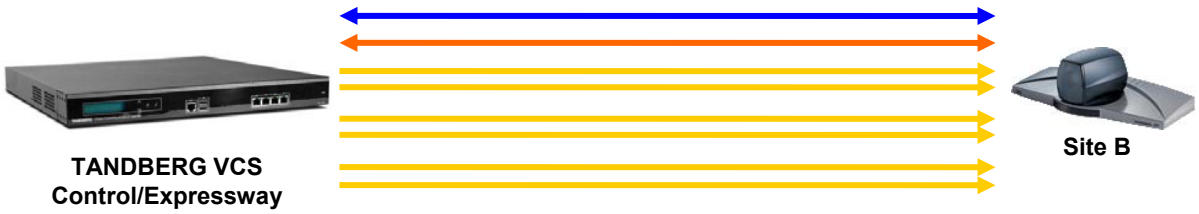
Function	Port	Type	Direction
Gatekeeper RAS	1719	UDP	Client → VCS Expressway
H.225 Call Signaling	1720	TCP	Client → VCS Expressway
H.245	2777	TCP	Client → VCS Expressway
RTP Media	50000-51199	UDP	Client → VCS Expressway
RTP Media	50000-51199	UDP	Client → VCS Expressway
RTP Media (Multiplexed)	2776	UDP	Client → VCS Expressway
RTCP Media (Multiplexed)	2777	UDP	Client → VCS Expressway

Note: all ports illustrated in the above example can be administratively configured.

VCS Unregistered System Interaction

When connecting to an unregistered system (e.g. an endpoint on a public IP address), the VCS will use a random association of ports within a specified range in order to complete the call. A reduced number of ports like those seen in either an Assent or H.460.18/.19 connection cannot be used for connecting to unregistered endpoints as the call must emulate a normal point-to-point H.323 call to be successful.

The below diagram and port chart discusses the ports the VCS will use when connecting to a public endpoint that is either not registered directly to the VCS or through a traversal proxy.



VCS outgoing	Protocol	Type	Site B incoming
15000:19999	Q.931	TCP	1720
15000:19999	H.245	TCP	Endpoint Defined
50000	Media (Audio)	UDP/RTP	Endpoint Defined
50001	Media (Audio)	UDP/RTCP	Endpoint Defined
50002	Media (Video)	UDP/RTP	Endpoint Defined
50003	Media (Video)	UDP/RTCP	Endpoint Defined
50004	Media (Dual Streams)	UDP/RTP	Endpoint Defined
50005	Media (Dual Streams)	UDP/RTCP	Endpoint Defined
50006	Media (FECC)	UDP/RTP	Endpoint Defined
50007	Media (FECC)	UDP/RTCP	Endpoint Defined

The TANDBERG VCS uses a TCP port range from 15000:19999 for both the H.225/Q.931[8] and H.245 connections. The ports will increment every time a new logical connection is required on H.225/Q.931 or H.245. When the port number reaches the top of the range, the port number will begin again from the start of the range.

The VCS also uses a pool of 2000 UDP ports (50000:51199) for all media (both RTP and RTCP). The ports are used in increments of 8 per call (e.g. the first call will use ports 50000-50007). After the first call is connected, the VCS will use the next consecutive 8 ports for the subsequent call and so on until all calls are disconnected. Once all calls are disconnected, the ports will reset to the beginning.

Note: Media will only route through the VCS Control or VCS Expressway in the event that at least one side of the call needs to participate in a traversal call. A traversal call will be used if one of the following conditions is true:

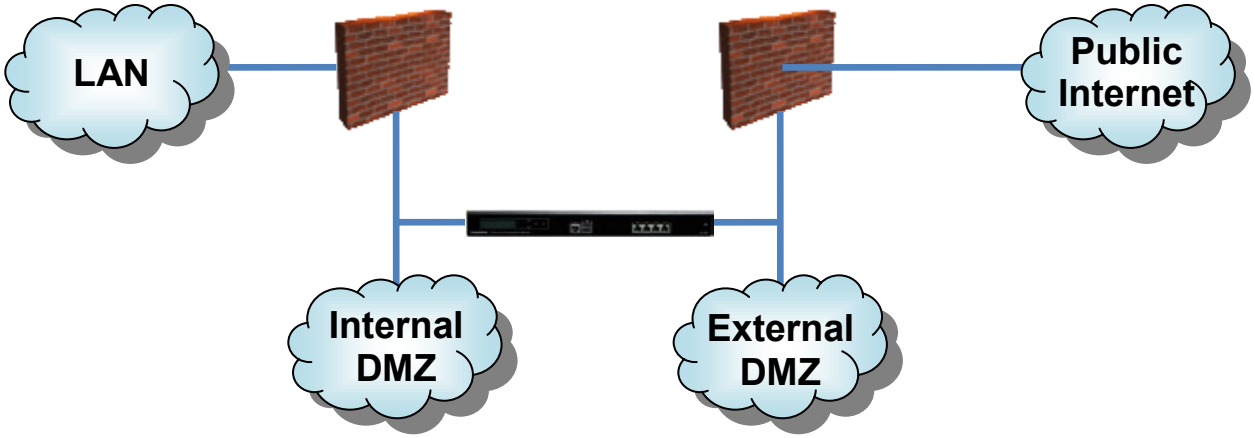
- One side of the call registers to a VCS Expressway with traversal client capabilities.
- One side of the call is IPv4 and the other is IPv6, causing the VCS to convert between the two.
- The VCS invokes interworking to connect an H.323-only system to a SIP-only system.

[8] Note: Incoming calls from systems not registered directly or through a proxy server will connect on port 1720 TCP for all H.225/Q.931 signaling.

VCS Advanced Networking

Dual Interfaces

When installed with the "Dual Networking" option key, the VCS supports up to two LAN/Ethernet interfaces. When deployed in this manner, the VCS Expressway can be configured to bridge two physically separate networks (i.e. an internally-facing DMZ that is physically disconnected to an externally-facing DMZ), similar to the same functionality that can be achieved using a web proxy.



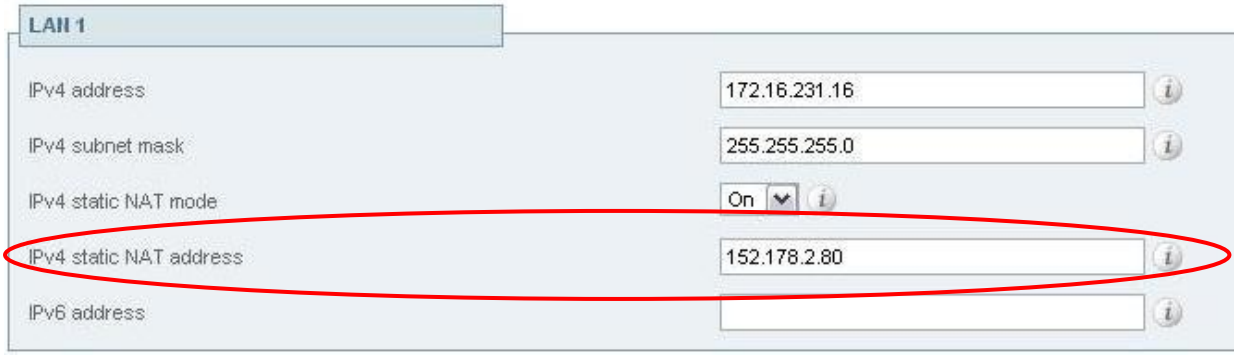
This feature is not designed as a firewall bypass utility; TANDBERG continues to recommend installing the VCS to work in conjunction with the existing security measurements deployed within a network infrastructure. Rather, the dual interfaces option allows the VCS to be deployed into networks that would have precluded the VCS from being deployed prior to release.

When deployed in this type of a model, routes will need to be configured in the VCS to dictate how traffic will flow between the two different networks to which the VCS is connected. More information on configuring routes within the VCS can be found in the VCS Administrator Guide on TANDBERG's main webpage (www.tandberg.com).

NAT Support

With the X4 software release, the VCS Expressway is now capable of supporting a NAT configuration on either of the LAN interfaces on the box. Once enabled, the VCS will lose all identity of the private address and will use the configured NAT address for all future communication. In other words, if a VCS is NAT'd from a private address to a public address, all future H.323 and SIP communication to that VCS will need to be directed to the public address; even if it comes from inside the same network.

For example, in the example below, the first LAN interface on the VCS is configured for a private address of 172.16.231.16 and the NAT is configured for a public address of 152.178.2.80. In this case, all future H.323 and SIP communication with that VCS will need to be directed to the 152.178.2.80 address, including any traversal links that are established from a VCS Control.



The reason for this requirement is due to the limited visibility that the VCS has within the network. Because many endpoints and traversal clients that register into the Expressway come from within their own private network using uncontrolled, private addressing, it is not possible for the VCS to determine if those addresses are local to its location. Therefore, the VCS will direct all future communication to the public address.

If, due to network requirements, internal traffic may only be routed to a private interface and NAT is required, the VCS should be implemented with dual networks.

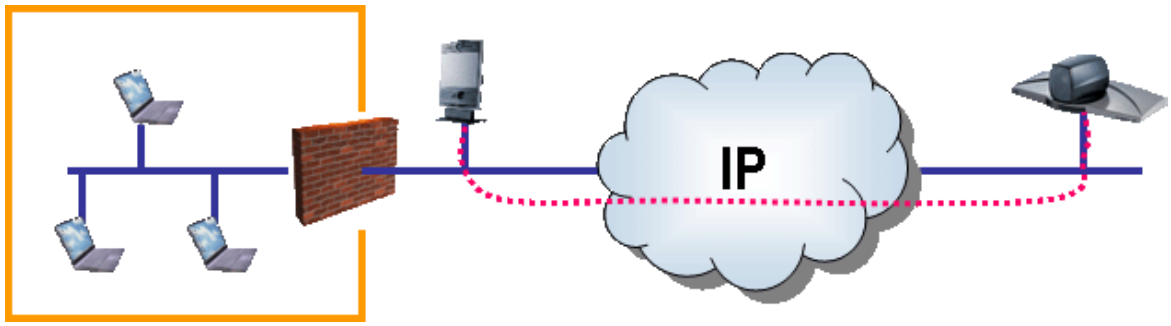
Note: The “Dual Networking” option key is required for NAT support on the VCS.

FIREWALL TRAVERSAL

Now that many videoconferencing connections are moving from ISDN to IP for increased functionality and lower costs, the need to overcome the firewall has become a high priority in video communications deployment. There are numerous methods to overcoming the challenges put forth by typical firewalls. Each one of these methods will be discussed below, along with the pros and cons.

Placing the codec in the public IP space

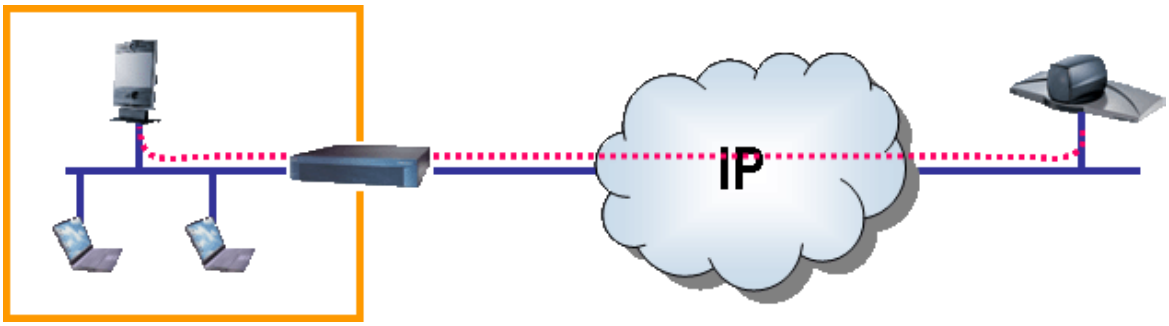
The easiest and most cost effective way to overcome the firewall is to place the unit completely outside the firewall, however this leads to serious security concerns. While many of today"s videoconferencing systems are not subject to the typical viruses found on the Internet, a system that is not properly locked down could be open to compromise.



Pro: No need to worry about firewall challenges
Con: Concern around exposure to the public Internet
This method does not scale as each endpoint will require a public IP address

Enabling the H.323 aware firewall

Some firewalls provide software upgrades that will make them H.323 aware. This means the firewall will now inspect all H.225/H.245 messaging to open and close ports dynamically. This also means the firewall must be compatible with all features of the endpoints, MCUs and gateways, which could cause issues with connectivity between endpoints that support very advanced features, such as encryption. Also, by processing all of the H.225/H.245 messages, a slight delay will be introduced to the handshaking and media streams.

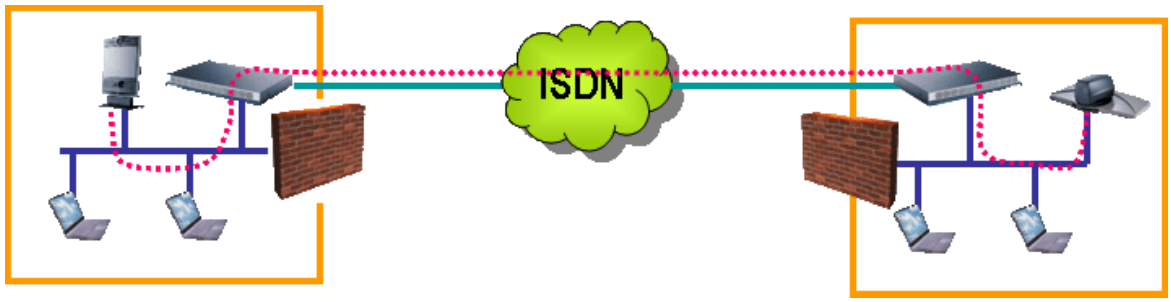


Pro: No need to permanently open ports on the firewall

Con: Firewall needs to be current on H.323 features and functionality. Some IT departments do not like the idea of ports opening and closing without their control. This solution will only solve the problem of traversing the local border – an additional border traversal method will be required on the far end in order to complete the call. Additionally, the system behind the firewall will be unable to receive any H.323 call from outside the firewall, thereby preventing communication between two organizations that both are implementing this method of firewall traversal.

IP to ISDN Gateways

To connect to separate IP islands, it is possible to use H.323<->H.320 gateways. This method is a solid alternative, but costs will be incurred when using the ISDN resources of the gateway. If the reason for moving to IP was so save ISDN costs, this may not be ideal.

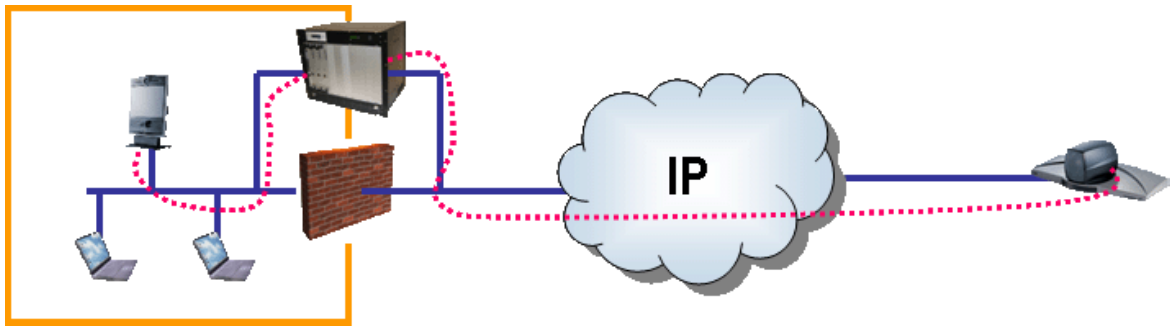


Pro: No need to adjust the firewall at all.

Con: Could result in increased spending for ISDN resources and calling. The gateway must also support all of the features of the endpoints and MCUs or the user experience could be altered when using the gateway as opposed to „on network" IP dialing. The far end will require a gateway that supports the endpoint features of both sides, otherwise the functionality of the conference will suffer. No firewall-level control over the traffic is possible as the firewall is completely bypassed.

MCU Firewall Traversal

This method uses a MCU that has IP ports in the public space and IP ports in the private space. The MCU receives media from both networks, strips the IP information and mixes the media into a conference. This protects one network from the other as no IP information is exchanged.



Pro: No need to adjust the firewall or open ports.

Con: Requires the use of costly MCU ports, even for point-to-point calls. This method does not scale as it requires an MCU at every location that needs to bypass a firewall. No firewall-level control over the traffic is possible as the firewall is completely bypassed.

NETWORK ADDRESS TRANSLATION (NAT)

One of the most widely adopted uses of firewall traversal in the market place today is Network Address Translation, or NAT. NAT works on the principle having an endpoint with a private IP address act as though it were assigned a public IP address for H.323 calls such that the far end system on the public internet does not know the difference – and calls are able to complete in both directions.

In order to be successful, configuration changes will need to be made to both the endpoint as well as to the firewall. The following sections will discuss these configuration changes and how they will affect the deployment of the videoconferencing network.

NAT and the Firewall

In order to properly support a NAT configuration, the firewall will need to be configured as a one-to-one relationship between a public IP address and the private IP address for all ports in the H.323 range (which include 1718 UDP, 1719 UDP and 1720 TCP as well as other vendor-specific TCP and UDP ports needed to complete H.323 calls). For the specific range needed, consult your endpoint manufacturer (the ports needed for a TANDBERG endpoint are discussed in the individual product sections of this document).

It is imperative that the firewall is configured for a one-to-one public-to-private relationship in order to allow for incoming H.323 calls on the public IP address. When a call is inbound to an endpoint, it will hit the public IP address on port 1720 TCP and must then be forwarded to the endpoint internally on that same port so the endpoint knows that the traffic is an incoming call. In addition, more ports will be negotiated during call setup that must be allowed to pass through the firewall untouched. The relationship from public to private is very specific in that both the source and destination ports of all H.323 communication must be translated exactly in the transition from public to private and private to public. This requirement exists because of the nature of H.323 traffic. During call setup, the endpoints directly negotiate the ports to be used for the rest of the call connectivity. If the traffic is received on different ports than those negotiated or dictated by the standard, the endpoints will not properly understand the traffic and, as a result, the call will fail.

NAT and the Endpoint

Getting the traffic through the firewall is the first step in completing a NAT call. The endpoint must also be configured to work in a NAT environment to ensure all communication occurs properly. This is done through configuring the NAT address on the endpoint; the NAT address tells the endpoint which public IP address to emulate when connecting into an H.323 call. While the firewall will handle the modifications of the IP packet headers to reflect the change from private addressing to public addressing, it will not handle the addressing information within the call setup payloads of those packets. These modifications will be required by the endpoint directly.

During call setup, the endpoint embeds addressing information within the call setup messages themselves in order to inform the far end how to reach back for future communication. While this is not much of an issue for TCP connections as the far end will use the connection-oriented properties of TCP to return all communication, UDP connections will fail if the endpoint does not properly communicate the return addressing information to the far end. By not providing the proper public address in the call setup, the far end will rely on improper information used within the H.245 call setup in order to open up the media connections. If this information is not valid (e.g. it is based on the private address assigned to the endpoint), the far end will send all media traffic back to an incorrect address, creating a failed call.

In order to prevent this connection failure from occurring, most H.323 endpoints on the market support a NAT feature that will then modify the addressing information used in the setup of the call appropriately. The details of this feature vary depending on the manufacturer, but work on the same general principle: substituting a public address for a private address within all call negotiation communication. In a NAT setup, the endpoint will be programmed in with a NAT address (usually a public address) that has been setup on the network to correspond directly with the private address associated with the endpoint. During call setup with the far end, the local endpoint will then transmit the programmed NAT address to

the far end, giving the other site a valid network path back to the originating side and allowing all connections, both TCP and UDP, to initiate for a successful video call.

NAT and TANDBERG Endpoints

As of software version B3.0, all TANDBERG endpoints support NAT to achieve the functionality described above. The NAT feature can be configured for one of three distinct settings: off, on and auto.[9] The following sections will discuss each one of these configuration options.

NAT Off

When NAT is turned off, the endpoint will connect and signal its physical IP address as the proper address to receive calls. This setting should be used if the endpoint does not need to utilize the NAT feature to traverse the firewall (e.g. the codec is installed on the public network or is installed in conjunction with TANDBERG Expressway, etc.).

NAT Always On

When NAT is turned on, the endpoint will always use the address that is programmed within the NAT Address field for all call and RAS signaling, no matter the IP address of the far end system/gatekeeper or where they are located on the network. This configuration setup is most useful if the endpoint will always connect to sites that are off the network (e.g. in a home office type of environment) as any calls with internal endpoints will fail, as internal endpoints will not be able to communicate properly with a system on the outside network.

AutoNAT

AutoNAT is designed for systems that sit on a private network behind a firewall and will consistently connect to video endpoints both behind the firewall and outside on the public Internet. When set to Auto, the endpoint will automatically utilize NAT signaling when required, depending on the remote address of the system. The endpoint will always make the decision on the address based on the address of the far end system.

Outbound Calls

When the endpoint is placing a call to a far end system on a reserved private address[10], the endpoint will use the private address associated with the box in all call setup, capabilities exchange and media communication. Because the endpoint is connecting to a private system, it does not need to provide the far end a valid route over the public internet for all return communication. Therefore, using the private address will allow proper communication between the endpoints over the LAN.

When placing a call to a system with a publicly routable IP address (e.g. a system that does not have a reserved private address), the endpoint will then utilize the NAT address configured within the system as the address for all call setup, capabilities exchange and media communication. When connecting to a public system, all information must then traverse through the firewall to the public Internet; as such, all return communication must have a valid route over the public Internet back to the endpoint on the internal LAN. By using the public NAT address programmed internally for all communication, the route will be properly established through the firewall between both endpoints.

Inbound Calls

Upon receipt of a call, the endpoint will make the same public/private determination based on the incoming calling address in order to decide which of the two addresses should be utilized. If the source address of the incoming call is a reserved private address, the endpoint will use the private IP address for all call signaling. However, if the source address of the incoming connection is a public address (e.g.

[9] AutoNAT was first implemented in software version E4.0/B9.0 for the TANDBERG Endpoints.

[10] Reserved private addresses include 10.0.0.0 to 10.255.255.255, 172.16.0.0 to 172.31.255.255 and 192.168.0.0 to 192.168.255.255.

not a reserved private address), the endpoint will substitute the NAT address for the private address to ensure proper call connectivity.

RAS Signaling

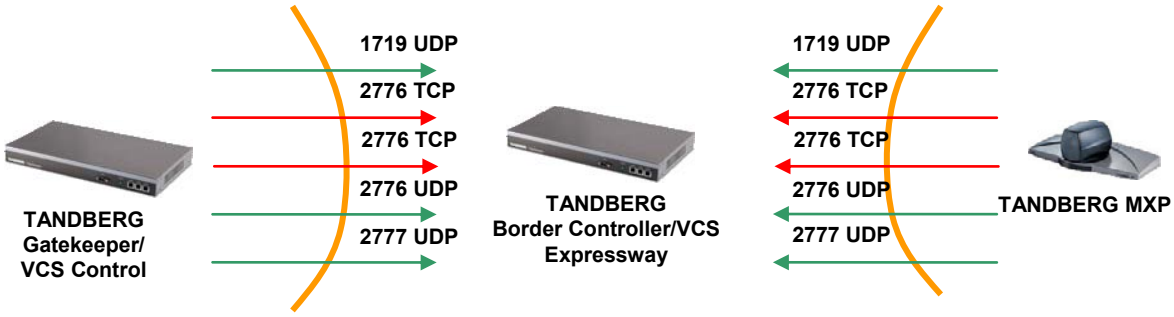
When registering to a gatekeeper, an endpoint will provide two very important pieces of information in order to aid in call connections: the RAS signaling Address and the Call Signaling Address. The addresses reported in the registration to the gatekeeper will vary depending on the address of the system as it relates to the address of the gatekeeper. If the endpoint on the private LAN is registering to a gatekeeper with an address in the reserved private addressing space, the endpoint will register the RAS and Call Signaling Addresses as the private address configured locally on the system. However, if the gatekeeper is configured with a public address, it will register using the address configured in the NAT field of the endpoint as both the RAS and Call Signaling Address.

TANDBERG EXPRESSWAY™ FIREWALL TRAVERSAL

The TANDBERG Expressway products have software embedded that allows for firewall traversal while maintaining security policies. The only requirement for these products is allowing outbound traffic on ports 1719 UDP, 2776 TCP, 2776 UDP, and 2777 UDP within the firewall rules[11]. If these conditions are met, successful videoconferencing through a virtually unlimited number of firewalls will take place. Using TANDBERG Expressway, the local and far end firewalls can be traversed.

Introduction

The TANDBERG Expressway enables products to traverse the firewall by using the normal behavior of firewalls by using a series of outbound connections only.

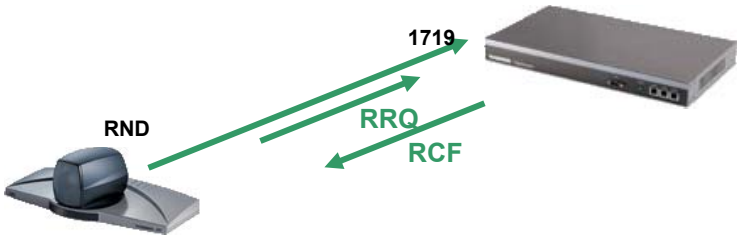


TANDBERG Expressway will allow any endpoint to call any publicly addressable endpoint on the public side of the firewall. By publicly addressable, we mean any unit that can be called from the public internet; this includes other endpoints that can be reached through the implementation of Expressway technology or standards-based H.460.18/.19 either through an MXP directly registered to a Border Controller/VCS Expressway or through a TANDBERG Gatekeeper/VCS Control, any endpoint that is accessible through port forwarding through the local firewall or any endpoint placed either on the DMZ or outside of a local firewall.

[11] Ports 2776 TCP, 2776 UDP and 2777 UDP can be modified within the configuration of the TANDBERG Border Controller or VCS Expressway if the use of other port numbers is desired.

Registration: Any Endpoint to TANDBERG Gatekeeper/VCS Control

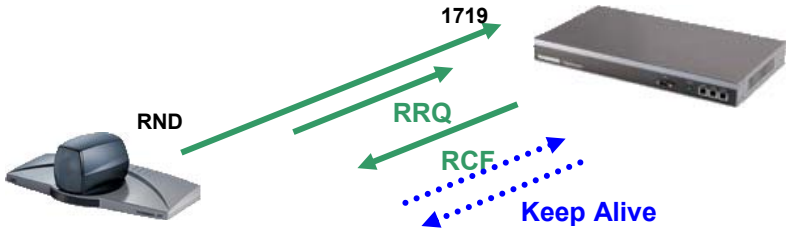
Registration of a generic endpoint to the TANDBERG Gatekeeper follows the same process as registering to any standard gatekeeper.



The endpoint registers by sending a Registration Request (RRQ) to the Gatekeeper on port 1719. The gatekeeper responds by sending a Registration Confirm (RCF) or Registration Reject (RRJ).

Registration: TANDBERG MXP Endpoint to TANDBERG Border Controller/VCS Expressway

Registration of a TANDBERG MXP to the TANDBERG Border Controller or VCS Expressway follows the same process as registering to any standard gatekeeper, with one exception: a continuous „keep alive" message that prevents a potential firewall port from closing down due to lack of traffic. In addition to normal RAS messages, the Expressway enabled endpoint also sends Expressway extensions to identify itself as an Expressway enabled.



The MXP endpoint registers by sending a Registration Request (RRQ) containing the Expressway enabled extension to the traversal server on port 1719; these extensions are sent within the non-standard data portion of the RRQ. The Border Controller responds by sending a Registration Confirm (RCF) or Registration Reject (RRJ) back to the source address of the RRQ message agreeing to use Expressway technology and not the RAS address embedded in the message. The Keep Alive signal outbound from the Expressway enabled endpoint and Keep Alive Acknowledge signal outbound from the traversal server, shown with dotted lines, is maintained to prevent port 1719 from closing due to inactivity.

Traversing the Firewall: MXP/Traversal Server/MXP

The simplest deployment of Expressway involves registering MXP endpoints to a TANDBERG traversal server (e.g. TANDBERG Border Controller or VCS Expressway).

Note: this solution might not be the best deployment, especially for organizations that have a larger concentration of endpoints within a single office. When an endpoint is registered to the traversal server, all calls will be considered traversal calls, regardless of the physical location of the far end system.

Note: due to the diversity of the potential traversal solutions, all diagrams below will refer to the traversal client and traversal server instead of specific boxes. Examples of traversal clients include the TANDBERG Gatekeeper and TANDBERG VCS Control; examples of traversal servers include the TANDBERG Border Controller and TANDBERG VCS Expressway.

Call Routing

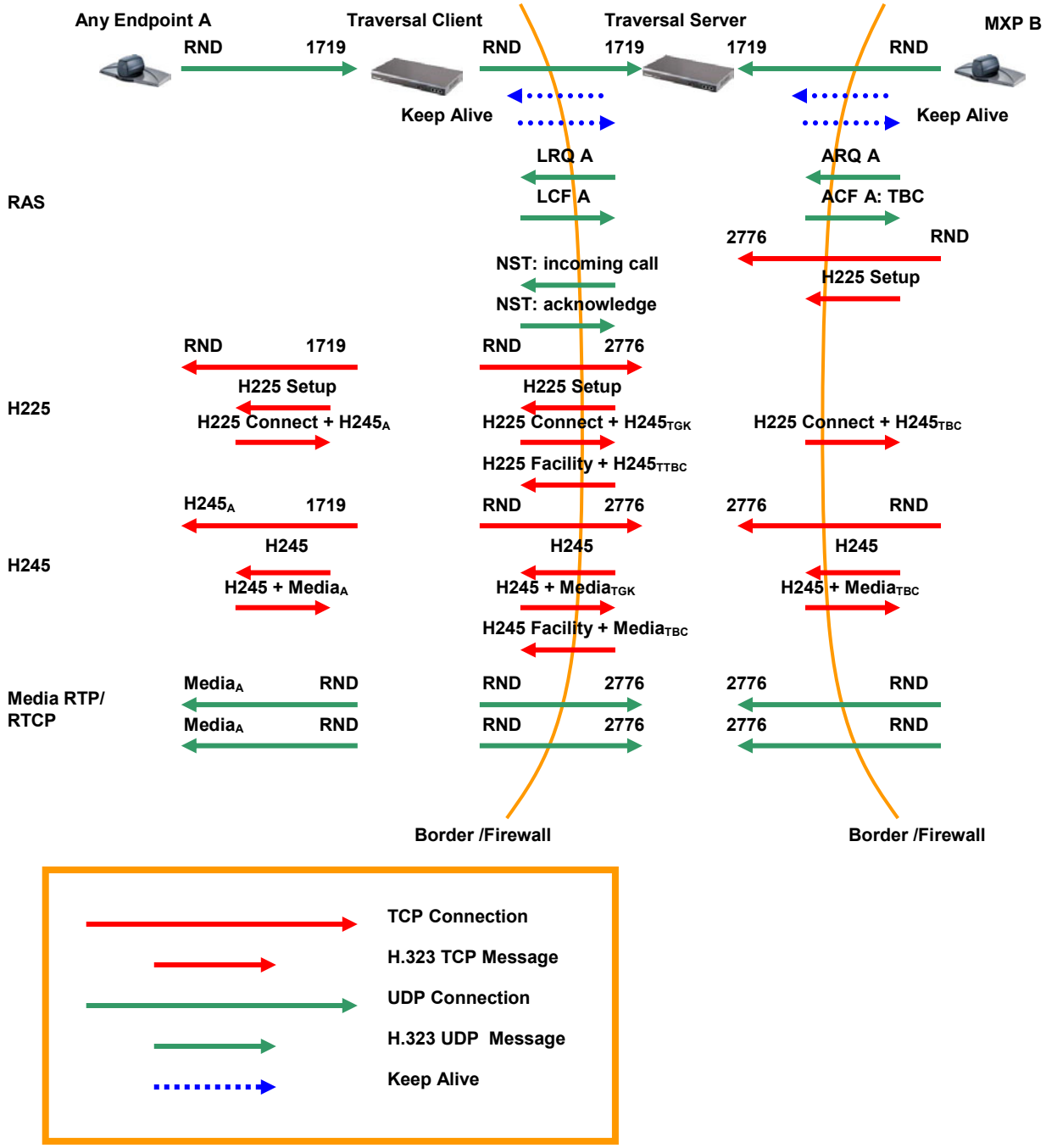
In this example, MXP B will call MXP A from outside the corporate firewall. MXP B can be behind its own firewall or can be on the public Internet.

Traversing the Firewall: Any Endpoint/Client/Server/MXP

By deploying a traversal client inside the firewall, any H.323 compliant endpoint can make use of Expressway to traverse the firewall.

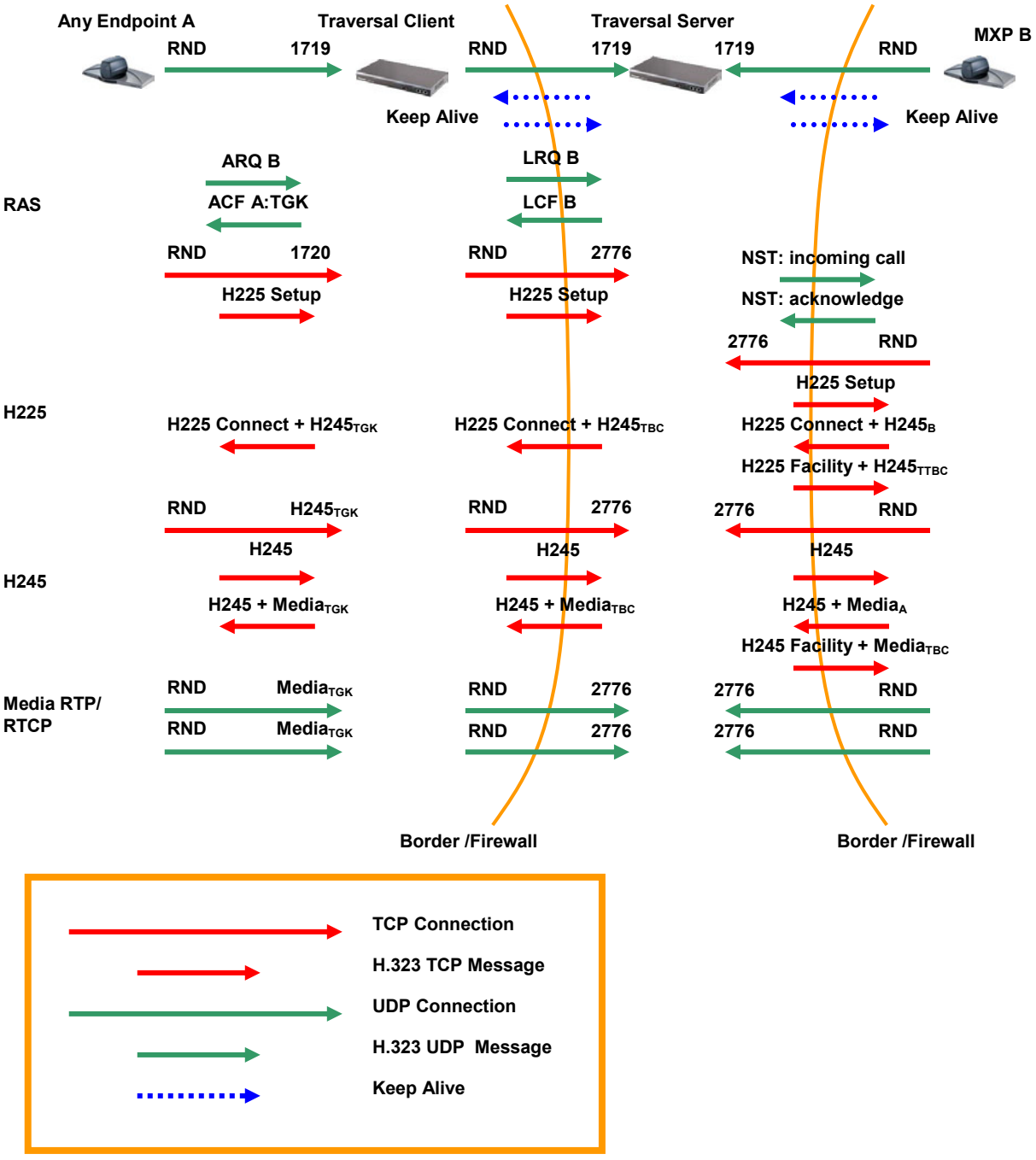
Incoming Call

In this example, MXP B will call „any endpoint A" from outside the corporate firewall. MXP B can be behind its own firewall or can be on the public Internet.



Outgoing Call

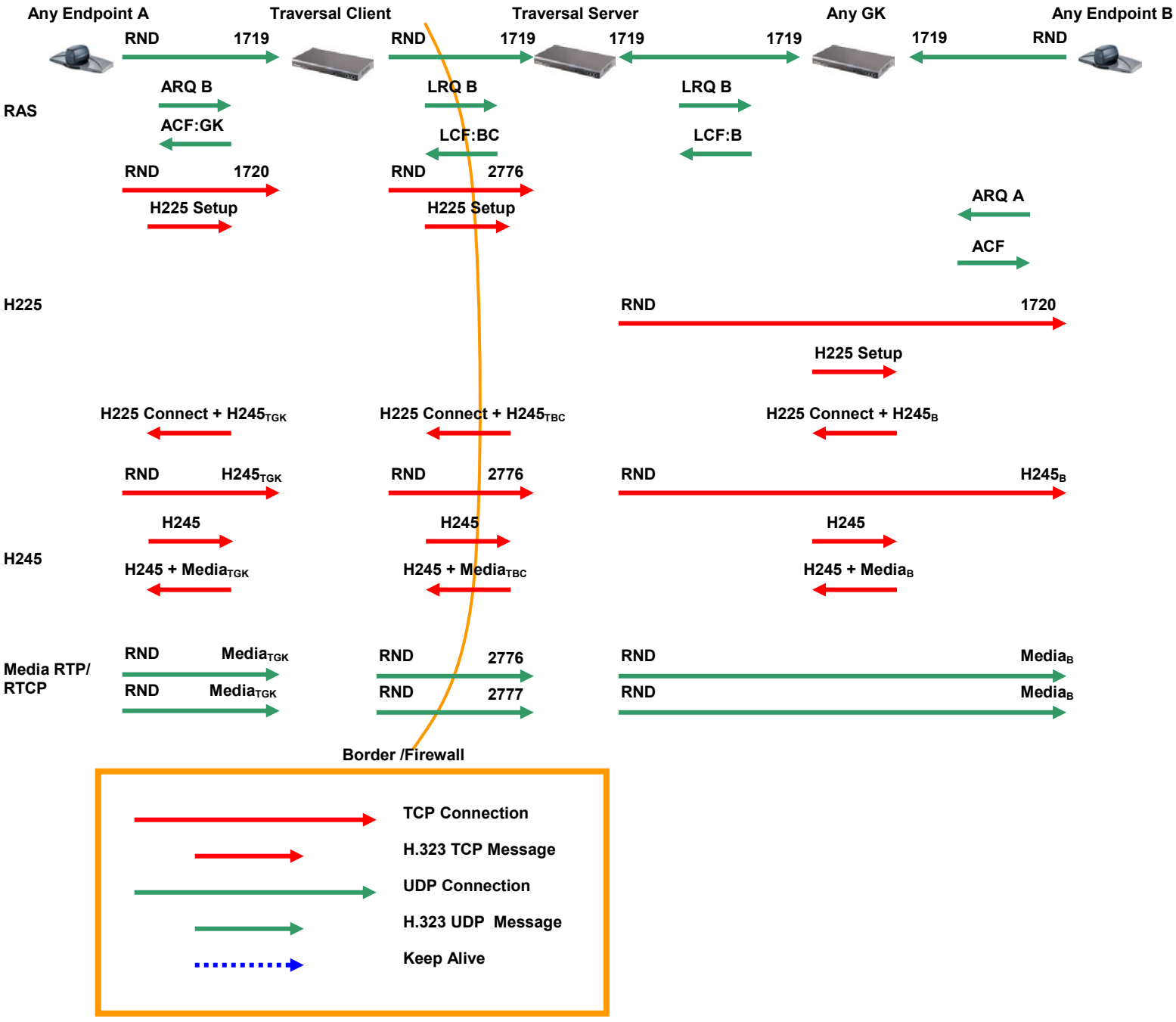
In this example, „any endpoint A" will call MXP B from inside the corporate firewall. MXP B can be behind its own firewall or can be on the public Internet.



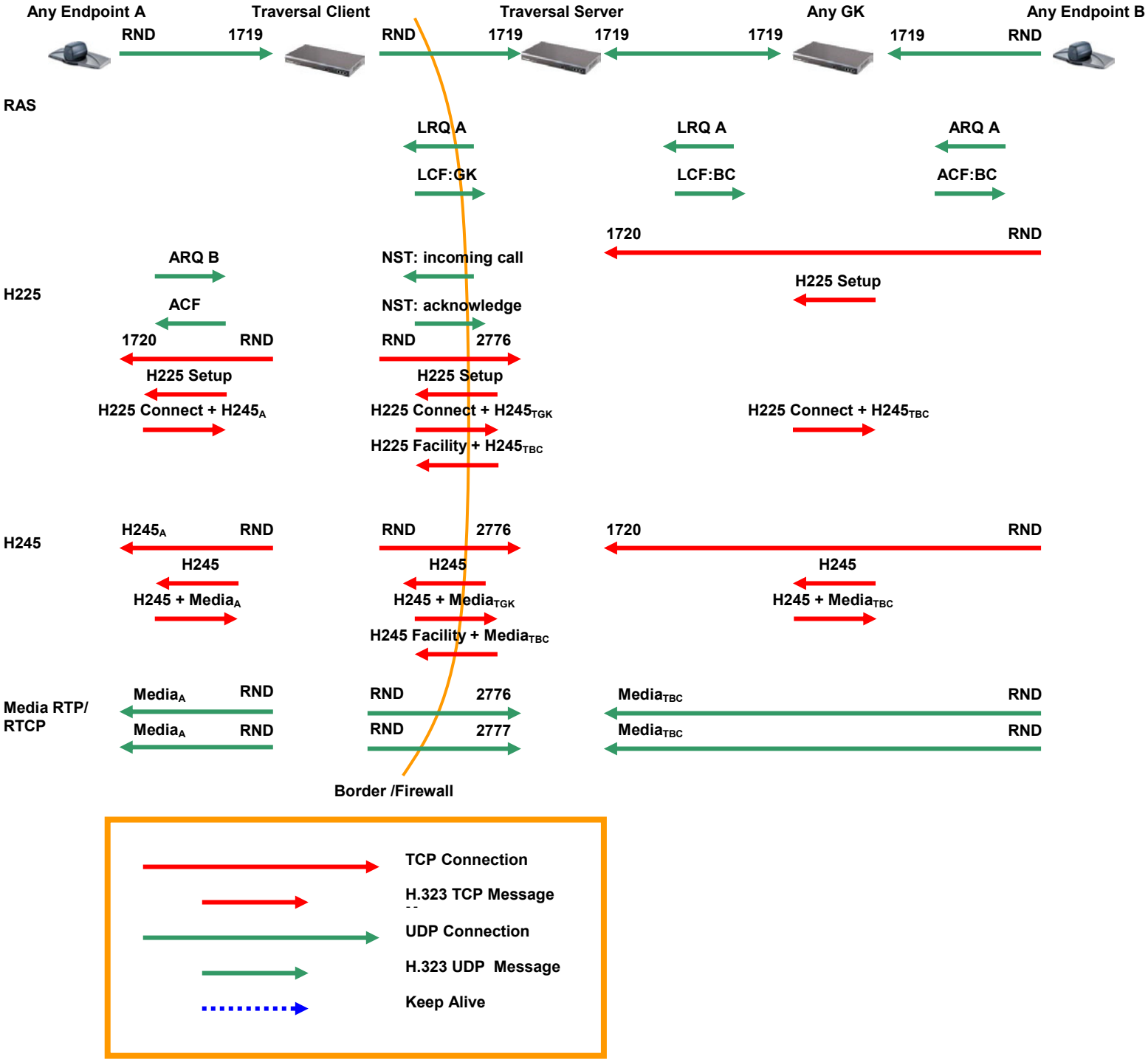
Traversing the Firewall: Any Endpoint/Client/Server/Any GK/Any Endpoint

By deploying a TANDBERG traversal client inside the firewall, any H.323 compliant endpoint can make use of Expressway to traverse the firewall. By neighboring any 3rd party gatekeeper to the public traversal server, any H.323 compliant endpoint on the public side of the firewall can also make use of Expressway to traverse the firewall.

Outgoing Call



Incoming Call

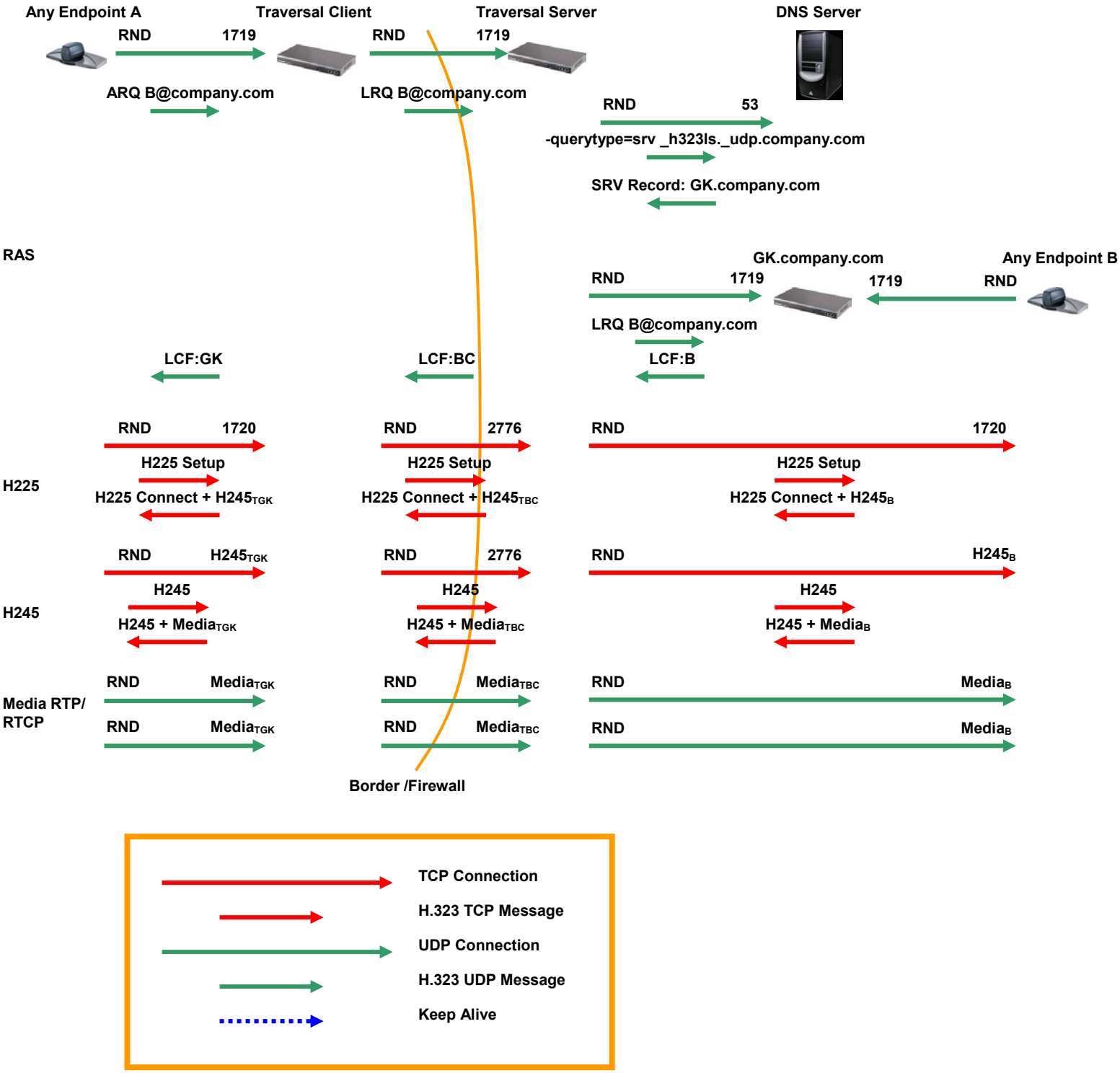


URI Dialing

By deploying a TANDBERG traversal client and traversal server outside the firewall, any endpoint registered into the solution can now take advantage of both making and receiving an H.323 call via standards-based URI dialing (H.323 v5 Annex O). To perform outbound URI dialing, either the client or the server will need to be configured towards a public DNS server. Upon then receiving the call request, the system will then perform the lookup of the remote H.323 island within the configured DNS server and will forward the call request to the remote island upon resolution of the DNS record.

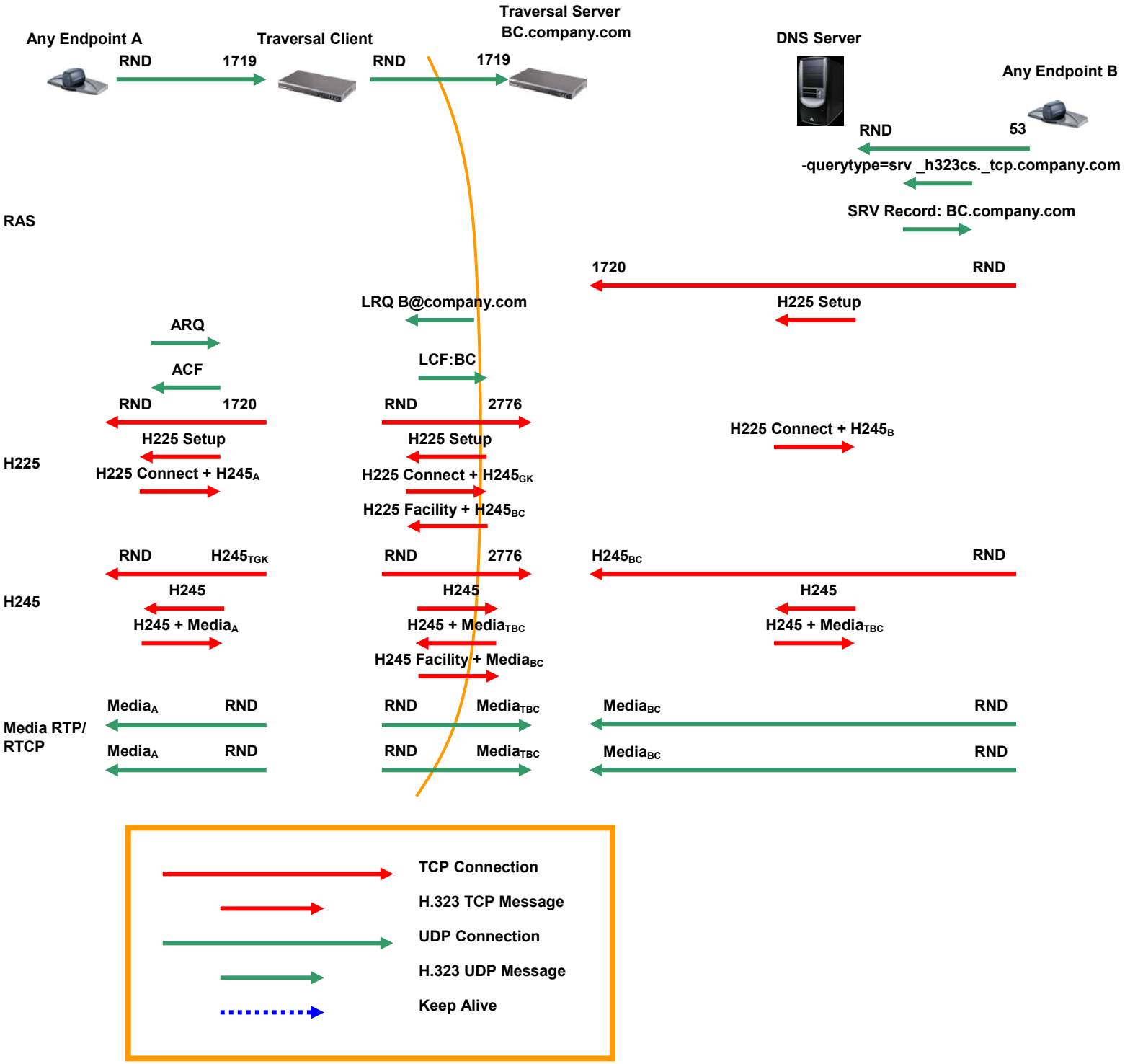
Outbound Call

The below diagram illustrates the connection of a URI call.



Inbound Call (Endpoint Not Registered)

The diagram below will illustrate the process an H.323 network goes through upon receiving a call request from an isolated endpoint that performed a lookup for the *_h323cs._tcp.<domain>* service record.



H.323 DNS Service Records

Two types of service (SRV) records compose the makeup of the DNS configuration for an H.323 island; each record serves its own purpose for the island. The location record (*_h323ls._udp.<domain>*) is the record that will be referenced by gatekeepers for resolution of a remote service gatekeeper. The call service record (*_h323cs._tcp.<domain>*) is the service record that is used by unregistered endpoints to connect calls to remote H.323 domains, without requiring a registration to any H.323 island, either local or remote.

As the RFC states, the SRV record must be added as:

_Service._Proto.Name TTL Class SRV Priority Weight Port Target

_Service defines the service type. In the case of the H.323 location record, this would be listed as: *_h323ls*. The call service record is *_h323ts*.

_Proto is the protocol that will be used for the communication. For H.323 RAS traffic, use the protocol *_udp*; call setup traffic will use *_tcp*.

For more information on creating service records for an H.323 island, please reference the TANDBERG Gatekeeper User Manual (document D11381), the TANDBERG Border Controller User Manual (document D13691) or the TANDBERG VCS Administrator Manual (document D14049).

STANDARDS-BASED FIREWALL TRAVERSAL – H.460.18/.19

The H.460 standard, approved by the ITU on 13 Sept 2005, was developed in order to standardize firewall traversal for H.323 traffic. Within the firewall traversal aspects of the standard, there are two major components – governing the traversal of call setup/signaling and media. The standards H.460.18 and H.460.17 govern call setup and signaling, while H.460.19 controls the process for media traversal.

H.460.18

H.460.18 is the primary standard governing the traversal of all call control and capabilities exchange for an H.323 call by opening up outbound connections from the traversal client to the traversal server. Each portion of the traffic – RAS, Q.931 call setup and H.245 call signaling – will maintain its own connection to the traversal server and will be signaled in its native form (i.e. the characteristics of the traffic do not appear any different to the network than they would in a normal H.323 call). H.460.19 requires support of H.460.18 for call signaling.

H.460.17

Similar to H.460.18, H.460.17 provides another mechanism for call signaling through a tunneled connection between the client and the server. In this case, all RAS and H.245 signaling is tunneled on top of an H.225 facility message through a TCP connection between the client and the server, while all H.225/Q.931 signaling is sent in native form. While fewer ports are needed in this type of a connection, the tunneling effectively hides the traffic from the network, making security decisions much harder to control from the network point of view.

H.460.19

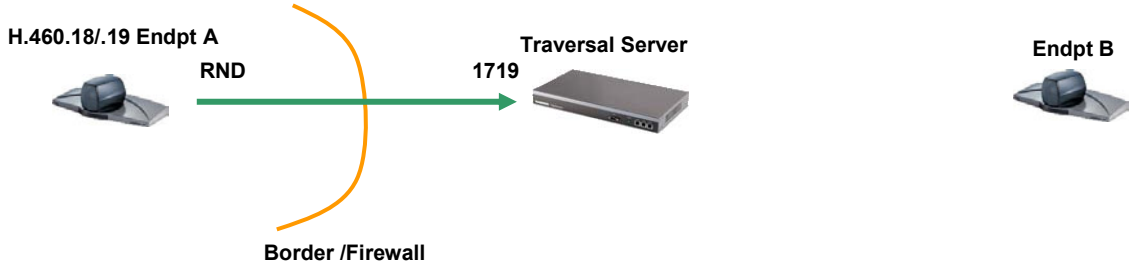
The H.460.19 standard controls the traversal of all media through a border using the same mechanism – the traversal client establishes outbound connections to the traversal server. H.460.19 requires the support for H.460.18 for signaling traversal; other traversal mechanisms can be used, but are not required by the standard. H.460.19 also includes optional support for multiplexing all media on a limited number of ports, thereby reducing the number of ports needed for all media connections within a single H.323 call.

This standard is very similar to the TANDBERG Assent architecture that was released in the N2/Q1 version of software for the TANDBERG Gatekeeper and Border Controller, respectively, as well as F2/L2 software for the TANDBERG MXP endpoints.

A standards-based firewall traversal (H.460.18 and H.460.19 capable) solution can be deployed in the exact same manner as the TANDBERG Expressway technology above. The following sections are dedicated to discussing the technology on a technology level, not a deployment level.

Network Setup

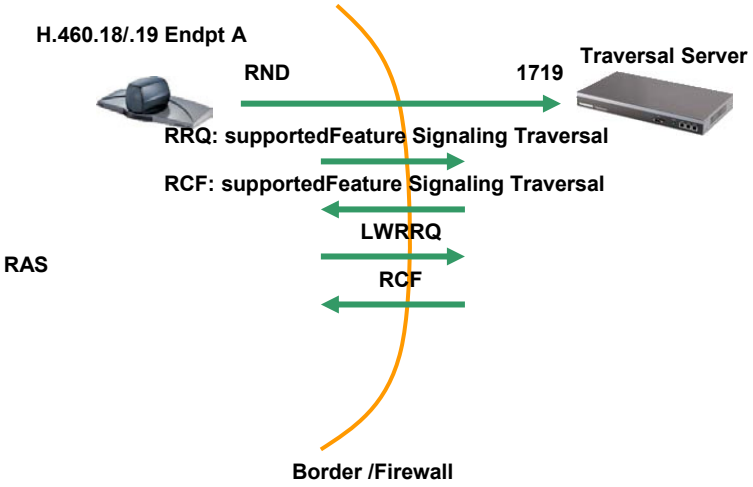
In the sections below, the following simplified network will be discussed. It is assumed that all endpoints are properly registered into the network in order to make inbound or outbound calls. The network infrastructure will not be discussed as it does not pertain to the technology itself but rather the deployment of the technology. For information regarding deploying the technology, please refer to the section discussing the TANDBERG Expressway technology as well as document D50362, TANDBERG Infrastructure Deployment Guide.

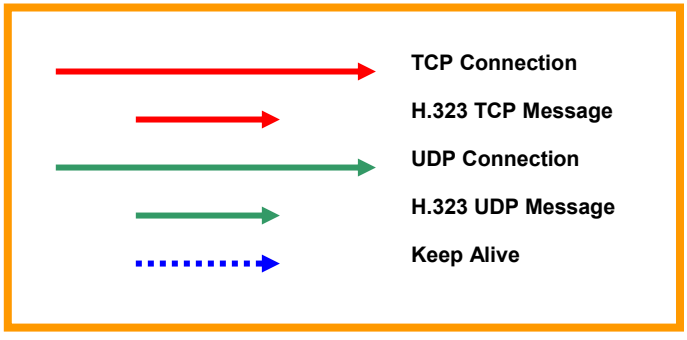


Registration

The standard is based on the concept of a client-server architecture, in which the traversal client is either a traversal-enabled endpoint or a traversal-enabled gatekeeper and the server is the traversal server (e.g. the TANDBERG Border Controller). The client will be based behind the firewall and, through a registration, will then communicate with the traversal server in order to facilitate traffic traveling both inbound and outbound through the firewall. Upon both discovery and registration to the server, the client will need to signal „`Signaling Traversal`" within the „`supportedFeature`" field of the GRQ and RRQ RAS message to the traversal server. If the traversal server then responds back with the „`Signaling Traversal`" within the confirmation message, the client will be aware that it is registering to a traversal server and use the H.460.18 and H.460.19 messaging when connecting H.323 calls (both inbound and outbound).

Upon registration confirmation, the client will receive a Time to Live (TTL) from the traversal server. Upon expiration of the TTL, the client will then send a Lightweight Registration Request (LWRRQ) to the traversal server to indicate both that the client is still available and to keep the firewall/NAT port from closing down and blocking communication between the client and the traversal server. This TTL message is a standard message within all gatekeeper registrations, but is significantly shorter within an H.460.18/.19 registration in order to prevent firewall ports from closing and preventing inbound and outbound communication.





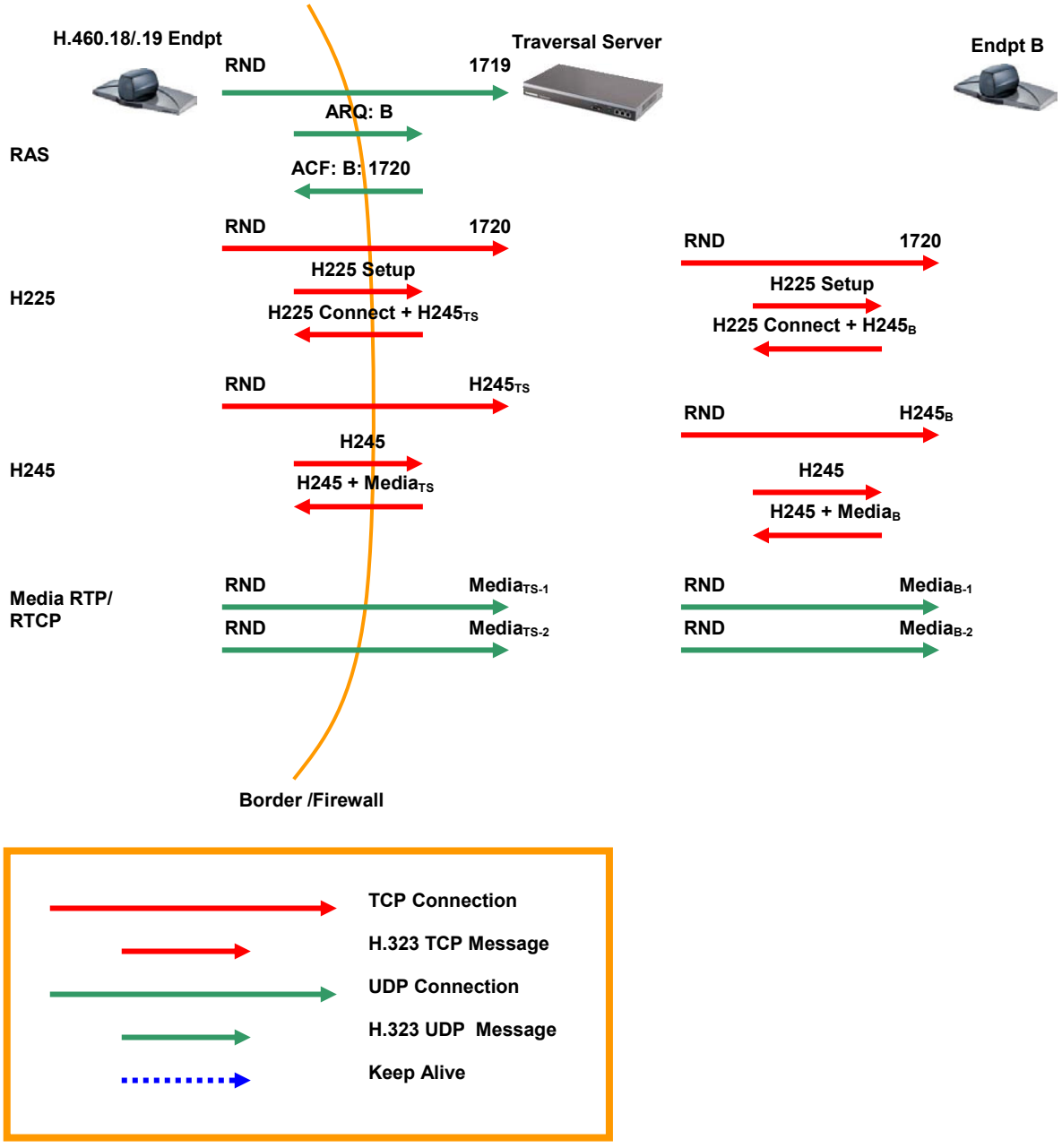
Outgoing Call (From Endpoint A)

In order to make an outgoing call, the endpoint will follow normal H.323 RAS procedures and sending an ARQ to the traversal asking permission to make a call. Upon receipt of the confirmation from the traversal server, the endpoint will then open up a TCP connection to the address and port returned within the ACF in order to begin the H.225 call connection procedures (this connection will usually open to destination port 1720 TCP on the traversal server). The traversal server will then open up a connection and send the H.225 Call Setup to endpoint B in order to begin the call connection. Upon receipt of the H.225 Call Connect information from endpoint B, the traversal server will then forward that into the internal endpoint over the same connection that was opened up from the client to initiate the H.225 call setup procedures. This H.225 Call Connect will include the H.245 address and port of the traversal server.

Upon receipt of the H.225 Call Connect message and H.245 address and port information, the endpoint will then establish another connection to the specific address and port and transmit its local H.245 capabilities directly to the traversal server, which will then open up another TCP connection to endpoint B and forward the information. Endpoint B will then return its H.245 messaging and media port information back to the traversal server, at which time the traversal server will then forward the H.245 information into endpoint A over the established TCP connection. Additionally, the traversal server will then forward its media address and ports to endpoint A to finalize call setup and initiate media connectivity.

Upon completion of all call setup signaling, endpoint A will initiate UDP media port connections to the traversal server on the addresses and ports that were signaled within the H.245 connection. The media connections will then be opened from the traversal server to endpoint B using the address and ports endpoint B specified in its H.245 connection previously. Once all media connections are opened, media will flow bi-directionally.

To prevent the firewall from closing down any of the connections opened from endpoint A to the traversal server, periodic keep-alive messages will be sent and returned from the endpoint to the traversal server. These messages will also include addressing information used by the traversal server to uniquely distinguish all of the incoming traffic to ensure it is forwarded to the far end properly.

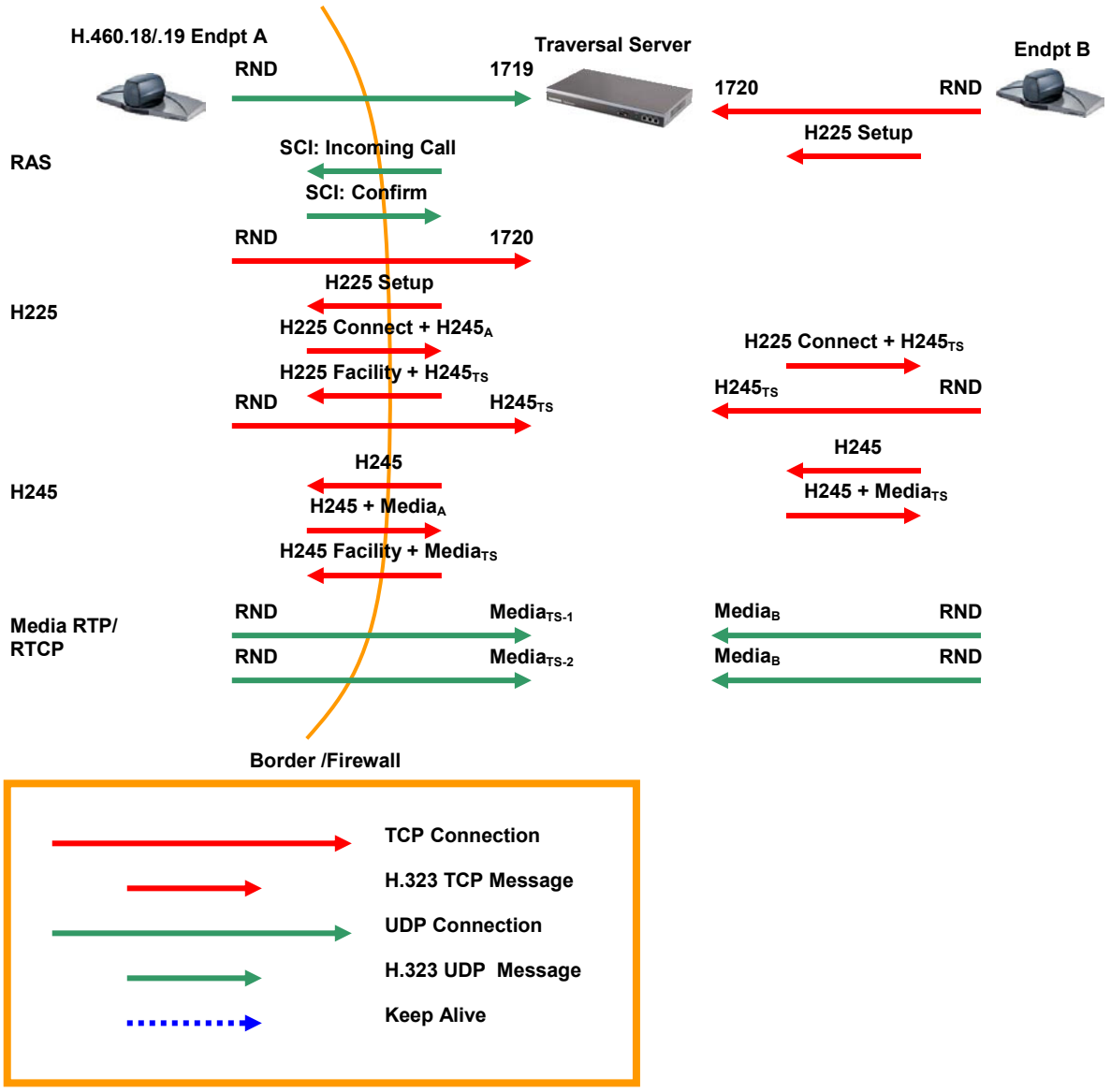

H.460.18/.19 Endpt
Traversal Server
Endpt B
RND
1719
ARQ: B
RAS
ACF: B: 1720
RND
1720
H225 Setup
H225
H225 Connect + H245TS
RND
1720
H225 Setup
H225 Connect + H245B
RND
H245TS
RND
H245B
H245
H245
H245 + MediaTS
H245
H245 + MediaB
Media RTP/
RTCP
RND
MediaTS-1
RND
MediaTS-2
RND
MediaB-1
RND
MediaB-2
Border /Firewall
TCP Connection
H.323 TCP Message
UDP Connection
H.323 UDP Message
Keep Alive

Incoming Call (Into Endpoint A)

In order to establish a call from outside the network back in[12], the traversal server will need to signal to the internal endpoint (endpoint A) that a call is waiting and instruct endpoint A to open up an outbound connection to the traversal server to forward the H.225 Call Setup messaging. This is done through a standard RAS message called a Service Control Indication (SCI). This message will include all necessary signaling to the H.460 compliant endpoint, along with the H.225 address for the traversal server.

Once the SCI reaches endpoint A, the H.225 setup message will come inbound and endpoint A will initiate its normal call accept procedures. In addition, the Traversal server will send an H.225 Facility message to the endpoint after the H.225 negotiation has completed. This facility message will include a message that will instruct the endpoint to open up an outbound connection for the H.245 capabilities exchange to the traversal server on the address specified within that facility message. Finally, at the end of the H.245 negotiation, the traversal server will send an H.245 facility message, instructing endpoint A to open up all media connections outbound to the address and port signaled within this facility message.

[12] It is assumed that endpoint B has the ability to dial into the network through a variety of means. This may include, but is not limited to alias, H.323 ID or URI.

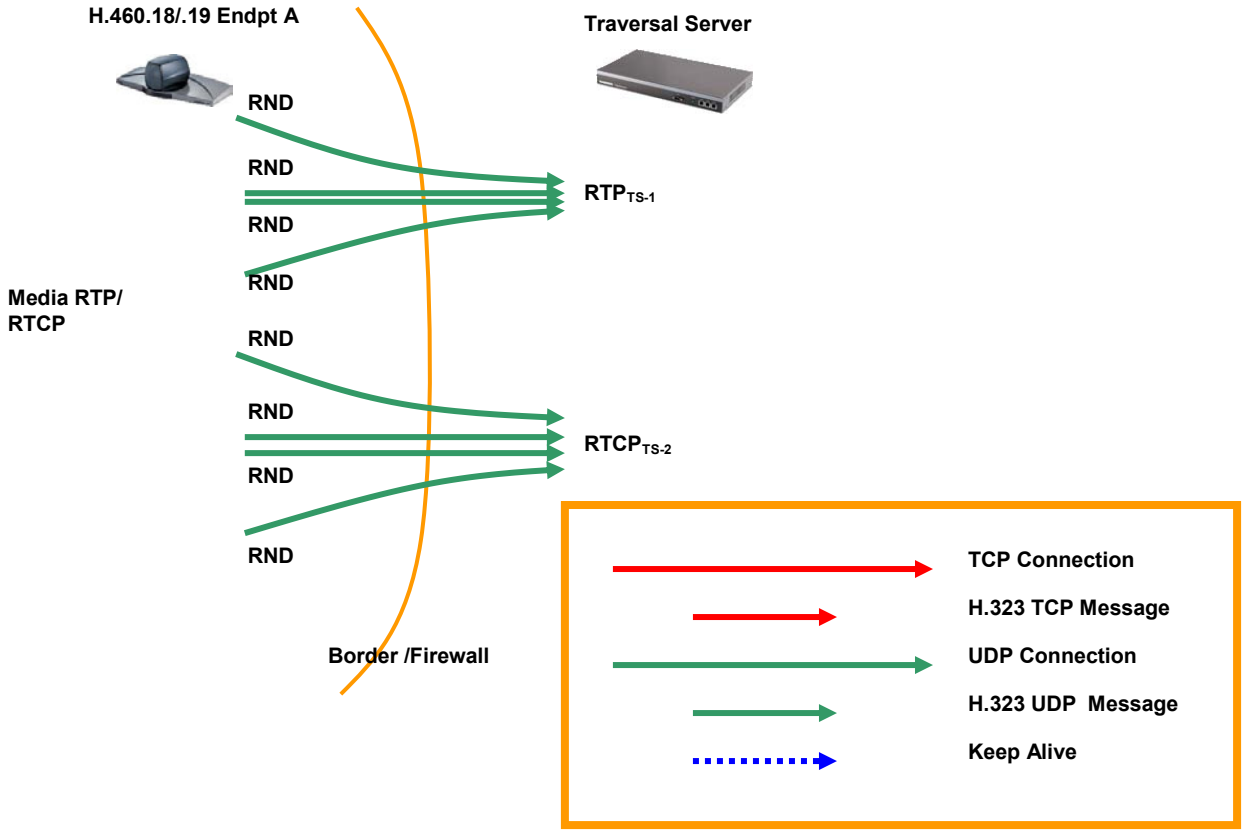

H.460.18/.19 Endpt A
Traversal Server
Endpt B
RND
1719
1720
RND
H225 Setup
RAS
SCI: Incoming Call
SCI: Confirm
RND
1720
H225 Setup
H225
H225 Connect + H245A
H225 Connect + H245TS
H225 Facility + H245TS
H245TS
RND
RND
H245TS
H245
H245
H245 + MediaA
H245 + MediaTS
H245 Facility + MediaTS
Media RTP/
RTCP
RND
MediaTS-1
MediaB
RND
RND
MediaTS-2
MediaB
RND
Border /Firewall
TCP Connection
H.323 TCP Message
UDP Connection
H.323 UDP Message
Keep Alive

H.460.19 Multiplexed Media

To reduce the number of ports needed for the media connections in an H.460.18/.19 traversal connection, multiplexed media can be utilized. As dictated by the traversal server, multiplexed media allows for the number of ports needed for outbound media connections to be significantly reduced. The N5/Q5 infrastructure software release and the F5 software release for the endpoints provided support for multiplexed media throughout the TANDBERG solution. By default, all media connections will be reduced down to ports 2776 UDP (for the RTP packet streams) and 2777 UDP (for the RTCP packet streams); thus emulating the Assent firewall traversal technology. Prior to multiplexed media, the H.460.19 media traversal stream required ports 50000 to 52400 to be allowed outbound to support the fully compliment of traversal calls.

Multiplexed media support is not negotiated upon registration, but rather upon call connection. If the traversal server attempts multiplexed media with an endpoint that does not support the protocol, the call attempt will not succeed as both portions of the connection do not support the same protocol for media traversal.

Note: Multiplexed media support is optional within the H.460.19 standard.



LIST OF TERMS

ASP: Application Service Provider.

Assent: The TANDBERG proprietary method of firewall traversal. The H.460.18/.19 standards are based on this technology.

Border: An imaginary line separating the public and private IP space by the use of a firewall.

Border Controller: A device that controls calling into and out of a NAT/firewall (border).

Call Signaling Address: The address and port on which an endpoint is listening for an incoming call.

Call TTL: Typically on a gatekeeper, this setting will specify the frequency in which the gatekeeper should query the local endpoint(s) involved in an H.323 call. Upon expiration of this TTL, the gatekeeper will send out an IRQ to each of the locally registered endpoints to validate the status of the call.

E.164: An endpoint identifier consisting of 0-9, *, or # that is used to register to an H.323 gatekeeper.

Endpoint: An H.323 terminal, gateway or MCU. An endpoint can call and be called. It generates and/or terminates information streams.

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, 100 or 1000 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).

H.323 ID: An endpoint identifier consisting of numbers or letters that is used to register to an H.323 gatekeeper.

H.460.17: ITU Standard that governs the traversal of all H.323 RAS, call setup and signaling messaging through a firewall/NAT using tunneling for traversal of the traffic. All communication can be signaled over a single TCP port.

H.460.18: ITU Standard that governs the traversal of H.323 call setup messaging through a firewall/NAT using standard H.323 signaling in a non-tunneled communications protocol.

H.460.19: ITU Standard that governs the traversal of all media within an H.323 call through a firewall/NAT. H.460.19 compliance requires compliance with H.460.18 as well.

H.460.19 Multiplexed Media: an optional portion of the H.460.19 standard that reduces the number of ports needed for media communication with a traversal server.

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.

LRQ TTL: The number of times the specific LRQ can be forwarded to additional gatekeepers.

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 and UDP IP 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.

RAS Signaling Address: The address and port an endpoint or gatekeeper listens on for all incoming RAS traffic.

Registration TTL: Typically configured on a gatekeeper, this setting specifies how often an endpoint needs to renew its registration through the submission of an LWRRQ.

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 time stamping. RTP does not address resource reservation and does not guarantee quality-of-service for real-time services.

Subzone: An area within a physical gatekeeper zone that exhibits its own network and bandwidth requirements.

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

Traversal Server: An H.460.18/19 server gateway logically combined with an H.460.18/19 server gatekeeper. The traversal server is located in the external network.

TTL: Time to live.

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.

Zone: a group of H.323 devices that are managed by the same gatekeeper.