

TANDBERG Gatekeeper N3 Software Release Document

TANDBERG

D50360, Rev 1.3

Table of Contents

1.	DOCUMENT REVISION HISTORY	3
2.	RELEASE NOTES FOR TANDBERG GATEKEEPER SOFTWARE VERSION N3.2	4
2.1	INTRODUCTION	4
2.2	NEW FEATURE OVERVIEW	4
2.2.1	<i>Standards-based Firewall Traversal (H.460.18 and H.460.19).....</i>	<i>4</i>
2.3	CHANGES AND IMPROVEMENTS SINCE PREVIOUS RELEASE.....	5
2.3.1	<i>RAS Bandwidth Signaling</i>	<i>5</i>
2.3.2	<i>DNS SRV Record Lookup</i>	<i>5</i>
2.3.3	<i>Link Bandwidth Limitation</i>	<i>5</i>
2.3.4	<i>Link Naming</i>	<i>5</i>
2.3.5	<i>Heavy LRQ Traffic</i>	<i>5</i>
2.4	KNOWN LIMITATIONS	5
3.	RELEASE NOTES FOR TANDBERG GATEKEEPER SOFTWARE VERSION N3.1	7
3.1	INTRODUCTION	7
3.2	NEW FEATURE OVERVIEW	7
3.3	CHANGES AND IMPROVEMENTS SINCE PREVIOUS RELEASE.....	7
3.3.1	<i>H.225 RAS Signaling.....</i>	<i>7</i>
3.3.2	<i>Software Upgrade.....</i>	<i>7</i>
3.3.3	<i>External Management</i>	<i>7</i>
3.3.4	<i>Links</i>	<i>7</i>
3.3.5	<i>Inter-Op.....</i>	<i>7</i>
3.4	KNOWN LIMITATIONS.....	7
4.	RELEASE NOTES FOR TANDBERG GATEKEEPER SOFTWARE VERSION N3.0	9
4.1	INTRODUCTION	9
4.2	NEW FEATURE OVERVIEW	9
4.2.1	<i>Increased Traversal Capacity</i>	<i>9</i>
4.2.2	<i>Alternate Gatekeeper.....</i>	<i>9</i>
4.2.3	<i>Improved Routing of Media.....</i>	<i>9</i>
4.2.4	<i>Increased Security</i>	<i>9</i>
4.2.4.1	<i>Local Database Authentication</i>	<i>10</i>
4.2.4.2	<i>LDAP Authentication.....</i>	<i>10</i>
4.2.4.3	<i>Encrypted LDAP Authentication</i>	<i>10</i>
4.2.5	<i>Call Processing Language</i>	<i>10</i>
4.2.6	<i>Network Modeling</i>	<i>11</i>
4.2.6.1	<i>Subzones</i>	<i>11</i>
4.2.6.2	<i>Links</i>	<i>11</i>
4.2.6.3	<i>Pipes.....</i>	<i>11</i>
4.2.7	<i>Improved Endpoint Communication.....</i>	<i>11</i>
4.2.8	<i>Call Logging.....</i>	<i>11</i>
4.2.9	<i>External Manager.....</i>	<i>11</i>
4.2.10	<i>Improved Event Log.....</i>	<i>11</i>
4.3	SUPPLEMENTAL NOTES TO MANUALS.....	12
4.3.1	<i>Software Versions.....</i>	<i>12</i>
4.3.2	<i>References/Related Documents</i>	<i>12</i>
4.3.3	<i>Network Support.....</i>	<i>12</i>
4.3.4	<i>Layer 4 Ports Used.....</i>	<i>12</i>
4.4	CHANGES AND IMPROVEMENTS SINCE PREVIOUS VERSION.....	12
4.4.1	<i>802.3 Issues</i>	<i>12</i>
4.4.2	<i>Allow/Deny List Issues</i>	<i>13</i>
4.4.3	<i>Call Routing Issues.....</i>	<i>13</i>
4.5	KNOWN LIMITATIONS	13
4.6	INTEROPERABILITY TESTING	14
4.6.1	<i>Gatekeepers</i>	<i>14</i>
4.6.2	<i>Gateway Interoperability.....</i>	<i>14</i>
4.6.3	<i>MCU Interoperability.....</i>	<i>14</i>
4.6.4	<i>Endpoint Interoperability.....</i>	<i>15</i>
4.6.5	<i>Firewall Interoperability.....</i>	<i>15</i>

1. Document Revision History

- Rev 1.3 - Removed Known Limitation between Polycom PVX and Microsoft NetMeeting
- Rev 1.2 - Release of N3.2, Minor Release
 - Updated Interoperability Testing
 - Updated List of Known Limitations of N3.0 and N3.1 Releases
- Rev 1.1 - Release of N3.1, Minor Release
 - Updated List of Known Limitations of N3.0 Release
- Rev 1.0 - Release of N3.0, Initial Version

2. Release Notes for TANDBERG Gatekeeper Software Version N3.2

2.1 Introduction

These release notes describe the features and capabilities included in the TANDBERG Gatekeeper software version N3.2 released on 18 Oct 2005.

2.2 New Feature Overview

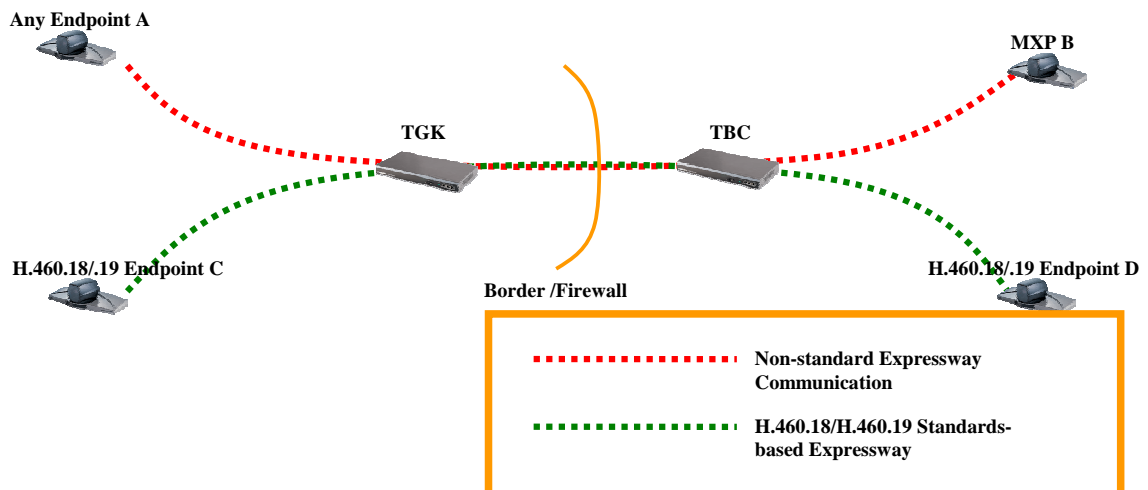
2.2.1 Standards-based Firewall Traversal (H.460.18 and H.460.19)

On 13 Sept 2005, the ITU-T ratified a pair of recommendations, H.460.18 and H.460.19, which are aimed at standardizing the communication between two H.323 components to achieve the goal of secure firewall traversal. Based on TANDBERG Expressway, these standards will give multi-vendor environments the opportunity to take advantage of a technology that TANDBERG customers have benefited from since its inception.

In conjunction with the TANDBERG Border Controller, the TANDBERG Gatekeeper now supports the firewall traversal using the H.460.18 and H.460.19 standards-based firewall traversal, giving multi-vendor environments the ability to take full advantage of the secure firewall traversal methodology that has been proven successful by TANDBERG customer deployments.

The standard is divided up into two distinct functions: signaling (H.460.18) and media (H.460.19). H.460.18, edited by Giles Chamberlin of TANDBERG, controls the process by which all call setup signaling and capabilities exchange occur within a traversal call. Media communication is governed by H.460.19, edited by Sasha Ruditsky of RADVISION.

For more information on H.460.18 and H.460.19, please reference document D50305, TANDBERG and H.323.



2.3 Changes and Improvements since previous release

2.3.1 RAS Bandwidth Signaling

The TANDBERG Gatekeeper now recognizes bandwidth in 100bps increments instead of 1000bps increments, thereby increasing the flexibility of the H.323 network.

2.3.2 DNS SRV Record Lookup

When the Gatekeeper performs a DNS service record lookup for an outbound URI call, it stores the results internally. The stored results are then used for subsequent calls to the same DNS suffix in order to speed up call connectivity. There was an issue within this mechanism that would store multiple entries for the same resolution which, upon recall, could create an issue within the Gatekeeper that would cause a system restart. This issue has been resolved.

2.3.3 Link Bandwidth Limitation

Corrected an issue where a Pipe configured for 'Unlimited' bandwidth would not allow an unlimited amount of bandwidth through.

2.3.4 Link Naming

Resolved issue that would cause a link to fail if it was renamed after it was initially created.

2.3.5 Heavy LRQ Traffic

N3.2 has resolved an issue that may cause the Gatekeeper to restart under a heavy LRQ stress caused by LRQ loops. LRQ loops within a network should be avoided within an H.323 network as they increase the LRQ traffic on the Gatekeeper and may slow the speed in which a call will connect.

2.4 Known Limitations

Equipment	Limitations
TANDBERG Gatekeeper ver N3.2	The Gatekeeper may show the Start and End times within the Call and Registration Histories as 'Not Set'.
TANDBERG Gatekeeper ver N3.2	If the Gatekeeper loses IP communication with the Border Controller, it will take approximately two minutes for the Gatekeeper to properly re-register to the Border Controller, once communication is restored.
TANDBERG Gatekeeper ver N3.2	If the Gatekeeper is configured with an Alternate list, is configured to not forward LRQs to neighboring Gatekeepers and it receives an LRQ for an endpoint that is not registered directly or with any of the configured alternates, the Gatekeeper may reset.
RADVision L2W Gateway ver 2.2.3.2.5	Due to the signaling coming from the RAD L2W GW, calls

	<p>will disconnect if it is not registered into its own subzone and the GK is set to indirect mode and registered to a BC. The reason behind this error is because the GW tries to connect a call to itself on a random port it has not registered with. In order to resolve this issue, either place the Gatekeeper into Direct mode for “Calls to Unknown IP Addresses” or create a subzone for the GW.</p>
Cisco Call Manager	<p>Registering multiple trunks from the same Call Manager is not supported. When trying to register multiple trunks, one of them may be rejected as ‘Insufficient Resources’.</p>

3. Release Notes for TANDBERG Gatekeeper Software Version N3.1

3.1 Introduction

These release notes describe the features and capabilities included in the TANDBERG Gatekeeper software version N3.1 released on 18 July 2005.

3.2 New Feature Overview

N3.1 is a maintenance only release. No new features or functionality are included within this version over the previous release, N3.0.

3.3 Changes and Improvements since previous release

3.3.1 H.225 RAS Signaling

Improved the method used to generate the Endpoint Identifier field within the endpoint registration. The new method will prevent duplicate Endpoint Identifiers from being generated.

Improved Bandwidth Confirmation signaling in order to confirm the absolute bandwidth as presented by the endpoint instead of a rounded value to the nearest 64 kbps. This issue presented itself when connecting to a Polycom MGC.

3.3.2 Software Upgrade

Resolved issue that would not transfer prefix-less remote zones in the upgrade for N2.x to N3.

3.3.3 External Management

Resolved issue that could cause an unexpected system restart upon continuous XML queries.

3.3.4 Links

Resolved issue that would not allow an administrator to rename a link once created.

3.3.5 Inter-Op

Resolved issue that caused the RADVision ViaIP Gateway to report the incorrect gatekeeper IP address.

3.4 Known limitations

Equipment	Limitations
TANDBERG Gatekeeper ver N3.1	The Gatekeeper may show the Start and End times within the Call and Registration Histories as 'Not Set'.
TANDBERG Gatekeeper ver N3.1	If the Gatekeeper loses IP communication with the Border Controller, it will take approximately two minutes for the Gatekeeper to properly re-register to the Border Controller, once communication is restored.

TANDBERG Gatekeeper ver N3.1	If the Gatekeeper is configured with an Alternate list, is configured to not forward LRQs to neighboring Gatekeepers and it receives an LRQ for an endpoint that is not registered directly or with any of the configured alternates, the Gatekeeper may reset.
RADVision L2W Gateway ver 2.2.3.2.5	Due to the signaling coming from the RAD L2W GW, calls will disconnect if it is not registered into its own subzone and the GK is set to indirect mode and registered to a BC. The reason behind this error is because the GW tries to connect a call to itself on a random port it has not registered with. In order to resolve this issue, either place the Gatekeeper into Direct mode for "Calls to Unknown IP Addresses" or create a subzone for the GW.

4. Release Notes for TANDBERG Gatekeeper Software Version N3.0

4.1 Introduction

These release notes describe the features and capabilities included in the TANDBERG Gatekeeper software version N3.0 released on 18 July 2005.

4.2 New Feature Overview

4.2.1 Increased Traversal Capacity

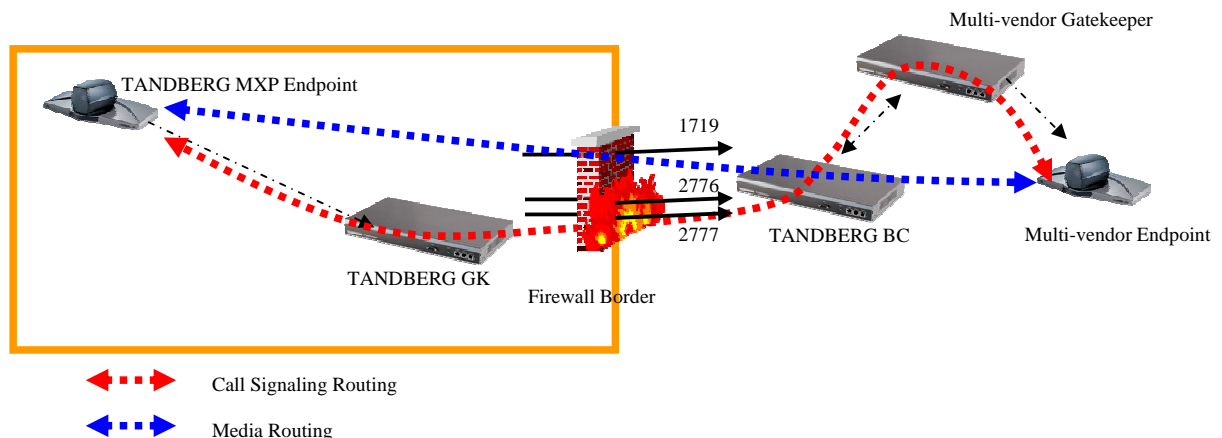
In conjunction with the TANDBERG Border Controller, the TANDBERG Gatekeeper can now support up to 100 simultaneous traversal calls at 384 kbps per call.

4.2.2 Alternate Gatekeeper

The TANDBERG Gatekeeper now supports alternate gatekeeper signaling, as defined within the H.225 standard. Up to five different alternates can be defined within the Gatekeeper itself and, upon registering, the five alternates will be forwarded to the endpoint that is registered. In the event that IP communication is lost with the Gatekeeper, the endpoint will fall back and register to the first alternate that is assigned in the list. If the endpoint is not able to register to the backup Gatekeeper, it will then attempt to register to the tertiary Gatekeeper. This process will then continue until the endpoint properly registers to a Gatekeeper. Once registered with an alternate, the endpoint will then be able to function in a normal manner.

4.2.3 Improved Routing of Media

For traversal calls from an Expressway enabled endpoint, the Gatekeeper can now be configured to allow direct media routing to the TANDBERG Border Controller. In this mode, the call does not count against the traversal call options on the TANDBERG Gatekeeper, thereby increasing the traversal capacity within the Gatekeeper.



4.2.4 Increased Security

The gatekeeper now supports standards-based H.235 Annex D authentication. Once enabled, the gatekeeper will require all endpoints to supply a username and password within all RAS messaging in order to authenticate for registration and call admission. The Gatekeeper can be configured to use one of two different forms of authentication, Local Database and LDAP Authentication.

Within the registration request packet, the endpoint will provide the Gatekeeper with the username, timestamp of the registration and password in hashed format. The MD5 hashing of the password allows for a truly secure authentication.

4.2.4.1 Local Database Authentication

If Local Database Authentication is enabled, the endpoint credentials are stored internally within the Gatekeeper. The credentials, consisting of a username and password, are then verified locally when an endpoint registers to the Gatekeeper. If the credentials from the endpoint match the credentials stored within the internal database on the Gatekeeper, the endpoint is allowed to register. However, if the credentials do not match those that are stored within the internal database, the registration request will be rejected.

4.2.4.2 LDAP Authentication

The Gatekeeper can be configured for LDAP authentication. In this deployment, the endpoint credentials are stored within an external LDAP server. The LDAP server must have the H.235 Identity installed so the Gatekeeper can authenticate properly. LDAP Authentication will also enforce the E.164 alias and the H.323 ID of the endpoint. When configuring the LDAP entry, the fields are:

h235IdentityEndpointID (required)
h235IdentityPassword (required)
h323IdentityDialedDigits (required)
h323IdentityH323-ID (optional)

If an endpoint tries to register to the Gatekeeper, the Gatekeeper will query the LDAP server for the h323IdentityDialedDigits and for the h323IdentityH323-ID (if present) in addition to the authentication credentials. When those values are returned, the Gatekeeper will verify that all information from the LDAP server matches that of the Registration Request from the endpoint. If all entries match, the registration will be confirmed. However, if any of the information in the Registration Request does not match any of the information stored within the LDAP account, the registration will be rejected.

4.2.4.3 Encrypted LDAP Authentication

The Gatekeeper supports two different forms of LDAP Authentication: TLS and LDAPS. If TLS encryption is desired, a valid TLS certificate must be uploaded to both the Gatekeeper and to the LDAP server. The Gatekeeper will then use that TLS certificate to send the query information to the LDAP server in an encrypted form. The Gatekeeper supports RFC 2830 for the TLS encryption.

To configure the Gatekeeper for LDAPS, configure the LDAP port to 636 instead of the default 389 (for unencrypted communication).

4.2.5 Call Processing Language

The Gatekeeper has the ability to support Call Processing Language (CPL), as described in RFC 3880. CPL will give the Gatekeeper the ability to restrict access to resources within the network, such as Gateways. The Gatekeeper supports the ability to accept calls, reject calls and forward calls to a different location. For more detailed information on implementing CPL within the Gatekeeper, please see the Gatekeeper User Manual, document D11381.

4.2.6 Network Modeling

The Gatekeeper now supports the ability to model the H.323 network down to a very granular network. Using network modeling, the administrator of the H.323 network can restrict total and per call bandwidths on a connection-by-connection basis.

4.2.6.1 Subzones

The TANDBERG Gatekeeper now supports defining up to 100 different subzones/network segments. A subzone allows you to define an area within the Gatekeeper that will allow you to define bandwidth characteristics for the endpoints that are registered within. A subzone is not, however, an entirely different gatekeeper zone within the same physical box. Subzones are defined based on the IP subnet of the endpoints that will register into the Gatekeeper.

4.2.6.2 Links

Links are defined within the Gatekeeper in order to model how specific subzones within the same Gatekeeper work together as well as communicate with other zones outside that single Gatekeeper.

4.2.6.3 Pipes

Pipes are used in order to control the call-by-call and total bandwidth used in the different links within the Gatekeeper.

4.2.7 Improved Endpoint Communication

N3.0 of the Gatekeeper software has been designed to improve the call disconnect messaging to all H.323 endpoints in order to provide more information on why calls disconnect, whether on purpose or by unexpected reasons.

4.2.8 Call Logging

The Gatekeeper will now provide call information about the calls that connect to and disconnect from the endpoints that are registered to the local Gatekeeper or routed through the Gatekeeper in a traversal mode. This information can be obtained through the web interface of the Gatekeeper under System Status or through the XML interface of the Gatekeeper.

4.2.9 External Manager

The Gatekeeper now supports external management via XML to an external management system, such as TANDBERG Management Suite. All call logging and event information will be transmitted to the external management system. The external management system can be configured via the API interface on the Gatekeeper by issuing the command: `xconfiguration externalmanager address: <IPAddress>`.

4.2.10 Improved Event Log

The event log for the Gatekeeper has been expanded to include all call processing information in addition to system events that might occur. The event log can also be viewed through the embedded web interface of the Gatekeeper by navigating to *System Status > Event Log*.

4.3 Supplemental Notes to Manuals

4.3.1 Software Versions

The base version of the Gatekeeper will include an option of 25 concurrent total calls, 100 registrations and 5 traversal calls.

The base Gatekeeper options can be expanded by adding total concurrent calls and registrations in increments of either 25 concurrent calls/125 registrations or 50 concurrent calls/250 registrations. These options can be increased up to a total of 200 total concurrent calls.

Expressway Options: The Expressway solution can be expanded by adding traversal calls in increments of either 5 concurrent calls or 10 concurrent calls. The number of traversal calls can be increased up to 100 concurrent calls with this software release. Traversal call options are not in addition to the total concurrent calls.

4.3.2 References/Related Documents

TANDBERG Website – <http://www.tandberg.net>

For all documentation, please see the TANDBERG Support Website at <http://www.tandberg.net/support/documentation.php>.

See the following documents for more information on the TANDBERG Gatekeeper:
 D11381 TANDBERG Gatekeeper User Manual
 D11380 TANDBERG Gatekeeper Installation Sheet

4.3.3 Network Support

The TANDBERG Gatekeeper is an H.323 device and is intended to be connected solely to an Ethernet network. Only the first Ethernet port is used, the other two are for future development. The Ethernet interface on the TANDBERG Gatekeeper supports auto speed and duplex detection as well as manually setting 100Mbit Full/Half Duplex or 10Mbit Full/Half Duplex.

4.3.4 Layer 4 Ports Used

Function	Port	Type	Direction
Gatekeeper RAS	1719	UDP	↔
Gatekeeper Discovery	1718	UDP	↔
SSH (Includes SCP)	22	TCP	↔
Telnet	23	TCP	↔
HTTP	80	TCP	↔
HTTPS	443	TCP	↔
SNMP (Queries)	161	UDP	↔
NTP	123	UDP	↔
Incoming H.323 Call	1720	TCP	↔
LDAP Communication	389	TCP	↔
LDAPS Communication	636	TCP	↔

4.4 Changes and Improvements since previous version

4.4.1 802.3 Issues

Resolved an issue that did not properly force speed and duplex of the 802.3 interface when configured in the web interface or through the API commands.

4.4.2 Allow/Deny List Issues

Increased the size of the “Allow” and “Deny” lists to 1000 entries.

If an endpoint is added to the deny list, the endpoint will now be unregistered from the Gatekeeper upon Time-To-Live expiration.

4.4.3 Call Routing Issues

It is now possible for an endpoint running version 2 or prior of the H.323 stack to call an endpoint running version 4 or later of the H.323 stack through the traversal link.

4.5 Known Limitations

Equipment	Limitations
TANDBERG Gatekeeper ver N3.0	The Gatekeeper may show the Start and End times within the Call and Registration Histories as 'Not Set'.
TANDBERG Gatekeeper ver N3.0	Any remote zones that are configured without a remote zone prefix will not be transferred from the Gatekeeper on an upgrade from N2.x to N3.0. These remote zones will need to be manually entered into the configuration after upgrade.
TANDBERG Gatekeeper ver N3.0	If the Gatekeeper loses IP communication with the Border Controller, it will take approximately two minutes for the Gatekeeper to properly re-register to the Border Controller, once communication is restored.
TANDBERG Gatekeeper ver N3.0	If the Gatekeeper is configured with an Alternate list, is configured to not forward LRQs to neighboring Gatekeepers and it receives an LRQ for an endpoint that is not registered directly or with any of the configured alternates, the Gatekeeper may reset.
Polycom MGC ver 6.03.2 and 7.0.1.11	If there is a conference on the Accord bridge running software version 7.0.1.11 at speeds of 768 kbps or higher and forced to either Transcoding or Continuous Presence and TANDBERG endpoints are present in the conference, all TANDBERG endpoints will connect as 'Secondary' and will not receive or transmit video.

RADVision L2W Gateway ver 2.2.3.2.5	Due to the signaling coming from the RAD L2W GW, calls will disconnect if it is not registered into its own subzone and the GK is set to indirect mode and registered to a BC. The reason behind this error is because the GW tries to connect a call to itself on a random port it has not registered with. In order to resolve this issue, either place the Gatekeeper into Direct mode for “Calls to Unknown IP Addresses” or create a subzone for the GW.
RADVision Gateway ver 3.0.0.12	When registering to the TANDBERG Gatekeeper, the RADVision Gateway will report that it is registered to its own IP address even through it is registered to the TANDBERG Gatekeeper. This is simply a reporting error – all call functionality will work without a problem. This issue will be resolved in the next release.

4.6 Interoperability Testing

The following systems have been tested and verified compatible with this software release.

4.6.1 Gatekeepers

Equipment	Software Revision
RADVision ECS	3.5.2.5
Cisco MCM	12.3(10a)
VCON MXM	4.12.M09.D01.Y04

4.6.2 Gateway Interoperability

Equipment	Software Revision
TANDBERG Gateway	G2.1, G3.0
RADVision gw-P20	3.0.0.12†
RADVision L2W GW	2.2.3.2.5
Polycom MGC 25/50/100	6.03.2, 7.0.1.11

4.6.3 MCU Interoperability

Equipment	Software Revision
TANDBERG MCU	D3.4, D3.5, D3.6
TANDBERG MPS	J1.1, J2.0, J2.1, J2.2
Polycom MGC 25/50/100	6.02.4, 7.0.1.11

RADVision ViaIP MCU	3.5.24•‡
RADVision OnLan MCU	2.2.1.0
Cisco IPVC 3540	3.2.224•‡

4.6.4 Endpoint Interoperability

Equipment	Software Revision
TANDBERG MXP	F1.4, F1.5, F2.5, F2.6, F3.0
TANDBERG 150	L1.1, L1.2
TANDBERG Classic Series	B1.2, B2.4, B3.4, B4.3, B5.1/B5.11, B6.2/E1.2, B7.4/E2.4, B8.4/E3.4, B9.1/E4.1, B10.0/E5.0
Polycom iPower 9000/970	6.1.0.511
Polycom iPower 680	5.3.0.1202
Polycom FX	6.03
Polycom ViewStation	7.5.2
Polycom VSX	7.01, 7.5
Polycom MP512	7.5.2
Polycom SP 384	7.5.2
Polycom ViaVideo	5.1.1.1009
Polycom PVX	6.01.1315
Sony 1600	3.33
Sony 6000	5.02
Sony PCS-1	2.44
VTEL Galaxy	2.2.0.070
Microsoft NetMeeting	3.01
VCON Vpoint	5.10.0160
Aethra VegaStar	5.1.35

4.6.5 Firewall Interoperability

Equipment	Software Revision
Checkpoint Firewall-1	NG with Application Intelligence (R54)
Cisco PIX	6.2(4), 6.3(1), 6.3(3), 6.3(4)
Sonicwall SOHO 3	6.6.0.2
Linksys BEFW11S4	1.44.2
Linksys WRT54G	1.30.7, 1.42.3, 3.01.3
Linksys BEFSR81	2.45.10
Linksys BEFSR41	1.05.00

† Must deselect "IVR Registers with gatekeeper"

• Must register MCU as a Gateway

‡ Must deselect "Register Conference ID"