

TANDBERG

Gatekeeper

Software Release Notes

Software Version N5.2

D50442 revision 1.3

August 2007

TABLE OF CONTENTS

DOCUMENT REVISION HISTORY.....	4
SOFTWARE RELEASE NOTES FOR TANDBERG GATEKEEPER VERSION N5.2	5
Introduction	5
New Features	5
<i>Call Control</i>	5
Changes and Improvements since Previous Version	7
<i>Security</i>	7
<i>RAS Messaging</i>	7
<i>Registration Control</i>	8
<i>Call Control</i>	8
<i>IP Connectivity</i>	8
<i>Usability</i>	8
Known Limitations.....	10
TANDBERG.....	10
Cisco.....	11
RADVISION.....	11
Linksys.....	11
Interoperability Testing	11
<i>Streaming Servers</i>	11
SOFTWARE RELEASE NOTES FOR TANDBERG GATEKEEPER VERSION N5.1	12
Introduction	12
New Features	12
<i>Alias Transforms</i>	12
<i>Zone Alias Transforms</i>	13
<i>ENUM Regular Expression Support</i>	13
<i>CPL Regular Expression Support</i>	13
Changes and Improvements since Previous Version	14
<i>Authentication</i>	14
<i>Call Routing</i>	14
<i>Registrations</i>	14
<i>System</i>	15
<i>Subzones, Links and Pipes</i>	15
<i>Additive Registrations</i>	16
<i>DNS Resolutions</i>	16
<i>Software Upgrade</i>	16
<i>Call Status</i>	16
<i>Interoperability</i>	16
<i>Usability</i>	17
Known Limitations.....	19
TANDBERG.....	19
Cisco.....	20
RADVISION.....	20
Linksys.....	20
Interoperability Testing	21
<i>Gatekeepers/Traversal Servers</i>	21
<i>Gateway Interoperability</i>	21
<i>MCU Interoperability</i>	21
<i>Streaming Servers</i>	22
<i>Endpoint Interoperability</i>	22
<i>Firewall Interoperability</i>	23

RELEASE NOTES FOR TANDBERG GATEKEEPER SOFTWARE VERSION N5.0	25
Introduction	25
New Feature Overview	25
<i>IPv4/IPv6 Support</i>	<i>25</i>
<i>H.460.18/.19 Support</i>	<i>27</i>
<i>Registration Control.....</i>	<i>28</i>
<i>Call Control.....</i>	<i>29</i>
<i>ENUM Support</i>	<i>33</i>
Supplemental Notes to Manuals.....	34
<i>Software Versions</i>	<i>34</i>
<i>References/Related Documents</i>	<i>34</i>
<i>Network Support.....</i>	<i>34</i>
<i>Layer 4 Ports Used.....</i>	<i>35</i>
Changes and Improvements Since Previous Release.....	36
<i>System Registration Improvements</i>	<i>36</i>
<i>Call Control.....</i>	<i>36</i>
<i>Security.....</i>	<i>37</i>
<i>External Manager</i>	<i>37</i>
<i>Usability Improvements</i>	<i>38</i>
<i>System Improvements.....</i>	<i>39</i>
Known Limitations.....	41
<i>TANDBERG.....</i>	<i>41</i>
<i>Linksys.....</i>	<i>42</i>
Interoperability Testing	43
<i>Gatekeepers/Traversal Servers</i>	<i>43</i>
<i>Gateway Interoperability.....</i>	<i>43</i>
<i>MCU Interoperability.....</i>	<i>44</i>
<i>Streaming Servers.....</i>	<i>44</i>
<i>Endpoint Interoperability.....</i>	<i>44</i>
<i>Firewall Interoperability</i>	<i>45</i>

DOCUMENT REVISION HISTORY

Revision 1.3	Release of N5.2, Minor Release
Revision 1.2	Release of N5.1, Minor Release
Revision 1.1	Update to Known Limitations section
Revision 1.0	Release of N5.0, Initial Version

SOFTWARE RELEASE NOTES FOR TANDBERG GATEKEEPER VERSION N5.2

Introduction

These release notes describe the features and capabilities included in the TANDBERG Gatekeeper software version N5.2 released on 3 July 2007.

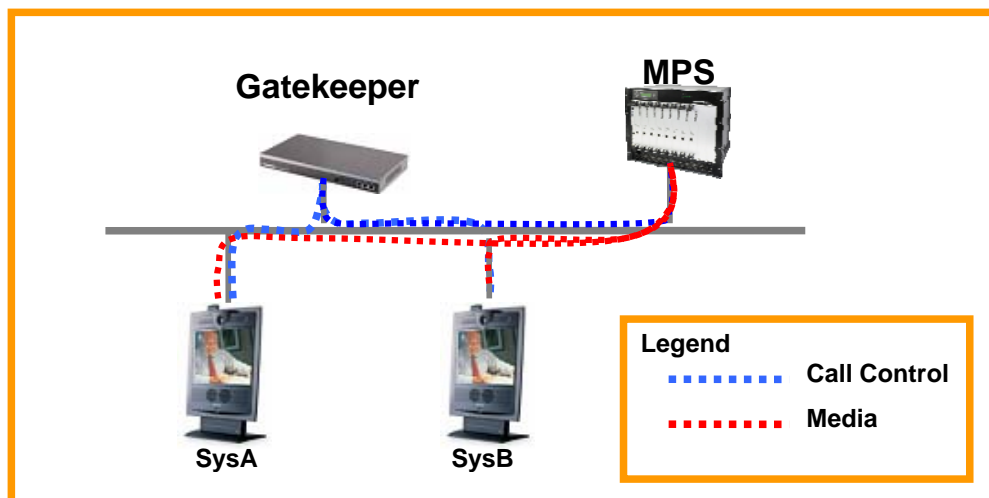
New Features

Call Control

Multiway (Beta)

In conjunction with the TANDBERG MXP endpoints and the TANDBERG MPS, the TANDBERG Gatekeeper now supports MultiWay, a unique ad-hoc conferencing feature for the TANDBERG solution. MultiWay provides automatic escalation of an ongoing conference to an MPS when the existing resources of the endpoint are exhausted. For systems that do not have MultiSite installed, the move to the MPS will happen immediately when a second call connects. For systems with the MultiSite option, the escalation procedure can be administratively configured to occur either to only use the MultiWay option or to use MultiWay after all MultiSite resources has been occupied, which moves the entire MultiSite call to the MPS.

MultiWay on the Gatekeeper can be configured either through the administrative web interface ('Gatekeeper Configuration' > 'Services') or via the API ('xConfiguration Services AdHocConferencing...').



Availability

Available on the TANDBERG Gatekeeper. An option key will be required for this functionality.

Restrictions

Requires TANDBERG MPS J3.2 or later and must be initiated from a TANDBERG MXP Endpoint running F6.0/L5.0 or later software.

The prefixes configured within the gatekeeper must match those of the MPS exactly.

Routed mode must be enabled on the gatekeeper.

Call Transfer Feedback

The TANDBERG Gatekeeper will now send feedback messages any endpoint involved in a call transfer via the H.245 control channel. This feedback will assist with call transfers off of Entrypoint.

Availability

Available on the TANDBERG Gatekeeper.

Restrictions

Routed mode must be enabled on the gatekeeper.

Changes and Improvements since Previous Version

Security

The following minor security issues have been diagnosed within all versions of the gatekeeper and Border Controller software prior to N5.2/Q5.2. If exploited, these issues would not pose a threat to the stability or security of the network; rather, they would cause the gatekeeper and Border Controller to simply reboot and return to normal operation. It is recommended that all customers upgrade to prevent these from occurring.

Invalid Conference and Call Identifiers

The gatekeeper and Border Controller failed to detect an improperly formatted conference id field received within a setup message. This issue would then cause the gatekeeper and Border Controller to restart unexpectedly (resulting in a Denial of Service vulnerability as the system would be unable to continue existing calls or start new ones until the application was restarted). The system will now properly detect, log and discard the invalid setup message, preventing this from occurring.

User-to-User Information Element Processing Errors

An issue within the H.323 implementation that could cause more user-to-user elements to be stored than memory allocated could cause the gatekeeper or Border Controller to unexpectedly restart (resulting in a Denial of Service vulnerability as the system would be unable to continue existing calls or start new ones until the application was restarted). The system will now properly check and discard any information that cannot be properly stored.

Forced Use of Invalid Pointer

A malformed message could cause the gatekeeper or Border Controller to attempt to de-reference an invalid pointer, causing the system to restart unexpectedly (resulting in a Denial of Service vulnerability as the system would be unable to continue existing calls or start new ones until the application was restarted). The system will now properly detect and discard any malformed messages that are received.

Incorrect Processing of Zero Length Alias Strings

The gatekeeper or Border Controller would fail to detect and filter any zero-length alias strings received within an incoming message, causing the system to restart unexpectedly (resulting in a Denial of Service vulnerability as the system would be unable to continue existing calls or start new ones until the application was restarted). The system will now properly detect any zero-length alias strings and discard them as appropriate.

Upgrade Access

Previous to version N5.2, one could access the administrative interfaces of the gatekeeper without a password for the first three seconds after the first of two reboots. This access will no longer be permitted.

RAS Messaging

Unallocated Sequence Number

The gatekeeper will no longer restart unexpectedly when it receives a RAS response with an unallocated sequence number.

Registration Control

Registration Keep Alive

The gatekeeper will now verify the 'endpointIdentifier' of incoming responses to Information Requests during registration keep alive. If the identifier within the response does not match that which is stored in the local registration database, the gatekeeper will consider that registration different and require a full registration.

H.460.18 Traversal Client Registration

The gatekeeper will now return an SCR with a failed code in the case where it fails to authenticate an incoming SCI sent as a gatekeeper request.

Registration Socket Handling

During extremely heavy load, the gatekeeper could stop responding to incoming registration requests. This issue has been resolved.

Call Control

Call Transfer

Improvements were made to the call transfer mechanism within the gatekeeper to prevent a failed transfer when one of the sites involved initiated a disconnect event at the time of the transfer.

Prefix Matching

Improvements were made to the prefix matching portion of call routing. These changes will prevent the call from routing to the incorrect registration.

IP Connectivity

IPv6

If the gatekeeper is configured for dual IPv4 and IPv6 networks, but is not configured within an IPv6 address, media forwarding problems could result with software versions previous to N5.2. Those issues have now been resolved.

Usability

Transforms

- Number of Transforms

The number of possible transforms has been increased from 100 to 200.

- Configuration of Transforms

If a transform is configured to replace text and, subsequently, is reconfigured to strip text, the replace text was visible within previous versions. This text will no longer be visible.

Telnet/SSH Session Release

The gatekeeper will now properly release any active telnet sessions that are disconnected without properly sending an 'EOF' release command.

Ethernet Status

The gatekeeper will now display the speed and duplex of the Ethernet connection under 'System Status' > 'System Information' on the administrative web interface.

Syslog

- Transforms

Alias transforms are now printed within a syslog level 2 and above.

- Lightweight RRQs

Lightweight registration requests (LWRRQs) are now only visible within syslog level 3.

Zone Configuration

The 'Replace' field will no longer be displayed within the web configuration of a remote zone unless 'Pattern Match' is chosen.

Web Management

The encryption status of the software build (e.g. whether the loaded software build includes AES encryption or not) is now displayed under 'System Status' > 'System Information.'

Known Limitations

TANDBERG

Equipment

TANDBERG Gatekeeper ver N5.2

Limitations

If the gatekeeper is ever set back to default values using the 'xCommand DefaultValueSet Level(r): <1..3>' command, the system will not automatically add the default links back into the configuration. In order to add the default links, issue the command 'xCommand DefaultLinksAdd'.

TANDBERG Gatekeeper ver N5.2

Within the registration status, the gatekeeper will always report the connection in which the RAS traffic uses for communication within the 'rasAddress' field, rather than the address specified within the RAS messages themselves. This is normal operation as the gatekeeper will always use the established RAS connection for communication with the endpoint.

TANDBERG Gatekeeper ver N5.2

If an IP gateway is not available for the IP network in which the system is installed, the gatekeeper must be configured with a non-occupied, valid IP address on the subnet.

TANDBERG Gatekeeper ver N5.2

Due to a limitation within RAS messaging, an endpoint that supports an IPv4/IPv6 hybrid configuration will not be able to register to the TANDBERG Gatekeeper with both an IPv4 and IPv6 call signaling address. This is due to the fact that only one call signaling address can be transmitted within the 'callSignalingAddress' field of any RAS message, thereby limiting the endpoint to only specifying either the IPv4 or IPv6 address when registering to the gatekeeper.

TANDBERG Gatekeeper ver N5.2

If connecting to the gatekeeper web interface using the DNS host name of the box and both HTTPS and session timeouts are enabled, the gatekeeper will not permit full login to the administrative interface. It is recommended that the IP address is used when the box is installed with this configuration as the issue is not present when using IP addressing.

TANDBERG Gatekeeper ver N5.2

If a gatekeeper running N5.0 software is downgraded to N4.1 software, remote zones may not be transferred correctly back to N4.1.

TANDBERG Gatekeeper ver N5.2

The TANDBERG Gatekeeper will always report TCP port 1720 for the destination call signaling port, regardless of what port is actually used. This report is sent over XML to an external management system (e.g. TANDBERG Management Suite)

TANDBERG Gatekeeper ver N5.2

If an incoming registration is received on port 65535, the gatekeeper will reject the registration as 'invalidRasAddress'. This will be improved in a later version.

TANDBERG Management Suite ver 11.6 and later

If 'Session time out' is enabled, TMS 11.1 will not be able to control the gatekeeper.

Cisco

Equipment

Cisco Call Manager

Limitations

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'.

RADVISION

Equipment

RADVISION L2W Gateway ver 2.2.3.2.5

Limitations

Due to the signaling coming from the RADVISION 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.

Linksys

Equipment

Linksys WRT54G hardware version 5

Limitations

Linksys Router WRT54G hardware version 5 appears to change the source ports of outbound connections opened for a prolonged period of time. As such, H.323 calls that are made from or to systems registered to either a gatekeeper or Border Controller behind this router will disconnect at random times. This issue has been presented to Linksys.

Interoperability Testing

Streaming Servers

Equipment	Software Revision	H.460.18/.19	Comments
TANDBERG Content Server	S2.2, S2.1, S2.0	Yes	S2.x supports H.460.19 multiplexed media.

SOFTWARE RELEASE NOTES FOR TANDBERG GATEKEEPER VERSION N5.1

Introduction

These release notes describe the features and capabilities included in the TANDBERG Gatekeeper software version N5.1 released on 1 December 2006.

New Features

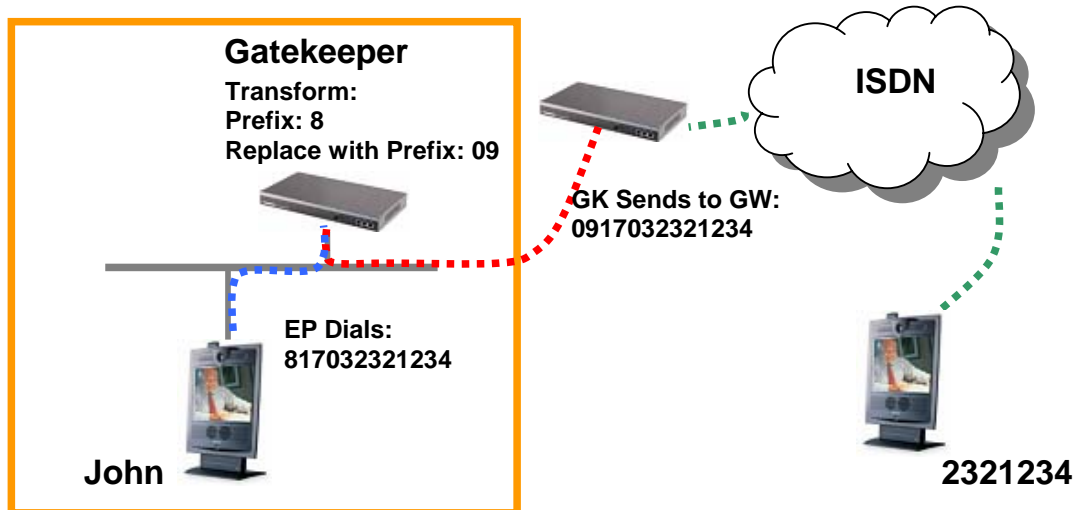
Alias Transforms

The TANDBERG Gatekeeper now supports the ability to transform an alias prior to attempting to connect the call through the normal call search mechanisms. Once the transforms are completed, the gatekeeper will perform the alias resolution as it normally would.

Aliases can be transformed using one of three different methods (prefix, suffix or regular expressions) giving the administrator complete control over call routing on the gatekeeper.

Prefix

Upon matching the pattern configured, the system can either strip or replace the prefix with another matching string to provide complete control over a network dial plan, including case-based digit manipulation (e.g. change the incoming dial string of 097035553030 to 817035553030 for gateway call routing).



Suffix

Similar to prefix, the suffix match allows the administrator to strip or replace the pattern match on the suffix of a call request (e.g. change the incoming dial string of 7035551313@tandbergusa.com to 7035551313@tandberg.net for continuity among DNS suffixes).

Regular Expression

Governed by RFC 3880¹, Regular Expressions allows the administrator to match and replace any portion of the incoming call expression in order to perform more complex operations on the call address to be called (e.g. an incoming pattern of “^9(.+)” can be replaced with “\1@tandberg.net”, which will match all incoming calls beginning with a prefix of ‘9’, strip the prefix and append @tandberg.net at the end of the call).

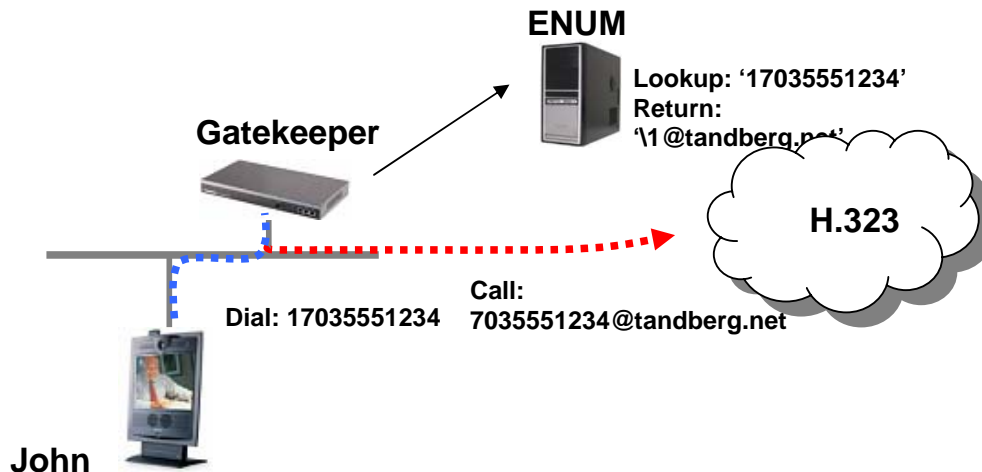
Zone Alias Transforms

The same transformations that can be applied globally to the gatekeeper can also be applied to the remote zones prior to sending any call requests to these zones. The zone configuration has been expanded to now include a ‘Replace’ selection under ‘Pattern Match’, allowing the outgoing call request to be manipulated prior to transmission.

Additionally, Regular Expressions have been added to the remote zone configuration to provide the administrator complete control over the call routing.

ENUM Regular Expression Support

ENUM support within the gatekeeper has been expanded to allow the return of Regular Expressions instead of explicit expressions, allowing an administrator to simplify the ENUM server setup. Through regex, the administrator is able to significantly reduce the number of entries to the ENUM directory by allowing the digits from the incoming call request to be dynamically used in the final URI routing.



CPL Regular Expression Support

CPL has also been modified within the gatekeeper to allow regex within the CPL code, allowing for a simplified call model when developing CPL scripts.

¹ For more information on RFC 3880, please consult the IETF document on the standard.

Changes and Improvements since Previous Version

Authentication

The number of authentication credentials that can be stored locally on the gatekeeper has been expanded to 2500, the maximum number of registrations of the gatekeeper.

Call Routing

Destination Alias

If the gatekeeper received a call setup message for a specific address (e.g. the IP address of the gatekeeper) and, through RAS messaging, the address was resolved to a different alias (e.g. the alias configured within the 'Fallback Alias' configuration setting), the gatekeeper will now ensure that the address presented within the forwarded call setup message is the resolved alias rather than the first address presented within the original call setup message. This is needed in order to ensure the call is routed properly by the receiving endpoint.

ENUM

The gatekeeper will now properly strip 'h.323:' if returned from an ENUM lookup.

CPL

The gatekeeper will no longer restart if the following CPL is run:

```
<location clear="yes" url="">
```

LCF Messaging

The gatekeeper will no longer provide the 'versionID' and 'enterpriseNumber' within a Location Confirm.

H.245 Signaling

When under heavy load and in routed mode, the gatekeeper could possibly miss a roundTripDelay message sent between the two endpoints involved in the call. This would then cause the call to end unexpectedly. This issue has been resolved.

H.460.18/19 Multiplexed Media Call Connectivity

The process used to establish the media channels in a multiplexed media call has been improved to reduce the amount of time it takes for the channels to be established.

Large Numbers of Aliases

Previously, the gatekeeper would not send call requests to neighboring gatekeepers/Border Controllers if the incoming call request had a large number of source aliases. This has been resolved.

Registrations

Special Characters

The gatekeeper will now properly handle any registrations with the characters 'r', 'n', '1' or similar.

Long Aliases

The gatekeeper will no longer truncate aliases longer than 30 characters.

RAS Addressing

If, during a registration, the RAS address changes from one that matches a registered Call Signaling Address to one that does not (or vice versa), the gatekeeper could previously restart unexpectedly. This will no longer occur.

Unregistration

Previously, if a system registered with multiple aliases unregistered one of the configured aliases, the gatekeeper could restart unexpectedly. This issue has been resolved.

Authentication Messaging

When authentication is enabled on a gatekeeper and an incoming GRQ does not present authentication capabilities, the gatekeeper will now respond with the reject reason of 'securityDenial' instead of a blank reason as it did previously.

H.460.18/.19 Traversal Zone Authentication

The gatekeeper will now send authentication credentials to the traversal server in H.460.18/.19 mode, regardless of the authentication settings on the local system.

System

RAS Responses

The gatekeeper will no longer unexpectedly restart if the response to an outbound Location Request (same sequence number) is received from a different address than it was originally sent.

System Responsiveness

The gatekeeper will no longer become unresponsive if the system is under an extremely heavy RAS load for an extended period of time.

The gatekeeper will no longer become unresponsive after a significant amount of call requests that contain significant amount of source aliases.

Subzones, Links and Pipes

Link Creation

The Link Creation mechanism within N5.1 has been improved to prevent the possibility for corrupt links being created after the upgrade from software versions previous to N5.0 or the creation of a Traversal Zone.

The gatekeeper will no longer allow the administrator to create two different links with the same nodes, thus creating a call routing conflict.

Subzone, Link and Pipe Naming

If a subzone, link or pipe was renamed and the gatekeeper was restarted, the name change would not be restored after startup due to the gatekeeper persisting the names that were previously configured. This is no longer the case and all name changes will now be persisted correctly within the configuration.

Additive Registrations

The gatekeeper will now properly confirm back the 'additiveRegistration' field within the RCF upon receiving an incoming additive registration.

DNS Resolutions

When resolving an A-record, the gatekeeper will now confirm back the correct port, 1720 TCP, instead of a previously incorrect random port.

Software Upgrade

Software Upload

The software upgrade mechanism has been improved to ensure that the entire .tar.gz file has been fully uploaded prior to attempting the extraction and installation of the package.

Software Integrity Check

The gatekeeper will now verify the software file uploaded to the gatekeeper is valid before attempting to install the new version.

Software Upgrade Progress Reporting

The software upgrade mechanism has also been improved to remove the potential for the status (as observed within an API session) to be displayed twice. Previously, the upgrade status would appear similar to:

```
Software upgrade in progress!  
Software upgrade in progress!  
[           ]  
[           ]  
[ *         ]  
[ *         ]  
[ **        ]  
[ **        ]  
[ ***       ]  
[ ***       ]
```

Call Status

The system has been improved to prevent a system restart when call status is reviewed in very specific scenarios. One of these scenarios includes registering two systems to the gatekeeper, making a call between them, unregistering one of the systems from the gatekeeper and viewing the detailed call status of the active call between the two systems.

Interoperability

RADVISION

The interoperability with the RADVISION ViaIP Gateway has been improved to now allow telephone calls through.

Usability

Registration and Call Status/History

The gatekeeper history has been improved to ensure that all data is now recorded correctly. Previously, the gatekeeper would rarely record a corrupted alias within the first leg of the call segment, causing the history to not be displayed correctly within the web interface.

The gatekeeper will no longer report calls up between endpoints that have been disconnected for a prolonged period of time.

The call status details as viewed from within 'Status' > 'Non-traversal calls' or 'Traversal calls' will now show the correct call status if a call is connected between viewing the status page and the details of a specific call.

Web-based User Interface

The 'TraversalZone' will no longer show up in the web-based user interface as this node is no longer valid within the system.

The colors and text presented within the H.460.18 Traversal Zone configuration have been improved and normalized with the rest of the web user interface.

The sort functionality within the web interface has been improved such that it considers both capital and lowercase letters of the same weight.

Telnet/SSH/API User Interface

Upon initiating a telnet/SSH API session to the gatekeeper, the system name is presented for login. Previously, however, if there was a space between different words of the system name, the entire system name would not be presented. This has been corrected.

The gatekeeper will now properly report the source and destination address information within the API interface when viewing the status through either the command 'xStatus Calls' or the status.xml document present on the gatekeeper.

The feedback reported upon issuing the 'xgetxml' command has been improved when the command is misused.

The 'xCommand Dial' API command has been improved to default to non-encrypted calls when issued on the non-AES version of the gatekeeper software.

The traversal configuration commands have been restored to the API control interface:

```
xConfiguration Traversal UDPProbe RetryInterval: 2
xConfiguration Traversal UDPProbe RetryCount: 5
xConfiguration Traversal UDPProbe KeepAliveInterval: 20
xConfiguration Traversal TCPProbe RetryInterval: 2
xConfiguration Traversal TCPProbe RetryCount: 5
xConfiguration Traversal TCPProbe KeepAliveInterval: 20
xConfiguration Traversal Media RTP Port: 2776
xConfiguration Traversal Media RTCP Port: 2777
xConfiguration Traversal AssentEnabled: On
xConfiguration Traversal H46018Enabled: On
xConfiguration Traversal Preference: H46018
xConfiguration Traversal H46019Demultiplexing: Off
```

Syslog

The number of hop counts present within an LRQ will now be present within a syslog, level 2.

Known Limitations

TANDBERG

Equipment

TANDBERG Gatekeeper ver N5.1

Limitations

If the gatekeeper is ever set back to default values using the 'xCommand DefaultValueSet Level(r): <1..3>' command, the system will not automatically add the default links back into the configuration. In order to add the default links, issue the command 'xCommand DefaultLinksAdd'.

TANDBERG Gatekeeper ver N5.1

Within the registration status, the gatekeeper will always report the connection in which the RAS traffic uses for communication within the 'rasAddress' field, rather than the address specified within the RAS messages themselves. This is normal operation as the gatekeeper will always use the established RAS connection for communication with the endpoint.

TANDBERG Gatekeeper ver N5.1

If an IP gateway is not available for the IP network in which the system is installed, the gatekeeper must be configured with a non-occupied, valid IP address on the subnet.

TANDBERG Gatekeeper ver N5.1

Due to a limitation within RAS messaging, an endpoint that supports an IPv4/IPv6 hybrid configuration will not be able to register to the TANDBERG Gatekeeper with both an IPv4 and IPv6 call signaling address. This is due to the fact that only one call signaling address can be transmitted within the 'callSignalingAddress' field of any RAS message, thereby limiting the endpoint to only specifying either the IPv4 or IPv6 address when registering to the gatekeeper.

TANDBERG Gatekeeper ver N5.1

If connecting to the gatekeeper web interface using the DNS host name of the box and both HTTPS and session timeouts are enabled, the gatekeeper will not permit full login to the administrative interface. It is recommended that the IP address is used when the box is installed with this configuration as the issue is not present when using IP addressing.

TANDBERG Gatekeeper ver N5.1

If a gatekeeper running N5.0 software is downgraded to N4.1 software, remote zones may not be transferred correctly back to N4.1.

TANDBERG Gatekeeper ver N5.1

The TANDBERG Gatekeeper will always report TCP port 1720 for the destination call signaling port, regardless of what port is actually used. This report is sent over XML to an external management system (e.g. TANDBERG Management Suite)

TANDBERG Gatekeeper ver N5.1

If an incoming registration is received on port 65535, the gatekeeper will reject the registration as 'invalidRasAddress'. This will be improved in a later version.

TANDBERG Management Suite ver 11.6 and later

If 'Session time out' is enabled, TMS 11.1 will not be able to control the gatekeeper.

Cisco

Equipment

Cisco Call Manager

Limitations

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'.

RADVISION

Equipment

RADVISION L2W Gateway ver 2.2.3.2.5

Limitations

Due to the signaling coming from the RADVISION 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 GK. 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.

Linksys

Equipment

Linksys WRT54G hardware version 5

Limitations

Linksys Router WRT54G hardware version 5 appears to change the source ports of outbound connections opened for a prolonged period of time. As such, H.323 calls that are made from or to systems registered to either a gatekeeper or Border Controller behind this router will disconnect at random times. This issue has been presented to Linksys.

Interoperability Testing

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

Gatekeepers/Traversal Servers

<i>Equipment</i>	<i>Software Revision</i>	<i>H.460.18/.19²</i>	<i>Comments</i>
TANDBERG Gatekeeper	N1.0, N2.1, N3.2, N4.1	No	
	N5.0, N5.1	Yes	
TANDBERG Border Controller	Q1.0, Q2.1	No	
	Q3.1, Q5.0, Q5.1	Yes	Q3.x does not support multiplexed media.
Cisco MCM	12.3(10), 12.3(10a)	No	
Polycom PathNavigator	7.00.03	No	
Polycom V2IU	6.1.6	Yes	
RADVISION ECS	4.1.0.0	No	

Gateway Interoperability

<i>Equipment</i>	<i>Software Revision</i>	<i>H.460.18/.19</i>	<i>Comments</i>
TANDBERG Gateway	G1.0, G2.1, G3.1	No	
TANDBERG 3G Gateway	R1.0, R2.0	No	
TANDBERG Video Portal	V2.0	No	
Cisco CallManager	4.1	No	
Ezenia Encounter 3000	2.0	No	
Polycom MGC 25/50/100	7.5.0.52	No	
RADVISION gw-P20	4.0	No	

MCU Interoperability

<i>Equipment</i>	<i>Software Revision</i>	<i>H.460.18/.19</i>	<i>Comments</i>
TANDBERG MCU	D2.3, D3.9	No	
TANDBERG MPS	J1.2, J2.4, J3.1, J3.2	No	

² This section of the tables denotes whether the device supports H.460.18/.19 firewall traversal natively (e.g. without the use of an H.460.18/.19 client gatekeeper).

Cisco IPVC 3540	4.2.10	No
Codian MCU 4210	1.4(1.6)	No
Polycom MGC 25/50/100	7.5.0.52	No
RADVISION Scopia MCU	5.0.0.0.58	No
RADVISION VialP	4.0.31	No

Streaming Servers

<i>Equipment</i>	<i>Software Revision</i>	<i>H.460.18/.19</i>	<i>Comments</i>
TANDBERG Content Server	S1.0, S1.1, S2.0	No	

Endpoint Interoperability

<i>Equipment</i>	<i>Software Revision</i>	<i>H.460.18/.19</i>	<i>Comments</i>
TANDBERG MXP	F1.7, F2.5, F3.4	No	F4.x does not support multiplexed media.
	F4.1, F5.0, F5.2	Yes	
TANDBERG 150 MXP	L1.2, L2.2, L3.1	No	L4.x does not support multiplexed media.
	L4.0	Yes	
TANDBERG Classic	B1.3, B2.4, B3.4, B4.4, B5.1/B5.11, B6.3/E1.3, B7.4/E2.4, B8.4/E3.4, B9.2/E4.2, B10.2/E5.2	No	
Aethra VegaStar	4.69	No	
Cisco VT Advantage	1.0(2)	No	The endpoint was tested in conjunction with an H.225 trunk from Cisco CallManager to a TANDBERG Gatekeeper.
LifeSize Room	2.0.0(15)	No	
Microsoft NetMeeting	3.01	No	
Polycom EX	6.0.5	No	
Polycom FX	6.0.5	No	
Polycom iPower 680	6.2.0.1208	No	
Polycom iPower 9000/970	6.2.0.1208	No	
Polycom PVX	8.0.2	No	

Polycom ViaVideo	5.1.1.1009	No	
Polycom ViewStation, MP512, SP384	7.5.4	No	
Polycom VSX	8.0.3	No	
	8.5	Yes	Version 8.5 does not support multiplexed media.
Polycom V-series	8.0.3	No	
	8.5	Yes	Version 8.5 does not support multiplexed media.
Sony PCS-1	3.22	No	
Sony PCS-TL50	2.21	No	
VCON VPoint	6.50.0064	No	
VTEL Galaxy	2.2.0.070	No	

Firewall Interoperability

<i>Equipment</i>	<i>Software Revision</i>	<i>H.460.18/.19</i>	<i>Comments</i>
Check Point NGX	R60	No	Due to some of the new signaling required by the H.460.18/.19 standard, H.323 awareness on the Check Point firewall can cause calls to fail. It is recommended that all H.323 awareness is disabled.
Cisco PIX	6.3(3), 6.3(4), 7.0(1), 7.0(4)	No	Due to some of the new signaling required by the H.460.18/.19 standard, H.323 fixup/inspect on the PIX firewall can cause calls to fail. It is recommended that all H.323 awareness is disabled.
DLink DI-514	1.03	No	
DLink DI-604	1.07DDM	No	
Juniper NetScreen SSG 550	5.4.0r1.0	No	Due to some of the signaling required by the H.460.18/.19 and Assent signaling protocols, H.323 awareness can cause calls to fail. It is recommended that all H.323 awareness is

disabled.

Linksys BEFW11S4	1.50.14	No
Linksys WRT54G (v1)	4.02.7	No
Linksys WRT54G (v4)	DD-WRT v23	No
Linksys WRT54GL (v3)	4.30.5	No
Linksys WRT54GR	1.01	No
Linksys WRT54GS	4.70.6	No
NetGear N314	V3.29(CF.0)b1	No

RELEASE NOTES FOR TANDBERG GATEKEEPER SOFTWARE VERSION N5.0

Introduction

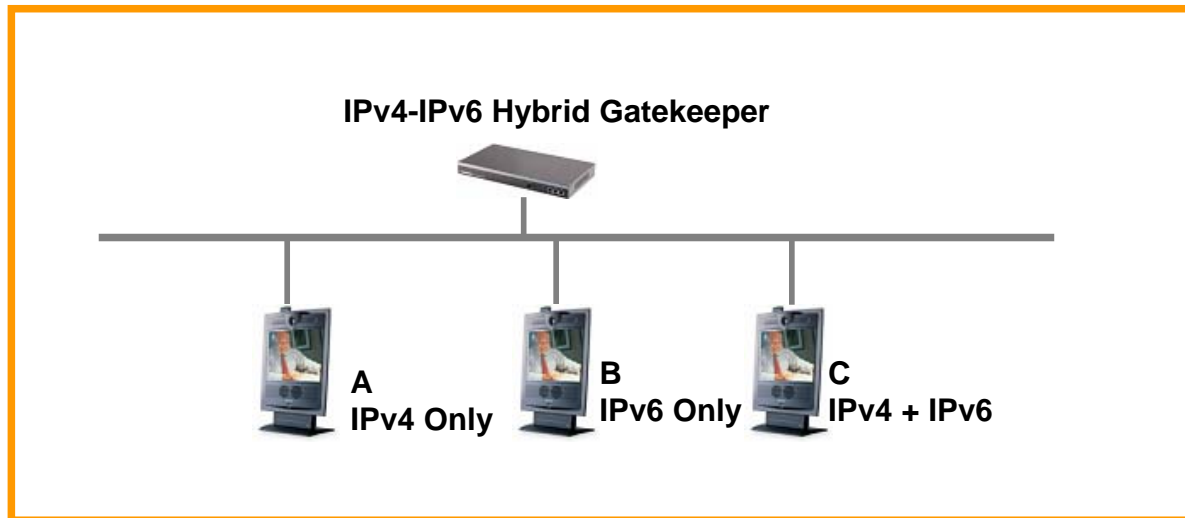
These release notes describe the features and capabilities included in the TANDBERG Gatekeeper software version N5.0 released on 17 July 2006.

New Feature Overview

IPv4/IPv6 Support

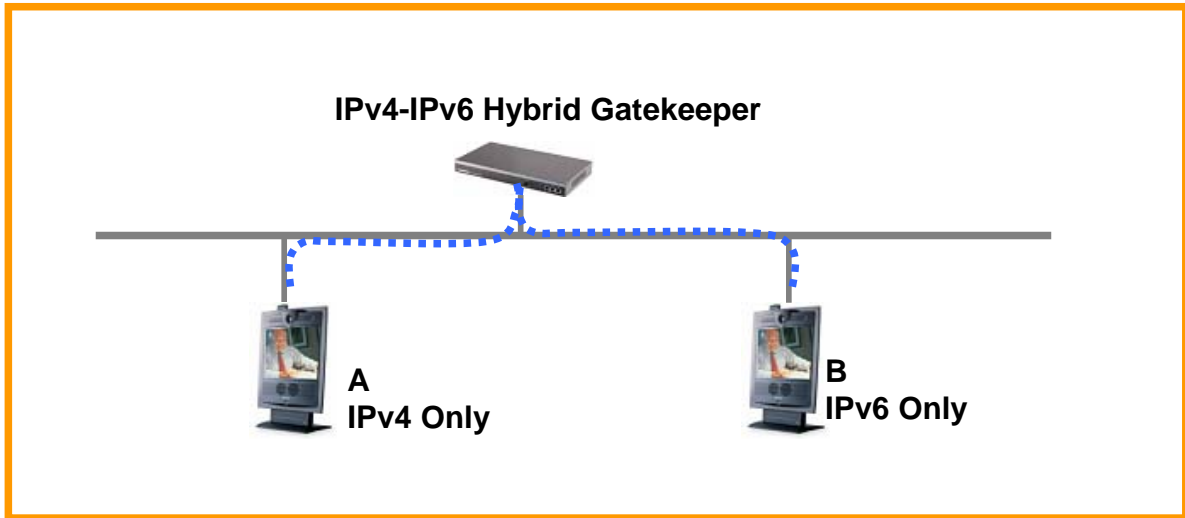
IPv4/IPv6 Hybrid Networks

The TANDBERG Gatekeeper has expanded the IPv6 network support, allowing for the configuration of IPv4-IPv6 hybrid in addition to the previously available IPv4 only and IPv6 only network configuration. When the system is setup for a hybrid configuration, the gatekeeper will support all types of endpoints to register and make calls.



IPv4-to-IPv6 Translation Services

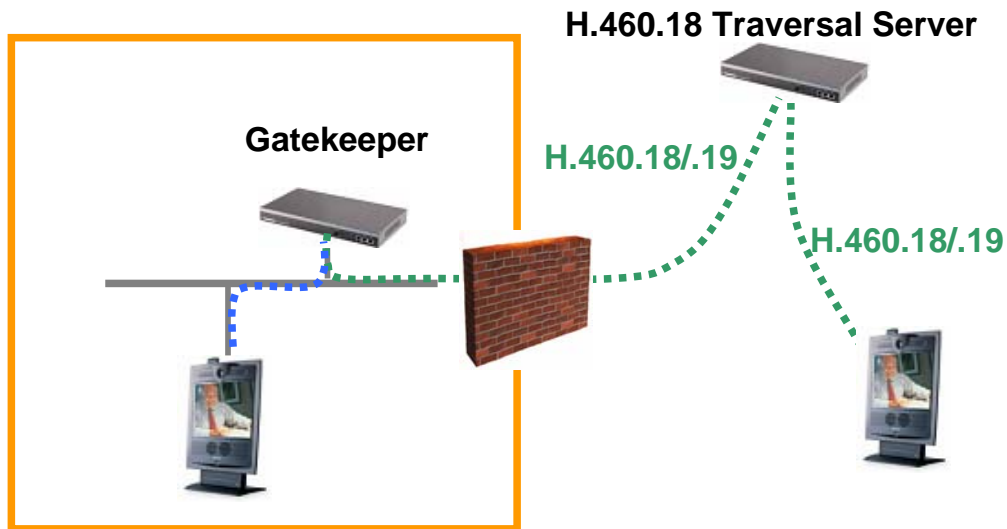
Additionally, when configured for a hybrid network, the gatekeeper can serve as a translation gateway between the two IP protocols, allowing IPv4 only endpoints and IPv6 only endpoints to communicate with each other as if they were using the same protocol. When translating between the two protocols, the gatekeeper will communicate with each endpoint in its native protocol, not requiring any further interaction from the end user.



H.460.18/19 Support

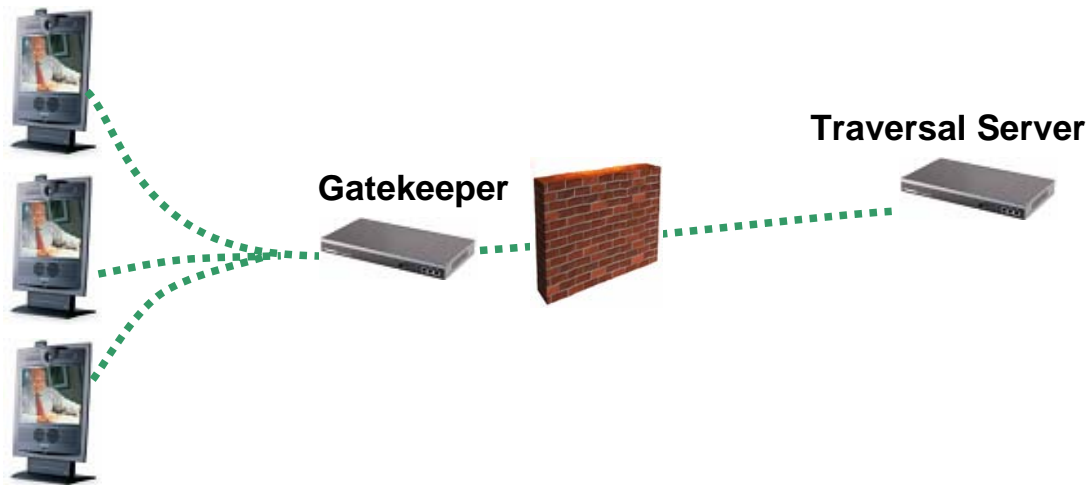
H.460.18 Client Gatekeeper Support

The TANDBERG Gatekeeper can now act as an H.460.18/19 proxy for systems that are registered internal to a firewall, providing the traversal technology to the traversal server on their behalf. Similar to the role that the gatekeeper would play using the Assent technology, the H.460.18/19 proxy functionality will provide the same benefits for traversing the local firewall as the endpoint registered directly with the traversal server.



H.460.19 Multiplexed Media

In conjunction with an H.460.19 traversal server, the TANDBERG Gatekeeper supports H.460.19 multiplexed media, allowing all media between the proxy and the client to be condensed to a limited number of ports. When combined with the TANDBERG Border Controller in H.460.18/.19 mode, all media will be transmitted and received on ports 2776 and 2777 UDP on the Border Controller. When combining the proxy functionality with third party servers, however, the ports utilized for media traversal are dictated by the traversal server directly.



Registration Control

Increased Capacity

The gatekeeper can now support up to 2500 registrations. This increase makes the gatekeeper more of a scalable solution for a larger install base.

Additive Registration Support

The TANDBERG gatekeeper now supports additive registrations from registered systems. Additive registrations allow a system to add, modify or remove registered aliases and/or prefixes without requiring a full un-registration and re-registration of the endpoint. These changes can then affect the call routing logic of the gatekeeper to ensure calls will always be routed to the appropriate system.

H.235 Enforced Dial Plan

The H.235 authentication mechanism can now be used to provide alias control to the endpoints. The three different available options on the gatekeeper will affect this behavior.

- LDAP Alias Origin

When the 'Alias Origin' is configured for 'LDAP', the gatekeeper will rely on the aliases provided from the LDAP server as the only aliases available for the endpoint. In this setup, the gatekeeper, within the Registration Confirm RAS message, will only confirm back the aliases that are returned from the LDAP server within the account lookup, requiring the endpoint to then comply with the new aliases. This scenario creates a central management system for endpoint aliasing, removing the possibility that an invalid configuration of the endpoint would cause a failure in connectivity within the network.

- Endpoint Alias Origin

If 'Alias Origin' is configured for 'Endpoint', the gatekeeper will ignore all aliases configured within the LDAP endpoint account and will only use the aliases presented by the endpoint within the Registration Request RAS message for call routing purposes.

- Combined Alias Origin

In 'Combined' mode, the gatekeeper will use both the aliases configured within the LDAP system account as well as those presented by the endpoint upon initiation of the registration for call routing.

Registration Location

Through the local API, the gatekeeper can be used to ensure that an endpoint is properly registered into a network. When the 'xCommand Locate' command is used, the gatekeeper will perform lookups on both the local registration table as well as through all remote and traversal zones using the same call routing logic it would to connect a call to locate the endpoint on the network.

Example

```
xcommand locate alias: 50196 hopcount: 255

*r Result (status=OK):
  Alias: "50196"
  HopCount: 255
  CallSerialNumber: 166
*r/end
```

Internationalization Support

To increase the international usability of the H.323 network, support for Unicode (UTF-8) character sets within registrations has now been included in the TANDBERG Gatekeeper software. This feature set will allow for endpoints to register with any international character within the UTF-8 character set.

Call Control

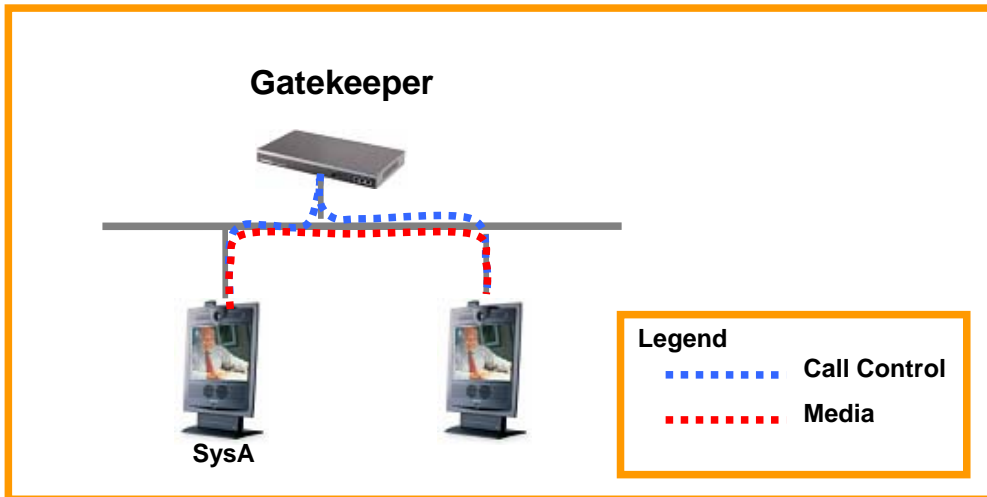
Increased Capacity

The gatekeeper now supports up to a total of 500 active concurrent calls within the N5.0 software release. all calls within the gatekeeper are fully featured without any negative impact to the capacity of the system.

Note: there is no increase to the traversal capacity within this release.

Routed Mode

In order to provide advanced functionality to the administrator, such as accurate and reliable call detail records, the TANDBERG Gatekeeper now supports the ability to route all call control. When enabled, this mode will route all H.225/Q.931 call setup and H.245 call control media through the gatekeeper, rather than directly to the endpoints as it would previously. Routed mode will not have any detrimental effect on the call capacity of the gatekeeper.



Ad-Hoc Dial-in

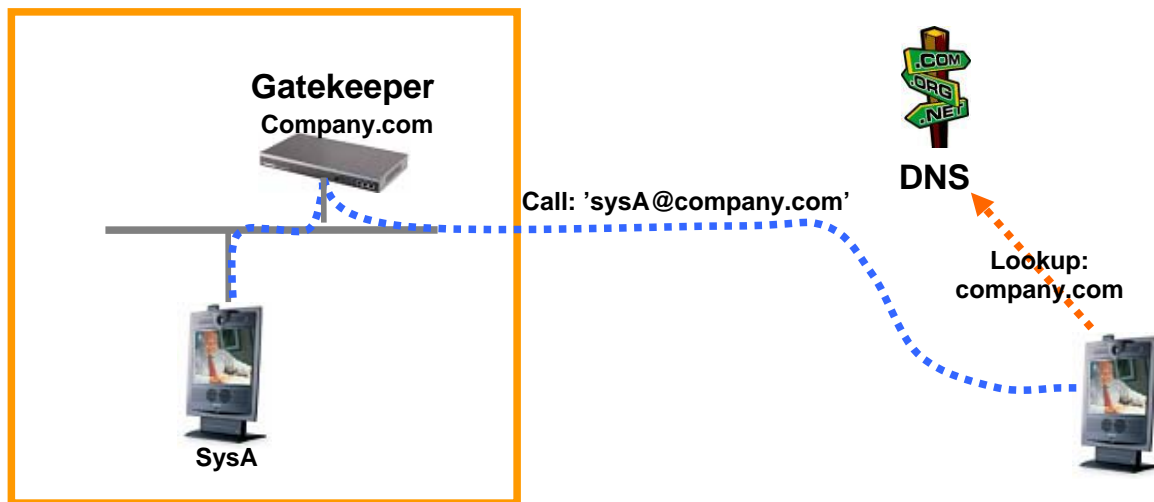
One of the challenges of implementing firewall traversal on an H.323 network is the loss of ad-hoc communication from stand-alone endpoints not registered to the H.323 network to those behind the firewall traversal. This has been overcome in the past through URI dialing between H.323 islands; however, the need still exists for endpoints not associated with any specific H.323 island to dial into the network.

- Unregistered URI Dialing

In previous versions the gatekeeper supported the ability to locate a remote H.323 island through the use of an SRV record for that island’s domain name. However, isolated endpoints that are not registered to any type of an H.323 island cannot take advantage of this location service to connect to remote endpoints.

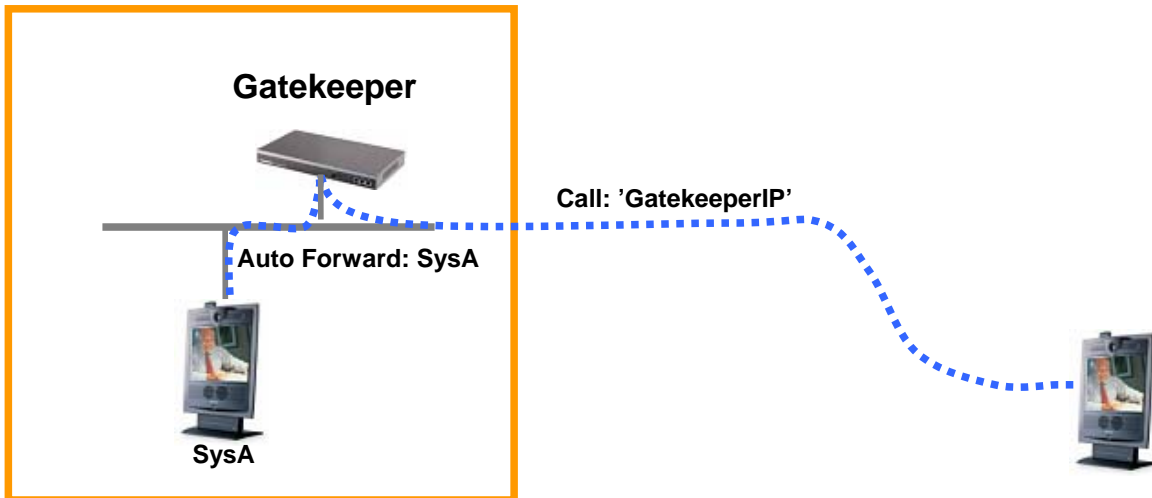
The gatekeeper now supports an additional SRV record – one that an endpoint can directly look up and locate a remote H.323 island. The ‘_h323cs._tcp.<domain>’ service record has been established for these isolated endpoints. To perform this type of a call, the unregistered endpoint will then dial the full URI of the far end system, just as it would if it were registered to a gatekeeper that will perform the URI lookup on the endpoint’s behalf. Upon attempt to connect the call, the endpoint will query its locally configured DNS server for the call setup SRV record. Once resolved, the endpoint will then establish an H.225 setup connection to the remote H.323 island to which the endpoint resolves the domain; at which point the receiving gatekeeper or gatekeeper will then look through the network to pinpoint the alias dialed within the URI string.

For example, if an endpoint dials ‘systemA@company.com’, it will send the setup message to the main gatekeeper or gatekeeper at the ‘company.com’ domain. Upon receipt of the call, the system will then look for system ‘systemA’ as it is the endpoint that is being called. Once ‘systemA’ is resolved, the call would connect as normal.



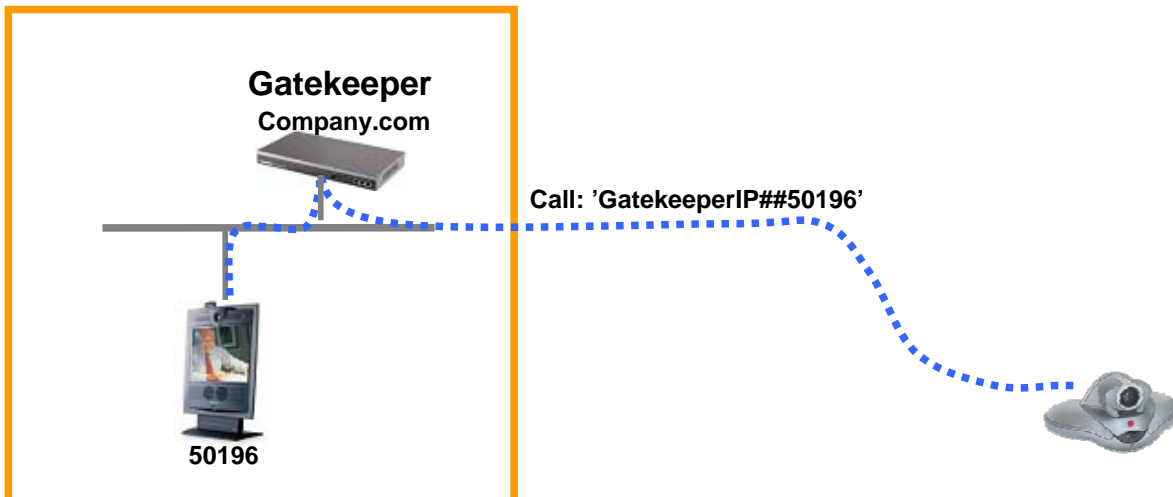
- Unsolicited Inbound IP Address Call

If a call comes into the gatekeeper's IP address that does not specify a particular alias within the setup message (e.g. the far end system dials the gatekeeper IP address directly), the gatekeeper will then forward the call directly to the alias that is configured within the 'Fallback alias for unregistered caller destination' configuration parameter of the system. This will allow a call that is made directly to the gatekeeper to be automatically forwarded to a specific alias within the organization without requiring the source endpoint to be registered to either the local or remote H.323 island or perform a DNS lookup directly.



- IP Plus Extension Dialing

The TANDBERG Gatekeeper will support inbound calls using the Polycom IP-Plus Extension dialing scheme. In this scheme, the Polycom VSX endpoints support the ability to dial an IP address and provide the alias information within the subaddress field of the dialing string. This alias information is then provided to the gatekeeper on the initial call setup message, allowing the gatekeeper to locate the endpoint through the H.323 network and the call will complete.



API Call Control

The API call control allows for a consistent interaction with the H.323 network to connect, transfer and disconnect calls on an ad-hoc basis. This will then allow for the development of a control system to interact with a centralized resource, rather than the remote endpoints in order to achieve call functionality.

Note: The API call control requires routed mode to be enabled on the gatekeeper. Transfer functionality requires that call transfer is also enabled on the system.

- Call Connect

A call can be connected through the gatekeeper just as it would through an endpoint; specifying both the "source" and "destination" of the call to the gatekeeper. These two endpoints can be any endpoints, so long as they can be reached through a normal endpoint dialing process; including those that are not registered directly to the gatekeeper and those that can be reached through URI resolution. Although both a call source and destination are specified to the gatekeeper, the gatekeeper actually initiates a call to both endpoints involved, specifying the other endpoint's address as the "source" of the call request.

- Call Transfer

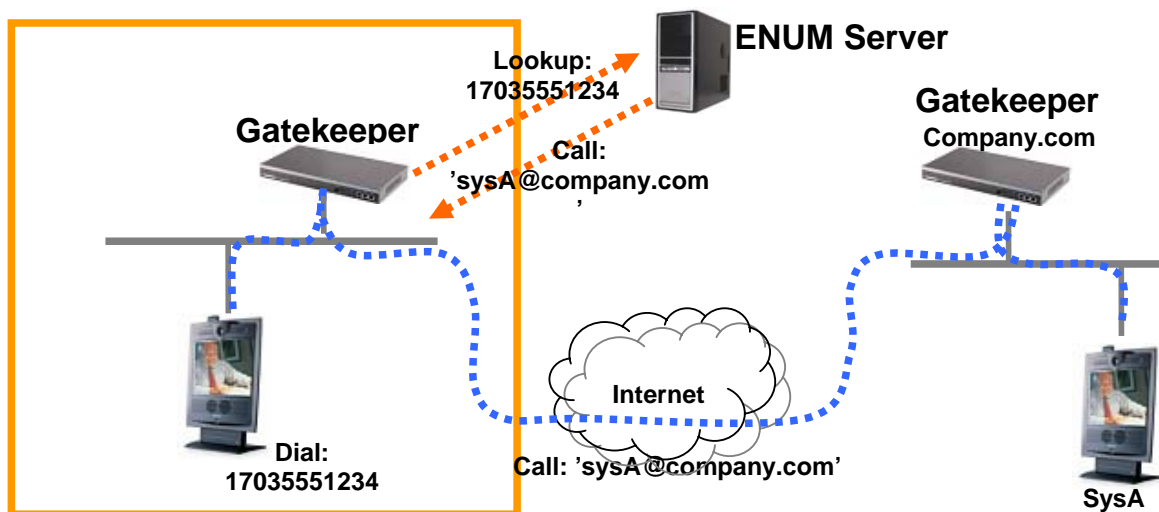
Once connected, the call can be transferred between endpoints through the gatekeeper API, thus allowing for the call to be re-routed throughout the network from a centralized interface.

- Call Disconnect

Any connected call can also be disconnected from the gatekeeper through the embedded API or administrative web interface.

ENUM Support

The TANDBERG Gatekeeper can now interact with an ENUM server to provide directory services for remote systems. ENUM lookup is a directory service that provides translation of a dialed number to the fully qualified URI associated with that directory entry. When resolved to the URI, the gatekeeper is then able to route the call appropriately, using the same call logic as if the URI were dialed directly by the end user. The support for ENUM lookup provides a user-friendly dialing mechanism to all end users in order to locate remote H.323 islands.



Supplemental Notes to Manuals

Software Versions

The base version of the TANDBERG Gatekeeper will include an option of 25 concurrent total calls, 125 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 2500 registrations and 500 total concurrent calls.

The TANDBERG Gatekeeper uses one of the following software files for N5.0 or later software, when n<xx> represents the software version (e.g. n50 represents N5.0).

<i>Software</i>	<i>Software File Properties</i>
s42000n<xx>	Supports AES
S42101n<xx>	Does not support AES

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.

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

Network Support

The TANDBERG Gatekeeper is an H.323 device and is intended to be connected to an 802.3 IP network. Only the first 802.3 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. If at all possible, Full Duplex should be used.

Layer 4 Ports Used

<i>Function</i>	<i>Port</i>	<i>Type</i>	<i>Direction</i>
Gatekeeper RAS	1719	UDP	↔
Gatekeeper Discovery	1718	UDP	Host → BC
SSH (Includes SCP)	22	TCP	Host → BC
Telnet	23	TCP	Host → BC
HTTP / XML	80	TCP	Host → BC
HTTPS / XML	443	TCP	Host → BC
SNMP (Queries)	161	UDP	Host → BC
NTP	123	UDP	↔
LDAP Communication	389	TCP	↔
LDAPS Communication	636	TCP	↔
Incoming H.323 Call	1720	TCP	Host → BC
H.225/Q.931 Call Setup	15000:16800	TCP	↔
H.245 Call Control	19000:20800	TCP	↔
Media (RTP, RTCP)	50000:52400	UDP	↔

Changes and Improvements Since Previous Release

System Registration Improvements

Simplified Registration Licensing

Registration licensing for the gatekeeper has been improved within the N5.0 software release. When a system registers, it will now count as a single license regardless of the number of E.164 aliases and/or H.323 IDs the system provides to the gatekeeper. Previously, the registered endpoint would occupy one registration license per alias with which the endpoint registered.

Duplicate Alias Handling

The gatekeeper will no longer reject a registration if an incoming registration specifies two H.323 IDs that differ only in capitalization.

Registration Conflict Handling

The process the gatekeeper uses to handle registration conflicts can now be administratively controlled. Particularly useful in environments where endpoint IP addresses change frequently, the 'Overwrite' setting will allow the gatekeeper to replace an existing registration with an incoming registration in the event of an alias conflict. If configured to 'Reject', the gatekeeper will reject an incoming registration with reject reason 'Duplicate Alias' if an alias of the incoming registration conflicts with an existing registration on the gatekeeper; this behavior is as the gatekeeper functioned in previous releases.

Subzone Definition

Subzones can now overlap, creating differing levels of precision for the network to allow an administrator complete control over all endpoints of the network, regardless of the address space in which they exist. For example, if the subzone of 10.1.6.0/24 (all endpoints from 10.1.6.1 to 10.1.6.255) have a specific bandwidth requirement. However, within that subzone, the MCU on address 10.1.6.224 has a different bandwidth requirement. In this case, one subzone will be created for the entire 10.1.6.0 subnet (with prefix length of 24) and another will be created for the MCU itself (subzone address 10.1.6.224 with a prefix length of 32).

Selective Unregistration

If an administrator forces an active system to unregister from the gatekeeper administrative interface, the gatekeeper will now disconnect all active calls for the endpoint and send an 'unregistrationRequest' (URQ) to the endpoint, thereby requiring the endpoint to unregister from the gatekeeper.

Call Control

Bandwidth Control

Within a specific subzone, bandwidth restrictions for calls that remain within a specific subzone can now be controlled independently of calls that will complete external to the current subzone. Any bandwidth restriction configured on the 'intra bandwidth mode' will only be applied if a call is made between endpoints within that subzone. If the call is required to connect to another subzone or zone on that gatekeeper, the 'inter bandwidth mode' restrictions will be applied.

Alias Addressing

The gatekeeper now supports the 'emailAddress' field for call request within an ARQ from an endpoint. It will treat this field as it would treat an incoming call to an H.323 ID.

CPL on Direct Endpoint IP Call

It is now possible for CPL logic to be run on a call that is connected directly to an endpoint IP address, without connecting via gatekeeper RAS messaging. This provides the ability to control all calls connected to a registered endpoint, regardless of how they are dialed.

Note: Routed mode must be enabled on the gatekeeper for this functionality. When routed mode is enabled, a call made to the endpoint's IP address will be re-directed to the gatekeeper, allowing it to run CPL prior to the acceptance of the call.

IP Address Dialing

The gatekeeper will no longer reference the locally registered E.164 aliases/prefixes or H.323 IDs upon receipt of a call request made to a specific IP address (when the IP address is dialed directly from an endpoint). This will remove the chance that a call made to an IP address will be incorrectly routed to an endpoint registered with a conflicting alias (e.g. a call placed to IP address 10.1.2.3 and is routed to a gateway is registered with service prefix of '1').

Security

Clear History

If necessary, the gatekeeper history (registration and call history) can be cleared through the API of the system, using the command:

```
clear history
```

Clear Eventlog

In addition to the history, the eventlog of the gatekeeper can be cleared through the API command:

```
clear eventlog
```

External Manager

External Manager Initialization

When initializing the External Manager connection, the gatekeeper will no longer send two phantom boot traps.

Call Event Notification

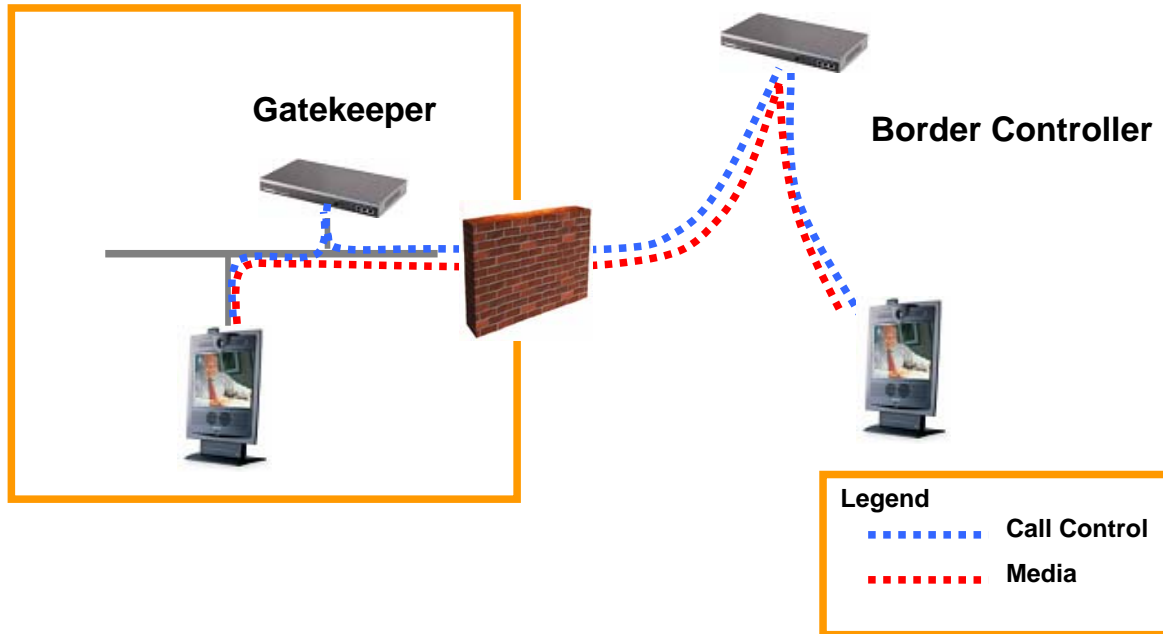
All Call Events will now be sent to an external management application, such as TMS, through a registered feedback channel.

Zone Failure Notification

If communication with a remote H.323 zone ever fails, an external management application, such as TMS, will be notified.

Allow Media Direct

When 'Allow Media Direct' is enabled on the gatekeeper, all call control messages will flow directly through the gatekeeper instead of directly to the gatekeeper. All media traffic, however, will still flow directly from the endpoint to the gatekeeper, if the endpoint supports traversal technology (e.g. Assent).



Usability Improvements

Syslog

- Syslog Readability

The syslog of the gatekeeper has been improved to provide more information prior to the message printout. This information includes the message type (e.g. ARQ), the sequence number of the message, the source and destination addressing information and detailed message information (e.g. bandwidth).

- Force Syslog to Specific IP Address

To improve the readability of the syslog output from a gatekeeper, the syslog can be forced to up to 10 IP addresses. By forcing the log to a specific IP address, the amount of information that is output to the log file can be significantly reduced as communication with other addresses will be omitted from the output.

- Timestamp in Syslog

The timestamp is now printed within the syslog of the gatekeeper in order to provide administrators with a reference for troubleshooting and debugging purposes. The timestamp printed will be the local time of the box, adjusted to the appropriate Time Zone and Daylight Savings Time, if applicable.

Web UI

- Password

The administrative password of the gatekeeper can now be modified through the administrative web interface, through 'System Configuration' > 'System'.

- System Configuration

The 'Misc' section within 'System Configuration' on the web interface of the gatekeeper has been renamed to 'System'.

- Authentication

The authentication parameter configuration of the gatekeeper configuration, previously located in 'Gatekeeper Configuration' > 'Gatekeeper' has now been broken out into its own section of the gatekeeper configuration, 'Authentication'.

- Redundancy Status

The gatekeeper will now provide the connectivity status of all redundant systems. This status can be located within 'System Status' > 'Alternates'.

- Subzone Status

Within 'System Status' > 'Subzones', the subzone details will now display the endpoints that are registered within that subzone as well as bandwidth details in regards to the total utilization, inter- and intra-subzone call bandwidths.

- Link Status

Within 'System Status' > 'Links', the gatekeeper will now display the current bandwidth being occupied within the individual links.

- Pipe Status

Within 'System Status' > 'Pipes', the gatekeeper will now display the current bandwidth being occupied within the individual pipes.

- System Information

The 'System Information' page within 'System Status' now provides in depth numerical data regarding both active and maximum active registrations, active, maximum and total calls, both traversal and non traversal .

- Link Configuration

The 'Links' page under 'Gatekeeper Configuration' has been expanded to display the pipes configured each specific link on the main page.

- Pipe Configuration

The 'Pipes' configuration page has been expanded to include the listing of the total bandwidth and per call bandwidth restrictions imposed on the pipe itself.

DNS Lookup

The TANDBERG Gatekeeper now supports the ability to define a remote syslog server address using the DNS name of the server.

API

When resetting the password using the 'pwrec' account, the "Error finding tty name: Inappropriate ioctl for device" reporting error will no longer be displayed.

System Improvements

Software Upgrade

An issue that would prevent the upgrade from software version Q1.x to Q3.x or higher has been resolved; a direct upgrade from N1.x to N5.0 and later is supported.

Telnet Access

It was possible that the TANDBERG Gatekeeper would allow for a client to connect to the telnet server of the system, even if the service was disabled. This issue is now resolved.

Known Limitations

TANDBERG

Equipment

Limitations

TANDBERG Gatekeeper ver N5.0	If the gatekeeper is ever set back to default values using the 'xCommand DefaultValuesSet Level(r): <1..3>' command, the system will not automatically add the default links back into the configuration. In order to add the default links, issue the command 'xCommand DefaultLinksAdd'.
TANDBERG Gatekeeper ver N5.0	Within the registration status, the gatekeeper will always report the connection in which the RAS traffic uses for communication within the 'rasAddress' field, rather than the address specified within the RAS messages themselves. This is normal operation as the gatekeeper will always use the established RAS connection for communication with the endpoint.
TANDBERG Gatekeeper ver N5.0	The local database used to store username and password credentials for authentication will only support a maximum of 1000 sets of credentials. If more credentials are required, TANDBERG highly recommends utilizing an external LDAP server.
TANDBERG Gatekeeper ver N5.0	The maximum number of allow and deny list entries is limited to 1000. If a larger install base is required for the gatekeeper, it is recommended that wild cards are used to increase the number of maximum active registrations that can be implemented in conjunction with the allow or deny list.
TANDBERG Gatekeeper ver N5.0	If an IP gateway is not available for the IP network in which the system is installed, the gatekeeper must be configured with a non-occupied, valid IP address on the subnet.
TANDBERG Gatekeeper ver N5.0	Due to a limitation within RAS messaging, an endpoint that supports an IPv4/IPv6 hybrid configuration will not be able to register to the TANDBERG Gatekeeper with both an IPv4 and IPv6 call signaling address. This is due to the fact that only one call signaling address can be transmitted within the 'callSignalingAddress' field of any RAS message, thereby limiting the endpoint to only specifying either the IPv4 or IPv6 address when registering to the gatekeeper.
TANDBERG Gatekeeper ver N5.0	When using the gatekeeper API to connect a call between two endpoints, the gatekeeper initiates the call with encryption capabilities within the setup message, even if the software loaded on the gatekeeper does not include encryption. If the software loaded on the gatekeeper does not contain encryption, this can lead to corrupted media between the endpoints.
TANDBERG Gatekeeper ver N5.0	If connecting to the gatekeeper web interface using the DNS host name of the box and both HTTPS and session timeouts are enabled, the gatekeeper will not permit full login to the administrative interface. It is recommended that the IP address is used when the box is installed with this configuration as the issue is not present when using IP addressing.
TANDBERG Gatekeeper ver N5.0	If a gatekeeper running N5.0 software is downgraded to N4.1 software, remote zones may not be transferred correctly back to N4.1.
TANDBERG Gatekeeper ver	If the gatekeeper is configured for an H.460.18 traversal link to the

N5.0	TANDBERG Border Controller and H.460.19 multiplexed media is enabled, video could take a few seconds to establish to the endpoint registered to the gatekeeper when the call is placed from an endpoint registered outside the network or to the Border Controller directly.
TANDBERG Gatekeeper ver N5.0	If an endpoint is registered with an alias that contains '\r\n', all reporting for that system, including call history, registration history and registration status will not be complete.
TANDBERG Gatekeeper ver N5.0	If a gatekeeper receives a call request to a gateway service prefix and the locally registered gateway has signaled that it is out of resources, the gatekeeper will not check the alternates for an available gateway.
TANDBERG Gatekeeper ver N5.0	The TANDBERG Gatekeeper will always report TCP port 1720 for the destination call signaling port, regardless of what port is actually used. This report is sent over XML to an external management system (e.g. TANDBERG Management Suite)
TANDBERG Gatekeeper ver N5.0	If an incoming registration is received on port 65535, the gatekeeper will reject the registration as 'invalidRasAddress'. This will be improved in a later version.
TANDBERG Gatekeeper ver N5.0	It is not possible to manually configure a link via the web management interface as the name for the specific traversal zone will not appear, but rather a generic 'Traversal Zone' name. Configuring a link to 'Traversal Zone' will not function properly. The API, however, can be used to create these links manually through the use of the 'xConfiguration Links' command.
TANDBERG Gatekeeper ver N5.0	The API must be used to configure a pipe for a link pointed to a traversal zone. The command 'xConfiguration Links Link [1..100] Pipe1 Name: <S: 0, 50>' or 'xConfiguration Links Link [1..100] Pipe2 Name: <S: 0, 50>' can be used.
TANDBERG Gatekeeper ver N5.0	Upon upgrade from a previous version, the links on the gatekeeper will not be created or restored correctly if one of the nodes contains a space within the name. To resolve this, change the name of the node (e.g. subzone or remote zone name) replace the space with an underscore ('_'), dot ('.') or other character.
TANDBERG Management Suite ver 11.5	If 'Session time out' is enabled, TMS will not be able to control the gatekeeper.

Linksys

Equipment

Linksys WRT54G hardware version 5

Limitations

Linksys Router WRT54G hardware version 5 appears to change the source ports of outbound connections opened for a prolonged period of time. As such, H.323 calls that are made from or to systems registered to either a gatekeeper or Border Controller behind this router will disconnect at random times. This issue has been presented to Linksys.

Interoperability Testing³

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

Gatekeepers/Traversal Servers

<i>Equipment</i>	<i>Software Revision</i>	<i>H.460.18/.19⁴</i>	<i>Comments</i>
TANDBERG Gatekeeper	N1.0, N2.1, N3.2, N4.1	No	
	N5.0	Yes	
TANDBERG Border Controller	Q1.0, Q2.1	No	
	Q3.1, Q5.0	Yes	Q3.x does not support multiplexed media.
Cisco MCM	12.3(10), 12.3(10a)	No	
Polycom PathNavigator	7.00.03	No	
Polycom V2IU	6.1.6	Yes	The V2IU does not support an H.460.18/.19 client proxy. As such, the proxy functionality within the TANDBERG Gatekeeper could not be tested with this system.
RADVISION ECS	4.1.0.0	No	

Gateway Interoperability

<i>Equipment</i>	<i>Software Revision</i>	<i>H.460.18/.19</i>	<i>Comments</i>
TANDBERG Gateway	G1.0, G2.1, G3.1	No	
TANDBERG 3G Gateway	R1.0, R2.0	No	
TANDBERG Video Portal	V2.0	No	
Cisco CallManager	4.1	No	
Ezenia Encounter 3000	2.0	No	
Polycom MGC 25/50/100	7.5.0.52	No	
RADVISION gw-P20	4.0	No	

³ All interop testing performed on systems that do not natively support either Assent or H.460.18/.19 were performed in conjunction with the TANDBERG Gatekeeper as the traversal client.

⁴ This section of the tables denotes whether the device supports H.460.18/.19 firewall traversal natively (e.g. without the use of an H.460.18/.19 client gatekeeper).

MCU Interoperability

<i>Equipment</i>	<i>Software Revision</i>	<i>H.460.18/.19</i>	<i>Comments</i>
TANDBERG MCU	D2.3, D3.9	No	
TANDBERG MPS	J1.2, J2.4, J3.1, J3.2	No	
Cisco IPVC 3540	4.2.10	No	
Codian MCU 4210	1.4(1.6)	No	
Polycom MGC 25/50/100	7.5.0.52	No	
RADVISION VialP	4.0.31	No	

Streaming Servers

<i>Equipment</i>	<i>Software Revision</i>	<i>H.460.18/.19</i>	<i>Comments</i>
TANDBERG Content Server	S1.0, S1.1	No	

Endpoint Interoperability

<i>Equipment</i>	<i>Software Revision</i>	<i>H.460.18/.19</i>	<i>Comments</i>
TANDBERG MXP	F1.7, F2.5, F3.4	No	
	F4.1, F5.0	Yes	F4.x does not support multiplexed media.
TANDBERG 150 MXP	L1.2, L2.2, L3.1	No	
	L4.0	Yes	L4.x does not support multiplexed media.
TANDBERG Classic	B1.3, B2.4, B3.4, B4.4, B5.1/B5.11, B6.3/E1.3, B7.4/E2.4, B8.4/E3.4, B9.2/E4.2, B10.2/E5.2	No	
Aethra VegaStar	4.69	No	
Cisco VT Advantage	1.0(2)	No	The endpoint was tested in conjunction with an H.225 trunk from Cisco CallManager to a TANDBERG Gatekeeper.
LifeSize Room	2.0.0(15)	No	
Microsoft NetMeeting	3.01	No	
Polycom EX	6.0.5	No	
Polycom FX	6.0.5	No	

Polycom iPower 680	6.2.0.1208	No	
Polycom iPower 9000/970	6.2.0.1208	No	
Polycom PVX	8.0.2	No	
Polycom ViaVideo	5.1.1.1009	No	
Polycom ViewStation, MP512, SP384	7.5.4	No	
Polycom VSX	8.0.3	No	
	8.5	Yes	Version 8.5 does not support multiplexed media.
Polycom V-series	8.0.3	No	
	8.5	Yes	Version 8.5 does not support multiplexed media.
Sony PCS-1	3.22	No	
Sony PCS-TL50	2.21	No	
VCON VPoint	6.50.0064	No	
VTEL Galaxy	2.2.0.070	No	

Firewall Interoperability

<i>Equipment</i>	<i>Software Revision</i>	<i>H.460.18/.19</i>	<i>Comments</i>
Check Point NGX	R60	No	Due to some of the new signaling required by the H.460.18/.19 standard, H.323 awareness on the Check Point firewall can cause calls to fail. It is recommended that all H.323 awareness is disabled.
Cisco PIX	6.3(3), 6.3(4), 7.0(1), 7.0(4)	No	Due to some of the new signaling required by the H.460.18/.19 standard, H.323 fixup/inspect on the PIX firewall can cause calls to fail. It is recommended that all H.323 awareness is disabled.
DLink DI-514	1.03	No	
DLink DI-604	1.07DDM	No	
Linksys BEFW11S4	1.50.14	No	
Linksys WRT54G (v1)	4.02.7	No	

Linksys WRT54G (v4)	DD-WRT v23	No
Linksys WRT54GL (v3)	4.30.5	No
Linksys WRT54GR	1.01	No
Linksys WRT54GS	4.70.6	No
NetGear N314	V3.29(CF.0)b1	No