

# **TANDBERG**

## **Border Controller Q3 Software Release Document**

---

TANDBERG

D50405, Rev 1.2

# Table of Contents

|           |  |           |
|-----------|--|-----------|
| <b>1.</b> | <b>DOCUMENT REVISION HISTORY .....</b>                                   | <b>4</b>  |
| <b>2.</b> | <b>RELEASE NOTES FOR TANDBERG BORDER CONTROLLER SW VERSION Q3.1.....</b> | <b>5</b>  |
| 2.1       | INTRODUCTION .....   | 5         |
| 2.2       | NEW FEATURE OVERVIEW .....   | 5         |
| 2.3       | CHANGES AND IMPROVEMENTS SINCE PREVIOUS VERSION .....                    | 5         |
| 2.3.1     | <i>RAS Signaling</i> .....   | 5         |
| 2.3.2     | <i>H.323 Signaling</i> .....   | 5         |
| 2.3.3     | <i>H.460.18/19</i> .....   | 5         |
| 2.3.4     | <i>TCP Port Allocation</i> .....   | 5         |
| 2.3.5     | <i>Remote Zone Match</i> .....   | 5         |
| 2.3.6     | <i>URI Domain Lookup</i> .....   | 5         |
| 2.3.7     | <i>Policy</i> .....  | 5         |
| 2.3.8     | <i>API</i> .....   | 6         |
| 2.3.9     | <i>Licensing</i> .....   | 6         |
| 2.3.10    | <i>Eventlog</i> .....  | 6         |
| 2.3.11    | <i>Registration Storage</i> .....  | 6         |
| 2.3.12    | <i>DNS Resolution</i> .....  | 6         |
| 2.3.13    | <i>Usability Improvements</i> .....                                      | 6         |
| 2.4       | KNOWN LIMITATIONS .....  | 6         |
| 2.4.1     | <i>TANDBERG</i> .....  | 6         |
| 2.4.2     | <i>Cisco</i> .....   | 7         |
| 2.4.3     | <i>RADVISION</i> .....   | 7         |
| 2.5       | INTEROPERABILITY TESTING .....   | 8         |
| 2.5.1     | <i>Gatekeepers</i> .....   | 8         |
| 2.5.2     | <i>Gateway Interoperability</i> .....                                    | 8         |
| 2.5.3     | <i>MCU Interoperability</i> .....  | 8         |
| 2.5.4     | <i>Streaming Servers</i> .....   | 8         |
| 2.5.5     | <i>Endpoint Interoperability</i> .....                                   | 8         |
| 2.5.6     | <i>Firewall Interoperability</i> .....                                   | 9         |
| <b>3.</b> | <b>RELEASE NOTES FOR TANDBERG BORDER CONTROLLER SW VERSION Q3.0....</b>  | <b>10</b> |
| 3.1       | INTRODUCTION .....   | 10        |
| 3.2       | NEW FEATURE OVERVIEW .....   | 10        |
| 3.2.1     | <i>Multiple Traversal Zones</i> .....                                    | 10        |
| 3.2.2     | <i>Support for IPv6</i> .....  | 10        |
| 3.2.3     | <i>Remote Zone Definitions</i> .....                                     | 11        |
| 3.2.4     | <i>Remote Syslog Server</i> .....  | 12        |
| 3.2.5     | <i>Neighbor and Alternate Health Check</i> .....                         | 12        |
| 3.2.6     | <i>Remote Zone Redundancy</i> .....                                      | 13        |
| 3.2.7     | <i>DNS Addressing</i> .....  | 13        |
| 3.2.8     | <i>Password Reset</i> .....  | 13        |
| 3.2.9     | <i>Management Session Timeout</i> .....                                  | 13        |
| 3.2.10    | <i>Local Time Zone</i> .....   | 13        |
| 3.3       | SUPPLEMENTAL NOTES TO MANUALS .....                                      | 14        |
| 3.3.1     | <i>Software Versions</i> .....   | 14        |
| 3.3.2     | <i>References/Related Documents</i> .....                                | 14        |
| 3.3.3     | <i>Network Support</i> .....   | 14        |
| 3.3.4     | <i>Layer 4 Ports Used</i> .....  | 14        |
| 3.4       | CHANGES AND IMPROVEMENTS SINCE PREVIOUS VERSION .....                    | 15        |
| 3.4.1     | <i>Usability Improvements</i> .....                                      | 15        |
| 3.4.1.1   | <i>Web Interface Readability</i> .....                                   | 15        |
| 3.4.1.2   | <i>Log Readability</i> .....   | 15        |
| 3.4.1.3   | <i>Time Stamping</i> .....   | 15        |
| 3.4.1.4   | <i>Zone Status</i> .....   | 15        |
| 3.4.2     | <i>Remote System Connection Status</i> .....                             | 15        |
| 3.4.3     | <i>Subzone Definition</i> .....  | 16        |
| 3.4.4     | <i>Calls to Unknown IP Addresses</i> .....                               | 16        |
| 3.4.5     | <i>NTP Server Connection</i> .....                                       | 16        |
| 3.4.6     | <i>LRQ Handling</i> .....  | 16        |

|       |                                  |    |
|-------|----------------------------------|----|
| 3.4.7 | <i>Default IP Address</i>        | 16 |
| 3.4.8 | <i>Web Interface</i>             | 16 |
| 3.5   | KNOWN LIMITATIONS                | 17 |
| 3.5.1 | <i>TANDBERG</i>                  | 17 |
| 3.5.2 | <i>Cisco</i>                     | 18 |
| 3.5.3 | <i>RADVISION</i>                 | 18 |
| 3.6   | INTEROPERABILITY TESTING         | 18 |
| 3.6.1 | <i>Gatekeepers</i>               | 18 |
| 3.6.2 | <i>Gateway Interoperability</i>  | 18 |
| 3.6.3 | <i>MCU Interoperability</i>      | 19 |
| 3.6.4 | <i>Streaming Servers</i>         | 19 |
| 3.6.5 | <i>Endpoint Interoperability</i> | 19 |
| 3.6.6 | <i>Firewall Interoperability</i> | 19 |

## 1. Document Revision History

- Rev 1.2 - Updated “Changes and Improvements” for Q3.1
- Rev 1.1 - Release of Q3.1, Minor Release
  - Updated “Changes and Improvements” for Q3.0 to include “Web Interface” vulnerability resolutions
- Rev 1.0 - Release of Q3.0, Initial Version

## 2. Release Notes for TANDBERG Border Controller SW Version Q3.1

### 2.1 Introduction

These notes describe the features and capabilities included in the TANDBERG Border Controller software version Q3.1 released on April 10, 2006.

### 2.2 New Feature Overview

Q3.1 is a maintenance only release. No new features or functionality are included within this version over the previous release, Q3.0.

### 2.3 Changes and Improvements since previous version

#### 2.3.1 RAS Signaling

An issue that would cause an incoming LRQ to be ignored when H.235 authentication is enabled on the Border Controller has been resolved.

This version of software has resolved an issue that would cause disabling ‘*Allow forwarding of location requests*’ to not have an affect on the incoming call processing engine.

#### 2.3.2 H.323 Signaling

The TANDBERG Border Controller will now properly construct the ‘Layer 1 Protocol’ portion of the ‘Bearer Capabilities’ section of the Q.931 setup message, as required by the H.225 and Q.931 standards. The resolution of this issue will resolve connectivity issues that existed with some third party endpoints and the TANDBERG Content Server.

#### 2.3.3 H.460.18/.19

This software release resolved an issue that would cause the establishment of an H.239 stream through the TANDBERG Border Controller when involved in an H.460.18/.19 call to fail.

#### 2.3.4 TCP Port Allocation

An issue that would result in the failure of traversal calls through the Border Controller due to a TCP port allocation error has been resolved. The allocation error can be attributed to a TCP port leak that would occur within the Border Controller as a result of a call to an endpoint that would fail due to border issues at the far end system (e.g. firewall rules that would prevent the success of the call).

#### 2.3.5 Remote Zone Match

The Border Controller will no longer consider calls made directly to an IP address when reviewing the match criteria for a remote zone.

#### 2.3.6 URI Domain Lookup

If a Border Controller is configured for a specific domain (e.g. company.com) and is then presented a call for a subdomain (e.g. test.company.com), the Border Controller would not perform the DNS lookup, resulting in a failed call. This has been resolved.

#### 2.3.7 Policy

An issue that would prevent executing policy on the H.323 ID of a registered gateway has been resolved.

### 2.3.8 API

The Border Controller will no longer print out all of the local registrations when the '*xcommand findregistration <alias>*' command is executed.

### 2.3.9 Licensing

The MD5 and MD5 Javascript license was added to the API of the Border Controller. This license can be viewed through the '*license*' API command.

### 2.3.10 Eventlog

An issue that may cause the Border Controller to reinitialize unexpectedly if an eventlog is run on a Border Controller under a heavy load has been resolved.

The 'Call Signaling Address' will no longer be required when logging all RAS messages to the eventlog.

### 2.3.11 Registration Storage

When storing aliases of a registration, the Border Controller will now check for validity of the aliases presented prior to saving the registration internally. This will prevent the Border Controller from restarting unexpectedly if an invalid alias is retrieved from the stored registration list.

### 2.3.12 DNS Resolution

If the Border Controller is configured with domain address 'company.com' and presented with a call for a URI with a subdomain of 'company.com' (e.g. 'support.company.com'), the Border Controller would not perform a DNS lookup of the subdomain. This issue has been resolved.

### 2.3.13 Usability Improvements

The wording of the web timeout wording has been changed from "Note: web session timeouts are only enabled if https is enabled" to "Note: web session timeouts are only active if https is enabled" to clarify that the presence of the timeouts will not be disabled on all other ports if HTTPS is not enabled.

## 2.4 Known Limitations

### 2.4.1 TANDBERG

| Equipment                           | Limitations   |
|-------------------------------------|---|
| TANDBERG Border Controller ver Q3.0 | The Border Controller does not currently support a hybrid of IPv4 and IPv6 networks. The system will only be able to function in an IPv4 network or an IPv6 network. Supporting hybrid networks is being investigated for future development.   |
| TANDBERG Border Controller ver Q3.0 | If the Border Controller is ever set back to default values using the ' <i>xcommand defaultvalueset level: 3</i> ' command, the system will not automatically add the default links back into the configuration. In order to add the default links, issue the command ' <i>xcommand defaultlinksadd</i> ' |
| TANDBERG Border Controller ver Q3.0 | Upon resetting the password on the Border Controller, an error of "Error finding tty name: Inappropriate ioctl for device" will be displayed on the local dataport connection. This error should be ignored – the process has completed   |

|                                     |   |
|-------------------------------------|---|
|                                     | successfully, it is just a reporting error.   |
| TANDBERG Border Controller ver Q3.0 | If an endpoint tries to register to the Border Controller with multiple H.323 IDs that differ only in capitalization, the Border Controller will reject the registration (e.g. H.323 IDs of 'ENDPOINT' and 'endpoint'). To resolve this issue, remove one of the H.323 IDs. |
| TANDBERG Border Controller ver Q3.0 | DNS lookup is not currently supported for addressing the syslog server – the IP address of the server must be entered.  |
| TANDBERG Border Controller ver Q3.0 | When initially configuring the External Manager address, the Border Controller will send out two boot traps to ensure proper communication has been established; the device itself does not actually reboot. This is normal operation.                                      |

#### 2.4.2 Cisco

| Equipment                        | Limitations  |
|----------------------------------|--|
| Cisco PIX ver 6.2(4) and earlier | If H.323 fixup is turned on for the RAS channel on port 1719, the protocol will strip the Non-Standard Data portion of the Registration Request, where the Expressway-enabled information is sent between the Expressway client and the Border Controller. This will cause the registration to be rejected with 'neededFeatureNotSupported' as the error. To resolve, turn off H.323 fixup on the RAS channel. This issue does not exist with PIX software versions 6.3 and later as the H.323 stack within the PIX was upgraded beyond version 1 in later versions of software. |
| Cisco PIX ver 7.0(4) and earlier | In order to implement H.460.18/.19 with the Cisco PIX firewall, disable H.323 Fixup on the firewall for port 1720. Because all call initiation transmits to port 1720, according to the H.460.18 standard, application awareness of the firewall may interfere with the call setup.  |

#### 2.4.3 RADVISION

| Equipment                      | Limitations  |
|--------------------------------|--|
| RADVISION viaIP MCU ver 4.0.31 | The RADVISION MCU cannot make outbound URI calls as it presents the outbound URI in the 'Email Address' field of the ARQ instead of the 'H.323 ID' field. The Border Controller does not currently support the 'Email Address' field within a request. |

## 2.5 Interoperability Testing

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

### 2.5.1 Gatekeepers

| Equipment             | Software Revision              |
|-----------------------|--------------------------------|
| TANDBERG Gatekeeper   | N1.0, N2.1, N3.2, N4.0, N4.1   |
| RADVision ECS         | 3.5.2.5                        |
| Cisco MCM             | 12.3(10), 12.3(10a), 12.3(13a) |
| Polycom PathNavigator | 7.00.03                        |

### 2.5.2 Gateway Interoperability

| Equipment             | Software Revision |
|-----------------------|-------------------|
| TANDBERG Gateway      | G2.1, G3.0        |
| TANDBERG 3G Gateway   | R1.0              |
| RADVision gw-P20      | 4.0.0.40          |
| RADVision L2W GW      | 2.2.3.2.5         |
| Polycom MGC 25/50/100 | 7.0.2.6           |
| Cisco CallManager     | 4.1(3)SR2         |
| Ezenia Encounter 3000 | 2.0               |

### 2.5.3 MCU Interoperability

| Equipment             | Software Revision            |
|-----------------------|------------------------------|
| TANDBERG MCU          | D3.4, D3.5, D3.6             |
| TANDBERG MPS          | J1.1, J2.0, J2.1, J2.2, J3.0 |
| Polycom MGC 25/50/100 | 6.02.4, 7.0.2.6              |
| RADVision ViaIP MCU   | 4.0.31                       |
| RADVision OnLan MCU   | 2.2.1.0                      |
| Cisco IPVC 3540       | 3.2.224                      |
| Codian MCU 4210       | 1.3(1.4)                     |

### 2.5.4 Streaming Servers

| Equipment               | Software Revision |
|-------------------------|-------------------|
| TANDBERG Content Server | S1.0              |

### 2.5.5 Endpoint Interoperability

| Equipment               | Software Revision  |
|-------------------------|--|
| TANDBERG MXP            | F1.4, F1.5, F2.5, F2.6, F3.0, F3.2, F4.0   |
| TANDBERG 150            | L1.1, L1.2, L2.2, L3.0, L3.1   |
| 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 | 6.2.0.1208   |
| Polycom iPower 680      | 5.3.0.1202   |
| Polycom EX              | 6.0.5  |
| Polycom FX              | 6.0.5  |
| Polycom ViewStation     | 7.5.4  |
| Polycom MP512           | 7.5.4  |
| Polycom SP 384          | 7.5.4  |
| Polycom VSX             | 8.03   |
| Polycom PVX             | 8.0.0.0522   |

|                      |           |
|----------------------|-----------|
| Sony PCS-1           | 3.14      |
| Sony PCS-TL50        | 2.11      |
| VTEL Galaxy          | 2.2.0.070 |
| Microsoft NetMeeting | 3.01      |
| VCON Vpoint          | 6.5       |
| Aethra VegaStar      | 6.0.18    |

### 2.5.6 Firewall Interoperability

| Equipment        | Software Revision                                      |
|------------------|--|
| Cisco PIX        | 6.2(4), 6.3(1), 6.3(3), 6.3(4), 7.0(1), 7.0(2), 7.0(4) |
| Sonicwall SOHO 3 | 6.6.0.2  |
| Linksys BEFW11S4 | 1.44.2   |
| Linksys BEFSR81  | 2.45.10  |
| Linksys BEFSR41  | 1.05.00  |
| Linksys WRT54G   | 1.30.7, 1.42.3, 3.01.3                                 |
| Linksys WRT54Gv5 | 1.00.4   |
| Checkpoint NGX   | R60  |

### 3. Release Notes for TANDBERG Border Controller SW Version Q3.0

#### 3.1 Introduction

These release notes describe the features and capabilities included in the TANDBERG Border Controller software version Q3.0 released on 30 Jan 2006.

#### 3.2 New Feature Overview

##### 3.2.1 Multiple Traversal Zones

In conjunction with the TANDBERG Gatekeeper, the TANDBERG Border Controller now supports up to 50 independent Traversal Zones, thereby allowing up to 50 independent gatekeepers to register to a single, centralized Border Controller on the H.323 network. Each of the gatekeepers can act as one component of a large H.323 network or can act independently of all other Traversal Zones on the network.

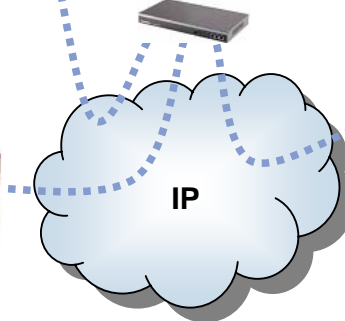
##### *EnterpriseA.net*



##### *EnterpriseC.biz*



##### Service Provider Border Controller



##### *EnterpriseB.com*

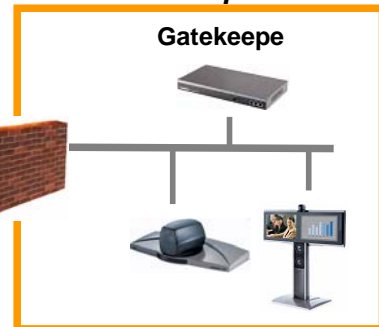


Figure 1. Possible H.323 Network Layout

##### 3.2.2 Support for IPv6

The TANDBERG Border Controller now supports communications over an IPv6 network, thereby allowing the system to function in either an existing IPv4 network or IPv6 networks both currently active and under development.

### 3.2.3 Remote Zone Definitions

When defining all Remote Zones of the TANDBERG Border Controller, including the Traversal Zones (e.g. Remote Zone relationship to the TANDBERG Gatekeeper), it is now possible to define up to five different matching criteria for that Remote Zone. Each one of these criteria can be classified into one of three different conditions:

**Prefix Match** – as with Q2, a Remote Zone can be configured to match based on a specific prefix on the incoming query. A successful prefix, match will be considered a “strong match” and will be fulfilled if the incoming query does not match a locally registered endpoint. All “strong match” Location Requests (LRQs) will be sent out simultaneously, including both prefix and suffix matches. All prefix matches can either be included or stripped from the outgoing LRQ.

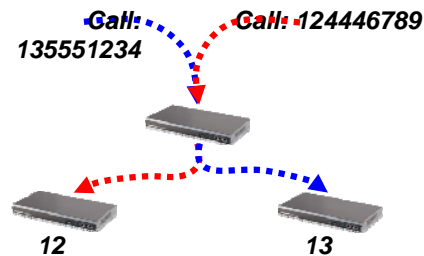


Figure 2. Prefix Match

**Suffix Match** – a Remote Zone can now be configured to match based on criteria that exists at the end of the incoming query to determine the proper Remote Zone to which the Border Controller will send the query (e.g. URI suffix match of ‘@company.com’). This match is considered to be a “strong match” and will be fulfilled if the incoming query does not match a locally registered endpoint. All “strong match” LRQs will be sent out simultaneously, including both suffix and prefix matches. As with the Q2 software release, the suffix match can be included or stripped with the outgoing LRQ.

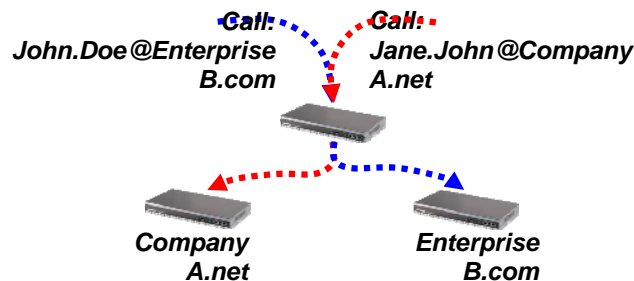
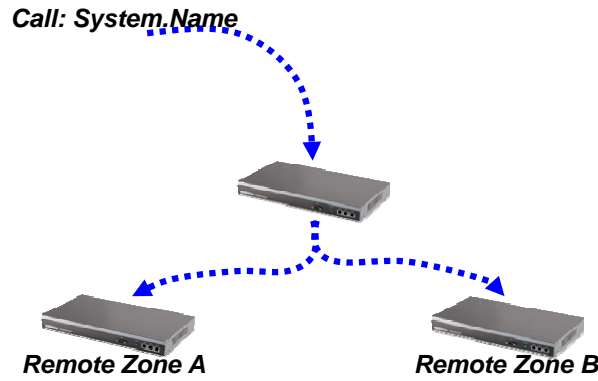


Figure 3. Suffix Match

**Always Match** – an “Always Match” Remote Zone is identical to a flat neighbor. The Border Controller will send all LRQs to these Remote Zones simultaneously as long as one of the following criteria is met:

- query does not match any local registrations *and* does not match any prefix or suffix match Remote Zones.
- any rejected query previously sent to a “strong match” Remote Zone.



**Figure 4. Always Match**

Each of the matching criteria can be used individually or in combination with each other when configuring all Remote and Traversal Zones on the Border Controller. The order in which the matches are defined within the Remote Zone does not affect the manner in which the Border Controller matches the criteria for the query – all comparisons are considered simultaneously and weighted equally.

### 3.2.4 Remote Syslog Server

The TANDBERG Border Controller now supports the ability to send log information to a remote syslog server, using standard syslog communications protocol, thereby allowing network administrators to record all Border Controller activity in the same way that all other network equipment is currently logged.

The Border Controller will send logs to the syslog server in one of three different levels:

**Level 1** – this level of logging includes only basic RAS messages, including call admission and registration messaging

**Level 2** – the second level of logging includes all RAS messaging

**Level 3** – the most verbose of all levels, level 3 includes all messages funneled through the Border Controller, including all non-standard and keep-alive messages.

### 3.2.5 Neighbor and Alternate Health Check

The Border Controller will actively monitor all neighbors and alternates within the configuration to monitor the health of the network and prevent prolonged call connectivity time due to a loss of communication with one of the Border Controllers on the network. The local system will utilize a combination of both normal call processing LRQs and the new “communication monitoring” LRQs (the monitoring process is performed every ten minutes).

The communications monitoring is performed by sending out an LRQ of H.323-Id of “*gatekeeper-monitoring-check*” and hop count of 1 to the Remote Zone and monitoring for a response from that Remote Zone (a hop count of 1 is used so the receiving gatekeeper or Border Controller does not send the LRQ to any of its configured neighbors). Any response, whether it is a confirmation or rejection of the LRQ, is considered positive communication with the Remote Zone and the far end gatekeeper remains active in the call logic. However, if the Remote Zone

fails to respond to either the monitoring LRQ or any LRQ sent during normal call logic, it is then considered inactive and is no longer used in normal call connection processing until it is returned to an active state. Any Remote Zone considered inactive will continue to be checked through the communications monitoring mechanism. As soon as a response is received to the monitoring LRQ, the Remote Zone will then be considered active and will be used in all future call processing.

### 3.2.6 Remote Zone Redundancy

The TANDBERG Border Controller now supports the ability to define up to five alternates for a Remote Zone. If a query needs to be sent to a Remote Zone that is determined inactive or the Remote Zone does not respond to a query sent in its direction, the local Border Controller will then send the LRQ to the first alternate in the list. If this Border Controller is “inactive,” the LRQ will be sent to the second alternate, and so on.

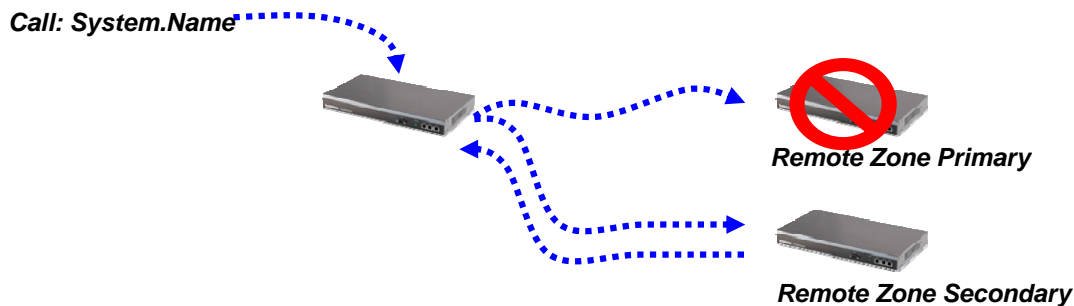


Figure 5. Remote Zone Redundancy

### 3.2.7 DNS Addressing

The TANDBERG Border Controller now will perform DNS lookup if any remote address is configured with the DNS host name instead of the IP address of the remote system, easing management and configuration of the system. In addition, configuring all remote addresses with DNS names will provide automatic redundant configuration (e.g. in the case of NTP server pools).

### 3.2.8 Password Reset

The TANDBERG Border Controller will now support the ability for administrative password reset, if needed. A user account ‘pwrec’ has been created for the Border Controller; this account will be used to reset the administrative password of the system. This account is only active on the local serial connection of the system and only for the first 60 seconds after startup. Once logged in using this username, the system will prompt for and confirm a new password. Afterwards, this password will be active for the administrator account. **Note:** both physical access and a restart of the Border Controller will be required to reset the password for the system. Because the ‘pwrec’ account does not have a password itself, the Border Controller should be located in a secure room to ensure access is limited to the system.

### 3.2.9 Management Session Timeout

The TANDBERG Border Controller now supports an inactivity timeout on the HTTPS, telnet and SSH remote management ports. If a management session on one of these ports is opened and inactive for a time configured by the administrator, the session will timeout and the administrator will need to reauthorize their username and password to resume the session. If changes have not been saved before the timeout, they will not be saved in the configuration upon the expiration.

### 3.2.10 Local Time Zone

With software release Q3.0, the internal clock of the TANDBERG Border Controller can now be configured to the local time zone. The time zone setting follows the standard time zone database

used in all major Linux distributions, FreeBSD, HP-UX, Mac OS X, and other Unix-based operating systems. Once configured, the time zone, used in the time stamps displayed on both the web interface and the remote syslog server, thereby assisting an administrator in determining when actions took place.

### 3.3 Supplemental Notes to Manuals

#### 3.3.1 Software Versions

The base version of the Border Controller will include an option of 5 concurrent Traversal Calls and 25 Registrations.

These options can be expanded by adding traversal calls and registrations in increments of either of 5 Traversal Calls/25 Registrations or 10 Traversal Calls/50 Registrations. The number of traversal calls can be increased up to 100 concurrent traversal calls with this software release.

#### 3.3.2 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 Border Controller:

D13691 TANDBERG Border Controller User Manual

D13380 TANDBERG Border Controller Installation Sheet

#### 3.3.3 Network Support

The TANDBERG Border Controller 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 Border Controller 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.

#### 3.3.4 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        | 2776 | TCP  | ↔         |
| Incoming H.323 RTP         | 2776 | UDP  | ↔         |
| Incoming H.323 RTCP        | 2777 | UDP  | ↔         |
| Incoming H.460.18/.19 Call | 1720 | TCP  | ↔         |
| LDAP Communication         | 389  | TCP  | ↔         |
| LDAPS Communication        | 636  | TCP  | ↔         |

## 3.4 Changes and Improvements since previous version

### 3.4.1 Usability Improvements

The following improvements have been made to improve the usability and user feedback of the TANDBERG Border Controller.

#### 3.4.1.1 Web Interface Readability

The TANDBERG Border Controller web management interface has been improved to allow sorting of all fields that contain lists, including the 'Registrations,' 'Registration History,' 'Call History' and other portions of the web interface that list status information.

#### 3.4.1.2 Log Readability

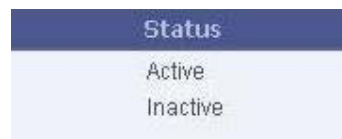
The Border Controller syslog text has been modified to improve the readability of all messages that are displayed while taking the log.

#### 3.4.1.3 Time Stamping

All events that take place within the event log will now include a timestamp when displayed in the web interface.

#### 3.4.1.4 Zone Status

The status of all remote Zones has been improved to show whether or not this Zone is 'Active.' If a Remote Zone is listed as 'Active,' it is considered alive and will be used normally when the Border Controller is processing a call. However, if a Remote Zone is listed as 'Inactive,' the Border Controller has lost communications with the system and it will not be used in normal call connection procedures until communication is restored and the Remote Zone responds to the health monitoring checks.

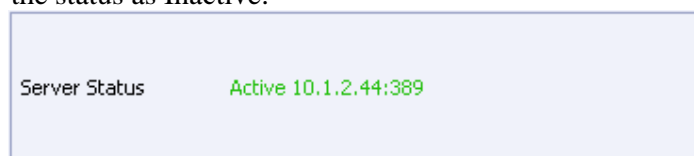


| Status   |
|----------|
| Active   |
| Inactive |

**Figure 6. Zone Status**

### 3.4.2 Remote System Connection Status

When the TANDBERG Border Controller is configured to connect to a remote system, such as an LDAP Server or NTP Pool, the success of the connection to that system will now be displayed on the web interface of the Border Controller. The 'Server Status' will display the IP address of the system it is trying to reach and whether the connection is 'Active' or 'Failed.' In addition, the color of the font will be displayed as **Green** for an Active connection or **Red** for an inactive connection. If the connection to the remote server has failed, the status will also display the reason for the failure. When the Border Controller is not configured to use this service, the system will display the status as Inactive.



|               |                      |
|---------------|----------------------|
| Server Status | Active 10.1.2.44:389 |
|---------------|----------------------|

**Figure 7. Remote System Connection Status**

### 3.4.3 Subzone Definition

Similar to Q2, Subzones are defined using subnets of endpoints that will register to that specific Subzone. However, instead of using the subnet mask as was used in previous versions, the subnet prefix length is now used. This number signifies the number of 1's used for the mask, instead of the mask itself. For example, in an IPv4 network, a subnet mask of 255.255.255.0 will now be represented by a subnet prefix of '24' as each of the 8 bits of the first 3 octets are set to 1, while the final octet is set to all 0's. For more examples of Prefix Lengths, please see the table below.

| Common Subnet Mask | Prefix Length |
|--------------------|---------------|
| 255.0.0.0          | 8             |
| 255.128.0.0        | 9             |
| 255.255.0.0        | 16            |
| 255.255.128.0      | 17            |
| 255.255.255.0      | 24            |
| 255.255.255.128    | 25            |
| 255.255.255.192    | 26            |

**Table 1. Prefix Lengths**

### 3.4.4 Calls to Unknown IP Addresses

When 'Calls to Unknown IP Addresses' is set to 'Indirect,' the TANDBERG Border Controller will now first check for the IP address to exist within any of the Subzone IP ranges, as dictated by the Subzone Address and Prefix Length. This will allow for a system registered to a Border Controller to then call a system on the same network that is not directly registered. For example, if a Subzone is configured with Subzone Address 10.1.2.0 and Prefix Length 24, a system registered to the Border Controller will be able to call an unregistered system with an IP address between 10.1.2.1 and 10.1.2.255.

### 3.4.5 NTP Server Connection

The process by which the Border Controller connects to a remote NTP server upon start-up of the system has been improved to retry the connection if it fails upon first attempt. The Border Controller will try to connect to the NTP server or pool up to five times on initial start-up. If, after five attempts, the connection still fails, the Border Controller will not attempt the connection again for up to 24 hours.

### 3.4.6 LRQ Handling

Upon receiving an LRQ from a gatekeeper other than any of the registered traversal gatekeepers for a system not locally registered, the Border Controller will now forward that LRQ to all configured Remote Zones prior to sending internal to the registered traversal gatekeeper.

### 3.4.7 Default IP Address

The Default IP Address of the TANDBERG Border Controller has now been changed to 192.168.0.100 (subnet mask 255.255.255.0) in order to allow for configuration of the system without the need for a serial cable. In order to configure the system without the serial cable, plug the Border Controller and a PC into a switch or hub completely disconnected from a network. Once connected, configure the PC with an IP address on the same subnet (e.g. 192.168.0.101) and then HTTP, HTTPS or SSH into the system in order to then configure the system as normal.

### 3.4.8 Web Interface

Resolved the Cross Site Scripting vulnerability at [https://host/calls\\_action](https://host/calls_action) page on the administrative web interface, as reported by ICSA labs. This vulnerability could only be executed with administrative access to the device.

A CRLF Injection Cross Site Scripting vulnerability located at [https://host/calls\\_action](https://host/calls_action) page was resolved. This vulnerability, as reported by ICSA labs, could only be executed with administrative access to the device.

### 3.5 Known Limitations

#### 3.5.1 TANDBERG

| Equipment                           | Limitations   |
|-------------------------------------|---|
| TANDBERG Border Controller ver Q3.0 | The Border Controller does not currently support a hybrid of IPv4 and IPv6 networks. The system will only be able to function in an IPv4 network or an IPv6 network. Supporting hybrid networks is being investigated for future development.   |
| TANDBERG Border Controller ver Q3.0 | If the Border Controller is ever set back to default values using the 'xcommand default tvalueset level : 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 default linksadd' |
| TANDBERG Border Controller ver Q3.0 | Upon resetting the password on the Border Controller, an error of "Error finding tty name: Inappropriate ioctl for device" will be displayed on the local dataport connection. This error should be ignored – the process has completed successfully, it is just a reporting error.         |
| TANDBERG Border Controller ver Q3.0 | If Authentication is enabled, the Border Controller will not properly process any Location responses from a Remote Zone. This will be resolved in the Q3.1 software release of software for the TANDBERG Border Controller.   |
| TANDBERG Border Controller ver Q3.0 | If an endpoint tries to register to the Border Controller with multiple H.323 IDs that differ only in capitalization, the Border Controller will reject the registration (e.g. H.323 IDs of 'ENDPOINT' and 'endpoint'). To resolve this issue, remove one of the H.323 IDs.                 |
| TANDBERG Border Controller ver Q3.0 | DNS lookup is not currently supported for addressing the syslog server – the IP address of the server must be entered.  |
| TANDBERG Border Controller ver Q3.0 | When initially configuring the External Manager address, the Border Controller will send out two boot traps to ensure proper communication has been established; the device itself does not actually reboot. This is normal operation.  |
| TANDBERG Border Controller ver Q3.0 | When two endpoints are connected in a traversal call using H.460.18/.19, an H.239 stream may not connect due to the Border Controller signaling the wrong port for the keep-alive probe.  |
| TANDBERG Border Controller ver Q3.0 | When involved in a traversal call, the TANDBERG Border Controller will not properly construct the   |

|  |   |
|--|---|
|  | 'Layer 1 Protocol' of the 'Bearer Capabilities' section of the Q.931 setup message as required by the H.225 standard. This missing field will cause calls to some third party endpoints to fail, specifically the TANDBERG Content Server. This issue will be resolved in Q3.1. |
|--|---|

### 3.5.2 Cisco

| Equipment                        | Limitations  |
|----------------------------------|--|
| Cisco PIX ver 6.2(4) and earlier | If H.323 fixup is turned on for the RAS channel on port 1719, the protocol will strip the Non-Standard Data portion of the Registration Request, where the Expressway-enabled information is sent between the Expressway client and the Border Controller. This will cause the registration to be rejected with 'neededFeatureNotSupported' as the error. To resolve, turn off H.323 fixup on the RAS channel. This issue does not exist with PIX software versions 6.3 and later as the H.323 stack within the PIX was upgraded beyond version 1 in later versions of software. |
| Cisco PIX ver 7.0(4) and earlier | In order to implement H.460.18/.19 with the Cisco PIX firewall, disable H.323 Fixup on the firewall for port 1720. Because all call initiation transmits to port 1720, according to the H.460.18 standard, application awareness of the firewall may interfere with the call setup.  |

### 3.5.3 RADVISION

| Equipment                      | Limitations  |
|--------------------------------|--|
| RADVISION viaIP MCU ver 4.0.31 | The RADVISION MCU cannot make outbound URI calls as it presents the outbound URI in the 'Email Address' field of the ARQ instead of the 'H.323 ID' field. The Border Controller does not currently support the 'Email Address' field within a request. |

## 3.6 Interoperability Testing

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

### 3.6.1 Gatekeepers

| Equipment             | Software Revision              |
|-----------------------|--------------------------------|
| RADVision ECS         | 3.5.2.5                        |
| Cisco MCM             | 12.3(10), 12.3(10a), 12.3(13a) |
| Polycom PathNavigator | 7.00.03                        |

### 3.6.2 Gateway Interoperability

| Equipment           | Software Revision |
|---------------------|-------------------|
| TANDBERG Gateway    | G2.1, G3.0        |
| TANDBERG 3G Gateway | R1.0              |
| RADVision gw-P20    | 4.0.0.40          |
| RADVision L2W GW    | 2.2.3.2.5         |

|                       |           |
|-----------------------|-----------|
| Polycom MGC 25/50/100 | 7.0.2.6   |
| Cisco CallManager     | 4.1(3)SR2 |

### 3.6.3 MCU Interoperability

| Equipment             | Software Revision            |
|-----------------------|------------------------------|
| TANDBERG MCU          | D3.4, D3.5, D3.6             |
| TANDBERG MPS          | J1.1, J2.0, J2.1, J2.2, J3.0 |
| Polycom MGC 25/50/100 | 6.02.4, 7.0.2.6              |
| RADVision ViaIP MCU   | 4.0.31                       |
| RADVision OnLan MCU   | 2.2.1.0                      |
| Cisco IPVC 3540       | 3.2.224                      |
| Codian MCU 4210       | 1.3(1.4)                     |

### 3.6.4 Streaming Servers

| Equipment               | Software Revision |
|-------------------------|-------------------|
| TANDBERG Content Server | S1.0              |

### 3.6.5 Endpoint Interoperability

| Equipment               | Software Revision  |
|-------------------------|--|
| TANDBERG MXP            | F1.4, F1.5, F2.5, F2.6, F3.0, F3.2, F4.0   |
| TANDBERG 150            | L1.1, L1.2, L2.2, L3.0, L3.1   |
| 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 | 6.2.0.1208   |
| Polycom iPower 680      | 5.3.0.1202   |
| Polycom EX              | 6.0.5  |
| Polycom FX              | 6.0.5  |
| Polycom ViewStation     | 7.5.4  |
| Polycom MP512           | 7.5.4  |
| Polycom SP 384          | 7.5.4  |
| Polycom VSX             | 8.03   |
| Polycom PVX             | 8.0.0.0522   |
| Sony PCS-1              | 3.14   |
| Sony PCS-TL50           | 2.11   |
| VTEL Galaxy             | 2.2.0.070  |
| Microsoft NetMeeting    | 3.01   |
| VCON Vpoint             | 6.5  |
| Aethra VegaStar         | 6.0.18   |

### 3.6.6 Firewall Interoperability

| Equipment        | Software Revision                                      |
|------------------|--|
| Cisco PIX        | 6.2(4), 6.3(1), 6.3(3), 6.3(4), 7.0(1), 7.0(2), 7.0(4) |
| Sonicwall SOHO 3 | 6.6.0.2  |
| Linksys BEFW11S4 | 1.44.2   |
| Linksys BEFSR81  | 2.45.10  |
| Linksys BEFSR41  | 1.05.00  |
| Linksys WRT54G   | 1.30.7, 1.42.3, 3.01.3                                 |
| Linksys WRT54Gv5 | 1.00.4   |