

TANDBERG Border Controller Q1 Software Release Document

TANDBERG

D50339, Rev 1.1

Table of Contents

1.	DOCUMENT REVISION HISTORY	3
2.	RELEASE NOTES FOR TANDBERG BORDER CONTROLLER SOFTWARE VERSION Q1.0	4
2.1	INTRODUCTION	5
2.1.1	<i>New Product Abstract</i>	5
2.2	NEW FEATURE OVERVIEW	5
2.2.1	<i>Firewall Traversal</i>	5
2.2.2	<i>Improved Addressing</i>	5
2.2.3	<i>Neighboring</i>	6
2.2.3.1	Flat Neighboring	6
2.2.3.2	Multiple Remote Neighbors and Zones.....	6
2.2.3.3	Control of Forwarding LRQs	6
2.2.4	<i>Registration</i>	6
2.2.4.1	Registration Control.....	6
2.2.5	<i>Local Management</i>	7
2.2.5.1	RS-232 Control	7
2.2.6	<i>Remote Management</i>	7
2.2.6.1	HTTP Management.....	7
2.2.6.2	HTTPS Management.....	7
2.2.6.3	Telnet	8
2.2.6.4	SSH	8
2.2.6.5	SNMP.....	8
2.3	SUPPLEMENTAL NOTES TO MANUALS	9
2.3.1	<i>Software Versions</i>	9
2.3.2	<i>References/Related Documents</i>	9
2.3.3	<i>Network Support</i>	9
2.3.4	<i>Layer 4 Ports Used</i>	9
2.4	CHANGES AND IMPROVEMENTS SINCE PREVIOUS VERSION	9
2.5	INTEROPERABILITY TESTING	10
2.5.1	<i>Gatekeepers</i>	10
2.5.2	<i>Gateway Interoperability</i>	10
2.5.3	<i>MCU Interoperability</i>	10
2.5.4	<i>Endpoint Interoperability</i>	10
2.5.5	<i>Firewall Interoperability</i>	11
2.6	KNOWN LIMITATIONS	11

1. Document Revision History

- Rev 1.1 - Release of Q1.1, Minor Release
- Rev 1.0 - Release of Q1.0, Initial Version

2. Release Notes for TANDBERG Gatekeeper Software Version Q1.1

2.1 Introduction

These release notes describe the features and capabilities included in the TANDBERG Border Controller Software minor release version Q1.1 released on 11 April 2005.

2.2 New Features Overview

2.2.1 Call Features

- The Call Time to Live field within the web interface of the Border Controller checks all calls at the specified interval (in seconds) to ensure they are still active calls. If the call is no longer active, the Gatekeeper will free up any resources not needed.
- Border Controller will now send a RIP (Request In Process) whenever it receives an LRQ.

2.3 Changes and Improvements Since Previous Version

2.3.1 RAS Signaling

- The Border Controller now responds with a GRJ if AutoDiscovery is turned off.
- Improved bandwidth restriction field such that calls that come in above maximum bandwidth connect at the maximum bandwidth specified, instead of being rejected.
- Improved calling far end that is registered to a routed mode gatekeeper.

2.3.2 Interoperability Improvements

- Resolved issue between Microsoft NetMeeting and Polycom ViaVideo.

2.3.3 Registration Restriction Improvements

- The Allow and Deny lists were expanded to 250 entries, the maximum number of registrations the Border Controller can have at any one time.

2.4 Known Limitations

- It is not possible to change the Ethernet speed from the web interface. In order to change this field, either telnet, SSH or connect to the dataport on the box and enter the command.
- Adding a system to the Deny List does not force that system to un-register from the Border Controller. It must be manually removed from the registration list.
- It is not possible to call between Microsoft NetMeeting and Polycom PVX over the traversal link.
- An Expressway-enabled endpoint (e.g. TANDBERG Gatekeeper or TANDBERG MXP Endpoint), cannot register to the TANDBERG Border Controller through a PIX firewall running software version 6.2 or prior. This particular version of software is only H.323 version 1 aware and, therefore, strips information from the Registration Request that identifies the endpoint as Expressway-enabled. This can be resolved either by upgrading the PIX firewall to a later version of software or turning off H.323 Fixup within the configuration of the firewall.

3. Release Notes for TANDBERG Border Controller Software Version Q1.0

3.1 Introduction

These release notes describe the features and capabilities included in the TANDBERG Border Controller software version Q1.0 released on 7 February 2005.

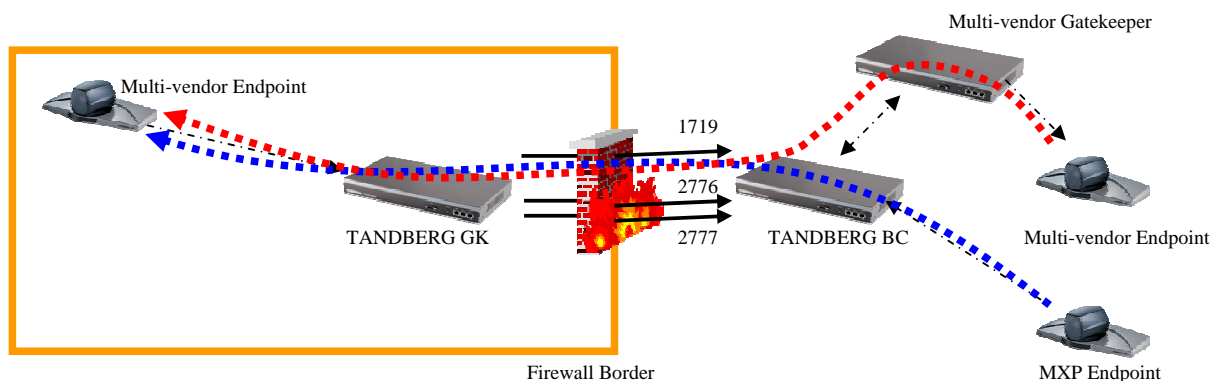
3.1.1 New Product Abstract

The TANDBERG Border Controller is a new addition to the TANDBERG Product Line. The Border Controller is designed to assist getting calls through an IP firewall and to ease IP dialing plans worldwide. The Border Controller will also provide bandwidth management and will control access to multiple network resources, such as an MCU or gateway.

3.2 New Feature Overview

3.2.1 Firewall Traversal

In conjunction with the TANDBERG Gatekeeper or TANDBERG MXP (running F2.0 or later), the TANDBERG Border Controller will allow a system to traverse a firewall for H.323 traffic without having to implement port forwarding, complex NAT rules or place systems on the public Internet. Utilizing this solution, an endpoint on a private network can call an endpoint on the public network by calling the IP address, E.164 alias or the H.323 ID of the far end system.



3.2.2 Improved Addressing

The TANDBERG Border Controller allows you to place and receive calls utilizing DNS (H.323 v5 Annex O) for the far end system. When an endpoint places a call to the far end system by DNS, one would dial either the H.323 ID or the E.164 alias of the far end system and append the DNS suffix of the far end organization.

Example: dialing john.doe@company.com would ask the gatekeeper or border controller with the DNS name of company.com to connect to the endpoint with the H.323 ID of john.doe.

Example: dialing 54321@company.com would ask the gatekeeper or border controller with the DNS name of company.com to connect to the endpoint with the E.164 alias of 54321.

3.2.3 Neighboring

3.2.3.1 Flat Neighboring

With Q1.0 software, the TANDBERG Border Controller will support neighboring with other gatekeepers and Border Controllers and zones without requiring a remote zone prefix. This allows for the creation of mesh networks within the H.323 infrastructure.

3.2.3.2 Multiple Remote Neighbors and Zones

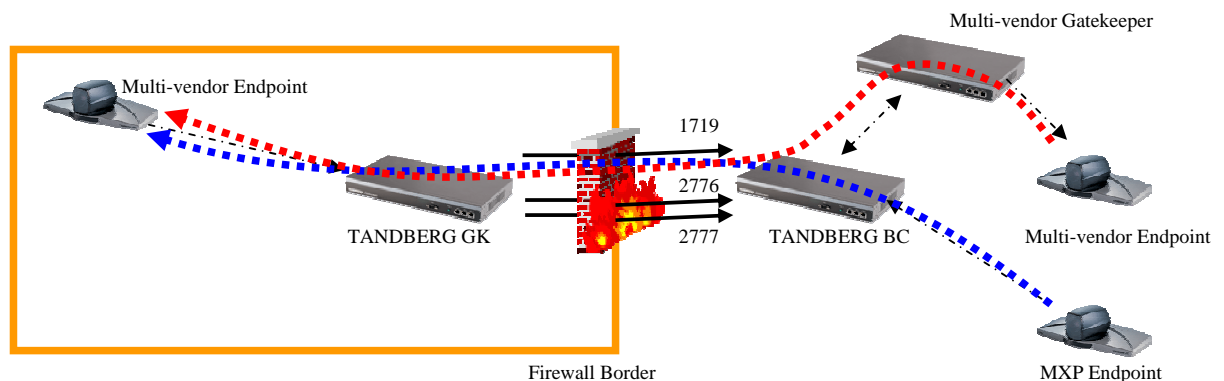
The TANDBERG Border Controller will allow the addition of multiple remote zones, both with and without remote zone prefixes. If the Border Controller receives a call that does not match any of the remote prefixes, the call will be forwarded to all remote zones that do not have a remote prefix.

3.2.3.3 Control of Forwarding LRQs

Q1.0 software will allow you to allow or deny the forwarding of LRQs to the remote neighbors in order to control network flow and remove LRQ loops from the network. You can choose to forward or not forward LRQs from the Border Controller.

3.2.4 Registration

The only devices that are able to register into a TANDBERG Border Controller directly are a TANDBERG Gatekeeper running N2.0 or later or a TANDBERG MXP Endpoint running F2.0 or later. Any other device must register into the TANDBERG Gatekeeper or another vendor gatekeeper that is neighbored either into the TANDBERG Border Controller or TANDBERG Gatekeeper in order to utilize the properties of the Border Controller.



3.2.4.1 Registration Control

The TANDBERG Border Controller will operate in one of three different modes in order to allow control of the systems that can register into the Gatekeeper, thereby allowing more control over the network in general.

- **Promiscuous Mode:** (Restriction Policy Off) anyone can register into the gatekeeper, regardless of the E.164 alias or H.323 ID
- **Allow List Mode:** the far end must register with an E.164 alias or H.323 ID that is on the list, otherwise the registration will be rejected.
- **Deny List Mode:** the far end will only be rejected if it tries to register into the Gatekeeper with one of the E.164 aliases or H.323 IDs that are on the Reject List.

3.2.5 Local Management

3.2.5.1 RS-232 Control

The Border Controller has 2 DB-9 serial ports that may be used for configuration and administration. The serial ports are also used for initial configuration using the embedded set-up wizard. Software upgrades may also be monitored via the serial ports.

In order to connect to either one of the RS-232 ports on the unit, you will need to connect using a null modem cable. You can connect using any RS-232 terminal emulation program, such as Microsoft HyperTerminal. The default connectivity parameters are:

Baud Rate: 115200 bps
Start Bits: 8
Stop Bits: 1
Parity: None

3.2.6 Remote Management

3.2.6.1 HTTP Management

The TANDBERG Border Controller has an embedded web interface for control. This interface offers a user friendly, graphically-driven method to configure and control the TANDBERG Border Controller on all features and functionality. The HTTP service is enabled by default.

You can disable the HTTP service on the Border Controller either through the embedded web interface or through telnet, SSH or the Dataport on the back of the unit. To disable it through the embedded web interface, navigate to System Configuration, Misc, uncheck the HTTP Service check box, click 'Save' and then click 'Restart'. To disable through the telnet, SSH or Dataport on the system, connect to the device and issue the command 'xconfiguration http mode: off'. Once confirmed, the box must be restarted for the change to take effect. NOTE: if the Border Controller is restarted, all active calls will be disconnected.

3.2.6.2 HTTPS Management

The TANDBERG Gatekeeper now has an embedded web interface for control. This interface offers a user friendly, graphically-driven method to configure and control the TANDBERG Gatekeeper on all features and functionality. The HTTPS service is disabled by default.

You can disable the HTTPS service on the Border Controller either through the embedded web interface or through telnet, SSH or the Dataport on the back of the unit. To disable it through the embedded web interface, navigate to System Configuration, Misc, uncheck the HTTPS Service check box, click 'Save' and then click 'Restart'. To disable through the telnet, SSH or Dataport on the system, connect to the device and issue the command 'xconfiguration https mode: off'. Once confirmed, the box must be restarted for the change to take effect. NOTE: if the Border Controller is restarted, all active calls will be disconnected.

3.2.6.3 Telnet

The Border Controller has an embedded telnet server for configuration and administration. The telnet server may be enabled if desired. The telnet service is disabled by default.

You can enable the telnet service on the Border Controller either through the embedded web interface, SSH or the Dataport on the back of the unit. To enable it through the embedded web interface, navigate to System Configuration, Misc, check the Telnet Service check box, click 'Save' and then click 'Restart'. To enable through SSH or Dataport on the system, connect to the device and issue the command 'xconfiguration telnet mode: on'. Once confirmed, the box must be restarted for the change to take effect. NOTE: if the Border Controller is restarted, all active calls will be disconnected.

3.2.6.4 SSH

The Border Controller has an embedded SSH (Secure Shell) server for configuration and administration. SSH provides a CLI (command line interface) similar to telnet but over a secure, encrypted connection. The SSH server may be disabled if desired. The SSH service is enabled by default.

You can disable the SSH service on the Border Controller either through the embedded web interface or through telnet, SSH or the Dataport on the back of the unit. To disable it through the embedded web interface, navigate to System Configuration, Misc, uncheck the SSH Service check box, click 'Save' and then click 'Restart'. To disable through the telnet, SSH or Dataport on the system, connect to the device and issue the command 'xconfiguration ssh mode: off'. Once confirmed, the box must be restarted for the change to take effect. NOTE: if the Border Controller is restarted, all active calls will be disconnected.

3.2.6.5 SNMP

The Border Controller has an embedded SNMP manager for proactive reporting of problems and systems status. Programs such as HP OpenView require this feature in order to work properly. The SNMP manager can be disabled if desired. The SNMP service is enabled by default.

You can disable the SNMP service on the Border Controller either through the embedded web interface or through telnet, SSH or the Dataport on the back of the unit. To disable it through the embedded web interface, navigate to System Configuration, Misc, uncheck the SNMP Service check box, click 'Save' and then click 'Restart'. To disable through the telnet, SSH or Dataport on the system, connect to the device and issue the command 'xconfiguration snmp mode: off'. Once confirmed, the box must be restarted for the change to take effect. NOTE: if the Border Controller is restarted, all active calls will be disconnected.

3.3 Supplemental Notes to Manuals

3.3.1 Software Versions

There are 3 different versions of software available for the TANDBERG Border Controller. These three versions separate the number of concurrent traversal calls that may be active at any single time.

- 5/25** - Allows for 5 concurrent traversal calls and 25 concurrent registrations.
- 10/50** - Allows for 10 concurrent traversal calls and 50 concurrent registrations.
- 20/100** - Allows for 20 concurrent traversal calls and 100 concurrent registrations.

3.3.2 References/Related Documents

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

TANDBERG FTP Site – <http://ftp.tandberg.net>

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 Gatekeeper is an H.323 device and is intended to be connected to an 802.3 IP network. Only the first 802.3 IP port is used, the other two are for future development. The 802.3 IP 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.

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	↔
SNMP (Traps)	162	UDP	⇒ (outgoing from Gatekeeper)
Incoming H.323 Call	2776	TCP	↔
Incoming H.323 RTP	2776	UDP	↔
Incoming H.323 RTCP	2777	UDP	↔

3.4 Changes and Improvements since previous version

- Version Q1.0 is the initial release of the TANDBERG Border Controller

3.5 Interoperability Testing

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

3.5.1 Gatekeepers

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

3.5.2 Gateway Interoperability

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

3.5.3 MCU Interoperability

Equipment	Software Revision
TANDBERG MCU	D3.4, D3.5
TANDBERG MPS	J1.1, J2.0
Polycom MGC 25/50/100	6.02.4, 7.0.0.57
RADVision ViaIP MCU	3.5.24
RADVision OnLan MCU	2.2.1.0
Cisco IPVC 3540	3.2.224

3.5.4 Endpoint Interoperability

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

Aethra VegaStar	5.1.35
-----------------	--------

2.5.5 Firewall Interoperability

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

3.6 Known Limitations

- Due to the H.323 awareness of later versions of Linksys Router software, encryption does not work through the WRT54G.
- Border Controller will not respond with GRJ when AutoDiscovery is turned off.
- Incoming calls will fail if a system not registered into the Border Controller makes a call to a system registered into the Border Controller and bandwidth restriction is turned on.
- Inconsistent calls from Microsoft NetMeeting to Polycom ViaVideo.
- When MCM is directly neighbored to the Border Controller and a system directly registered to the Border Controller calls a system directly registered to the MCM, the MXP will not receive video.
- Outbound registration from either the TANDBERG Gatekeeper or TANDBERG MXP running F2.0 or later will not succeed to the TANDBERG Border Controller through a Cisco PIX running 6.2.x software as this version of Cisco PIX software only supports H.323 version 2 and, therefore, strips the non-standard data information that is necessary for proper registration with the Border Controller. In order to resolve this issue, disable H.323 Fixup on the PIX and registration will occur properly.