



Cisco BTS 10200 Softswitch Incremental Shared-Memory Restoration Feature Module

Revised: July 31, 2008

This document describes the Incremental Shared-Memory Restoration (ISMR) feature for Release 6.0 of the Cisco BTS 10200 Softswitch and explains how to use it. The ISMR feature is part of an operational solution that addresses comprehensive recovery from disastrous system incidents like an abrupt power-cut.

Understanding the Incremental Shared-Memory Restoration Feature

The ISMR feature represents a means to recover the Cisco BTS 10200 shared-memory (SHM) on a platform by bringing it back to the state where it was at the time of a system disaster (ex.: power-cut). The Cisco BTS 10200 ISMR works in conjunction with the Cisco BTS 10200 ASMB (Automated Shared-Memory Backup) feature, which restores all of the BTS 10200 shared-memory contents to a point-in-time of the latest SHM backup. However, several provisioning and control commands (incremental commands) might have changed the contents of the SHM after the latest periodic backup. An audit/sync step after an ASMB operation could take considerable time if the incremental commands are not applied in the database in an efficient manner.

The ISMR feature working in conjunction with the Shared-Memory Synchronization (SMS) feature bridges the gap in SHM between the latest backup snapshot and disaster-moment snapshot in an extremely efficient manner. When the disaster-moment snapshot is restored, post-ASMB-backup commands restored, the Cisco BTS 10200 restarted, and EMS database audited/synchronized, the system is ready to restart operations from a system internal disaster incident.



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2008 Cisco Systems, Inc. All rights reserved.

The ISMR feature provides:

- A comprehensive solution for automatic ongoing logging of Post-Backup Incremental Commands (PBIC) (such as provisioning and control commands that were affected in the SHM after latest successful backup).
- A configurable manual incremental restoration of SHM using the incremental commands.
- A best-effort solution with the no specific time constraints. The time for the ISMR to complete depends on the number of PBICs present in the system.
- A complete snapshot of the SHM in conjunction with SMS feature.

The ISMR feature consists of the following logical components:

- **Recording**—The recording component of ISMR feature is responsible to continuously intercept and log the provisioning and control command in a redundant manner to the ISMR log archive.
- **Editing**—The editing component of ISMR feature is responsible for sequencing, filtering and formatting an ISMR log file in such a manner that is ready for ISMR replay. The original recording will have certain annotations that need to be filtered out.
- **Playback**—The playback component of ISMR feature, which is activated after an ASMB restore, is responsible for performing the necessary editing of the ISMR log archive and for using the logged commands to restore provisioning into the applicable shared memory.

Feature Interactions

The ISMR feature works in conjunction with the ASMB feature and the SMS feature.

Prerequisites

The ASMB feature is a prerequisites for the ISMR feature.

Assumptions

The ISMR feature implementation assumes that all mated-pair Cisco BTS 10200 network-elements work within the same time-zone.

Operating

This section explains how to perform operational tasks for the ISMR feature.

- [Recovery Operations](#)
- [Single Platform Disaster Operations](#)
- [Multi-Platform Disaster Operations](#)

Recovery Operations

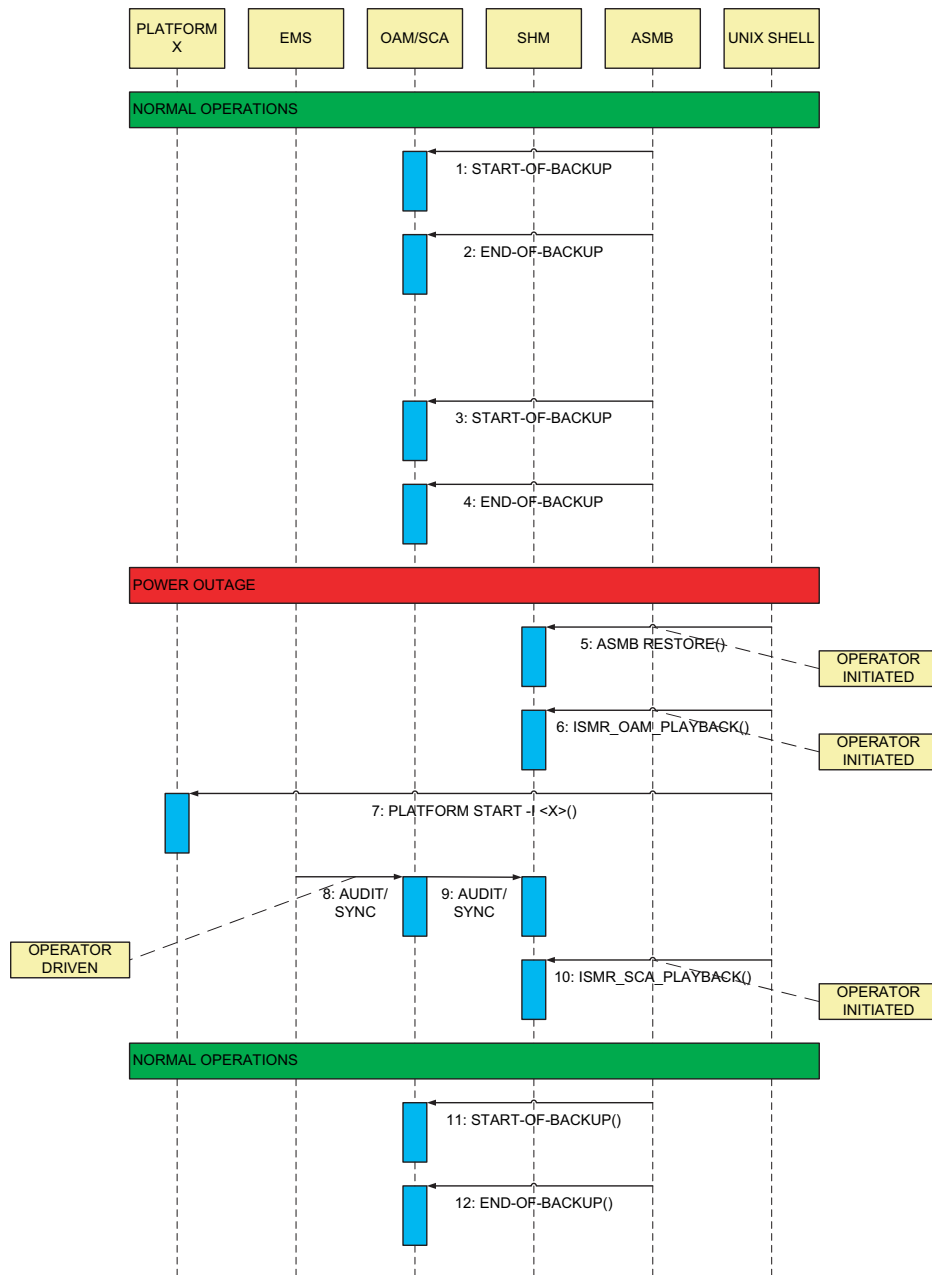
The ISMR recovery operations are shown in Figure 1. As a convention, the “()” shown along side tasks in Figure 1 implies a predefined set of sub-procedures.



Note

Since at the time of ISMR playback the platform is *not* supposed to be up, there is no active/standby classification. The ISMR provisioning playback should work on either side during this phase. Once the platform is up, ISMR playback will only work on the active side.

Figure 1 Comprehensive Shared Memory Backup and Restoration - Operations



Single Platform Disaster Operations

When a single Cisco BTS 10200 platform encounters a disastrous condition resulting in SHM corruption, the following ISMR operational procedures must be followed in order to comprehensively recover from the disaster or SHM corruption:

-
- Step 1** Perform the operational steps recommended for the ASMB feature.
 - Step 2** Execute the **ISMR_prov_playback** command as per its command-line syntax.
 - Step 3** Perform a platform start.
 - Step 4** Synchronize SHM database with EMS by use of the CLI audit or sync facility.
 - Step 5** Execute the **ISMR_ctrl_playback** command as per its command-line syntax.
-

The Cisco BTS 10200 SHM should now be the same as the post disaster-moment snapshot.

Multi-Platform Disaster Operations

In [Table 1](#), a Y in a column indicates that the corresponding platform (in the column header) has been struck with a disaster, while a — indicates normal operation. The fourth column identifies the sequence in which the platforms are restored. The specific recovery steps are noted in the [Single Platform Disaster Operations](#) section. If both primary and secondary sides of a network-element are down, it is recommended to recover the primary side first. In order to save time to restore, CA and FS can be restored simultaneously if they are restored on different hosts. EMS restoration must always follow CA/FS restorations.

Table 1 *Multi-Platform Disaster Operations Matrix*

| EMS | CA | FS | Recovery Sequence for Platforms |
|-----|----|----|--|
| — | — | — | FS Note If every platform is normal, recovery sequence of platforms should also be normal (-). If needed, all platforms can be included (CA, FS, EMS not only FS). |
| — | Y | — | CA |
| — | Y | Y | CA, FS |
| Y | — | — | EMS |
| Y | — | Y | FS, EMS |
| Y | Y | — | CA, EMS |
| Y | Y | Y | CA, FS, EMS |

Troubleshooting

This section explains how to troubleshoot the following conditions:

- [Secure File Transfer Protocol Transfer Failed—Database \(25\)](#)

Secure File Transfer Protocol Transfer Failed—Database (25)

The Secure File Transfer Protocol Transfer Failed alarm (major) indicates that a secure file transfer has failed. The primary cause of the alarm is that the SFTP was unable to connect between active and standby call agents. To troubleshoot and correct the primary cause of the alarm, verify communication between primary and secondary call agent (CA). On each CA, ping the other node. The secondary cause of the alarm is that the system was unable to login to the remote host. To troubleshoot and correct the secondary cause of the alarm, verify that the SSH keys have been pre-configured for user root on both active and standby call agents. The tertiary cause of the alarm is that a file transfer error has occurred. To troubleshoot and correct the tertiary cause of the alarm, check the Error dataword to see if it gives an indication of the kind of error that occurred. It could be a file-system error on the remote host, or a communication failure between the active and standby call agents.

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0807R)

Copyright © 2008 Cisco Systems, Inc. All rights reserved.

