



**Verizon Technology Organization
Systems Integration and Testing**

**Technical Memorandum
Power Failure Recovery Test
For Network Elements**

Version 2.1 March 4, 2005 – APPROVED

© Verizon 2005. All Rights Reserved.

Doc Identifier: **SIT.TST.TM.OTH.2005.001**

Document Identification & Approval

Document	SIT.TST.TM.OTH.2005.001
Document Name:	Power Failure Recovery Test for Network Elements
Version Number:	2.1
Effective Date:	April 4, 2005
Document Status:	APPROVED
Document Author(s):	John Kim, Stan Lee, Cliff Santos, Muzaffer Kanaan, Shuoru Wang
Contract Number:	N/A
Approved Date:	April 4, 2005
Approved By: (Signature)	<i>Alex Laparidis</i>

The information contained herein is subject to change without notice and should not be construed as a commitment by Verizon. Verizon assumes no responsibility for any errors that may appear in this document.

Verizon makes no representations that the use of its products in the manner described herein will not infringe on existing or future patent rights, nor do the descriptions in this document imply the granting of licenses to make, use, or sell equipment or software in accordance with the description.

Document File Name: Power Failure Recovery-v2.1APPROVED.doc

© Verizon 2005. All Rights Reserved. Information contained herein is subject to change without notice.

Last Revised: April 4, 2005

Document Revision History

Document Name: Power Failure Recovery Test for Network Elements
Technical Memorandum

Document Identifier: SIT.TST.TM.OTH.2005.001

Version & Date	Section & page	Contact Name & Tel.	Action Taken	Comments
1.0 2/18/05		John Kim 781-466-2702	New Document	
2.0 2/23/05		John Kim 781-466-2702	Change	Edits incorporated from internal review.
2.1 4/4/05		Stan Lee 781-466-2454	Change	Reference to Network Elements not only transport NE. Addition of restoration time for data elements. Formatting and grammatical changes.

Note: Actions taken are: New = new document, Add/Delete/Change = a section or topic that has been added, deleted or changed.

Reviewed by:

Alex Laparidis

Alex Laparidis, Director-Transport Systems Testing

Additional Approvals:

James E. Sylvester, Vice President, System Integration and Testing

Table of Contents

DOCUMENT IDENTIFICATION & APPROVAL	II
DOCUMENT REVISION HISTORY	III
TABLE OF CONTENTS	IV
1 INTRODUCTION	5
2 PURPOSE AND SCOPE.....	5
3 GR-472 HIGHLIGHTS	6
3.1 STANDARDS.....	6
3.2 NETWORK ELEMENT.....	6
3.3 NETWORK SYSTEM	7
3.4 SIZE	7
3.5 AUTOMATIC RESTORATION.....	7
3.6 RESTORATION TIMES.....	7
4 TEST PROCEDURES	8
4.1 MEASURABLE EVENTS.....	9
4.1.1 <i>Test scenario #1: Worst Case</i>	9
4.1.2 <i>Test scenario #2: Typical Configuration Without Database Change</i>	10
4.1.3 <i>Test scenario #3: Typical Configuration With Database Change</i>	10
5 REFERENCES	11

1 Introduction

Verizon strives to provide the most reliable network to our customers. In addition to the highest possible reliability, Verizon strives to have the least amount of down-time and interruptions to the customer's services and to the customer. With this reliability and availability considerations, this document is designed specifically to address power interruption impact to our Network Elements (NE).

Even with redundant power sources or backup supplies, it is still possible that under rare circumstances the Network Element may lose all or partial power. Because the possibility exists that power will fail, Verizon has to be sure that, on those rare occasions, all the equipment in Verizon's network in all locations, including Central Offices (CO), Controlled Environmental Vaults (CEV) and huts, and telephone closets at customer locations can recover. Verizon should be confident that the equipment in its network can recover from a partial or complete power failure with no human intervention and in a reasonable amount of time. Recovery includes restoration of provisioning and configuration databases, service traffic, and normal management access.

2 Purpose and Scope

The Verizon network is composed of Network Elements, each of which should have some form of non-volatile memory to allow it to recover from a failure, and restore all traffic with no manual intervention. Failure might be caused by human error, power failure, Network Element or Network System (NS) design flaws, software bugs, etc. This document focuses on recovery and restoration from power failure of the Network Element.

This document highlights the requirements from Telcordia Generic Requirements (GR-472) for Network Element Configuration Management as key Verizon requirements, and outlines test procedures that can be used when testing Network Elements in a controlled laboratory environment of Verizon Laboratories, the Network Element manufacturer, or third party certification labs.

The restoration times outlined in this document are only recommendations based on GR-472. Not all equipment will be able to recover in the same time frame. Not all Network Element types have restoration times specified in GR-472 or other standards documents. Each Network Element or Network System should be tested separately and documented. This characterization of the restoration time is a requirement of the Verizon Systems Integration & Testing Lab Entry process.

3 GR-472 Highlights

3.1 STANDARDS

In GR-472-CORE (Network Element Configuration Management), Telcordia outlines their view of memory administration that pertains to the Configuration Management functions in a Network Element or a Network System. Section 6.6 of GR-472 describes memory backup and restoration guidelines for Network Elements (NE) and Network Systems (NS). In addition, Telcordia sets requirements and objectives for restoration times for these NEs and NSs.

3.2 NETWORK ELEMENT

Definitions of an NE are described in section 1.1 of GR-472:

“An NE is a program-controlled processor entity in the Telecommunications Network (TCN) that provides existing and emerging digital and/or analog services. Switching systems with stored program control are called switching NEs. Transport systems consist of distribution and interoffice transmission facilities terminated by equipment that performs signal termination functions and various related functions; processor-controlled transport systems are called transport NEs.

The NEs considered in this GR range from very small (e.g., small transport NEs) to very large systems (e.g., large switching NEs). Therefore, the implementation complexity and functional robustness of these elements will vary according to the resources and capabilities of the individual NEs. The intent, however, is for remote Operations Systems (OSs) to have a common conceptual view of the database of each of the NEs to which they are interfaced regardless of their respective classifications.

The two basic characteristics common to all NEs regardless of their functions and types are as follows:

- NE internal processes and functions are controlled by a system of embedded software or firmware programs that may interface with, be programmed by, or customized by external systems equipment.
- Each NE contains a data store in which a database is maintained to support the functional operations of the NE.

Within each NE, it is assumed that the software programs include the following functions in addition to their main tasks of supervising and executing NE functions:

- An operations interface function that supports the interface protocols and services of the interworking Configuration Management Operations System (CMOS)¹
- Input command interpreter, command execution software, and message generation software functions
- A database management function that provides an external conceptual view of the internal NE data and their inter-relationships and manages access to the internal NE database.”

3.3 NETWORK SYSTEM

An NS is defined in section 1.2 of GR-472:

“An NS is a program-controlled processor entity of the TCN that provides ancillary network functions and the associated network operations functions. An example of an NS is the Service Control Point (SCP), which provides service-specific information to a switching NE communicating over the Common Channel Signaling (CCS) network using Signaling System Number 7 (SS7) protocols. Other examples of NSs include Advanced Information Network (AIN) Release 1 adjuncts and service nodes.”

3.4 SIZE

Network elements and network systems come in a variety of sizes. GR-472 section 6.6 categorizes NE and NS into three size categories:

- Large NEs or NSs (e.g., large switching NEs) for which a Configuration Management OS (CMOS) will, in general, provide only incremental backup and restoration, or will not back up
- Intermediate-sized NEs or NSs (e.g., large transport NEs or small switching NEs) that a CMOS will back up and restore using bulk transfer of a binary image of the data
- Small NEs or NSs (e.g., small transport NEs) that a CMOS can back up and restore by sequentially sending the same commands originally used to configure and provision the NE or NS (command-by-command restoration).

3.5 AUTOMATIC RESTORATION

GR-472 requirement R6-28 states:

R6-28 [88] An NE or NS shall be capable of automatically initiating memory restoration from the primary local backup on power-up after a power failure or after a similar problem causing volatile data loss. It shall be possible to disable this feature before a failure has occurred and to abort it by entering a command immediately after power-up. The purpose of aborting or disabling this feature can be exemplified by any one of the following situations:

- The backup data is or is suspected to be “corrupted”
- The NE or NS is unable to restore itself from the primary local backup after it has attempted to do so
- A different copy of the backup data will be used to restore the memory.

Verizon views this requirement as enabling power failure recovery to require no manual intervention.

3.6 RESTORATION TIMES

Some restoration time requirements are described in GR-472:

R6-32 [92] To protect against data loss because of power failures, human error, etc., transport NEs shall provide a primary non-volatile backup memory within or close to the equipment frame. This backup shall provide rapid restoration of data after a loss has occurred and this backup shall meet a 5-minute required restoration time requirement in a cold start.

R6-55 [115] It shall be possible to restore a switching NE database from a snapshot stored in a DBMS in less than 15 minutes. The snapshot may have been created online or reentered into a DBMS from an external copy.

R6-56 [116] It shall be possible, within a period of 1 hour, to restore the database from the most recent snapshot and reenter from the log all updates since the snapshot was taken. This may require more frequent snapshots to be taken than would be needed to satisfy the 30-hour requirement.

Based on these requirements, Verizon requires that on a single transport NE, traffic should be fully restored within 5 minutes of a cold start. A switching NE must restore from the last database snapshot within 15 minutes, and with all recent changes from the last snapshot within 1 hour.

For data NEs, e.g. routers, ATM switches, etc., which are not clearly defined by GR-472 or any standards reference document, Verizon recommends that traffic should be fully restored within 15 minutes of a cold start.

Not all NEs will meet these requirements. SIT documents all exceptions observed of this type. However, the full impact assessment of the results, as well as the final decision to deploy a particular platform (even if it does not meet the 5-minute requirement), rests with the Verizon entity responsible for the deployment.

No differentiation in restoration times has been made in GR-472 for different size elements, how much the element is loaded, or how the element is configured in terms of type or quantity of interfaces. Therefore, for characterizing the restoration times, Verizon requires at least two configurations:

- the worst-case scenario, which could include maximum number of cross-connects, interfaces, and 100% traffic load.
- a more typical field deployment configuration example representing a realistically diverse mix of cross-connect types, interfaces, and 80% traffic load.

The actual configurations must be reviewed and approved by Verizon prior to actual lab assessment of restoration time.

4 Test Procedures

In the following sections, the test scenarios described are intended to reflect the worst case situation for power failure recovery and a more typical situation in terms of NE configurations regarding traffic load and provisioning. Within the typical scenario are separate test requirements to show any differences in restoration if a database change has been backed up or not backed up. The changes should still restore whether they have been backed up or not.

The power failure should be exercised by either pulling the breaker or fuse at the external fuse alarm panel associated with the NE's A and B power feeds or at the Battery Distribution Fuse Bay (BDFB) if the NE power feeds are directly cabled there, or disconnecting or turning off AC power supplies if the NE is powered via AC adaptors. Essentially, the intention is to safely disconnect both external power supply feeds A and B to the NE shelf, one feed at a time.

Measurable events during these test scenarios are described below and must be observed and documented.

4.1 MEASURABLE EVENTS

During the testing of power failure recovery, several events should be timed. Multiple test cycles may have to be run in order to capture all of these times.

- Local login availability (The point at which a local user can use the craft interface such as TL-1 and log into the element).
- Local provisioning (The point at which the user at the craft interface can make local provisioning changes to the element).
- Full recovery of TDM (i.e., DS1, DS3, OC-n) traffic (The point at which traffic is fully recovered for every STS and VT1.5 connection on the system) as applicable to the Network Element.
- Full recovery of narrowband traffic (i.e., POTS, specials, ISDN, DDS) as applicable to the Network Element.
- Data traffic recovery (The point at which traffic is recovered for services like 10/100MB, Gigabit Ethernet, Fibre Channel, FICON, etc.) as applicable to the Network Element.
- SDCC communication (The point at which SDCC communication channels are recovered and remote SDCC access is allowed to other elements) as applicable to the Network Element.
- Remote login availability (The point at which a user can login remotely to the network element over in-band channels like the SDCC) as applicable to the Network Element.
- Remote provisioning (The point are which a user can make provisioning changes remotely over in-band channels like the SDCC channel) as applicable to the Network Element.
- Alarm-free state (The point at which the element is alarm-free, or the state at which it was prior to the incident).

4.1.1 Test scenario #1: Worst Case

- Establish test traffic
- Include appropriate types and quantities of circuits, optical, electrical, EOS, etc. for worst-case configuration.
- Fully load System to stress the system to its maximum capacity and worst-case recovery.
- Ensure element is in an alarm-free state
- Perform a database back up according to manufacturer procedures
- Cause a complete power failure of the "A" feed
- Cause a complete power failure of the "B" feed
- Wait 30 seconds

- Restore power to the “B” feed
- Measure recovery times as outlined in section 4.1 of this memorandum
- Restore power to the “A” feed
- Ensure element is in an alarm-free state once again

4.1.2 Test scenario #2: Typical Configuration Without Database Change

- Establish test traffic
- Include appropriate types and quantities of circuits, optical, electrical, EOS, etc. for a typical field deployment configuration.
 - Example: the system should be sufficiently loaded to stress the system, typical of a field deployed system: 80%; systems with ring capabilities loaded with various facility protection group types and rates.
- Ensure element is in an alarm-free state
- Perform a database back up according to manufacturer’s procedures
- Cause a complete power failure of the “A” feed
- Cause a complete power failure of the “B” feed
- Wait 30 seconds
- Restore power to the “B” feed
- Measure recovery times as outlined in section 4.1 of this memorandum
- Restore power to the “A” feed
- Ensure element is in an alarm-free state once again

4.1.3 Test scenario #3: Typical Configuration With Database Change

- Establish test traffic
- Include appropriate types and quantities of circuits, optical, electrical, EOS, etc. for a typical field deployment configuration.
 - Example: the system should be sufficiently loaded to stress the system, typical of a field deployed system: 80%; systems with ring capabilities loaded with various facility protection group types and rates.
- Ensure element is in an alarm-free state
- Perform a database back up according to manufacturer’s procedures
- Create a change in the database (delete cross-connection, equipment or facility)
- Do NOT repeat database back-up
- Cause a complete power failure of the “A” feed
- Cause a complete power failure of the “B” feed

- Wait 30 seconds
- Restore power to the “A” and “B” feed
- Restore database from the file saved at the beginning of this cycle
- Ensure element is in an alarm-free state once again

5 References

- Telcordia GR-472-CORE, *Network Element Configuration Management*, Issue 2, Revision 2, February 1999.
- TR-NWT-000170, *Digital Cross-Connect System Generic Requirements and Objectives*, Issue 2, January 1993.

{End-of-document}