APPENDIX 1

B

Description of Proposed Work

The team working this issue should consider the following total quality process to quantify signaling network vulnerability, identify major reliability issues and propose problem solutions.

1. Collect appropriate data from all available industry sources to determine and/or confirm areas of greatest criticality and risk, and with the greatest potential for signaling network reliability improvement.
2. Perform sufficient analysis of the data to determine the root cause(s) of the problem(s). Sub-analysis should include:
   - Design shortcomings
   - Alarms
   - Alarm response
   - Procedures
   - Training
   - Documentation
   - Testing
   - Customer Education (Public service agencies, users, etc.)
3. From the root cause analysis determine an appropriate action plan to reduce/eliminate the possibility or severity of failures in high risk areas. Also consider ways that recovery procedures may be implemented more quickly or efficiently.
4. Determine industry "Best Practices" for dealing with the root cause analysis findings and share this information with industry participants as soon as possible. Also consider cost/benefit tradeoffs of these "Best Practices."
5. Develop a timeline and metrics to measure the effectiveness of the team's recommendations.
6. Consider the following tactics/ideas offered by the Steering Team as potential means to address the findings of the root cause analysis. These represent ideas from the Steering Team which we want to share. They may be accepted or rejected by the signaling network systems focus team.

   A. Improve Network Node Reliability
      - Improvements in the protocol
      - Improved testing of nodes (hardware and software, and interoperability of nodes and networks)
      - Outage information sharing among the industry to help service providers prevent/react to events in their own networks.

   B. Improve the robustness of the CCS network architecture implementations
      - Assure initial design and ongoing maintenance of link diversity for intra-company (e.g. A-Link) and cross carrier interconnect

Network Reliability Council
Issue Statement

Issue Title: Signaling Network Systems

Author: Gary Handler
Bellcore

Problem Statement/Issues to be Addressed

With the development and growing implementation of Common Channel Signaling (CCS) networks, the reliability of telephone services as seen by the customers has become heavily dependent upon the reliability of the CCS networks. The signaling function for basic call set-up and Intelligent Network (IN) services is now concentrated into a common network containing a small number of nodes and links. To reduce the chances of service interruptions, the CCS network design contains many levels of protection against failure modes ranging from error correction and retransmission in the protocol to redundant nodes and links in the architecture. Although service failures are unlikely, no network is fail safe and when a major failure of the CCS network occurs it has the potential to cause long duration loss of telephone service to a very large number of telephone customers. Moreover, because the CCS network is highly distributed across multiple carriers, a failure in one carrier's network can adversely affect another's. National service reliability as well as individual carrier network reliability needs to be assured.

Areas of Concern & Problem Quantification

Following are the main areas of concern:

A. *CCS node reliability* - One data set over the last 18 months indicates that STP total system downtime is approximately 46 minutes/year (if we exclude the major outages of June and July, 1991, the number falls to just over 6 minutes/year) as compared to the Bellcore objective of 3 minutes/year. About 60% of the downtime is attributed to software design problems. For SSPs, about half of their downtime is attributed to procedural errors. In addition, node and network interoperability problems have been observed.

B. *CCS network architecture, intra-company and cross-carrier* - CCS network architectural design guidelines were developed so that the CCSN will continue to provide service when single elements fail, and in many cases when multiple elements fail. A failure mode attributed to a common STP software fault resulting in the spread of congestion has been observed in 8 incidents and causing 5 mated STP pair outages in 1991. Based on these incidents, the probability of a serious mated pair outage is estimated to be about 3% per year (if we exclude the major outages of June and July, 1991, the number falls to 0.04%) as compared to the design objective which is almost zero. Node isolations due to lack of implementation or maintenance of link diversity have also been observed and may increase in importance with interconnect.

C. *CCS network operations, trouble detection and recovery including cross-carrier interactions* - Bellcore data indicates that about 25% of single STP outages are lasting more than one hour, with the longest being about 9 hours. About 80% of the mated pair STP outages lasted longer than 100 minutes.

D. *The inability to effectively measure the scope and impact of network outages* in order to a) target corrective actions, and b) measure long term trends in performance. No industry agreed upon parameter or method is currently available.

failures - No Activity

- Establishment of a Maintenance Clearing House to assist in network "Change Management" and help resolve minor CCS troubles on a routine basis. - NOF - Information Sharing on Operational Problems that Contribute to Network Outages. Issue #161
- Institution of an Emergency Response Plan for cross-carrier coordination of major network restoration activities. - NOF - SS7 Emergency Communications Issue #128.

D. Development of quantitative methods and parameters to measure the scope and impact of a network outage. - NOF - SS7 Network Outage Measurement, Issue #162

Team Leader

John Seazholtz - Bell Atlantic

Team Participants

Phil Binley - Pacific Bell
Rich Baseil - Bellcore
Rick Harrison - NOF
Gene Phillip & Ken Boheim - NCS
Charlene Greene - BellSouth
Kelly Gaylord - Bellcore SCP Vendor
Jack Walters - MCI
Bob Hirsch - AT&T (NSD)
STP Vendors:
Matt Ryan - Ericsson
Al Loots - AT&T (NS)
Peter Budihardjo & Bob Kenedi - NTI
John Bishoff - DSC

- Develop and implement new network architectures that are more robust to failures (e.g., 1.544 Mb/s links with protection, standard level 2 & 3 protocol for all interconnecting parties)

C. Improve CCS network operations:

- Share Industry "Best Practices" to prevent, detect and recover quickly from network failures†
- Establish a "Maintenance Clearing House" to assist in network "Change Management" and help resolve minor CCS troubles on a routine basis.
- Institution of an Emergency Response Plan for cross-carrier coordination of major network restoration activities.

D. Development of quantitative methods and parameters to measure the scope and impact of a network outage.

Confidential Information

Arrangements must be established to protect confidential and proprietary information and to insure that any such information is included in reports only on an aggregate masked basis.

As indicated in the following section on **Existing Work Efforts**, there is a great deal of work being done by various industry groups to address the CCS/SS7 concerns. The committee established to address these issues should work closely with, and take advantage of, the existing industry infrastructure to solve these issues.

† - Major new activity that needs national attention.

Existing Work Efforts

A number of existing efforts on critical CCS issues are currently in progress and must be *strongly encouraged* and *aggressively brought to closure.*

A. Improve Network Node Reliability

- Protocol improvements - ECSA T1S1 & CCITT SG XI - Various SS7 Protocol Issues
- Improved Testing of Nodes and Networks - Network Operations Forum (NOF) - Internetwork Interoperability Test Plans (IITP), Testing Information Exchange Issue # 141, and Hardware/Software Validation Issues #139 & 141.
- Outage information sharing among the industry to help service providers prevent/react to events in their own networks. NOF - CCS Outage Information Exchange, Issue 145; CCITT SG XI International Outage Reporting.

B. Improve the robustness of CCS Network Architecture - T1S1.3 & CCITT SG XI have defined the original CCSN architecture; NOF - Signaling Network Architecture, Issue #146 (In the process of being forwarded to the ICCF) and T1A1.2 - General Network Survivability Techniques

C. Improve CCS network operations:

- Share Industry "Best Practices" to prevent, detect and recovery quickly from network

B

APPENDIX 2

B

NRC SIGNALING NETWORK SYSTEM FOCUS TEAM
QUESTIONNAIRE II: SYSTEM FAILURE ANALYSIS REPORT

1. Report Number	2. OCC Code	3. Date of Report / /	4. SCC Name
5. Company	6. Originator's Name	7. Originator's Telephone # / -	8. Central Office (Location & State)
9. Date of Incident	10. Time of Incident (24hr clock) : :	11. System Type:	11(a) Host ☐ Remote ☐ / 12. System Cutover Date
13. Equipped Terminations Links: ____ Lines: ____ Trunks: ____	14. Software (Issue & Point Release)	15. Software Load Date / /	16. Latest Patch Input
	17. DURATION OF SERVICE IMPAIRMENT: ☐ 2 minutes & over ☐ Less than 2 minutes		

17(a). Total System Outage & Recovery: ____ ____ ____ HR MIN SEC	17(b). Partial System Outage & Recovery ____ ____ ____ HR MIN SEC	17(c) Number of terminations affected: Lines: ____ Trunks: ____ Links ____ Total % affected: ____

18. Recovery Action Durations(hrs:min:sec): Identification/Detection:	Travel:	Recovery Action(s):	19. LEVEL OF ASSISTANCE:

20. DESCRIPTION OF SERVICE FAILURE: Describe in detail the incident including a chronological description of events: (a) leading to the outage; (b) during recovery activities; (c) in response to any remaining service effects following initial recovery. Specify all recovery actions initiated on or by the system. (Add attachments if necessary.)

Services Affected: Intra LATA Switch-to-Switch calls. Toll calls to IEC Intra-switch (local) calls 800 Service calls

CLASS calls Alternate Billing Services Operator Service calls Cellular calls

21. CAUSES OF FAILURE: Describe the Major and Secondary (if appropriate) cause of the outage and state the outage duration resulting from each cause of failure. Refer to the categories A through N listed below and on the reverse for guidelines on failure classification.

21(a). Use the categories below when describing outage cause(s) (check appropriate boxes):

☐ A. Procedural—Telco	☐ F. Design—Hardware	☐ K. Environmental	☐ P. Interconnection
☐ B. Procedural—System Vendor	☐ G. Hardware Failure	☐ L. Power Failure	☐ Q. Unknown
☐ C. Procedural—Other Vendor	☐ H. Scheduled Event	☐ M. Remote facilities	☐ R. Other
☐ D. Software Fault	☐ I. Lightning Related	☐ N. Incompatibility	
☐ E. Design—Firmware	☐ J. Traffic Overload	☐ O. Standard	

Software Fault summary: ____

22. Is Service Failure Analysis Committee Review required? ☐ YES ☐ NO

B

CONTINUED ON REP

QUESTIONNAIRE II: SYSTEM FAILURE ANALYSIS REPORT
(continued)

23. CONTRIBUTING FACTORS Check the appropriate box(es) for factors (if any) that contributed to or prolonged the outage.

_ Work Error - Operational
_ Work Error - Data Entry
_ Work Error - Hardware
_ Documentation Error
_ Fix Available - Not Applied
_ Recovery Action - Escalated
_ Defective Patch
_ Reserved
_ Insufficient Data
_ Retrofits
_ Hardware Growth
_ Software Administration
_ Firmware Administration
_ Diversity Problem
_ Reserved
_ Reserved
_ Central Control Unit
_ Switching Fabric Unit
_ Peripheral Control Uit
_ Link/Trunk Unit
_ SS7 Unit
_ Clock Unit
_ Database Error - Dynamic
_ Database Error - Static
_ Data Synchronization
_ Routin Exercise (REX)

24. OUTAGE CLASSIFICATION (Enter the appropriate letter in the box — see above for classifications.)

25. SFAC Chair-person Name	27. Telephone Number	26. Analysis Closure Date
	( ) -	/ /

28. **Recommendations and plans for corrective or preventive actions:** State the recommendations and plans for corrective or preventive actions, including time table, any plans, commitments, or recommendations to: (a) prevent future occurrences; (b) lessen the impact of future occurrences; (c) speed recovery in future occurrences; or (d) otherwise improve the performance of the system. (Add attachments if necessary.)

B

APPENDIX 3

B

NRC Signaling Network Systems Focus Team
Questionaire II
Supplier System Outage/Failure Information Report Form

1 No	2 Date (m/d/y)	3 Time (hr:min)	4 Location		5 Application	6 Outage/ Failure Duration (hr:min:sec)	Cause		9 Services Affected	10 Fix Status
			Met/Sub/R	State			7 Code	8 Root Cause Description		
	11 CLLI		12 Recommendations and Plans for Corrective or Preventive Actions:							

1 No	2 Date (m/d/y)	3 Time (hr:min)	4 Location		5 Application	6 Outage/ Failure Duration (hr:min:sec)	Cause		9 Services Affected	10 Fix Status
			Met/Sub/R	State			7 Code	8 Root Cause Description		
	11 CLLI		12 Recommendations and Plans for Corrective or Preventive Actions:							

1 No	2 Date (m/d/y)	3 Time (hr:min)	4 Location		5 Application	6 Outage/ Failure Duration (hr:min:sec)	Cause		9 Services Affected	10 Fix Status
			Met/Sub/R	State			7 Code	8 Root Cause Description		
	11 CLLI		12 Recommendations and Plans for Corrective or Preventive Actions:							

Page Number ________

B

APPENDIX 4

B

NRC Signaling Network Systems Focus Team
Questionnaire I
Carrier Systems Population Information Request Form*

Product Name	Total number of such product in service that are SS7-equipped within your company as of the end of						
	1Q91	2Q91	3Q91	4Q91	1Q92	2Q92	9/30/92

* Please provide population information for SSPs, STPs, SCPs, and other SS7-equipped network nodes.

Date Request Period (1/1/91 - 9/30/92) or
Other _____

Page _____

B

APPENDIX 5

B

SCC Field Technicians and Control & Analysis Responsible for STP

Vendor	Course Name/ID	Length	Tuition	Suitcase	Location
LS/NT	CCS/SS7 Network Overview 3218	1 Day		Yes	Lakewood
		Available through Self Directed Learning Center on video.			
	SS7 Protocol Analysis 3219**	4 Days		Yes	Lakewood
BCR TEC	CCS/Network Oper & Maintenance CCS/NORM	2 Weeks		Yes	Lisle, IL
LS	Protocol Concepts 1 3217	5 Days		Yes	Lakewood
AT&T*	Data Com I: Intro to Data Concepts UC4113	Video		Available by Request	On-site
	Data Com II: Ntwk Components & Technical Aspects UC 4114	4 Days		Yes	Variable
Tekelec	MGTS	1 Day		Yes	Variable
Ericsson	AXE STP BMO 1210	3 Days		Yes	Texas
	AXE STP Maint 1280	15 Days		No	Texas
	AXE IOG Maint 1188	5 Days		No	Texas
	AXE Advanced Hardware Maint for STP/SCP 1287	10 Days		No	Texas
	AXE Software 1189	15 Days		No	Texas
	AXE Advanced Software Fault Handling 1191	10 Days		No	Texas

B

SCC Field Technicians and Control & Analysis Responsible for STP Cont

Vendor	Course Name/ID	Length	Tuition	Suitcase	Location
Ericsson	AXE STP Surveillance 1202	2 Days		Yes	Texas

DEC SCP (VAX) Dependent on SCP relocation to CO. Training requirements will be identified in and SCP relocation plan. There are no current plans for this through 1993.

LS	ISDN-Comprehensive Overview 3216	3 Days		Yes	Lakewood
BCR TEC	CLASS Services	3 Days		Yes	Lisle, IL

B

APPENDIX 6

B

Network Operations Forum
Reference Document
Issue 1, April 1993

INFORMATION SHARING

Table of Contents

B

INFORMATION SHARING

1. INTRODUCTION

1.1 PURPOSE OF THIS DOCUMENT

This document is intended to provide the appropriate guidance to facilitate the sharing of information. It identifies types of information which may be shared, the circumstances under which it should be shared, the extent to which sharing is appropriate, and the mechanisms and timing for that sharing. It represents industry consensus arrived at with the full participation of members of the Network Operations Forum which consists of Access Service Providers, Access Service Customers and Vendor/Manufacturers.

1.2 APPLICABILITY

This document is intended to be a living document, therefore subject to revision and upgrading under the Carrier Liaison Committee guidelines.

This document does not replace or supersede any existing Contracts, Tariffs or any other legally binding documents.

1.3 DEFINITION

For the purposes of this document the term Service Provider is used to indicate both Access Service Providers (ASP) and Access Service Customers(ASC).

1.4 DOCUMENT ORGANIZATION

The remainder of this document is organized into the following sections:

- Purpose of Information Sharing
- Basic premises
- Criteria
- Operating principles
- Scope
- Service Provider responsibilities
- Vendor/Manufacturer responsibilities
- Information to be shared
- Modes of communication(s)

1.5 PURPOSE OF INFORMATION SHARING

THE PURPOSE OF INFORMATION SHARING AS DESCRIBED IN THIS DOCUMENT IS TO ENABLE ALL SERVICE PROVIDERS AND VENDOR/MANUFACTURERS TO UTILIZE INFORMATION UNCOVERED BY OTHER SERVICE PROVIDERS AND/OR VENDOR/MANUFACTURERS THROUGH THE TESTING, VALIDATION AND APPLICATION OF SOFTWARE, HARDWARE, AND DOCUMENTATION; PROCEDURAL ISSUES; AND CONFORMANCE TO AGREED UPON STANDARDS IN ORDER TO:

1.) MINIMIZE THE POSSIBILITY OF MAJOR OUTAGES AND SERVICE INTERRUPTIONS THAT CAN AFFECT OUR COLLECTIVE CUSTOMERS' SERVICE,

B

Page-2-VII intentionally missing

B

4.4 Implementation of these guidelines represents a cooperative effort on the part of industry participants to assure the reliability of the interconnected telecommunications networks. It may occur that in the interest of promoting network reliability, parties may exchange information about their networks/products that could be used in a negative fashion against that companies image, products or network. Use of such information for purposes of securing a competitive advantage is contrary to the spirit and intent of these guidelines. Misuse of information provided under these guidelines may jeopardize subsequent information exchange.

5. SCOPE

5.1 The scope of this Document includes the exchange of information between the following parties:

- A Vendor/Manufacturer and its Customer(s)
- A Vendor/Manufacturer and its Customer and that Customer's interconnected Service Providers
- Vendors/Manufacturers
- Access Service Providers
- Access Service Providers and Access Service Customers

5.2 The exchange of information between the following parties is explicitly outside the scope of this Document:

- Access Service Customers/Providers and the FCC
- Bellcore Client Companies (BCCs) and Bellcore
- Access Service Customers

5.3 This Document is intended both to supplement existing practices and to establish new practices for information exchange.

The following list is intended to represent a complete list of sources of information for sharing. The identified sources include:

- Service Provider Stand alone Testing environment
- Compatibility testing between Service Providers
- Service Provider daily operations
- Service Provider outage reports and analysis
- Service Provider and/or Vendor/Manufacturer documentation
- Vendor/Manufacturer development testing
- Vendor/Manufacturer trouble information reports and analysis
- Vendor/Manufacturer trouble resolution reports
- Observed ambiguities or differences in requirements interpretations

6. SERVICE PROVIDER RESPONSIBILITIES

This section describes the responsibilities of Access Service Providers and Access Service Customers in the area of information exchange.

Service Provider sharing of information is subject to the "General Operating Principles" described in Section 4 of this Document.

B

6.1 SERVICE PROVIDER STAND ALONE TESTING ENVIRONMENT

Any testing results obtained by the Service Provider that identify defects or potential defects with a Vendor/Manufacturer product should be communicated to the Vendor/Manufacturer within 1 business day of the completion of testing analysis.

Where conformance to accepted industry standards is in question the Service Provider should inform/consult with their Vendor/Manufacturer within 1 business day of such a determination.

6.2 COMPATIBILITY TESTING BETWEEN SERVICE PROVIDERS

Where compatibility testing between interconnected Service Providers identifies an incompatibility or problem due for example to translations, differences in software releases, software changes, network architecture, and/or differences in requirements interpretations between Vendor/Manufacturer products, they should work individually or cooperatively to ascertain the cause of the problem. Once identified they should initiate information sharing to potentially affected Carriers/Vendor/Manufacturers as per these guidelines.

6.3 SERVICE PROVIDER DAILY OPERATION

Any problems encountered during the normal course of day-to-day operations that are identified as resulting in whole or part from problem(s) with the Vendor/Manufacturer's product should be communicated to the Vendor/Manufacturer within 1 business day of such a determination.

The information to be shared is described in Section 9.

Any problems encountered during the normal course of day-to-day operations that are identified as resulting from problem(s) other than with a Vendor/Manufacturer product and that have the potential to cause loss of service or compromise in the reliability, capacity, or performance in an interconnected network should be communicated by the identifying Service Provider to potentially affected Service Provider(s) within 1 business day of such a determination.

6.4 DOCUMENTATION

When the utilization of Standards or Methods and Procedures identifies a problem with Service Provider and/or Vendor/Manufacturer documentation that could result in the loss of service or compromise in the reliability, capacity, or performance of the network, this problem should be reported to the issuing company within 1 business day.

The company that issued the methods and procedures should evaluate the identified problem and initiate a correction. The correction should be provided to all known users of the affected documentation.

7. VENDOR/MANUFACTURER RESPONSIBILITIES

This section describes the responsibilities of the Vendor/manufacturer in the area of information exchange.

Vendor/Manufacturer sharing of information is subject to the "Operating Principles" described in Section 4 of this Document.

B

Page-5-VII intentionally missing

B

The information to be shared is described in Section 8.

7.5 DIFFERENCES IN SPECIFICATIONS INTERPRETATION

Where industry standards are perceived to be ambiguous or flawed, and are believed to have the potential to cause loss of service, compromise in the reliability, capacity, or performance in the network of a Customer(s) the Vendor/Manufacturer implementing such standards should inform their Customer(s) in writing of their interpretation and their concerns. The affected Vendors/Manufactures and or Service Providers should address the issue with the appropriate standards bodies.

8. INFORMATION TO BE SHARED VENDOR/MANUFACTURER TO CUSTOMER

The following information should be provided by Vendors/Manufacturers to their Customers (per sect 7.1):

Background: Introductory information on how the problem was identified and under what circumstances.

Problem: Technical description of the problem.

Service Impact: The actual or potential impact to service that the problem poses.

Products/Generics Affected: A list of the products and generics/ releases that are affected by the problem.

Interim Solution: When available, a description of how to recover the node or prevent the problem from occurring should be provided until a long-term solution is available.

Contact: A single point of contact through whom the Customer can communicate regarding the problem for clarification, and/or request additional information.

Resolution: A Customer view of what is being done to resolve the problem and when a solution might be generally available. This will probably not be available on initial notification, but will require subsequent updates to the Customer.

9. INFORMATION TO BE SHARED CUSTOMER TO VENDOR/MANUFACTURER

Customers should report to their Vendor/Manufacturers all known problem(s) and/or potential problem(s) associated with the Vendor/Manufacturer's product(s) based on agreements between the parties. For this information sharing purpose the Vendor/Manufacturers products include hardware, software, firmware and documentation.

The information provided is dependent on the nature of the problem. As such, not all of the items listed below may be applicable. The information provided for the problem or potential problem should/could include the following:

B

Date: Date problem was encountered.

Time: Time problem was encountered.

Product: Specify which of the Vendor/Manufacturer's product(s) are involved.

Priority: Severity of problem

Problem Description: Complete description of the problem.

Affected Sites: Location/Site identification.

Services Impacted: Identify services impacted (e.g. 800)

Customer Impact: Describe end user and/or service provider impact (e.g. blocked calls).

Actions Taken: Describe work around as applicable.

Office Print outs: Maintenance terminal output or equivalent 1 hour prior to and 2 hours after the event or as requested.

Product Version: Identify version of product(s) (e.g. software release level and patch level).

Product Logs: Maintenance/error logs and measurements as specified in advance or as requested.

Protocol data: If applicable

Hardware: Provide suspected hardware information as requested.

Contact: Service providers point of contact and phone number for issue resolution.

The timing of the sharing of this information is specified in section 6 of this document.

10. MODES OF COMMUNICATION

Established communication channels should be used wherever applicable. Changes to existing communication channels should be driven by the affected user organizations (e.g., technical support organizations).

Two modes of communication are recommended:

- Proactive notification
- Vendor/Manufacturer Electronic Message System

B

10.1 PROACTIVE NOTIFICATION MODE

In this communication mode the Vendor/Manufacturer or Service Provider should notify its Customers, interconnected Service Providers and or Vendor/Manufacturer(s) in accordance with the timing requirements defined in Section 6 or 7.

This mode of communication should be used either when there is imminent danger of an outage or significant impact known for the reliability, capacity or performance of network operation. When possible, it is desirable that the notification refer to additional related information (e.g., related trouble reports).

10.2 VENDOR/MANUFACTURER ELECTRONIC MESSAGE SYSTEM MODE

This mode of communication is applicable between Vendor/Manufacturers and their Customers.

In the Vendor/Manufacturers Electronic Message System communication mode, the Customer has the ability to receive/retrieve, prioritized trouble report information. How this communication mode is provided should be determined as part of the Vendor/Manufacturer Customer relationship. Examples include Vendor/Manufacturer systems and paper records.

11. FACILITY OUTAGE REPORTING GUIDELINES

It is recommended that companies that are directly interconnected should establish procedures, where they currently do not exist, for notification and information exchange in the event a facility outage (cable, fiber, microwave) occurs that directly impacts the other company.

It is recommended that the following information be exchanged upon notification of an outage to the directly interconnected company. This information should be exchanged upon detection of the outage or as soon as possible.

- **DATE AND TIME OF OUTAGE**
- **LOCATION**
- **CAUSE IF KNOWN**
- **ESTIMATED RESTORATION**
- **CONTACT NAME AND NUMBER**
- **TYPE OF FACILITY OUTAGE (IF KNOWN)**

Guidelines should be established to define minimum levels or thresholds for outage reporting. Minimum level recommendations:

- **>30,000 customers or**
- **>90,000 blocked calls**

It is also recommended that when service is restored, notification be provided to the companies impacted. The notification should be provided upon restoral of service. This notification should include the following information:

- **TIME OF RESTORATION**
- **CAUSE**
- **TEMPORARY SOLUTION OR PERMANENT FIX**

APPENDIX 7

B

C.O. Equipment Element Diversity
Check List Page: 1 of 3

C.O. CLLI: _____ LINK TYPE: _____ STP CLLI: _____
STP CLLI: _____ LINK TYPE: _____ STP CLLI: _____

Diversity Item	Date Checked	Meets Yes/No	Resp Person	Remarks

1. Power and Fusing
   No components of a paired CCS link transmission path should share a common fuse or load.

2. Cabling
   There should be diverse cable routes between individual CCS link paths in the central office.

3. Distributing Frames/Mounting Blocks
   Termination of diverse CCS links must be on separate Main Distributing Frame (MDF) mounting blocks.

4. Office Repeater Bays, DSX Bays, Patch Bays
   Not all of a given type of CCS link (A, B, C, or D) should transverse a single bay of these types.

5. DCS
   Not all of a given type of CCS link should transverse a single DCS.

6. D4/D5 Bays (and associated channel bank equipment)
   The channel bank equipment associated with each CCS link should be located in separate bays.

B

C. O. Equipment Element Diversity
Check List Page: 2 of 3

C.O. CLLI: _____ LINK TYPE: _____ STP CLLI: _____
STP CLLI: _____ LINK TYPE: _____ STP CLLI: _____

Diversity Item	Date Checked	Meets Yes/No	Resp Person	Remarks
7. Fiber Optic Terminals and Multiplexers Paired CCS links should not transit a common fiber terminal or common multiplex equipment.				
8. Test Access Equipment Not all of a particular CCS link type should transverse a single test access unit.				
9. Analog/Digital Radio Not all of a given type of CCS link should traverse the same analog or digital radio.				
10. Link Interface Equipment For DMS-100F offices equipped with a SuperNode processor, the Link Peripheral Processor (LPP) is to be used as the CCS interface.				
11. Timing/Synchronization Every office is assumed to be equipped with a Building Integrated Timing Supply (BITS) clock as defined in PUB 60110.				

B

C. O. Equipment Element Diversity
Check List Page: 3 of 3

C.O. CLLI: _____ LINK TYPE: _____ STP CLLI: _____
STP CLLI: _____ LINK TYPE: _____ STP CLLI: _____

Diversity Item	Date Checked	Meets Yes/No	Resp Person	Remarks
12. State specific diversity item.				
13. State specific diversity item.				
14. State specific diversity item.				
15. State specific diversity item.				

B

TIMING/SYNCHRONIZATION EQUIPMENT:

LOCATION: _____ CLLI: _____ EQPT TYPE: _____
LATA/AREA: _____

	YES	NO
1. SEPARATE A AND B BATTERY FEEDS (-48VDC) TO EACH MASTER AND SLAVE SHELF?	____	____
2. A AND B BATTERY FEEDS DIVERSELY ROUTED FROM THE BDFB TO THE BITS AND SECONDARY CLOCKS?	____	____
3. TWO SEPARATE AND DIVERSE DS1 INPUT SYNCHRONIZATION SIGNALS?	____	____
4. DIVERSE CABLING FROM BITS CLOCK TO SECONDARY CLOCKS WITH EACH FEED TAKEN FROM DIFFERENT DS1 OR COMPOSITE OUTPUT CARD?	____	____
5. BITS AND SECONDARY CLOCKS EQUIPPED WITH AUTOMATIC SWITCHING OF THE OUTOUT CARDS (DS1 AND COMPOSITE CLOCK OUTPUT CARDS)?	____	____
6. TIMING FEED TO EACH CCS LINK FROM DIFFERENT OUTPUT CARD ON THE BITS OR SECONDARY CLOCKS?	____	____
7. LOCAL ALARMS WIRED TO OFFICE AUDIBLE/VISUAL ALARM SYSTEM?	____	____
8. REMOTE ALARMS WIRED TO TELEMETRY DEVICE?	____	____

REMARKS AND RECOMMENDATIONS: _____

B

LOC/LATA: CLLI:

AC/AF#: CAC: LINK TYPE: / LSTP CLLI:

	EQPT. CABLING	POWER CABLING	FUSE LOCATION	POWER DIST.	TIE/HOUSE CABLES	DIST FR LOCATION
SWITCH/LINK INTERFACE EQPT -						
ORB/DSX/PATCH EQPT -						
DCS/DACS EQPT -						
/D5 EQPT -						
TEST ACCESS EQPT -						
FIBER OPTIC TERMINAL OR MULTIPLEXER EQPT -						
OTHER EQUIPMENT -						

REMARKS AND RECOMMENDATIONS:

B

APPENDIX 8

B

CCS Link Interconnectivity

Physical Link diversity is achieved first in the provisioning process and then maintained by operational procedures.

1) Provisioning

The provisioning process should take into account facility routing and equipment assignments such as:

- Cable routing
- Separate Equipment
- Powering and Fusing
- Building Entrance locations
- Distribution Frames
- Equipment Cable Racks
- Nailed Up Connections, e.g. Digital Cross Connect Equipment

2) Maintenance

In order to maintain link diversity, operational procedures should address the following link set maintenance considerations:

- Notification of Control Centers (IC/EC)
- Determination of the status of all links in the combined link set
- Expeditious return of the impaired link to service

Once diversity is designed into a combined link set, the IC/EC should ensure that the diversity is maintained:

- Diversity on all link sets should be routinely confirmed
- Whenever maintenance or circuit order activity occurs on a link, or a failed link is restored, diversity on the combined link set should be confirmed.

Diversity Requirements for CCS7 Network Interconnect

The information below is based upon, and largely extracted from the Network Operations Forum (NOF) - Installation & Maintenance Responsibilities - SS7 Link and Trunk Installation & Maintenance - Access Services. AT&T believes that these recommendations represent the minimum requirements for SS7-NI Link Diversity.

General

CCS/SS7 route diversity, which assumes a network architecture that encompasses interconnecting mated STPs, is defined as signaling link sets that are on physically and electrically separate routes.

Such diversity, which dictates that link sets share no common resources (e.g., electronic equipment) and are physically separated should eliminate common cause failures; that is, single failures that disable more than one link set.

In general, n-way diversity between two networks connected by multiple link sets means that no instance of (n-1) or less simultaneous failures will cause there to be an absence of link sets between the two networks.

Specific Criteria

The following are recommended criteria for interconnecting link diversity:

> An architecture with EC STPs connected to IC STPs requires interoffice and intraoffice three-way physical diversity of facilities which comprise a CCS D-link quad.
>
> An architecture with EC STPs connected to IC SPs requires interoffice and intraoffice two-way physical diversity of CCS link facilities.

Three-way physical diversity between EC STPs and IC STPs means that for a given D-Link quad, no two simultaneous failures should disable all three physically diverse link sets between EC STPs and IC STPs associated with that quad.

Two-way physical diversity between EC STPs and IC SPs means that no single failure should disable both physically diverse link sets between the EC STP and the IC SP.

B

Intra-Office Equipment Specific Diversity

Intra-Office Link Path

Each intra-office link path must have a physically separate route (minimum 6 feet apart). In locations where the 6 foot guideline is not possible, it is acceptable for different paths to cross at right angles, but they must be at different cable rack levels. It is acceptable for two paths to follow one route, but one of the paths *MUST* be in a raceway (separate conduit).
Links may be physically separated by steel conduits where a single riser exists between floors.

Power

Under no circumstances are any of the components of one link path to share power sources with components of another path. The preferred configuration would have each link path fused on separate Battery Distribution Fuse Bays (BDFB), each at least six feet apart, fed from separate power plants. If this configuration is not possible the next configuration of choice would be separate BDFBs, fed from the same power plant. The minimal configuration would utilize a single BDFB, same power plant, using different loads. The minimal configuration is not recommended for NI, unless it is the only available option. This means the equipment cannot share a common fuse of a common Load (A or B) from a single BDFB. However, powering all the components of one path from Load A and all the components of another path from Load B of a single BDFB is acceptable, if this is the only available configuration.

DCS

If DCS or DCS equivalent equipment is utilized, each path will have a separate DCS frame associated with it connected to the other DCS frames only by Inter-DCS T1Es. These T1Es are hard-wired facilities from one digroup of one DCS frame, to one digroup of another frame. This arrangement is necessary for the connectivity of links and to attain diversity.

D4 Banks

If D4 Channel Banks, or their equivalent, are utilized, the D4 Channel Banks of each path are to be located in separate frames. A D4 Channel Bank terminates two DS-1s and shares common equipment circuit packs, power supplies and extracts and regenerates synchronization from the DCS digroup connected to only one of the D4 digroups. Due to this shared arrangement and synchronization scheme, both the "A" and "B" digroups of a single bank may be used for CCS7 service, with the provision that they be incorporated within the same path.

Digital Multiplex Equipment

On the DDM1000, the link paths shall terminate on separate DDM1000 bays. Power feeds for the DDM1000 bays should also be assigned separate routes and loads on the BDFB in accordance with the load patterns on the other equipment on the link path.

Network Channel Office Equipment (NCOE) or Extended Super Frame (ESF)

On the NCOE, or equivalent the link paths shall terminate on separate NCOE shelves. Power feeds for the NCOE shelves should also be assigned separate routes and loads on the BDFB in accordance with the load patterns on the other equipment on the link path.

Automatic Bit Access Test Set - Digital Service Access Unit (ABATS-DSAU)

On the ABATS or equivalent type of Link Access Test equipment, the link paths shall terminate on separate ABATS shelves. Power feeds for the ABATS shelves should also be assigned separate routes and loads on the BDFB in accordance with the load patterns on the other equipment on the link path.
The Digital Test Access Unit (DTAU) manufactured by Hekimian Laboratories, Inc. (HLI) is an acceptable substitute for the ABATS-DSAU. All guidelines that apply to ABATS-DSAUs will also apply to the HLI-DTAUs.

Synchronization

The BCC CCS networks consist of digital switching and digital transmission systems that require synchronization to prevent transmission impairments. When the digital switching and transmission systems of BCC and other CCS networks are interconnected by digital facilities, some means of synchronizing clock rates is required.

The synchronization of BCC CCS networks and other CCS networks to achieve established performance objectives requires the application of "The Digital Synchronization Network Plan" described in Technical Advisory TA-NPL-000436, Issue 1, November, 1986.

This plan calls for the establishment of a single master timing supply per administrative building (i.e., a Building Integrated Timing Supply or BITS). A BITS distributes all DS1 and DS0 timing required by other clocks within that building. The timing for BITS in BCC and other synchronization networks which supply clocking for CCS Networks is traceable to a Primary Reference Source (PRS) as described in ANSI standard T1.101-1987.

Inter-Office Diversity Requirements

Buried Facility Depth Requirements

The minimum cable depth is 48 inches except if buried in rock. If buried in Ledge Rock, the minimum cable depth without steel pipe protection is 36 inches (it is assumed that ledge rock is encountered at 30 inches or less below the surface. Cable must be at least 6 inches deep into ledge rock to eliminate the need for steel pipe protection). The minimum cable depth in rock is 24 inches. Steel pipe protection is required when cable is placed between 24-36 inches below the ground surface in the ledge rock. The minimum depth for multiple duct conduit with manhole access is 36 inches to the top duct.

Cable Intersections

One cable must cross at a minimum depth of two feet below the other. One of the cables must be placed in steel pipe at least 10 feet in length.

Major River Crossings

Requirement for diverse Right of Way dictates separate river crossings. If two separate crossings do not exist, the minimum diversity requirement dictates that one of the cables must occupy its own steel pipe duct with a minimum 3 foot separation from the other cable. Armored submarine crossings must be at least 15 feet apart.

Terminal Entrances

To be considered diverse, one of the cables entering a terminal building must have steel pipe protection and maximum possible physical separation, if a common building entrance is used. Separation must be at least 12 inches. Steel pipe protection must extend from within the building entrance vault to the point of divergence of the diverse routes, not to exceed one-half mile.

Buried Cable

To be considered diverse, two digital cables cannot share the same Right of Way, no exceptions. Cables son separate paralleling Right of Ways must be at least 100 feet apart, to be considered diverse.

Underground Cable (multiple duct conduit system with Manhole Access)

To be considered diverse, two cables cannot share the same conduit system .

Repeater Huts

To be considered diverse, two cables cannot share the same hut structure.

GLOSSARY

ABATS	Automatic Bit Access Test Set
ABATS-DSAU	Automatic Bit Access Test Set-Digital Service Access Unit
ANSI	American Nation Standards Institute
BCC	Bellcore Client Company
BDFB	Battery Distribution Fuse Bay
BITS	Building Integrated Timing Supply
CCS	Common Channel Signaling
CCS7	Common Channel Signaling 7
DACS	Digital Access Cross Connect System
DCS	Digital Cross Connect System
DDM1000	Digital Multiplex 1000
EC	Exchange Company
ESF	Extended Superframe Format
HLI	Hekimian Laboratories, Inc.
HLI-DTAU	Hekimian Laboratories, Inc.-Digital Test Access Unit
IC	Interexchange Carrier

NCOE	Network Channel Office Equipment
NI	Network Interconnect
PRS	Primary Reference Source
SP	Signaling Point
SS7	Signaling System 7
STP	Signal Transfer Point

APPENDIX 9

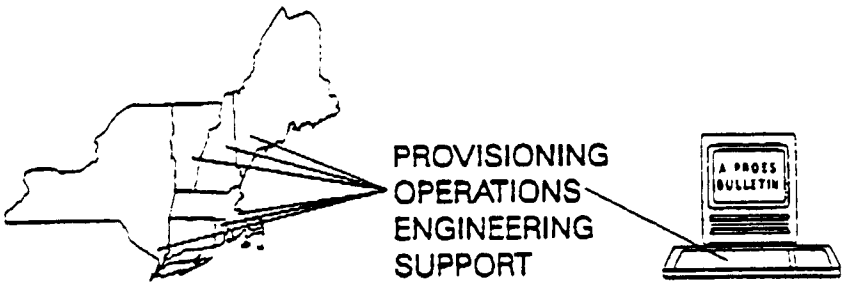
B

OPERATIONS SERVICES

FLASH

Doc. No. NOS93W-014

Issue Date 2/17/93



New Products and Technology Staff

Subject: CCSN Dual STP Failure Prevention; Condition Red Procedures

Purpose To describe procedures that will help prevent STP pair failures

Personnel Affected SCC, NSMAC, NSC

Distribution Codes S-50, S-112, S-130, S-138

Effective Date Immediately **Retention** Until NX 256-010-903, Issue B

Training Required No training required

Contact John Scaldaferri **Phone** 212-643-4573 **Fax** 212-629-9759

References NX 256-010-903, Issue A

(OVER)

Telesector Resources Group

A subsidiary of New England Telephone and New York Telephone

TRG-NP&T (7/92)

B

COMMON CHANNEL SIGNALING NETWORK
DUAL STP FAILURE PREVENTION
CONDITION RED PROCEDURES

Table Of Contents

Page

B

1. INTRODUCTION

1.1 BACKGROUND

1.1.01 Overview

This NYNEX FLASH describes the actions which must take place in a STP (Signal Transfer Point) building and other locations deemed essential when the STP's mate goes out of service. Its purpose is to suspend all work activities in the mated STP building and other essential sites until the original STP is restored to service. These procedures are designed to prevent mated STP pair outages. This FLASH is considered a disaster prevention procedure and is closely associated to techniques described in the NYNEX SS7 Disaster Recovery M&Ps, document NX 256-010-903. Therefore, this FLASH will be incorporated into the next issue of the NX 256-010-903 document.

1.1.02 Reasons For Reissue

Whenever this FLASH is reissued, the reasons for reissue will be stated in this paragraph.

1.1.03 Disaster Recovery

The procedures contained in this FLASH are related to the SS7 Disaster Recovery M&Ps because the failure of a single STP in the NYNEX CCSN (Common Channel Signaling Network) is considered a severe crisis. As a result, the escalation and trouble referral procedures as outlined in the SS7 Disaster Recovery document should be followed.

1.2 DEFINITIONS AND WORK CENTERS

1.2.01 Overview

This document contains new terms that have to date not been used in the CCS (Common Channel Signaling) environment. As a result, these terms are defined in this section. Also, the work centers mentioned in this document are described in this section.

1.2.02 Definitions

CONDITION RED	A network condition in which a single STP has failed and the appropriate SCC organization has notified the proper work entities to have certain work suspended immediately.
CONDITION GREEN	A network condition in which a previously failed STP has completely recovered and is in the stable state; and the appropriate SCC organization has notified the proper work entities to allow previously suspended work to commence.
ESSENTIAL EQUIP.	Equipment defined by the SCC as essential to the health of the STP.

1.2.03 Work Centers

WORKING SCC	The SCC supporting the working STP (the mate has failed). In many cases in NYNEX the same SCC supports both STP sites.
SEAC	The NYT Signaling Engineering and Administration Center.

SNSC	The Signaling Network Support Center in NET.
NMC	The Network Management Center. One exists in NYT and in NET.
NSC	The Network Service Center. One exists in NYT and in NET.
NSMAC	The Network Surveillance Management and Analysis Center in NYT. This center includes the SEAC, NMC, NSC, etc.

2. COMMON PROCEDURES

2.1 GENERAL RESPONSIBILITIES AND FORMS

2.1.01 Introduction

This section describes the roles and responsibilities for implementing the condition red and condition green procedures.

2.1.02 Vision of Failure

When an STP in the NYNEX CCSN goes out of service, the following organizations should be aware of the failure via their maintenance and surveillance operational support systems:

In NYT:
SEAC (Signaling Engineering and Administration Center)
NMC (Network Management Center)
SS7SCC (Signaling System 7 Switching Control Center)
SCC for STP and Mate

In NET:
SNSC (Signaling Network Support Center)
NMC
SCC for STP and Mate

2.1.03 Condition RED Requirement

When an STP in the NYNEX CCSN goes out of service, all appropriate work (as defined in this FLASH) in the mate STP's building must immediately be suspended. Furthermore, all work in those non-collocated (not located in the STP building) toll locations deemed essential to the "health" of the STP must also immediately be suspended.

2.1.04 Essential Equipment

Each turf SCC must identify those toll locations not in the STP building which are essential to the health of the working STP. An emergency contact number for that location should be obtained by the turf SCC and placed on the CONDITION RED/GREEN Form explained later in this document. This would ensure the suspension of toll work in those facilities when a condition red is declared.

An example of such a location would be a site housing a Digital Cross Connect System (DCS) that contains a large percentage of links which terminate at the STP site. If the DCS contains enough links to cause the STP problems if it (the DCS) were to fail while the mate STP was already out of service, the DCS should be deemed essential by the turf SCC and considered part of the condition red procedures.

2.1.05 NSMAC (New York Telephone) Responsibilities

When a single STP goes out of service in the NYT area, the NSMAC (Network Surveillance Management and Analysis Center) in NYT is responsible for notifying the SCC supporting the remaining working STP and declaring a condition red.

Under certain failure conditions, (i.e. the SCC supports both the working and failed STP sites), the NSMAC may have to place a second call (after calling the SCC) to the first level or AOM (Area Operations Manager) of the SCC to request they perform the call outs to the other appropriate organizations. The NSMAC is <u>not</u> responsible for notifying each of the organizations listed on the CONDITION RED/GREEN Form to indicate that a condition red is in effect. This is the SCC's responsibility.

When the STP has recovered and is in a stable condition, the NSMAC is responsible for declaring a condition green by notifying the same SCC contact as used to declare a condition red.

Given SCC input, the NSMAC should maintain a list of the SCC telephone numbers (for normal and out of hours) used when declaring a condition red.

2.1.06 NSC (New England Telephone) Responsibilities

When a single STP goes out of service in the NET area, the NSC (Network Surveillance Center) in NET is responsible for notifying the SCC supporting the remaining working STP and declaring a condition red.

Under certain failure conditions, (i.e. the SCC supports both the working and failed STP sites), the NSC may have to place a second call (after calling the SCC) to the first level or AOM (Area Operations Manager) of the SCC to request they perform the call outs to the other appropriate organizations. The NSC is <u>not</u> responsible for notifying each of the organizations listed on the CONDITION RED/GREEN Form to indicate that a condition red is in effect. This is the SCC's responsibility.

When the STP has recovered and is in a stable condition, the NSC is responsible for declaring a condition green by notifying the same SCC contact as used to declare a condition red.

Given SCC input, the NSC should maintain a list of the SCC telephone numbers (for normal and out of hours) used when declaring a condition red.

2.1.07 Notification Communication

The NYNEX Emergency Communications Network (the upgraded MF Corporate Communications Network), the NYT Disaster Communications Network or radio technology (where deployed), should be utilized by the Tier II organizations to declare a condition red if communication via the NYNEX CCSN is blocked.

2.1.08 SCC Responsibilities

The SCC responsible for the maintenance and monitoring of the failed STP must recognize this situation as a severe crisis and follow the escalation procedures in NYNEX practice NX 256-010-903. Normal SCC notification to local management should take place.

The SCC responsible for the working STP (may be the same one as mentioned above) should expect a call from the proper Tier II organization, declaring a condition red/green.

The SCCs are responsible for creating and maintaining the required contacts on the CONDITION RED/GREEN Forms, listing these contact telephone numbers on these forms, and ensuring these forms are readily available to all SCC personnel.

The SCCs, once contacted by the Tier II center, are responsible for contacting the organizations listed on the form and having all work suspended or resumed, depending upon the condition declared. Copies of these forms should be retained at the home locations of the first and second level management supporting the SCC in the event they are called at home from the Tier II organization and requested to perform the call outs from their home.

If the contact telephone number of the SCC changes, the SCC is responsible for notifying the Tier II center of the change in writing, to ensure the SCC numbers are accurately maintained at the Tier II center.

2.1.09 Form CONDITION RED/GREEN

For reproduction purposes, the CONDITION RED/GREEN Form is found in exhibit A. For each of the work areas shown on the form (Power, Frame, etc.), a work suspension or clearance should be given depending upon the condition.

2.2 DETAILED REQUIREMENTS

2.2.01 Introduction

This section contains the details of the different functional work areas mentioned on the CONDITION RED/GREEN Form, found in exhibit A. Its purpose is to provide the reader with a greater understanding of the intent behind the condition red procedures and to clarify those areas requiring a work suspension.

2.2.02 Intention

The condition red work suspension procedure mentioned in this practice is intended to prevent the accidental simultaneous isolation of a mated STP pair. As NYNEX's network is converted from MF trunking to SS7 trunking, the impact that a mated STP pair failure could have on a particular LATA is extremely severe.

B

This condition red procedure is not intended to prevent SSP isolations. Accidental SSP isolations will still occur if work is performed on the link connected to the working STP at some intermediate building location. The procedures in this document are to only take place at the working STP building site or essential equipment designations.

2.2.03 SCC/TSAC Work

All SCC/TSAC routine maintenance work on the STP (i.e. REX) must be suspended when a condition red has been declared. Since the routine exercises (REX) can not be suspended once they have started, they must be allowed to continue if they have started before a condition red has been declared. Otherwise, the translations controlling the timing of the REX should be changed to support a different REX start time.

Routine maintenance work does not include the restoral of links to recover an SSP from complete SS7 isolation or to recover a B/D link set to re-establish signaling with another STP pair. If an SSP/STP pair is isolated from the working STP under condition red, the appropriate A, B, or D links should be worked on and brought back in service immediately. If links are down at the working STP site but these links are not associated with an SSP/STP pair isolation, they should not be worked on. This is what is meant in the CONDITION RED/GREEN Form as unnecessary link maintenance.

Once a condition green has been declared, all routine maintenance and non-SSP isolation associated link work can continue. As a reminder, no link should be inhibited without the approval of the SEAC/SNSC organizations.

2.2.04 Software Work

All translations downloading, generic/BCS upgrades and patch loads on the working STP must be suspended when a condition red is declared. The Tier II centers creating the STP translations and releasing the patches in CSCANS should already be aware of the condition red and therefore not release any new software changes. Any previous translations changes or software upgrades that have already been released to the SCC for loading into the STP must not be loaded by the SCC into the STP until a condition green has been declared.

2.2.05 Toll Work

All toll work (by toll technicians, the FMAC, the NTEC, the SCC, etc.) on the equipment supporting SS7 links in the STP building must immediately be suspended when a condition red has been declared. This would effect:

- D4/D5 Banks
- DCS Products
- CSU/DSU
- DSX
- Clocking

When the Tier II sites have declared a condition green, this work can continue.

2.2.06 Engineering Work

All engineering work such as work performed by the engineering installation groups in NET or the turf equipment engineers in NYT on equipment supporting the working STP or equipment designated as essential, must immediately be suspended when a condition red has been declared.

When the Tier II sites have declared a condition green, this work can continue.

2.2.07 Essential Equipment

All work on previously designated essential equipment must immediately be suspended when a condition red has been declared. This would include but not be limited to any Digital Cross Connect systems supporting a large percentage of the STP's links. Large (for this purpose) is defined as a quantity of links sufficient enough to cause the working STP to congest or go out of service if that equipment were to fail while the mate were already out of service.

When the Tier II sites have declared a condition green, this work can continue.

2.2.08 Power Work

All power work (by the power engineers or SCC technicians) on any of the power equipment supporting the STP or its links must immediately be suspended when a condition red has been declared. This would include suspending all planned power routines and suspending the transition to battery power at the request of the electric utilities company. This would effect all of the appropriate aspects of the power distribution facilities:

- Batteries
- Rectifiers
- Converters/Inverters
- Control Bays
- Distribution Bays
- Switches/Fuses
- STP AC Switch Gear

When the Tier II sites have declared a condition green, this work can continue.

2.2.09 Frame Work

All frame work (by the frame technicians) on any of the frame blocks supporting SS7 links terminating to the STP must immediately be suspended when a condition red has been declared.

When the Tier II sites have declared a condition green, this work can continue.

2.2.10 Outside Plant Work

All outside plant work in the cable vaults supporting the SS7 links at the STP building must immediately be suspended when a condition red has been declared.

When the Tier II sites have declared a condition green, this work can continue.

B

2.2.11 Buildings Work

All buildings work in any of the toll, power, or switch floors must immediately be suspended when a condition red has been declared. All cleaning, air conditioning, electrical, and fuel line (for the engines) work planned or in progress must immediately be suspended.

When the Tier II sites have declared a condition green, this work can continue.

2.2.12 Off-Line Equipment

In general, any equipment within the working STP that happens to simultaneously go out of service while a condition red is in effect must immediately be identified and spares obtained. No replacement work should occur without the concurrence of the Tier II severe crisis control organization (SEAC in NYT, SNSC in NET), with the exception of the statements regarding SSP/STP isolations.

2.3 LABELING REQUIREMENTS

2.3.01 Introduction

As SS7 links are provisioned in the NYNEX CCSN, certain key components of the link designs should be marked with SS7 sticker or tag indications in order to avoid accidental outages.

Accidental outages could occur at many levels of the facility or common power, electrical or timing equipment supporting the links or the entire STP.

2.3.02 Sticker/Tag Availability In NYT

Stickers and tags are going to be supplied to each of the SCCs in NYT following the distribution of this FLASH. Once your SCC has used up the initial supply of stickers and tags, additional orders should be sent directly into the NYT Corporate Services Purchasing Department. They are currently located at 1095 Avenue of the Americas, Room 1000, NYC, NY. The SCC should utilize form GSB 100FA when ordering and originals should be sent in with the completed form. Ordering in bulk quantities of at least 1000 units of each item is recommended for cost efficiency.

2.3.03 Sticker/Tag Availability In NET

Stickers and tags have already been made available to the NET toll/SCC arena. If SCCs or other organizations are interested in additional tags for CCS purposes and the transmission maintenance engineering group at 350 Cochituate Rd., Framingham, Mass. is unable to supply them, the same ordering procedures as mentioned above for the NYT groups may be utilized.

2.3.04 Sticker/Tag Types

The stickers produced by the Corporate Services Purchasing Department can be utilized for a variety of places involved with supporting SS7 link and STP equipment. The following table outlines some of the areas of desired application for each of the stickers/tags. These stickers and tags may be used in other areas. The purpose of the stickers and tags is to quickly identify SS7 link and STP supporting equipment to the technicians working in the area in order to avoid accidental outages. Furthermore, the labeling of the STP supporting equipment will clearly indicate to the technicians working in the area what equipment is not to be worked on in a condition red situation.

Table 1
SS7 Stickers And Tags

ITEM	INSCRIPTION	AREA OF USAGE	ORGANIZATIONS
3/4" Diameter Circular Stickers	SS7 Circuit Do Not Remove	DS0DP Card In D4 DCS 1/0 Unit 2500 Data Set	Toll Toll Toll/SCC
SS7 Tag	CAUTION SS7 CKT DO NOT REMOVE ETC.	DSX Pins Frame Area	Toll/SCC Frame/SCC
SYNC Tag	CAUTION SYNC SYSTEM DO NOT REMOVE ETC.	BITS Leads	Toll/SCC
DSX Type B Protector	CCS	DSX Type B	Toll
DSX Type C Protector	CCS	DSX Type C	Toll
Larger Rectangular Stickers	CAUTION SS7 EQUIPMENT	STP Batteries STP Rectifiers STP Converters STP Inverters STP Control Bays STP Distribution Bays STP Switches/Fuses Frame Blocks Supporting SS7 Links	Power Engineers Frame

2.3.05 Red Slip-On Pin Covers

In addition to the materials described above, the field also may utilize the red slip on covers on any bare pins supporting SS7 links, i.e. the bare DSX pins or the frame pins. These covers are already in ample supply at the SCC sites and in the toll area.

2.3.06 Reorder Note For DSX Protectors

The DSX type B and C protectors can not be reordered through the NYT Corporate Services Purchasing Department. Reorder procedures are still under development and will be communicated to the field at a later date, via a FLASH.

B

2.4 EXHIBIT A

FORM CONDITION RED/GREEN

*Failed STP Identification:*_____
*Mate STP Identification:*_____

Checklist Requirements:
Condition Red: Declare a work suspension in the following areas:
Condition Green: Declare a work clearance in the following areas:

*SCC/TSAC Work Number:*_____(Normal Hours)_____(Out Of Hours)
i.e., All STP Maintenance, STP REX (If it has not already begun), Unnecessary Link Maintenance

*Software Work Number:*_____(Normal Hours)_____(Out Of Hours)
i.e., All STP Translations, Patches/BCS Loads

*Toll Work Number:*_____(Normal Hours)_____(Out Of Hours)
i.e., D4/D5 Banks, DCS Products, CSU/DSU, DSX, Clocking (BITS)

*Engineering Work:*_____(Normal Hours)_____(Out Of Hours)
i.e., Eng. Installation work in NET or turf Equipment Engineering work

*Essential Equip. Number:*_____(Normal Hours)_____(Out Of Hours)
i.e., Non-collocated DCS

*Power Work Number:*_____(Normal Hours)_____(Out Of Hours)
i.e., Battery, Rectifiers, Converters/Inverters, Control Bays, Distribution Bays, Switches/Fuses, Switch Gear

*Frame Work Number:*_____(Normal Hours)_____(Out Of Hours)
i.e., SS7 Frame Blocks

*Outside Plant Work Number:*_____(Normal Hours)_____(Out Of Hours)
i.e., Cable Vaults at STP containing the links

*Buildings Work Number:*_____(Normal Hours)_____(Out Of Hours)
i.e., Cleaning, Air Conditioning, Electrical, Fuel lines supporting the engines

APPENDIX 10

B

Appendix A

EMERGENCY SS7 RESTORATION OPERATIONS PLANNING CONSIDERATIONS

INTRODUCTION

PREFACE: Throughout this document the CCSN and PSTN are addressed as separate networks, even though both subnetworks comprise the new public switched network and both are necessary to complete calls. This is done in order to better focus on their uniqueness and concerns, separately, before attempting to merge the two, and perhaps miss some important issues. In addition, although more is presented on the maintenance side, maintenance should not be construed as more important than network traffic management. In the order of things, however, maintenance is vital with the advent of the CCSN. The CCSN must evolve to a consistently stable network to allow Network Traffic Management (NTM) efforts to be effective. Additionally, NTM functions can greatly assist in this stability.

Recent Common Channel Signaling Network (CCSN) outages are causing speculation that more severe problems will occur in the future. The industry in general is concerned that they may not be properly prepared to diagnose troubles quickly and contain their proliferation in an integrated CCSN. One of several areas being addressed in this document is the recovery procedures for CCSN failures. Also addressed are actions that might be taken to contain the spread, or worsening, of network failures when Access Service Providers (ASPs) and Access Service Customers (ASCs) are interconnected. These two areas of concern are inter-related and require both an understanding of their inter-relationship and a comprehensive plan of action.

This document assumes a 100% deployment of CCS interconnection between an ASP and ASC.

Purpose of Document

The purpose of this document is to coalesce in one paper relevant subjects and concerns related to the control and restoration of networks from an operations perspective.

It provides a view of factors that a typical Network Provider might consider in planning responses to potential network events.

FAILURE TYPES

As with any network, there are numerous events (triggers) that can cause failures. In this respect the CCSN is quite similar to other networks. Unlike most other networks, however, the CCSN comes the closest to being self-managed. It automatically takes preprogrammed actions (via the SS7 protocol) to continue functioning when various abnormal conditions exist. Signaling Network Management functions provide for reconfiguration of CCSN resources in the event of signaling link or signaling point failures. When a failure occurs, the objective is that, the reconfiguration should be carried out so that messages are not lost, duplicated or put out of sequence and that the number of messages in the network does not become excessive. These types of failures, which are transparent to the PSTN and the traditional Network Traffic Management (NTM), are not reviewed in this document except when, in combination with other events, they will have an impact on service. A point to be made, however, is that efforts are being made to review and enhance the protocol, if necessary, to make it more reliable and effective in failure scenarios since self-healing networks is the strategic direction. We do not suggest that these failures are not important. Any failure in the CCSN must be viewed as extremely crucial and expeditiously dealt with since combinations of events can impact customers and have potentially far reaching consequences.

Failures that will be discussed in this document include those described in the following subsections.

Signaling Transfer Point (STP) Failures

STP failures, at present, represent the greatest threat to the overall reliability of a CCSN, since links from all associated Signaling End Points (SEP) terminate on the STP pair. The failure of a single STP should not, in and of itself, cause any severe impact on the ability of the PSTN to route calls. It is only when an STP failure is coupled with another condition in the CCSN that signaling traffic is impaired, causing an impact on the PSTN. Examples of conditions under which an STP failure will impact the CCSNs message processing capabilities are as follows:

– If software errors in either the mated STP or an associated SEP trigger an abnormal reaction to the failed STP, individual SEPs or all associated SEPs could become isolated from the CCSN.

-- If individual signaling linkset failures to the mated STP are in effect prior to and during the STP failure; offices could be isolated.

-- If the CCS network and its components have not been engineered adequately, congestion etc. could be encountered.

Link and Linkset Failures

As in the case of a single STP failure, the failure of a single link or linkset should have no severe impact on signaling traffic since the CCSN is engineered to self manage. It is only when coupled with other conditions in the CCSN that there would be an impact. The impact could range from complete SEP isolation (no messages to or from an SEP) to a condition where some individual SEPs cannot send and receive messages to or from other individual SEPs. Conditions which could impact an SEP's ability to send and receive signaling messages include the following:

-- Failure of an SEP's combined linkset to communicate with the mated STPs due to one or a combination of causes: .DL

-- SEP hardware

-- SEP software

-- facility failure

-- facility failure and no physical route diversity of links making up combined linkset

-- Failure of a combination of linksets in the routing path to another SEP due to the same causes listed above.

Congestion

The levels of congestion in the CCSN refer to the queued messages in the buffers associated with the network elements. There are four congestion levels (0, 1, 2 and 3) that are specified by the SS7 protocol. There are also four levels of priorities for messages, such as Transaction Capabilities Application Part (TCAP) messages which are usually a priority one. These priorities are used in concert with levels of congestion. For example, a congestion level of two would indicate to all nodes coming into an STP not to send any messages with priority less than two. A congestion level of three would advise not to send any messages with priority less than three.

Since maintenance messages are assigned a priority three, and the highest congestion level is three, maintenance messages would continue to flow (which is mandatory for the CCSN to function).

The SS7 protocol is designed to throttle-back volumes of messages when experiencing congestion. In the event this process fails, the congestion may become unmanageable, resulting in internal STP congestion which can then cause links and linksets to fail. If this condition is replicated in mated STPs, network outages may occur, isolating an office.

LINES OF DEFENSE

Controlling the impact of network failures, particularly with common channel signaling, is an essential activity. The spread of certain type failures (e.g. STPs) is not only extensive, but rapid. ASPs and ASCs should carefully review the layout of their PSTN, with an overlay of their CCSN, and consider key lines of defense. There should be a realization that the impact of one network event can be boundless across network boundaries. It is not only widespread, but deep, in its effect. One ASP event may not only impact a Local Access Transport Area (LATA), and all its offices, but also the inter-LATA traffic. Conversely, trouble in an ASC network can affect one or more ASP networks and possibly other ASC networks. For these reasons, this Section reviews activities applicable to the CCSN, including a discussion on Network Management in a CCSN environment and pre-plans for the PSTN. The following section divides traffic into unique categories with corresponding lines of defense and activities to be considered.

Traffic Categories and Considerations

The transition from MF signaling to common channel signaling demands a new awareness of the potentially widespread outages due to CCSN failures. The result can be total loss of service to a customer. This section categorizes traffic into groups whose vulnerabilities are similar and whose control activities may be unique.

After each discussion regarding outages affecting each category, there is a brief discussion on action considerations.

NOTE: In the considerations that are addressed in the following sections, F-links are suggested as a possible alternative. It should be noted that requirements for F-links do not currently exist, but are being reviewed. It should also be noted that with the advent of new services that may require the use of an SCP, F-links may not be a good long term investment in some scenarios. This is an individual assessment and should depend on the strategic directions of the interconnecting companies.

Intraswitch (AP)

During the failure types discussed in Section 2, calls outside the switch will not be completed, causing abnormal numbers of retries, in turn, congesting the switch and potentially disabling it. Network Traffic Management techniques, such as call-gapping, would be ineffective in this situation, since dial tone is not selective, but responsive to any off-hook condition, and the dialed digits must still be entertained. Switch processing is not split between pre-disposition and final disposition, i.e., there is no capability to up-front drop any NXX code not resident in the switch and only process resident codes. The capability to introduce an announcement (e.g., "only calls to the following NXX codes will be processed at this time"), before dial tone, is also not available.

Consideration: The objective here is to alert the public in an effort to stop redialing calls that have no chance of being completed, hence avoiding switch congestion. There needs to be a review of requirements or techniques that can be implemented to prevent congesting the switch, so intraswitch traffic can still be executed. It should be noted that the introduction of Integrated Services Digital Network (ISDN) may reduce congestion since these calls would not require an analog, sequential, time-consuming process. Announcements before dial tone may be a practical solution for digital switches, although perhaps not for analog switches.

It should be understood that the concern stated here is applicable to the following categories.

Interswitch/Intraoffice

Two different switches that are co-located are introduced to a new concern with CCS. In the CCS environment, signaling for trunks connecting these switches may venture well beyond the co-located office. The reader is reminded that a mated pair of STPs does not reside in a common location, for purpose of diversification, and on any specific call set up, if both STPs are in service messages will most likely visit both STPs. So, even in those cases where an STP shares a location with co-located switches, some of those call set up and tear down messages will route via the distant, mated STP.

Consideration: Co-located switches may be a prime candidate for F-links (CCS links connecting two switches - no STP involved), eliminating the need for any trunking or signaling beyond a central office. Assuming that there is no switch congestion (see Section 3.1.1) those interswitch trunks would be excluded from any propagation of CCSN failures and events involving STPs. .

Interswitch/interoffice

These calls have been reviewed, to some extent, in a previous section. The isolation of an end office due to a combined link set failure introduces a situation in which network traffic management and/or other techniques may be ineffective (other than code blocking) until the A-links can be restored. .

Consideration: Similar to Section 3.1.2, these groups may be candidates for F-link deployment and/or possibly some retention of MF trunking. In addition, E-link deployment can be considered.

Sections 3.1.1, 3.1.2 and 3.1.3 present three different categories of traffic whose elimination would have a dramatic impact on ASP/AC customers, especially since these categories represent traffic that is particularly sensitive to emergency situations. The above has introduced two important lines of defense - the switch and any local trunk group associated with local emergency traffic.

Restoration for 800 DB Isolations

See NOF Issue #168.

InterLATA Access

InterLATA access is a major concern, particularly as it affects major businesses and the complexities that are introduced with the interaction of other CCSNs. Current network management procedures between local

exchange and interexchange carriers (ASCs) will remain in place assuming the CCSN is stable. Serious CCSN failures, however, will require new contingency plans. These are addressed in some detail in this document.

Preventing Propagation and Lessening Impacts of Failures

Recent CCSN outages created some concern that the protocol, designed to manage the network, may not be sufficient in some failure scenarios. The potential for propagating a trouble in an integrated network increases that concern, causing speculation that some form of manual network management may be needed. What is included in the following section addresses the subject of manual intervention (e.g., in cases of Network Instability/Node Corruption).

What seems to be appropriate are predetermined contingencies that address the subject of isolating a CCSN from one or more interconnected CCSNs. These CCSN capabilities should be identified and ways found to implement these blockages when necessary. It should be stated, however, that all efforts should be made to mechanize these contingencies where possible.

Manual Intervention in the CCSN

It should also be noted that some manual controls applied to the CCSN represents a serious undertaking and must be implemented only under extreme failure conditions. In these circumstances the interconnecting carrier should be informed.

As one component of an overall network recovery plan, ASP/ASC personnel could prepare to take, as contingencies, manual intervention actions that may be used to mitigate the effects of CCSN failures, alleviate traffic overloads in the CCSN, and/or allow CCS network elements (NEs) to be restored to their proper operation.

The specific actions to be taken will be dependent upon the particular network failure or trouble scenario anticipated and the carrier's network traffic management strategy, as well as the manual control capabilities facilitated by supplier implementations of the CCS NEs, their operations interfaces, and supporting operations systems (OSs). Apriori knowledge of the percentage and number of trunks using CCS and MF signaling on a per switch, per LATA, and per interconnected network will facilitate the network managers anticipation of customer isolation impacts that will result from manual control actions that are suggested below to obtain nodal and network CCS isolations.

The following subsections provide at least a partial list of the manual intervention actions that might be prepared.

Node Isolation

Network operations personnel may wish to prepare contingencies to isolate individual signaling points from the remainder of the network, in cases where hardware or software failures may result in the inability of a given node to detect internal outages and/or trigger the appropriate automatic SS7 signaling route management and signaling traffic management actions to divert or throttle signaling message traffic.

Currently, network operations personnel may accomplish this objective by executing prepared scripts maintained in a maintenance OS to invoke supplier-specific NE commands that deactivate the signaling links connecting the subject signaling point to its adjacent signaling points. Contingency preplans should be made if a Network Element (NE) does not respond to supplier-specific commands to deactivate the signaling links. In such a case, a contingency preplan to remove the links physically (e.g. removing a circuit pack) should be employed.

There are currently no published generic requirements for uniform capabilities or procedures to accomplish this action. The control would involve the forced manual declared failure of signaling links in designated link sets.

Network Isolation

Network operations personnel may wish to prepare contingencies to isolate a CCSN from one or more interconnected CCSNs, in cases where replicated software errors in CCS NEs may cause a failure condition to propagate or co-exist across the network boundary or in instances where automatic SS7 congestion controls may fail to operate to protect a CCSN from severe traffic overloads originating in the interconnected CCSN. Procedures should be prepared for cases involving both directly connected CCSNs and remote CCSNs interconnected via an intermediate network or networks.

There may be occasion when access to the Network Management OS is blocked, the OS, or the intermediate OS is not on-line, or access from the OS to the switch is unavailable. In certain critical situations this may be unacceptable and require an alternative plan. Such a plan is envisioned by implementing critical preplans (also resident in the network management OS) via the maintenance OS over the switch maintenance channel interface. Some service providers do not use an automated method to apply preplans.

Customer Notification

A concern in any major failure is the potential to congest a switch due to reattempts on dialing a call that cannot be completed. A knowledgeable public at this point can lessen that concern. Not being able to call a distant relative or business partner is one thing; not being able to call the police, doctor, fire department, neighbor, etc. can be a different matter. Every effort must be made to complete emergency calls .

The advent of CCS increases the potential of end office isolation due to the greater potential for widespread disruption, causing fewer call completions and consequently, dramatic increases in redialing.

If customers know the only calls that can be completed are to NXX numbers within their switch, the potential for switch congestion could greatly diminish.

Media

One of the ways to inform the public is via the media (e.g. radio and TV). Prearranged agreements and plans for quick notification can be most beneficial in alerting the customers.

Announcements

Announcements were discussed in previous section.

Operator Alert

Operator calls dramatically increase during network congestion or failures. An uninformed operator can add to the problem. An informed operator can advise the public. What is needed here is the capability to alert operators via their operator service position screen, etc., using a maintenance workstation. There should be the ability to quickly instruct operators on options available.

RESTORATION

The introduction of common channel signaling has significantly complicated the restoration process involving failures that impact the PSTN. CCSN failures, particularly those necessitating node restart procedures (e.g., STP), have the potential for message loss and congestion problems. In addition, careful coordination is required between the CCSN and PSTN in any restoration procedure. These concerns are discussed in some detail in the following two sections.

Restoring the CCSN

A failed CCSN should be restored in accordance with the type of outage encountered. The following are examples of different scenarios involving failed STPs:

- Both STPs in a mated pair have failed gracefully
- If both STPs can be restored, normal SS7 restoration procedures should be followed.

It is difficult to provide specific details on how to restore a CCSN after a major failure because of the uniqueness of each network and each failure. There are, however, several factors to be considered when developing any restoration strategy. They include:

- Whether the Failure cause has been determined and remedied
- The number of signaling links connected to the STPs
- The number of links used for STP interconnections (B and D links)
- Amount of traffic left on the CCSN, if any, at the time of restoration
- Any known idiosyncrasies of the Vendor STP product.

In the case of a directly interconnected CCSN (i.e., one to whose STPs or CCS serving office a CCSN is directly connected via signaling links), such a network isolation action may be achieved as discussed above by network personnel invoking prepared scripts to deactivate all links in all appropriate internetwork gateway link sets.

However, in the case of a remote CCSN interconnected through an intermediate CCSN or "hub provider," such actions would not be sufficiently selective to ensure isolation of the a CCSN from the subject network only. There are two alternatives that may be used in order to isolate a remote CCSN. The first alternative uses 1) Gateway STP screening to block all incoming traffic from the remote CCSN and 2) Trunk Group (TG) protective controls (e.g. CANT) to block traffic destined to the remote CCSN network. The second alternative would require coordinated action from the hub provider to fail the signaling links used to access the signaling services by the remote CCSN.

NM Preplans

The use of NM preplans via a Network Management Operations System (NMOS) is a viable way to lessen the impact of a CCSN failure. Although the signaling network is capable of protecting itself for most failures, when CCSN failures do occur, the impact on the PSTN can be quite severe, and reaction time very limited.

One of the capabilities of controlling the severity of a failure is via the implementation of preplans. Preplans are used to protect or route around sector or access tandems and/or a major facility failure. Preplans are built by the Network Manager and reside in the NMOS database.

There are two types of plans: Code control and Trunk Group control. Controls fall into two categories: Protective and Expansive.

Protective controls CANCEL the traffic and route it to an announcement. Expansive controls REROUTE the traffic to trunk groups that do not normally carry that traffic.

Protective Controls

Code controls (Call Gaps) limit the number of attempts from a controlled office to a particular called number or NXX. A code control is typically effective on from three (3) to sixteen (16) digits. Nominally, Call Gaps are in levels of 1 to N. The disposition of the call is determined by the Network Manager. The call can be sent to an Emergency Announcement (EA) with a timely announcement pertaining to the situation or to the normal No Circuit Announcement (NCA).

Cancel To (CANT) and SKIP are Prehunt controls; CANT prevents the affected traffic from making an attempt on the controlled trunk group. SKIP causes the affected traffic to skip the controlled trunk group and hunt for a trunk in the next alternate trunk group.

Cancel From (CANF) is a Posthunt control; CANF prevents the affected traffic from overflowing from the controlled trunk group.

Expansive Controls

Immediate Reroute (IRR) and Overflow Reroute (ORR) also called a Regular Reroute (RR), are Expansive Trunk Group Controls.

IRR is a prehunt control, IRR diverts the affected traffic away from the controlled trunk group and causes it to hunt for a trunk in the designated trunk group. ORR or RR is posthunt control. ORR diverts the affected traffic after it overflows the controlled trunk group.

Some restrictions of such plans may be:

- Maximum number of controls in a plan.
- Maximum total of controls in all plans.
- Maximum number of plans.

Preplans must be updated whenever a change takes place in the network. An outdated Preplan is of little use in a failure scenario.

Access to Preplans

As described earlier in this document, a major failure is one that has affected both STPs of a mated pair to the point where the CCSN can't support the services using the network. After such a failure, as much normal traffic as possible should be prevented from entering the network until all available components are up and stable; e.g., no links going up and down and no unusual maintenance messages being generated in the STPs. NM control actions on the traffic network may be necessary subsequent to signaling network controls in order to allow the gradual return of traffic to the recovering node(s). These traffic controls may also be necessary to reduce congestion conditions that may arise from CCS controls. Note that when Trunk Group or Code Controls are used, strategies should allow MF trunk groups (if and while they exist) to continue to operate at full capacity thus avoiding unnecessary isolation or overcontrol.

If the failure cause has been remedied, the CCSN may restore itself. If not, normal vendor provided STP node restart procedures should be sufficient to restore the CCSN to normal. The recommended order to restore signaling links is C, then B and D, and finally A. If, however, the cause of the trouble has not been determined or remedied, consideration should be given to restoring the STPs in the simplex mode (C links forced out of service). If necessary, consideration should also be given to manually restoring B and D links, observing that the network remains stable as the links are restored. If any instability appears, the C links should be forced out of service and the network should be operated in the simplex mode until the problem has been resolved. If any A link linksets have failed, signaling point isolations may result from forcing the STPs into simplex operations.

Once the network has been restored and all appears stable, traffic should be restored according to a pre-planned strategy. The CCSN should be closely monitored to confirm that the restoration of traffic doesn't cause any instability.

Release and Patch Administration

It is important that a database or databases containing information on current release level and patches that have been applied to all Network Elements (NEs) exist and be kept current. This information must be readily available to center personnel responsible for trouble resolution. In many cases these databases are currently resident in an Electronic Systems Assistance Center (ESAC) administration system and are kept current with the aid of network element vendor OSs which support the patch administration process. It is advisable that this database is updated concurrent with the update to the NE. It is also advisable that when new releases are received from an NE provider that they be loaded in only one NE for a period sufficient to evaluate performance of the software. It is desirable that the NE chosen for this SOAK period be one that does not serve a major downtown area or critical service element; e.g., 911. In analysis of a trouble condition, consideration of release and patch level may be beneficial in resolution.

It is also preferable that these databases provide the ability for:

CCSN Stabilization

CCSN stabilization can be defined in many ways, but as a minimum, to be considered stable a CCSN must be prepared to receive traffic. Various indicators and parameters can be watched for signs of CCSN stabilization or destabilization. General criteria for CCSN stabilization are the following:

- Number of change-overs and change-backs is within acceptable limits.
- Number of congestion status changes over parts of CCS network is within acceptable limits.
- Number of MTP flow-control messages is within acceptable limits.
- Number of MTP traffic control and MTP-user restricting messages are within acceptable limits.
- Number of ISUP automatic control messages is within acceptable limits.
- Number of TCAP and OMAP control and test messages are within acceptable limits.

If all these parameters are within acceptable limits, then it is a good indication that the CCSN is stable. In all other cases the limits must be defined on a regional basis prior to CCS operation within the region.

Node Restart Procedures

Node restart procedures enable an unavailable node, which is in the process of becoming available, to bring a sufficient number of signaling links into the available state and to update its routing tables before user signaling traffic is restarted to that node. A node is considered to be unavailable when all of its connected signaling links

are unavailable. Node restart is a network management function and occurs at Level 3 of the Message Transfer Part (MTP) of a node. The node restart procedures are specified in Bellcore Specification of Signaling System Number 7 (TR-NWT-000246), where the procedures are referred to as MTP Restart. These procedures should help alleviate the burden placed on restarting nodes, allowing them to enter a stable state before accepting user signaling traffic. This is expected to reduce the potential for problems which may cause a restarting node to regress to an unavailable state.

Motivation

The primary motivation for the node restart procedures is the potential for message loss which currently exists in the way a signaling point, specifically an STP, behaves upon restart. No requirements currently specify special procedures for how a restarting signaling point should behave in order to accept traffic from adjacent nodes in a graceful and efficient manner. Currently, a restarting signaling point activates its signaling links serially, until all links, or a sufficient number of links, are available. Problems may occur due to this situation. Link congestion, for example, may occur when the STP receives traffic on a newly available links and an insufficient number of links have been activated on which to route outgoing signaling traffic, or traffic is destined for a point code that is not yet available. In addition to the potential for lost signaling traffic, there also exists the potential for congestion problems to occur on the newly available links.

The proposed node restart procedures prevent signaling points from sending user signaling traffic to an adjacent node which is restarting before the restarting node is ready to receive traffic. Being ready to receive traffic means having accurate routing information, as well as having a sufficient number of signaling links in the available state in order to perform the appropriate signaling point functions effectively and efficiently. Having accurate routing information prevents an unusual amount of signaling route management messages being transmitted across the network.

Overview of Node Restart Procedures

Two new network management messages to be used in conjunction with the node restart procedures have been defined in standards. The Traffic Restart Waiting (TRW) message is an indication to the receiving node that user signaling traffic should not be sent to the originator of the TRW until a Traffic Restart Allowed (TRA) message is received from the same node. A TRA is an indication to the receiving node that all signaling traffic may be resumed to the originator of the message.

The node restart procedures are not only performed at a restarting node, but also at nodes adjacent to the one which is restarting. >From the perspective of the restarting node, the procedure can be broken down into several stages. First, the restarting node attempts to make available, in parallel, its signaling links. As links become available, the starting node sends TRWs to adjacent nodes, indicating that it is not ready to receive any user signaling traffic. The restarting node expects to receive a TRW from adjacent STPs, as well as signaling route management messages, specifically Transfer Prohibited (TFPs), Transfer Restricted (TFRs), Transfer Cluster Prohibited (TCPs) and Transfer Cluster Restricted (TCRs) from adjacent STPs, and will update its routing tables upon receipt of these signaling route management messages. Also, the restarting node expects to receive TRAs from each adjacent node indicating that they are themselves ready to receive user signaling traffic. When a sufficient number of signaling links have been made available, and a sufficient number of adjacent nodes have indicated that they are ready to receive traffic, the restarting node, if an STP, will then broadcast to adjacent nodes the status of its routes using TFPs and TFRs, as well as TCPs and TCRs if cluster mangement is implemented. Upon completing the broadcast of signaling route management messages, the restarting STP will be ready to receive all signaling traffic, and will indicate this to adjacent nodes by broadcasting TRAs. If the restarting node is not an STP, it will not broadcast signaling route management messages, and will simply broadcast TRAs. At this point, the restarting node will have reasonably accurate routing tables, and will have a sufficient number of signaling links available to handle the expected traffic.

>From the perspective of a node adjacent to one which is restarting, the procedure can also be broken down into stages. When the first link of a link set to a previously unavailable node comes up, the adjacent node will behave in one of two ways, depending on its capabilities. More specifically, if the adjacent node is an STP, it will first send the restarting node a TRW, followed by the necessary signaling route management messages indicating the status of each destination to which it routes which is not allowed. No signaling route management messages will be sent by the adjacent STP if all the point codes to which it directly routes have a status of allowed. These messages allow the restarting node to update its routing tables prior to receiving any user signaling traffic. Once all the necessary signaling route management messages have been sent to the restarting node, the adjacent STP should send it a TRA indicating that it is ready to receive all signaling traffic. If the adjacent node is not an STP, a TRW will not be sent, and a TRA should be sent to the restarting node when it is ready for user signaling traffic. The adjacent node will then wait for an indication from the restarting node that it is ready to receive user signaling traffic.

B

Restoring Service

Before any public switched traffic is allowed to proceed, every effort should be made to make certain the CCSN is up and stable. It is recommended that the first traffic to flow should be the POTS traffic since other services, such as 800 Service, etc. require a POTS network.

How that POTS traffic is reintroduced depends upon the type of outage (e.g., entire LATA, single isolated office, etc.), the type of traffic in offices involved (heavy business, heavy residential, combinations), time of day (busy office hour, etc.), those concerns that network managers currently take into account. Consideration must also be given to any pre-plans activated in defense of the failure, i.e., how they were deactivated, were they deactivated, etc.

Applications on the CCSN will intensify and acceleration of extremely high-speed transmission capabilities will follow. In short, managing the CCSN, in the manner traditionally used to manage the PSTN, will not only not be feasible, it will not be advisable. Every effort must be made to enhance the protocol to enable self-management of the CCSN. There may be a manual role required to prevent propagation of a failure. This was discussed in some detail in a previous section.

Acknowledging the fact that the Public Network (for want of a better reference) will transition to two subnetworks, the CCSN and the PSTN, both required for call completion, does not eliminate the need to view these sub-networks on an individual basis from a Network Management perspective. On an individual basis, one should begin with the CCSN. When the CCSN is stable, NTM of the PSTN is implemented in the traditional manner. Most, but not all, of the failures experienced in the CCSN will be transparent to the PSTN, a product of redundancy and protocol.

Some failures in the CCSN will impact the PSTN and, unexpected, high concentration of traffic loads (e.g., media) may cause congestion in the A-links associated with that traffic load.

Network Management and CCSN Events

Events in the CCSN that impact the PSTN will probably occur at one of two levels, isolation of an end office or isolation of a complete LATA (assuming a mated pair of STPs per LATA and no E-links). Other events such as SCP isolations have been referenced by this plan, and should be considered in any comprehensive operations plan.

APPENDIX 11

B

COMMITTEE T1 - TELECOMMUNICATIONS
STANDARDS CONTRIBUTION

DOCUMENT NUMBER:	T1S1.3/93-02113
DATE:	February 22, 1993 (Raleigh, NC)
STANDARDS PROJECT: SUB-WORKING GROUP:	T1X1-02: Common Channel Signaling General, OMAP/MTP
SUBJECT:	Signaling Network Systems (SNS) Committee Prioritization of Recent Protocol Enhancements (MTP/OMAP)
SOURCE:	Bellcore Navesink Research and Engineering Center P.O. Box 7030, Room NVC 2Z-231 Red Bank, New Jersey 07701-7030 Stan Wainberg Tel: (908) 758-2122 Fax: (908) 758-4343
ABSTRACT:	This contribution presents for information the SNS Committee's prioritization of recent protocol enhancements listed in Contribution T1S1.3/92-11212R1, *Report to the Signaling Network Systems (SNS) Committee on SS7 Network Architecture Evaluations and Protocol Enhancements*.
DISTRIBUTION:	T1S1.3 Technical Subcommittee Working Group Members

B

1. Introduction

In support of the efforts addressing signaling network robustness by the Signaling Network Systems (SNS) Committee of the FCC's Network Reliability Council, T1S1.3 provided some CCS network architecture evaluations and described the SS7 protocol enhancements that have been recently worked and agreed on. These results were reported to the SNS Committee in contribution T1S1.3/92-11212 R1. This report was presented by T1 Chair, Art Reilly, to the SNS Committee in December and further discussed at the January 8, 1993 meeting. The report was well received and endorsed by the Committee. However, there were some concerns about the need for providing some additional guidance to facilitate uniform industry deployment.

As a result, the SNS Committee (1) established a subgroup of SNS volunteers to prioritize the protocol enhancements described in the report from T1S1.3 into two or three levels and (2) requested an addendum to the report with additional downtime analysis related to the architectures evaluated. Bellcore volunteered to chair and host the meeting related to the prioritizing effort. This contribution focuses on the outcome of this latter meeting, held in Newark, New Jersey on February 4, 1993, and provides T1S1.3 with the results for information purposes only. This contribution also serves as the report to the SNS Committee. The SNS Committee members and their representatives that attended this meeting are listed in Attachment "A".

2. Results

Since the SS7 protocol enhancements were designed to increase CCS network robustness, the prioritizing was based mainly on relative measure of improved network integrity to be achieved by the enhancements and the greatest perceived network need. The enhancements were placed into two priority categories, where category 1 reflected the highest network integrity benefits. Thus, category 1 enhancements would have the greatest impact on minimizing the effects of CCS network failure scenarios; minimize impact on the remaining network or interconnecting networks; and maximize the CCS network (and telephone network) stability. Category 2 enhancements reflect lesser impact in that these enhancements do not apply to severe network failure scenarios and may be more localized in their network impact. In addition to help categorize these enhancements, the following additional considerations were used:

(a) Indication that a specific failure scenario has occurred, and
(b) The need for internetwork compatibility has been identified.

Although two priorities were used, all the enhancements in each category should be considered as important and dealt with in a degree of urgency. Although the outcome of this SNS-initiated subgroup is a recommended priority list to the industry, the final priority and deployment by a carrier can be influenced by factors other than those considered by the subgroup.

Of the seventeen protocol enhancements completed and described in the report to the SNS, nine were placed in category 1 and eight in category 2. The detailed list is shown below with several added notes. The items within each category are not prioritized or ranked. The location of each enhancement in the T1S1.3 report to SNS is described in the parentheses.

B

Priority Category 1

SMH Congestion Control Procedures (Section 1.1)
Procedures to Eliminate False Link Congestion (Section 1.2)
Prevention of Congestion on Newly Available Link Sets (Section 1.3)
Prevention of Congestion from Rerouted Traffic (Section 1.4)
Prevention of MTP Circular Routes (Section 1.6) - Note 1
Prevention of Link Oscillation (Section 1.9)
Procedures for Restarting the MTP (Section 1.13)
Procedures for Recovery from Processor Outage (Section 1.15)
Cluster Routing and Management Procedures (Section 1.16)

Priority Category 2

SCCP Routing in Response to MTP Congestion (Section 1.5)
Prevention of SCCP Circular Routes (Section 1.7) - Note 2
Prevention of Trunk Looping Caused by the ISUP (Section 1.8)
SLS Code Expansion (Section 1.10)
Improved SLT Procedures (Section 1.11)
Backup Procedures against Loss of TFR/TCR Messages (Section 1.12)
MTP User Flow Control (Section 1.14)
Optional TFP Broadcast Across Network Boundaries (Section 1.17)

Note 1. The protocol enhancement described in Section 1.6 includes two separable protocol procedures; that is,
(1) MTP procedures which are automatic and on-going in preventing circular message routing and
(2) OMAP procedures which are initiated manually by operations craft to check for routing table errors.

Note 2. The protocol enhancement described in Section 1.7 was not considered for the higher priority since this protocol procedure is related to a new routing capability called ISNI (Intermediate Signaling Network Identifier) which is presently not deployed in the existing CCS networks and would require nationwide deployment for effectiveness.

B

ATTACHMENT "A"

SNS Members	Representatives attending working group to prioritize protocol enhancements
Bellcore Rich Baseil	Stan Wainberg - Chairman/host Andy Jacob, Gobin Ganguly
Ameritech Joel Engel (NRC)	Tony Brinkman
AT&T - Network Systems Al Loots	Tom Marciani
AT&T - Comm. Bob Hirsch	Jeff Azam, Janey Cheu Doris Lebovitz
Bell Atlantic John Seazholtz - Chair	Dana Shillingburg
BellSouth Charlene Echols	Janine Irwin
DSC Peter Jackson	Jeff Copley
GTE Telops Lonnie Allen/Dave Fiasco	Lonnie Allen, Brian Foster
MCI Jack Walters	Luis Reto
NTI Peter Budihardjo	Siva Ananmalay, Peter Budihardjo Rakesh Gupta
Pacific Bell Dick Bostdorff	Steve Sposato
U S WEST Mike Carlson	Char Meins

B

APPENDIX 12

B

IITP Phase 0 Final Report

Prepared by:

IITP Phase 0 Participants:
Ameritech Services
AT&T- Network Systems
Bellcore
DSC Communications Corporation
Northern Telecom
NYNEX Science and Technologies
NYNEX Telesector Resources Group
Sprint

Preamble

As detailed in documentation of the Internetwork Interoperability Test Plan (IITP) Committee, the companies providing lab facilities for Phase 0 IITP testing are submitting this final report to the IITP Phase 0 library. Per the Network Operations Forum's (NOF's) information sharing guidelines, this report is being released after the affected carriers and suppliers have had the opportunity to review and comment on these findings. As appropriate, their comments are included in this final report.

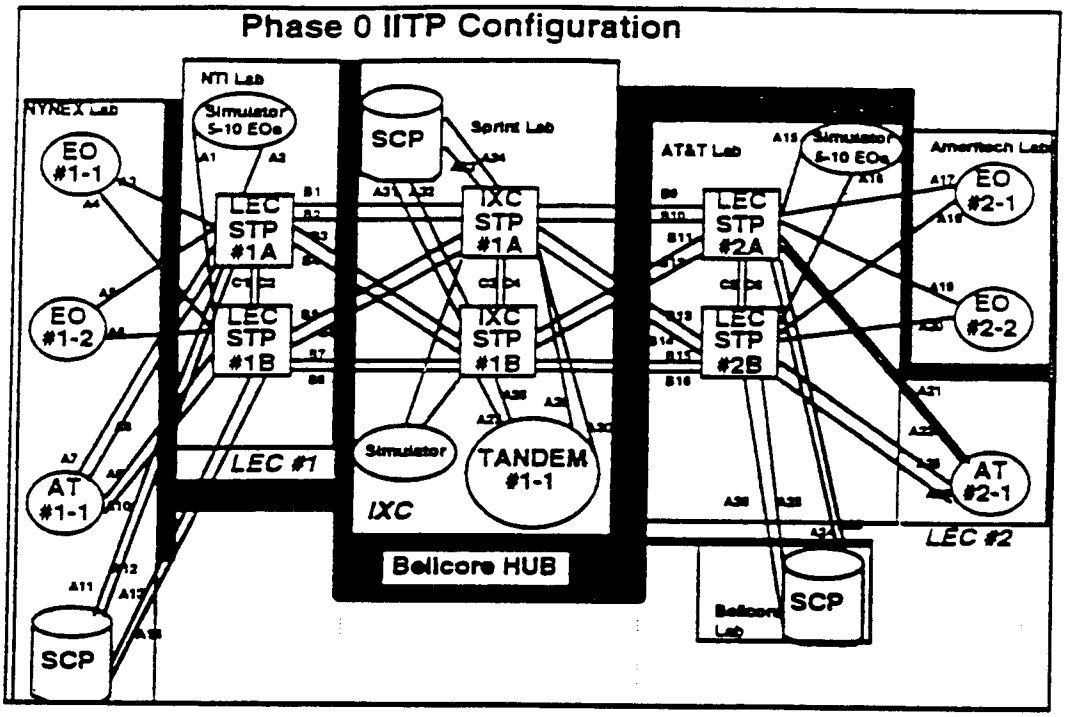
The format of this report is intended to be as defined in the "IITP Report Definitions".

This report is developed by the test participants, including Ameritech Services, AT&T Network Systems, Bellcore, DSC Communications Corporation, Northern Telecom, NYNEX Science and Technologies, Sprint, and Telesector Resources Group (a NYNEX company). The responsibility for development of this report belonged to the participating carriers, as defined in the NOF's information sharing guidelines.

1. Configuration and Participation

The test configuration is as shown below. It included laboratory facilities provided by AT&T-Network Systems, Ameritech, Bellcore, Northern Telecom, NYNEX, and Sprint. These companies were also the principal participants, although other suppliers, whose equipment was involved in the testing, provided additional support. These suppliers include DSC Communications Corporation, Ericsson Network Systems, Siemens-Stromberg Carlson, and Tandem Computer.

B



2. Number of Tests Scheduled/Completed

The Phase 0 Test Scenarios (IITP Phase 0 Test Scripts, August 2, 1992) include 13 test cases, with one test having six parts. All tests were scheduled and executed, except for:

- Test 1.f, Oscillating A Links (not executed on LEC 2 side ONLY),
- Test 1.i, External Clock Failures,
- Part 3 of Test 2.a, B/D Link Congestion,
- Parts 1 and 3 of Test 2.b, A Link Congestion, and
- Test 2.c, Incoming Link Congestion.

3. Reasons for Any Tests Not Executed

- Test 1.f, part 2 (LEC 2 side), was not executed because the specialized test equipment to induce oscillations could not access the LEC 2 A links.

B

- Test 1.i was not executed because it was assumed that the test script was not applicable for the STPs under test.
- Test 2.a, part 3 was not completed because of an apparent facilities problem.
- Test 2.b, part 1, was not completed because of an apparent facilities problem.
- Test 2.b, part 3, was not executed because of a problem with the specialized test equipment needed for that test.
- Test 2.c was not executed because, at the time the test was attempted, it was determined that the test equipment on-hand was insufficient for developing the test conditions stated in the script.

4. Justification for Any Test Cases Added, Deleted or Modified

No other tests were added or deleted.

Tests 1.f and 1.g (Oscillating A links and Oscillating B/D links) were modified to include additional oscillation characteristics beyond those specifically called out in the scripts.

Test 1.g (Oscillating B/D links) was also modified to reduce the traffic load for part of one section of the test, because the load required by the test script resulted in congestion. Having congestion on the links violated the intent of the script, so traffic levels were reduced to better meet the script's intent.

Test 2.b, parts 1 and 3, was modified to remove direct end office trunking from the basic configuration because it was implied (although not directly stated) in the script.

Test 3.a (High Level of Network Management Traffic) was modified to include fewer than 110 route sets on the LEC #2 side being full point code routed. Because of time constraints, including 110 route sets would have made it impossible to execute the test.

B

5. Overall Observations Based on Phase 0 IITP Testing and Analysis

In this section, we provide general recommendations based on the IITP testing and subsequent data analysis. Specific findings are detailed in the following section.

Several of the IITP Phase 0 anomalies were found to be a direct result of inappropriate or inadequate data fills or translations. The IITP test participating carriers collectively are stressing the importance of checks on translations, particularly as they relate to alternative routes/route sets and load sharing. It was observed that the IITP scripts effectively called for the use of alternative or secondary routes or route sets, and as such, during the course of testing (or later data analysis) some expected alternate routes were found to be unavailable.

6. Issues, Abnormalities, and Ambiguities Identified with Associated Action Items

This section details the Issues, Abnormalities, and Ambiguities ("findings") of the Phase 0 IITP testing and subsequent analysis. The findings detailed below relate to network implementations, network interfaces, and node implementations. Some of the findings are specific to varying implementations resulting from recent changes in Standards and requirements, and those issues are discussed separately. Listed below are the definitions used by the testers/analysts relative to the impact of the observations on the interconnected network.

6.1 Definitions of Network Implications

Included among the findings detailed below are **"Network Implications"** that attempt to detail the observed or possible effect each of the findings had on the interconnected networks. The categories used, and their definitions, are detailed below.

- **SERVICE AFFECTING - DENIAL** - The testers and/or analysts observed one or more calls being directly denied service due to network managed conditions.
- **SERVICE AFFECTING - POTENTIAL FOR LOST CALLS** - The testers and/or analysts observed potential for one or more calls to be directly denied service due to network managed conditions. Lost calls were not directly observed.

B

- **SERVICE AFFECTING - DELAYS** - The testers and/or analysts observed potential for delays in completing one or more calls directly as a result of network managed conditions.

- **POTENTIAL IMPROVEMENT (PROTOCOL)** - The testers and/or analysts observed no impact on call completion as a result of this finding, but this is viewed by the testers and/or analysts as an area for potential protocol (or requirement) improvement. For example, the testers may have observed multiple interpretations of the same protocol item.

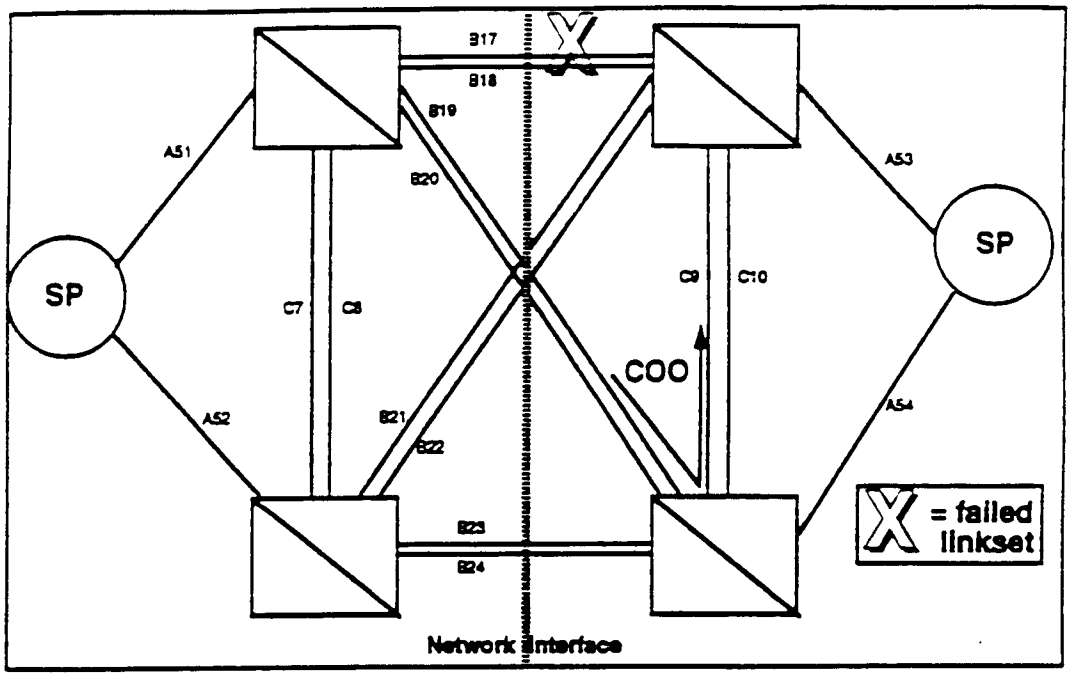
- **POTENTIAL IMPROVEMENT (IMPLEMENTATION)** - The testers and/or analysts observed no impact on call completion as a result of this finding, but this is viewed by the testers and/or analysts as an area for improved network or product implementation.

- **OPERATIONS AFFECTING** - The testers and/or analysts observed no impact on call completion as a result of this item, but this is viewed by the testers and/or analysts as an area for potential confusion during routine or emergency operations.

- **OTHER** - This finding was not observed to have direct impact on call completion or operations, but this anomaly was observed by the testers and/or analysts and is included here, per NOF guidelines.

DEFERRED FOR FURTHER REVIEW - This observation needs further investigation before it can be stated as a conclusive finding.

B



Network Implication: SERVICE AFFECTING - POTENTIAL FOR LOST CALLS AND DELAYS

Disposition: The affected supplier has commented to the affected carrier that detailed analysis of the messaging collected during the testing is inconclusive as to determining the cause of the anomaly. Analysis of the translations and messaging suggest that the message would have been sent, but was not observed in the network management messages captured during the testing. It is possible that the anomaly is a result of an improper translation, a lost message in the data collection, or some other reason. As such, the affected supplier has commented that additional testing, either in a stand-alone or interconnected environment or both will be performed in early December 1992. If the testing and subsequent analysis result in an anomaly associated with a network implementation or product, an Addendum to this report will be issued.

B

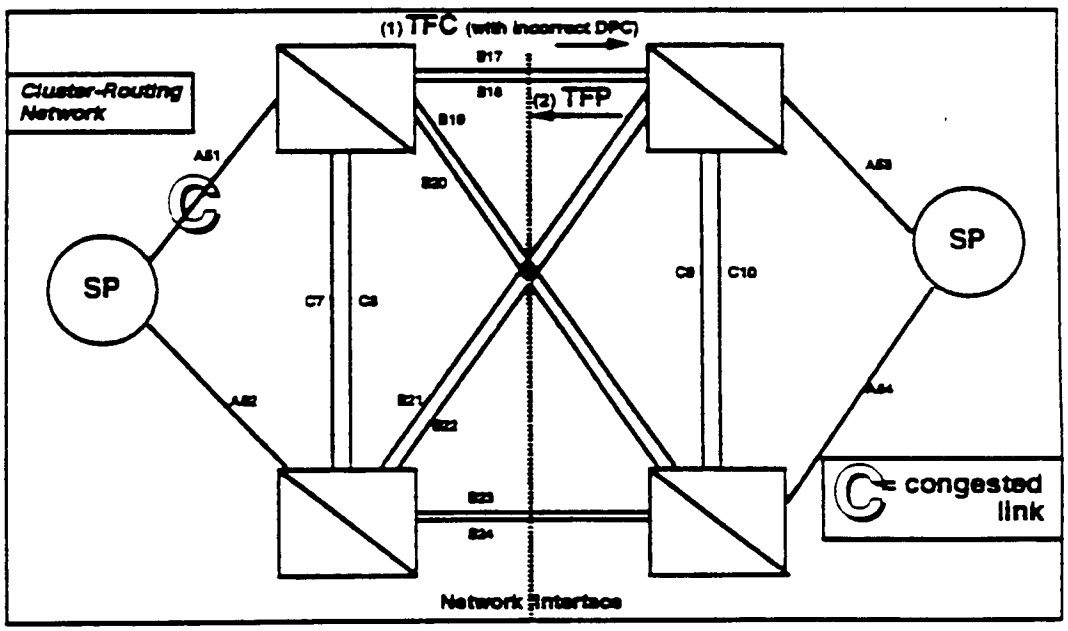
6.2 Anomalies Related to Varying Implementations

6.2.1. ***It appears that gateway screening prevented use of COO/COA within linkset failures.*** During execution of several tests, it was observed that during changeover and changeback, some STPs did not respond with the corresponding acknowledgments. For example, as shown below, in the event of a linkset failure, a COO is required to take the path shown, however, it was observed that the COO goes across the B/D-links but fails to continue along the C-links. This resulted in lost messages on changeover and delayed messages on changeback. The analysts believe that gateway screening is the cause. With gateway screening implemented, the screening function will examine the DPC of certain incoming network management messages (including COO, COA, ECO, and ECA) to insure that the DPC is that of the gateway STP or its mate. It was observed that when the DPC was that of the receiving gateway STP's mate, the message was discarded. In the case of a link set failure (recovery), attempts to route the changeover (changeback) messages via an alternate route resulted in message discard. The consequence of this is that during changeover any messages in the retransmission or transmission buffer are lost and during changeback messages are delayed. It was possible that some calls could have been lost and some calls may have been delayed.

B

6.2.2. ***One network cluster-routes and the adjoining network full point code-routes. With cluster routing in place, TFCs with DPC or APC incorrectly addressed (member = 0) were sent; the incorrect DPCs led to excessive TFPs being returned, which were ignored.*** The TFCs with incorrect DPCs (member=0) were observed when the A-links to a simulator were forced into congestion and the traffic was originating from the remote network. The network experiencing congestion directed the Transfer Control messages (TFCs) to the cluster originating traffic instead of the individual point codes that were originating traffic. These TFCs caused the remote network to generate TFPs concerning the non-existent member 0; in turn, the TFPs were ignored by the home network. The TFCs with incorrect APCs (member=0) were observed when the B-links to the remote network were brought into congestion.

The TFCs sent to nodes in the home network contained the affected point code (APC) of the remote cluster instead of the destination point code of the message that put the transmit buffer over the congestion threshold. The analysts believe that in the small time period that this occurred, it was possible that some calls could have been lost. Also, this condition would prevent the effective use of TFCs in reducing congestion by shutting traffic off at the source.

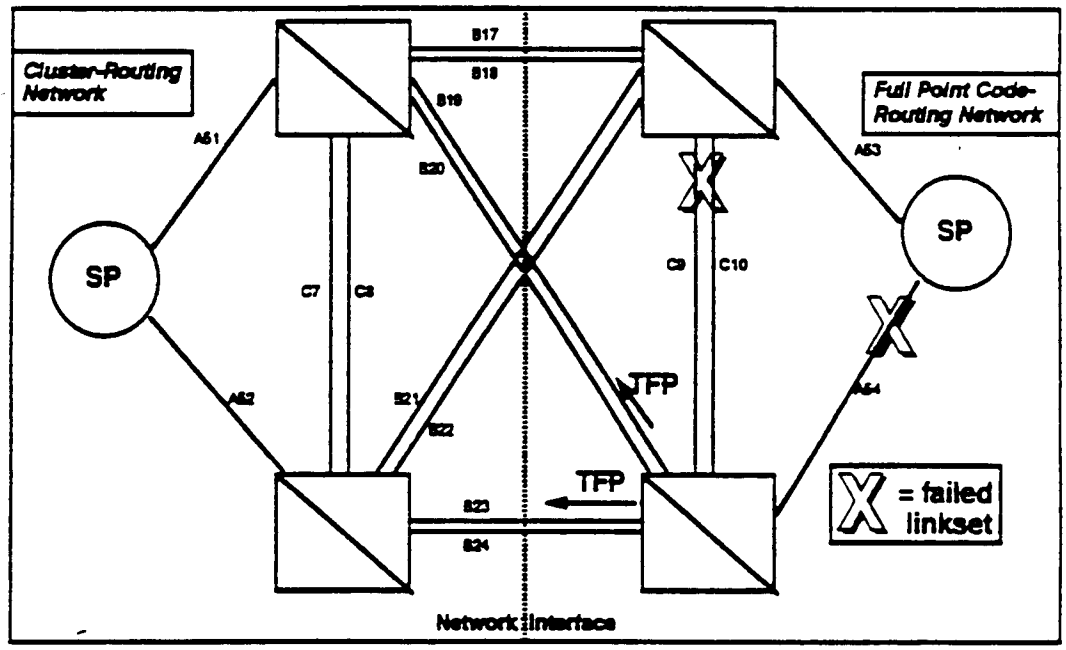


B

Network Implication: SERVICE AFFECTING - POTENTIAL FOR LOST CALLS

Disposition: The affected supplier has commented that a fix for this issue will be available in a generic to be released to the field in mid-1993. Details for this issue are being provided by the supplier to its customers during December 1992.

6.2.3. ***One network cluster-routes and the adjoining network full point code-routes. TFPs and TFRs from full point code-routed network, with correct member number were ignored.*** This occurred when the full point code routed network had failures of its C-linkset and one or more A-linksets to SPs in that network had also failed. This resulted in the partial isolation of a switch. When this occurred, TFPs and TFRs with correct member number were generated from the full point code routed network to the cluster routed network. These messages were ignored because the cluster routed network did not recognize those member numbers. The analysts believe that when this happened, many calls were launched toward the STP that was unable to access the partially isolated switch and calls were lost.



Network Implication: SERVICE AFFECTING - DENIAL

B

Disposition: The affected supplier has stated that this will be corrected in a feature to be available in a generic scheduled for release in mid-1993. The affected supplier has also stated that it is notifying its customers of this concern during December 1992.

6.2.4. ***re: Test 1g, on B-link oscillation, potential anomaly seen on other (mate) B-Linksets.*** During the link oscillation test (test 1.g) for the B-links, it was observed that when the bit error rate was fixed at either 5 x 10-5 or 8 x 10-5 and traffic was at 40%, one of the STPs experienced a severe case of receive congestion. The congestion was first observed, as expected, on one of the links with the high error rate. However, unexpectedly, the receive congestion was next observed on two of the links not being errored. The links were observed to oscillate between congested and not congested. One of the links went into and out of receive congestion in excess of 300 times during the 5 minute test. This may not be compliant to T1 Standards.

Network Implication: DEFERRED FOR FURTHER REVIEW

Disposition: The affected carriers and suppliers have attempted to reproduce this effect in off-line testing. Thus far, those attempts have not resulted in a recreation of the conditions shown. Possible explanations include unrecognized conditions with facilities during the testing or difficulties by those attempting to recreate the effect in simulating the Phase 0 test conditions.

One affected carrier has provided the following comment: "[Carrier name] can neither agree or disagree. [Carrier name]'s primary responsibility was to monitor the C and A links. The B links were secondary, and only the bit-errored link was monitored. Therefore we have insufficient data on the other B links and would like the test to be re-run. We think this is important and warrants further investigation before any action is taken to pursue corrective measures."

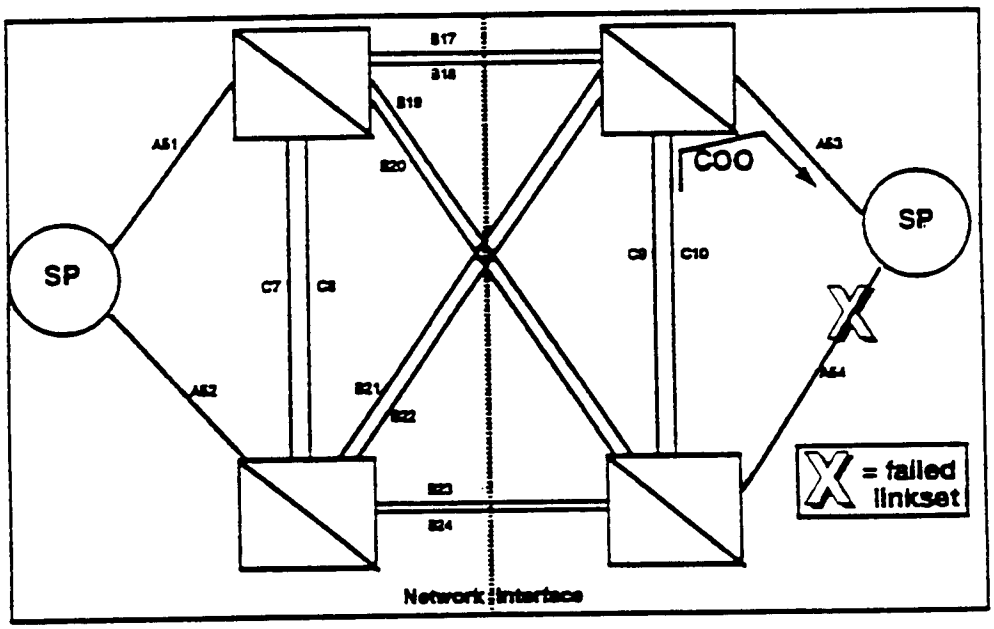
The affected supplier of another affected carrier has provided the following comment: "While this observation was under study, [Supplier name] requested this test be executed in another test effort between the same suppliers."

B

Further investigation by participants is needed to determine whether the observation during this test can be reproduced. As such, all affected parties (two carriers, two suppliers and the Hub provider) have agreed to a retest in an internetwork lab environment in a final attempt to recreate this condition. This testing is scheduled for early December 1992. If the testing and subsequent analysis result in an anomaly associated with a network implementation or product, an Addendum to this report will be issued.

6.3 Node Observations

6.3.1. *3 SPs each did not send COA or ECA if linkset failed AND COO is sent.* This situation occurred when an A-link set from an SP to an STP failed and a COO was sent via the C-link and the mate STP. The analysts believe that time controlled diversions took place, but in the small time period before that happened, it was possible that some calls could have been lost and some calls may have been delayed (messages in the transmission and retransmission buffers could possibly be discarded).



Network Implication: SERVICE AFFECTING - DELAYS and POTENTIAL FOR LOST CALLS

B

Disposition: More than one supplier's products were observed to have this occur. As a result of this finding, at least one supplier had an open customer service request. Further investigation into the cause of this resulted in recognition of missing or erroneous data in the SPs' data fills relative to existence of alternate routes and/or load sharing capabilities. It is important to recognize that verification of the associated translations can be difficult and time-consuming, but is essential (critical) in the event that alternate routes become necessary. The affected carriers recommend that carriers pay special attention to verifying the existence of alternate routes so as to avoid the situations observed in this testing.

6.3.2. ***SP sends TFx messages.*** The STPs and not the SPs have the function of generating TFx (TFP, TFR, and TFA) messages. During Phase 0, we saw one SP generating these messages. Although this did not cause additional problems in Phase 0, it is possible that these messages might cause problems in other configurations. The analysts believe that this has potential for leading to an operations issue in other interoperability environments and could cause confusion for operations when attempting to diagnose or resolve other problems.

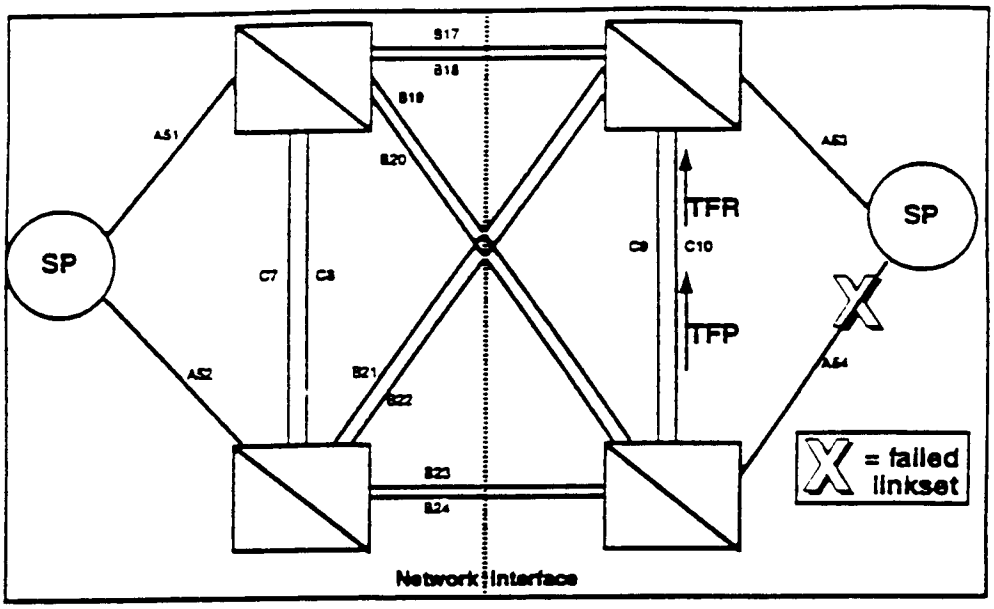
Network Implication: POTENTIAL IMPROVEMENT (IMPLEMENTATION) and OPERATIONS AFFECTING

Disposition: Discussion with representatives to T1 indicate that this is non-compliant to current Standards. The affected supplier has provided the following input to the affected carrier on November 19, 1992 relative to this item: "This letter is to inform you that [supplier name] has notified all of our current customers that have an SS7 end node product of an item that was discovered during IITP testing. This Item is described in [reference to correspondence from affected carrier to affected supplier].

"Based upon [supplier name]'s current development schedule, a solution to this item is scheduled for delivery 2Q1993."

6.3.3. ***STP sends TFR then TFP on C-links when route fails. Note: T11 not implemented and all TFRs (A- B- and C-links) are sent before TFPs.*** This situation occurred when one A-link from an SP to an STP failed. It may be related to the non-implementation of the T11 timer in one or more of the STP pairs. The implication may be some confusion as a result of the message sequencing.

B



Network Implication: OTHER

Disposition: One affected supplier has stated to the affected carrier that the T11 timer implementation is optional and is not presently supported by its STP product. Further clarification of T11 requirements needs to be addressed in the Standards before implementation is recommended.

Another affected carrier provided the following comment, which includes a response from their affected supplier (section b, below): "(a) The T11 timer is not presently supported by [the affected carrier]'s STP supplier, [Supplier name].

"(b) **[Supplier name] RESPONSE:** [Supplier name] feels that the procedures defined for T11 are too vague. The T11 will work very well for a small number of short duration linkset failures. If there is a large number of linkset failures then T11 could be detrimental by driving the alternate route (C linkset) into congestion. T11 will only be an asset in a large failure if there is no chance of driving the alternate route into congestion.

B

"If the TFR is not broadcast and the C linkset is driven into congestion and results in TFCs being sent to the SPs, the resulting ISUP load could cause more harm to the network than the controlled rerouting. The controlled rerouting is hidden from user parts while TFC is not. The existing procedures provide a method to not start T11 for danger of congestion.

"If the alternate "C linkset" does get into congestion there are no procedures for aborting T11.

"[Supplier name] plans to bring a contribution to standards addressing issues on T11.

"(c) [Carrier name] does not think T11 is a critical issue, but is continuing investigation of the issue.

"(d) [Carrier name] will consider an upgrade if or when the feature becomes available from [Supplier name]."

6.3.4. ***Optional timer T11 not implemented in two pairs of STP (used for TFR timers).*** This situation occurred when link failure resulted in a restricted route from an STP. This results in the immediate sending of TFRs and remote nodes rerouting instead of delaying the action for T11.

Network Implication: OTHER

Disposition: One affected supplier has stated to the affected carrier that the T11 timer implementation is optional and is not presently supported by its STP product. Further clarification of T11 requirements needs to be addressed in the Standards before implementation is recommended.

Another affected carrier provided the following comment, which includes a response from their affected supplier (section b, below): "(a) The T11 timer is not presently supported by [the affected carrier]'s STP supplier, [Supplier name].

B

"(b) **[Supplier name] RESPONSE:** [Supplier name] feels that the procedures defined for T11 are too vague. The T11 will work very well for a small number of short duration linkset failures. If there is a large number of linkset failures then T11 could be detrimental by driving the alternate route (C linkset) into congestion. T11 will only be an asset in a large failure if there is no chance of driving the alternate route into congestion.

"If the TFR is not broadcast and the C linkset is driven into congestion and results in TFCs being sent to the SPs, the resulting ISUP load could cause more harm to the network than the controlled rerouting. The controlled rerouting is hidden from user parts while TFC is not. The existing procedures provide a method to not start T11 for danger of congestion.

"If the alternate "C linkset" does get into congestion there are no procedures for aborting T11.

"[Supplier name] plans to bring a contribution to standards addressing issues on T11.

"(c) [Carrier name] does not think T11 is a critical issue, but is continuing investigation of the issue.

"(d) [Carrier name] will consider an upgrade if or when the feature becomes available from [Supplier name]."

6.3.5. ***STP (test 1B) did not send all TFAs expected.*** In one test, the analysts observed that one STP-pair in one network did not generate all expected TFAs upon route recovery. The analysts believed that time controlled diversions took place, but in the small time period before that happened, it was possible that some calls could have been lost.

Network Implication: SERVICE AFFECTING POTENTIAL FOR LOST CALLS

B

Disposition: The affected carrier and affected supplier have been working closely and retesting in attempts to duplicate the test conditions and results. The affected supplier has also provided the following comments: "In two test sessions, we have not been able to reproduce the events reported in this issue. Testing was performed using the same generic and databases of IITP Phase 0. Recently, Bellcore shared the signaling message data associated with this test. This has given us some further ideas for a subsequent test session planned for the week of 11/9.

"As it stands, we have illustrated the correct functioning of this capability through 2 of 3 test sessions. We will notify the customer about the status of the third test session."

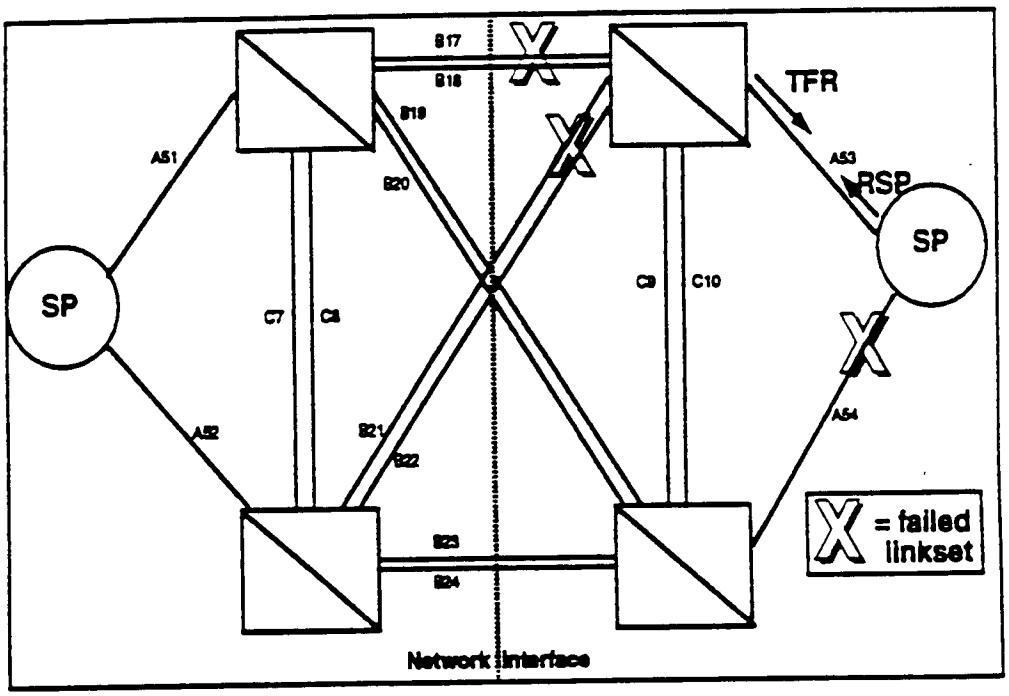
Subsequently, the affected supplier provided the following comment: "On November 11, 1992, we had a third test session in an attempt to replicate this issue. Using the same [STP] generic and translation base, we repeated the test utilizing [simulators] to emulate the [affected carrier]'s end offices. The conditions and methods of the original test were duplicated, but all TFAs were sent to the proper locations when A-links were restored.

"[Supplier name]'s testing has shown the proper operation of the [STP name] for this test. The final status of this issue is that it cannot be reproduced."

Nevertheless, all affected parties (two carriers, two suppliers and the Hub provider) have agreed to a retest in an inter-network lab environment in a final attempt to recreate this condition. This testing is scheduled for early December 1992. If the testing and subsequent analysis result in an anomaly associated with a network implementation or product, an Addendum to this report will be issued.

B

6.3.6. ***SP receives TFP followed by TFR on only available route but still considers the route prohibited.*** The scenario under test was one in which an SP was connected to a mated-pair of STPs (called STP A and STP B). The A-link from the SP to STP B was out of service and the B/D links from STP A to the adjacent network were out of service. A TFP, followed much later by TFRs were generated from STP A toward the SP, and the SP responded with RSP (route set prohibit) messages. The SP considered the route prohibited (it should have been considered restricted) and the SP would not route calls on its one remaining A-link. The analysts believed that calls were lost during the duration of this condition. This was verified by the inability to complete calls during the testing.



Network Implication: SERVICE AFFECTING - DENIAL

Disposition: The affected carrier received the following response from the affected supplier: "[Supplier name] acknowledges ... there is a problem handling Transfer Restricted messages when a Transfer Prohibited message has been previously received for the same route (i.e., once a Transfer Restricted message is received, the route should be updated to reflect the availability of the route). The [product name] continued sending Route Set Test messages concerning the prohibited route for which it had previously received a Transfer Prohibited.

B

"From our perspective, this issue has been acknowledged and will be addressed by way of a software fix or work-around within the standard interval based on priority, e.g., 30 days for service affecting problems or 90 days otherwise from the date the problem was reported to our Technical Assistance Center. Also, if found to be service affecting, a Technical Assistance Center bulletin will be issued to our customer base as soon as possible."

On November 24, 1992, the affected carrier received the following from the affected supplier: "A software work-around in the form of a patch has been developed and tested and is being prepared for release to the field. In the meanwhile, a bulletin has been issued to our customers to inform them of the condition. A permanent software fix will be incorporated into our planning process for an upcoming software release."

The affected supplier has not provided a customer notification schedule.

6.3.7. ***SP sends incorrect RCT for TFC(2) and sends RCT(2) instead of RCT(1). Also, does not reset congestion level in response to subsequent TFCs until after RCT(0).*** During the congestion test (test 2a), one SP was observed to send route congestion test messages (RCTs) with a priority higher that expected (congestion level was 2 and priority 2 was sent). Also, the SP sent the subsequent RCTs with priority reduced by one, regardless of intermediate TFCs. The RCT's priority was reset to 2 after a RCT of priority 0 was sent.

Network Implication: SERVICE AFFECTING - POTENTIAL FOR LOST CALLS and POTENTIAL IMPROVEMENT (IMPLEMENTATION)

B

Disposition: The affected supplier provided the following comment to the affected carrier: "Currently we are analyzing the data from the protocol analyzer received from you and have scheduled lab time to reproduce the problem you have described. In reviewing our functional specification and discussing the issue with our developers, there appears to be a conflict with our understanding of the issue and your observations. We will update you when we have progressed further in our investigation. If a software fix or work-around is needed, we will provide a patch or suitable instructions to the field within the standard interval based on priority, e.g., 30 days for service affecting problems or 90 days otherwise from the date the problem was reported to our Technical Assistance Center. Also, if found to be service affecting, a Technical Assistance Center bulletin will be issued to our customer base as soon as possible."

On November 24, 1992, the affected carrier received the following from the affected supplier: "[Supplier name] acknowledges the correctness of the observation and agrees that this is not a serious service affecting problem, since it only has a potential for lost calls. Nevertheless, a software work-around in the form of a patch is being developed and will be released to the field as soon as possible. A permanent software fix will be incorporated into our planning process for an upcoming software release."

6.3.8. ***In test 3a, no TFx was observed from STP to intra-network SP (this potentially is a translations issue. TFxs observed were destined for other network, not locally).***

Network Implication - DEFERRED FOR FURTHER REVIEW

B

Disposition: The affected supplier has commented to the affected carrier that detailed analysis of the messaging collected during the testing is inconclusive as to determining the cause of the anomaly. Analysis of the translations and messaging suggest that the messages would have been sent, but were not observed in the network management messages captured during the testing. It is possible that the anomaly is a result of an improper translation, a lost message in the data collection, or some other reason. As such, the affected supplier has commented that additional testing, either in a stand-alone or interconnected environment or both will be performed in early December 1992. If the testing and subsequent analysis result in an anomaly associated with a network implementation or product, an Addendum to this report will be issued.

6.3.9. ***SP sends RSx messages to its STP about itself.*** In some link failure scenarios, the analysts observed that an SP would send messages to an STP about itself (the SP).

Network Implication: POTENTIAL IMPROVEMENT (PROTOCOL) and OPERATIONS AFFECTING

Disposition: Affected supplier has provided the following comment: "We recognize this as a problem in the version of the [product] software which was used in the IITP tests. The version of software used was [noted version number]. As this is a recognized problem in the [SP], it has been corrected and validated in the current [SP] offered by [supplier name] in the [revised product name]."

The supplier also indicates that all customers using that particular product have received updated versions of the software to resolve this issue.

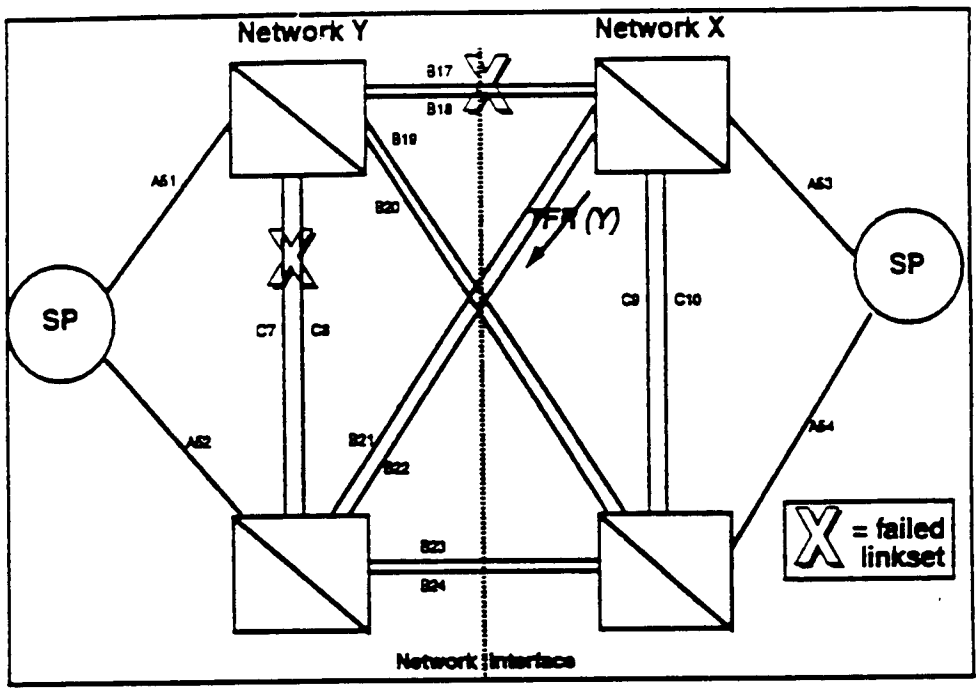
6.4 Anomalies Related to Recent Changes in Standards or Requirements

This section includes discussion of items observed in one or more, but not all network implementations. Each of these items has been discussed in great detail with authors/editors of Standards and requirements. In each case, the Standards and/or requirements have recently been revised and agreed to (although they may not have completed letter ballot) and as such, each of the anomalies observed reflects differing implementation schedules by suppliers and/or carriers. It is important to note that products performing as detailed below meet recently

B

(within a few months) issued criteria or nearly issued Standards. Products not performing as detailed below meet earlier versions of requirements or Standards. It is important to recognize that the "**Network Implications**" result from the current variations in implementations and are expected not to be of concern, as full implementation is put in place. Note also that because full implementation is underway, no Disposition is suggested for the items.

6.4.1. *TFx messages sent from Network X to Network Y re: Network Y.*



On B linkset failure, TFR followed by TFP sent from Y(0) to X(1) re: X(0).

Network Y broadcasts TFA followed by TFP to Network X re: Network X on C-Link restoral with B-linkset unavailable.

STP sends TFA then TFP to X about X on link recovery.

These situations appear to be related to broadcast of TFx implementations. The analysts believe that these situations were consistent with the protocol but could cause confusion for operations when attempting to diagnose or resolve other problems. Recent updates to Bellcore requirements clarify when such messages should be sent.

B

Network Implication: POTENTIAL IMPROVEMENT (PROTOCOL), POTENTIAL IMPROVEMENT (IMPLEMENTATION), and OPERATIONS AFFECTING

6.4.2. ***STP employs "bounce suppresser" on links (to avoid multiple link bounces).*** During oscillations tests (tests 1f and 1g), we attempted to insert three three-second link corruptions, separated by ten seconds. These oscillations were induced either on A-links (test 1f) or B/D-links (test 1g). One STP-pair was observed to have a "bounce suppresser" built in that would take the affected links out of service for a short time period (one minute) when one of the STPs observed a link failure for a second time within a short (but defined) period of time.

Network Implication: POTENTIAL IMPROVEMENT (PROTOCOL)

6.4.3. ***STP takes its links OOS after 30 seconds of congestion at the same level.*** During congestion tests (tests 2a through 2c), the scripts called for attempting to maintain congestion levels for several minutes. It was observed that one STP-pair had a built-in mechanism that would take the affected links out of service when it observed congestion remaining at the same level for thirty seconds.

Network Implication: POTENTIAL IMPROVEMENT (PROTOCOL)

6.4.4. ***Different degrees of cluster routing/management implementation observed.*** This item is intended as a note that not all STPs/networks were at the same degree of implementation of cluster routing and management. As such, it is possible for a carrier with more than one implementation to have differing reactions in different implementations. These reactions would be due to different degrees of cluster routing and management in place. Suppliers have announced their time schedules for full implementation.

Network Implication: POTENTIAL IMPROVEMENT (IMPLEMENTATION)

B

7. Date Final Analysis Due

As stated in the IITP documentation, the final analysis is due 10-13 weeks following completion of testing. Because testing ended on September 4, 1992, the preliminary report is due from November 13, 1992 to December 4, 1992. To accommodate meeting this schedule, comments to this report should be provided to affected carriers by November 6, 1992.

8. General Comments on Test Activity

Because of several problems found in the pre-test set-up, it was agreed that testing would be extended to a four week period (originally scheduled for a three week period). As such, the completion date of testing moved forward one week.

9. Acronyms and Abbreviations

ANSI	American National Standards Institute
APC	Affected Point Code
AT	Access Tandem
CBA	Changeback Acknowledgment
CBD	Changeback Declaration
COA	Changeover Acknowledgment
COO	Changeover Order
DPC	Destination Point Code
ECA	Emergency Changeover Acknowledgment
ECO	Emergency Changeover Order
EO	End Office
IITP	Internetwork Interoperability Test Plan Committee
IXC	Interexchange Carrier
LEC	Local Exchange Carrier

B

NOF	Network Operations Forum
OOS	Out Of Service
RCT	Route Congestion Test
RSP	Route Set Prohibited
RST	Route Set Test
RSx	Route Set-type messages
SCP	Signaling Control Point
SP	Signaling Point
SS7	Signaling System 7
STP	Signaling Transfer Point
TFA	Transfer Acknowledgment
TFC	Transfer Control
TFP	Transfer Prohibited
TFR	Transfer Restricted
TFx	Transfer-type messages

B

APPENDIX 13

B

Network Reliability Industry Initiatives

Focus Area: Signaling System

Topic	Industry Group	Doc. No. Issue No. Standards No.	Version No. and Date	Title	Brief Description
Network Reliability Performance Objectives	Bellcore	TR-NWT-000082	I4, 12/92	Signaling Transfer Point Generic Requirements	STP reliability requirements
	Bellcore	TR-NWT-000246	I2,R2, 12/92	SS7 Protocal Specification	Protocal enhancement for more robust CCS networks
	Bellcore	TR-NWT-000606	I2, 10/92	Common Channel Signaling	CCS reliability requirements for switching offices
	Bellcore	SR-NWT-000821	I3,12/90	Field Reliability Performance Study Handbook	Generic guidelines for conducting field performance studies
	Bellcore	TR-TSY-000929	I1,6/90	Reliability and Quality Measurements for Telecommunications Systems (RQMS)	Bellcore's view of generic requirements regarding supplier measurements
	Bellcore	TR-TSY-000929	I1,R1,5/92	Reliability & Quality Measurements for Telecommunications Systems (RQMS)	Bellcore's view of generic requirements regarding supplier measurements
	Bellcore	TR-TSY-000929	I1,S1, 3/91	Reliability & Quality Measurements for Telecommunications Systems (RQMS) RQMS Performance Report	Bellcore's view of generic requirements regarding supplier measurements

Network Reliability Industry Initiatives

Focus Area: Signaling System

Topic	Industry Group	Doc. No. Issue No. Standards No.	Version No. and Date	Title	Brief Description
Network Reliability Performance Objectives	Bellcore	TR-NWT-001245	I1, 6/92	CCS Node Requirements to Support Routing Verification Tests	Provides requirements for implementation of MTF and SCCP routing tests
	Bellcore	TR-NWT-001272	I1, 9/92	Gateway STP Local Message Screening Test Capability Generic Requirements	Provides requirements for testing the gateway screening tables in the gateway STPs
	Comm T1	T1.403	89	Carrier to Customer Installation, DS1 Metallic Interface Specification	
	Comm T1	T1.404	89	Customer Installation-to-Network	DS3 Metallic Interface Specification
	Comm T1	T1.408	90	ISDN Primary Rate	Customer Installation Metallic Interfaces, Layer 1 Specification
	Comm T1	T1.601	92	ISDN Basic Access Interface for Use on Metallic Loops for Application at the Network Side of NT, Layer 1 Specification	
	Comm T1	T1.605	91	ISDN Basic Assess Interface for S and T Reference Points - Layer 1 Specification	

Network Reliability Industry Initiatives

Focus Area: Signaling System

Topic	Industry Group	Doc. No. Issue No. Standards No.	Version No. and Date	Title	Brief Description
Network Reliability Performance Objectives	Comm T1	T1 Committee Technical Report #2	3/89	The Performance of AMI Signals Through B8ZS Optional Equipment Across Network Boundaries	
	ANSI	T1A1.2/93-015	2/93	Draft Proposed Technical Report on Network Survivability Performance, Project T1Q1/90-004R2	Survivability as a function of architecture
	ANSI	T1S1.3/92-11212R1	11/92	Report to the Signaling Network Systems (SNS) Committee on SS7 Network Architecture Evaluations and Protocol Enhancements	CCS architecture and protocal enhancements for CCS network robustness
	ANSI	T1S1.3/92-10203WD	10/92	Evaluation of various A-link Concentrator Interconnection Architectures	CCS interconnection arrangement for reliability
	ANSI	T1S1.3/92-10208WD	10/92	Evaluation of Logical STP Architectures	CCS architecture analyses for robustness
	ANSI	T1S1.3/93-02112	2/93	Signaling Network Systems Prioritization of Recent Protocal Enhancements	SNS initiated meeting and results for uniform industry deployment

Network Reliability Industry Initiatives

Focus Area: Signaling System

Topic	Industry Group	Doc. No. Issue No. Standards No.	Version No. and Date	Title	Brief Description
Network Reliability Performance Objectives	National Engineering Consortium	National Reliability and Survivability Conference	11/92	Talk on E-Links and Survivability	Talk on use of E-links to improve CCS Network reliability
	IEEE	Special Issue of JSAC	in 93	Performability Impacts of CCS Performance Objectives	Impacts of AIN on CCS performance
	Bellcore	WCF Talk	2/92	Bellcore Activities in Response to 1991 CCS Failure	CCS testing and protocal enhancement activities

Network Reliability Industry Initiatives

Focus Area: Signaling System

Topic	Industry Group	Doc. No. Issue No. Standards No.	Version No. and Date	Title	Brief Description
Network Architecture and Design	Bellcore	TR-NWT-000078	I3,12/91	Generic Physical Design Requirements for Telecommunications Products and Equipment	Bellcore's view of minimum generic physical design requirements for telecommunication products
	Bellcore	TR-NWT-000246	I2,R2, 12/92	SS7 Protocal Specification	Protocal enhancement for more robust CCS networks
	Bellcore	TR-NWT-000332	I4,9/92	Reliability Prediction Procedure for Electronic Equipment	Contains the recommended parts count, laboratory and field tracking methods for predicting and measuring hardware reliability
	Bellcore	TR-TSY-000357	I1,12/87	Generic Requirements for Assuring the Reliability of Components Used in Telecommunication Equipment	Defines practices for equipment suppliers to ensure satisfactory component reliability
	Bellcore	SR-TSY-000385	I1,6/86	Bell Communications Researchitecture Reliability Manual	A tutorial on reliability concepts and methods
	Bellcore	TR-NWT-000870	I1,2/91	Electrostatic Discharge Control in the Manufacture of Telecommunications Equipment and Component	Bellcore's minimum generic requirements for controlling electrostatic dischange during manufacture

Network Reliability Industry Initiatives

Focus Area: Signaling System

Topic	Industry Group	Doc. No. Issue No. Standards No.	Version No. and Date	Title	Brief Description
Network Architecture and Design	Bellcore	TR-TSV-000905	I1, 7/91	Common Channel Signaling (CCS) Network Interface Specifications Operations Guidelines (Section 8)	
	Bellcore	TR-NWT-000930	I1,12/90	Generic Requirements for Hybrid Microcircuits Used in Telecommunications Equipment	Bellcore's minimum generic physical design and reliability assurance requirements
	Bellcore	SR-TSY-001130	I1,5/89	Reliability and System Architecture Testing	Describes the Bellcore RSAT procedure on circuit switching systems
	Bellcore	SR-TSY-001171	I1,1/89	Methods and Procedures for System Reliability Analysis	Outlines the general methods and procedures Bellcore uses to predict hardware reliability
	Bellcore	SR-NWT-002419	I1,12/92	Software Architecture Review Checklists	Bellcore's view of SAR methodology and checklists
	Comm T1	T1.401	88	Interface Between Carrier and Customer Installations	Analog Voicegrade Switched Access Lines Using Loop-Start and Ground-Start Signaling
	Comm T1	T1.403	89	Carrier to Customer Installation, DS1 Metallic Interface Specification	
	Comm T1	T1.404	89	Customer Installation-to-Network	DS3 Metallic Interface Specification

Network Reliability Industry Initiatives

Focus Area: Signaling System

Topic	Industry Group	Doc. No. Issue No. Standards No.	Version No. and Date	Title	Brief Description
Network Architecture and Design	Comm T1	T1.405	89	Interface Between Carriers and Customer Installations	Analog Voicegrade Switched Access Using Loop Reverse Battery Signaling
	Comm T1	T1.407	90	Interface Between Carriers and Customer Installations	Analog Voicegrade Special Access Line Using Customer Installation Provided Loop-Start Supervision
	Comm T1	T1.408	90	ISDN Primary Rate	Customer Installation Metallic Interface, Layer 1 Specification
	Comm T1	T1.409	91	Interface Between Carriers and Customer Installations	Analog Voicegrade Special Access Using E&M Signaling
	Comm T1	T1.410	92	Carrier to Customer Metallic Interface	Digital Data at 64kbit/s and Subrates
	Comm T1	T1.601	92	ISDN Basic Access Interface for Use on Metallic Loops for Application at the Network Side of NT, Layer 1 Specification	
	Comm T1	T1.605	91	ISDN Basic Access Interface for S and T Reference Points, Layer 1 Specification	
	Comm T1	Technical Report #2	3/89	The Performance of AMI Signals Through B8ZS Optional Equipment Across Network Boundaries	

Network Reliability Industry Initiatives

Focus Area: Signaling System

Topic	Industry Group	Doc. No. Issue No. Standards No.	Version No. and Date	Title	Brief Description
Network Architecture and Design	ANSI	T1A1.2/93-015	2/93	Draft Proposed Technical Report on Network Survivability Performance, Project T1Q1/90-004R2	A study of survivability for different network architectures
	ANSI	T1S1.3/92-10208WD	10/92	Evaluation of Logical STP Architectures	CCS architecture analyses for robustness
	ANSI	T1S1.3/92-11212R1	11/92	Report to the Signaling Network Systems (SNS) Committee on SS7 Network Architecture Evaluations and Protocol Enhancements	
	ANSI	T1S1			Congestion in SS7 networks
	CCITT	Study Group II			Survivable architectures
	CCITT	Study Group XVIII			Survivable architectures

Network Reliability Industry Initiatives

Focus Area: Signaling System

Topic	Industry Group	Doc. No. Issue No. Standards No.	Version No. and Date	Title	Brief Description
Network Interconnection and Interoperability	Bellcore	TR-NWT-000246	I2,R2, 12/92	SS7 Protocal Specification	Protocal enhancement for more robust CCS networks
	Bellcore	TR-EOP-000352	I1, 5/86	Cellular Mobile Carrier Interconnection Transmission Plans	
	Bellcore	TR-NWT-000690	I1, 3/91	IC/INC Interconnection FSD 20-24-0000 SPCS InterLATA Carriers/International Carriers	
	Bellcore	TR-TSV-000905	I1, 7/91	Common Channel Signaling (CCS) Network Interface Specifications Operations Guidelines (Section 8)	
	Bellcore	SR-NWT-001944	I1, 1/92	Common Channel Signaling Interoperability Analysis Program	
	Bellcore	SR-NWT-002371	I1, 7/92	Signaling Transfer Point (STP) Technical Audit and Interoperability Analysis	

B

Network Reliability Industry Initiatives

Focus Area: Signaling System

Topic	Industry Group	Doc. No. Issue No. Standards No.	Version No. and Date	Title	Brief Description
Network Interconnection and Interoperability	Comm T1	T1.401	88	Interface Between Carrier and Customer Installations	Analog Voicegrade Switched Access Lines Using Loop-Start and Ground-Start Signaling
	Comm T1	T1.403	89	Carrier to Customer Installation, DS1 Metallic Interface Specification	
	Comm T1	T1.404	89	Customer Installation-to-Network	DS3 Metallic Interface Specification
	Comm T1	T1.405	89	Interface Between Carriers and Customer Installations	Analog Voicegrade Switched Access Using Loop Reverse Battery Signaling
	Comm T1	T1.407	90	Interface Between Carriers and Customer Installations	Analog Voicegrade Special Access Line Using Customer Installation Provided Loop-Start Supervision
	Comm T1	T1.408	90	ISDN Primary Rate	Customer Installation Metallic Interfaces, Layer 1 Specification
	Comm T1	T1.409	91	Interface Between Carriers and Customer Installations	Analog Voicegrade Special Access Using E&M Signaling

Network Reliability Industry Initiatives

Focus Area: Signaling System

Topic	Industry Group	Doc. No. Issue No. Standards No.	Version No. and Date	Title	Brief Description
Network Interconnection and Interoperability	Comm T1	T1.410	92	Carrier to Customer Metallic Interface	Digital Data at 64 kbit/s and Subrate
	Comm T1	T1.601	92	ISDN Basic Access Interface for Use on Metallic Loops for Application at the Network Side of NT, Layer 1 Specification	
	Comm T1	T1.605	91	ISDN Basic Access Interface for S and T Reference Points, Layer 1 Specification	
	Comm T1	T1 Committee Technical Report #2	3/89	The Performance of AMI Signals Through B8ZS Optional Equipment Across Network Boundaries	
	Comm T1	T1 Committee Technical Report #5	6/90	Carrier to Customer Installation Interface Connector Wiring Configuration Catalog	
	Industry Conference	Telephony and Bellcore	5/92	The SS7 Summit	Interconnection and regulatory matters discussed

Network Reliability Industry Initiatives

Focus Area: Signaling System

Topic	Industry Group	Doc. No. Issue No. Standards No.	Version No. and Date	Title	Brief Description
Network Management	Bellcore	TR-NWT-001306	I1, 12/92	CCS Network Maintenance Generic Requirements: Manual Controls to Force a Signaling Link Out-Of-Service	Provides requirements for forcing a link out of service
	Bellcore	TR-NWT-001321	I1, 12/92	Generic Requirements for Priority Processing of Surveillance Messages at CCS Nodes Under Overload	Provides requirements for messaging during overload conditions
	Comm T1	T1.403	89	Carrier to Customer Installation, DS1 Metallic Interface Specification	
	Comm T1	T1.404	89	Customer Installation-to-Network	DS3 Metallic Interface Specification
	Comm T1	T1.408	90	ISDN Primary Rate	Customer Installation Metallic Interfaces, Layer 1 Specification
	Comm T1	T1 Committee Technical Report #2	3/89	The Performance of AMI Signals Through B8ZS Optional Equipment Across Network Boundaries	

Network Reliability Industry Initiatives

Focus Area: Signaling System

Topic	Industry Group	Doc. No. Issue No. Standards No.	Version No. and Date	Title	Brief Description
Operations, Administration, Maintenance	Bellcore	TR-TSY-000815	I1, 11/89	Network Element (NE) Memory Administration - NE Operations Security	
	Bellcore	SR-NWT-000821	I3,12/90	Field Reliability Performance Study Handbook	Generic guidelines for conducting field performance studies
	Bellcore	TR-NWT-000835	I3, 1/93	Operations Technology Generic Requirements (OTGR): Network Element and Network Security Administration Messages	
	Bellcore	TR-TSY-000929	I1,6/90	Reliability and Quality Measurements for Telecommunications Systems (RQMS)	Bellcore's view of generic requirements regarding supplier measurements
	Bellcore	TR-TSY-000929	I1,R1,5/92	Reliability & Quality Measurements for Telecommunications Systems (RQMS)	Bellcore's view of generic requirements regarding supplier measurements
	Bellcore	TR-TSY-000929	I1,S1, 3/91	Reliability & Quality Measurements for Telecommunications Systems (RQMS) RQMS Performance Report	Bellcore's view of generic requirements regarding supplier measurements

Network Reliability Industry Initiatives

Focus Area: Signaling System

Topic	Industry Group	Doc. No. Issue No. Standards No.	Version No. and Date	Title	Brief Description
Restoration and Recovery	Bellcore	TR-NWT-001306	I1, 12/92	CCS Network Maintenance Generic Requirements: Manual Controls to Force a Signaling Link Out-Of-Service	Provides requirements for forcing a link out of service
	Bellcore	TR-NWT-001321	I1, 12/92	Generic Requirements for Priority Processing of Surveillance Messages at CCS Nodes Under Overload	Provides requirements for messaging during overload conditions
	Comm T1	T1.403	89	Carrier to Customer Installation, DS1 Metallic Interfaces Specification	
	Comm T1	T1.404	89	Customer Installation-to-Network	DS3 Metallic Interface Specification
	Comm T1	T1.408	90	ISDN Primary Rate	Customer Installation Metallic Interfaces, Layer 1 Specification
	Comm T1	T1.601	92	ISDN Basic Access Interface for Use on Metallic Loops for Application at the Network side of NT, Layer 1 Specification	
	Comm T1	T1.605	91	ISDN Basic Access Interface for S and T Reference Points-Layer 1 Specification	
	ANSI	T1S1			Congestion in SS7 networks
	CCITT	Study Group IV			Restoration studies

Network Reliability Industry Initiatives

Focus Area: Signaling System

Topic	Industry Group	Doc. No. Issue No. Standards No.	Version No. and Date	Title	Brief Description
Operations, Administration, Maintenance	Comm T1	T1.601	92	ISDN Basic Access Interface for Use on Metallic Loops for Application at the Network Side of NT, Layer 1 Specification	
	Comm T1	T1.605	91	ISDN Basic Access Interface for S and T Reference Points-Layer 1 Specification	
	Comm T1	T1 Committee Technical Report #2	3/89	The Performance of AMI Signals Through B8ZS Optional Equipment Across Network Boundaries	

Network Reliability Industry Initiatives

Focus Area: Signaling System

Topic	Industry Group	Doc. No. Issue No. Standards No.	Version No. and Date	Title	Brief Description
Operations, Administration, Maintenance	Bellcore	SR-TSY-000963	I1,4/89	Network Switching Element Outage Performance Monitoring Procedures	Procedures to monitor the performance of a telecommunication network
	Bellcore	TR-NWT-001306	I1, 12/92	CCS Network Maintenance Requirements: Manual Controls to Force a Signaling Link Out-Of-Service	
	Bellcore	TR-NWT-001316	I1, 12/92	Generic Requirements for Improved CCS Trouble Reporting	Provides requirements for detection and reporing of additional failure modes
	Comm T1	T1.403	89	Carrier to Customer Installation, DS1 Metallic Interface Specification	
	Comm T1	T1.404	89	Customer Installation-to-Network	DS3 Metallic Interface Specification
	Comm T1	T1.405	89	Interface Between Carriers and Customer Installations	Analog Voicegrade Switched Access Using Loop Reverse Battery Signaling
	Comm T1	T1.408	90	ISDN Primary Rate	Customer Installation Metallic Interfaces, Layer 1 Specification
	Comm T1	T1.410	92	Carrier to Customer Metallic Interface	Digital Data at 64 kbit/s and Subrates

Network Reliability Industry Initiatives

Focus Area: Signaling System

Topic	Industry Group	Doc. No. Issue No. Standards No.	Version No. and Date	Title	Brief Description
Human Factors Design	Bellcore	TR-TSY-000439		OTGR User System Interface. Section 10.1	
	Comm T1	T1 Committee Technical Report #5	6/90	Carrier to Customer Installation Interface Connector Wiring Configuration Catalog	

Network Reliability Industry Initiatives

Focus Area: Signaling System

Topic	Industry Group	Doc. No. Issue No. Standards No.	Version No. and Date	Title	Brief Description
Survivability Analysis Models and Tools	Bellcore	SR-TSY-001130	I1,5/89	Reliability and System Architecture Testing	
	Bellcore	SR-TSY-001171	I1,1/89	Methods and Procedures for System Reliability Analysis	
	Bellcore	SR-TSY-001547	I1, 1/90	The Analysis & Use of Software Reliability & Quality Data	
	Bellcore	SR-NWT-002419	I1,12/92	Software Architecture Review Checklists	Bellcore's view of SAR methodology and checklists
	RAM	Proceedings of the Annual Reliability and Maintainability Symposium	pp. 320-327, 83	Hardware/Software FMECA	
	RAM	Proceedings of the Annual Reliability and Maintainability Symposium	pp. 274-279, 92	Assuring Software Safety	

Network Reliability Industry Initiatives

Focus Area: Signaling System

Topic	Industry Group	Doc. No. Issue No. Standards No.	Version No. and Date	Title	Brief Description
Network Security	Bellcore	TR-TSY-000815	I1, 11/89	Network Element (NE) Memory Administration - NE Operations Security	
	Bellcore	TR-NWT-000835	I3, 1/93	Operations Technology Generic Requirements (OTGR): Network Element and Network Security Administration Messages	
	Comm T1	T1.401	88	Interface Between Carriers and Customer Installations	Analog Voicegrade Switched Access Lines Using Loop-Start and Ground-Start Signaling
	Comm T1	T1.407	90	Interface Between Carriers and Customer Installations	Analog Voicegrade Special Access Lines Using Customer Installation Provided Loop-Start Supervision
	Comm T1	T1.409	91	Interface Between Carriers and Customer Installations	Analog Voicegrade Special Access Lines Using E&M Signaling

Network Reliability Industry Initiatives

Focus Area: Signaling System

Topic	Industry Group	Doc. No. Issue No. Standards No.	Version No. and Date	Title	Brief Description
Regulations	Congress	H.R. 4789	4/92	Telephone Network Reliability Improvement Act of 1992	This bill would have required the FCC to establish and enforce network reliability standards (failed to pass in 92)
	Congress	S.237	1/93	National Network Security Board Act of 1993	Bill to create NS board to investigate and make recommendations regarding network security and reliability
	Congress	S.238	1/93	Telecommunications Network Security and Reporting Act of 1993	Bill to require FCC to report to Congress network security and reliability matters
	Industry Conference	Telephony and Bellcore	5/92	The SS7 Summit	Interconnection and regulatory matters discussed

APPENDIX 14

B

CCS Internetwork Test Assessment

1. Executive Summary

In February 1992, a one-year trial of Common Channel Signaling (CCS) internetwork interoperability testing was initiated by the Network Operations Forum (NOF). That one-year trial is now completing and this paper details an assessment of the accomplishments of the trial and suggestions for moving forward. Specific technical findings from the testing are documented separately from this memo. We intend to assess the CCS Internetwork Testing program annually as the program improves and moves forward.

The key areas of success during the first year of the program are based on (1) the test participants taking advantage of the opportunity to test in a laboratory-based internetwork environment and (2) volunteering to report test results to the entire industry in an expeditious manner. The successes include:

- **A new high level of cooperation was established between suppliers and carriers** - Suppliers and carriers worked cooperatively to collect and analyze data and report on results.
- **Development of a voluntary, distributed national CCS laboratory** - In carrying out each of the first several series of tests, the Internetwork Interoperability Test Plan (IITP) members volunteered their laboratories and effectively created a distributed national laboratory by the resulting interconnection of major CCS carriers and suppliers. If these interconnections could continue, those volunteering their facilities will have made a major step could toward resolving varied CCS interconnection issues or problems as they might arise in live networks.
- **Industry-generated test scripts targeting CCS network integrity** - The industry has voluntarily worked together in generating test scripts related to network interconnection, but this is the first time that the industry worked together to develop scripts that were used specifically to identify potential internetwork weaknesses.
- **Cooperative test execution** - With one company (Bellcore) playing the central role as Hub provider and testing coordinator, the tests themselves have been run cooperatively, successfully and speedily.
- **Cooperative problem resolution** - As the analysis uncovered problems with various equipment included in the testing, the affected carriers took responsibility for working with their affected supplier(s) to have the issues resolved. This resolution included supplier/carrier confirmation of the problem and sharing it and its resolution by the affected supplier(s) with their affected customer base.

B

- **Test results sharing** - The NOF's SS7 Workshop saw a need for and then created a process for the appropriate sharing of test results in a timely manner across the entire industry while protecting supplier-specific or carrier-specific proprietary information.
- **Cooperative venue for CCS test needs** - One side benefit to this effort is the opportunity these meetings provide for off-line discussions of testing approaches and testing needs across companies among technical experts who might not otherwise have the opportunity to share information.

In assessing the process, we observe that the CCS internetwork program is meeting *the intent* of the original objectives. Another important objective not in the original proposal, that is, to **Create and utilize an industry-wide mechanism for (1) lab-oriented, network integrity testing and (2) information sharing** was met. In our view, the objectives set forth above have been largely but not completely met. The areas of improvement detailed in this assessment are an attempt to more fully and cost-effectively meet the original objectives.

Areas for enhancing the testing process and improving the analysis and reporting processes, including expanding the focus of testing and reporting beyond basic network integrity tests accomplished through the IITP are discussed in this report and many are underway. For example, the IITP recently developed operating principles that include enhancing the IITP's capabilities to perform additional reporting functions on behalf of the industry.

The IITP has shown that the industry can work extremely well together and can, in a short time span, propose and agree on tests, execute those tests, and analyze results. The IITP's frequent meetings to resolve these technical issues have resulted in extensive gains to the entire industry and should be continued and enhanced to further improve productivity and value.

2. Background

On October 4, 1991, in response to concerns regarding network reliability (arising from recent CCS outages), Bellcore proposed additional CCS internetwork testing beyond that underway at the time. The proposal was forwarded to carriers, suppliers, end users and others involved in Common Channel Signaling (CCS) using the Signaling System 7 (SS7) protocol. This proposal was generated from a request made to Bellcore during a special meeting on network reliability called by the Federal Communications Commission (FCC) on September 12, 1991. The proposal detailed objectives for any such internetwork testing program and suggested options for implementations, including testing in live networks, interconnecting existing lab facilities, and building some new lab facilities expressly for this testing. The proposal also noted that

B

> *Input from all sectors of the industry is needed to formulate and agree to the specific tests, configurations, and conditions as they relate to internetwork, intra-network, product-to-product, and stand-alone equipment modeling and testing.*

In response to the proposal, the industry agree to the need for additional CCS internetwork testing without collectively agreeing on specific implementations, tests, or configurations. The industry's comments also led to the following conclusions:

- *The most feasible near-term approach for internetwork testing is to coordinate use of existing supplier and carrier labs*
- *Industry consensus is needed to address standardization, scheduling, coordination and reporting of internetwork testing*[2]

Bellcore recommended that a one-year trial be established for implementing industry-wide internetwork testing. The industry's comments directed the implementation to the Network Operations Forum (NOF), and in January 1992 the NOF's SS7 Workshop chartered the Internetwork Interoperability Test Plan (IITP) committee to develop specific tests, configurations, and conditions relative to internetwork testing.[1] Participation in the IITP is strictly voluntary.

The IITP has met frequently since its inception, with representatives from all major carriers, several smaller carriers, network equipment suppliers, test equipment suppliers, Bellcore, and government agencies in attendance. The IITP, under its SS7 Workshop parent, has focused itself on developing test scripts and configurations for lab-oriented testing targeting CCS network integrity. It identified a configuration for testing that was felt to provide the best opportunity to verify the robustness of the interconnected CCS networks. The testing thus far has been extensive. Each phase of testing has been designed to stretch the limits of network integrity and has involved an intensive multi-week effort of interconnected laboratories. These tests have identified several critical situations that could impact service or operations and all of these have been addressed rapidly by affected carriers and suppliers. The test results are also being used to enhance other tests done in stand-alone and other less-complicated configurations. The IITP is now using the knowledge gained in 1992 testing to create new and revise existing tests to be more comprehensive and to provide additional network integrity assurance.

---

1. Needs for intra-network, product-to-product, and stand-alone equipment modeling and testing were viewed as outside the charter of this group and are not being addressed by the industry as a whole.

B

3. IITP Accomplishments

The IITP's accomplishments to date directly correlate to there being a cooperative mindset at IITP meetings. The IITP itself is a demonstration of how the various entities in the industry (exchange carriers, interexchange carriers, network equipment suppliers, and test equipment suppliers) can work cooperatively toward the common goal of helping to improve network integrity.

The IITP's continuing success is predicated on the quality of its work and its ability to provide a level playing field for all participants. The initial premise for the group was that while any entity desiring to participate would volunteer and pay its own way, the results would be available to all. For the first year, the cost for Bellcore's involvement has been borne fully by its owners.

IITP accomplishments include physical accomplishments (e.g., tests performed and test scripts and analysis results generated and distributed) and the cooperative technical exchange of information between interconnected entities. The principal early accomplishments of the IITP are related to the development of a methodology for the industry as a whole to discuss and agree on what tests have the potential for providing the most technical insight, and then agreement on how those tests should be performed and the results shared. As a result of these agreements, the IITP provided the medium for cooperative testing in an off-line environment between several carriers and suppliers that provided insight into unexpected service affecting conditions. This information was expeditiously shared across the industry. Suppliers took direct action by notifying their customers of issues and timeframes for resolution.

Since it first met, the IITP (1) developed a test plan targeting network integrity together with a generic test configuration, (2) cooperatively implemented the test plan three times ("Phases 0, 1A, and 1B"), and (3) developed Information Sharing Guidelines,[2] and (4) a process for sharing test results quickly across the industry. This information sharing process includes notifying carriers of potential service or operations affecting conditions and proposed or implementable resolutions. Testing has been accomplished using a configuration that included a local exchange carrier interconnected to an interexchange carrier connected to another local exchange carrier. Each time, suppliers supplemented the carrier labs by providing their labs to supplement the carrier labs. The industry-generated scripts were implemented in August 1992 by interconnecting six supplier and carrier labs for testing ("Phase 0") using Bellcore's Hub for interconnection and data monitoring and collection. This set of tests with the same generic configuration but different carriers and labs has been executed twice more, in October ("Phase 1A")

2. This was accomplished together with the NOF's SS7 Workshop.

B

and November ("Phase 1B").[3] Again, participants interconnected via Bellcore's Hub. For this first year, industry participation in the IITP has been purely voluntary with interconnection fees being paid for by those who choose to participate.

The Phase 0 tests were completed over an intensive four-week test period. After the testing, the participants worked together to analyze cooperatively the data collected during the testing, share those results across the industry in a timely manner, and issue a report detailing the observed anomalies and their resolutions. In order to facilitate rapid sharing of test results, the IITP and SS7 Workshop set an ambitious reporting schedule, and the test participants completed their work nearly two weeks ahead of that schedule. The Phase 1 tests were completed over a seven-week test period and, just as in Phase 0, the the cooperative analysis process resulted in the timely release of test reports.

Bellcore served as a catalyst for all of this testing. This process began with the proposal originated by Bellcore and shared with the industry. The proposal, together with the industry's comments, led directly toward the IITP's development and the industry's developed test cases and test plans. The industry agreed to use Bellcore's Hub for laboratory interconnections and link monitoring. As central test facilitator, Bellcore coordinating the analysis and reporting effort.

The one-year trial period is complete and the IITP participants have completed three sets of tests thus far. Reports of all three test sets are complete. The results have been shared across the industry promptly and have been used to improve future tests, improve implementations, and simplify operations. A process is also in place for feedback to those organizations developing industry Standards or requirements if improvements are found to be needed there.

4. Assessment

Based on informal feedback provided to NOF and IITP participants from the industry, the IITP effort has been viewed as successful. The IITP has offered the industry an opportunity for helping to assure and improve internetwork integrity in a way not available before. However, any assessment of the CCS Internetwork Test Plan needs to be viewed relative to the areas of success for the testing as a whole as well as a comparison of the process in place to the objectives originally proposed by Bellcore and agreed to in the industry.

3. Scripts used for Phases 1A and 1B included updates based on attempts to execute the tests in Phase 0.

B

4.1 Areas of IITP Success

The basic successes of this CCS Internetwork Testing effort stem from the cooperative approaches by IITP attendees and test participants. Specifically, areas that this test effort have included are

- **A level playing field** - The IITP committee began with the unusual approach of being chaired by *three* industry representatives reflecting three different industry groups. Traditionally, such NOF-based groups have chairs from only the carrier community (one local exchange carrier and one interexchange carrier) but considering the necessities of this effort, we began with an additional chair from the supplier community. The IITP holds that all three groups have a stake in this effort and throughout 1992, all three groups participated and showed dedication to the effort. For example, the IITP chairs include an interexchange carrier (AT&T-Communications), a local exchange carrier (GTE), and a supplier (Northern Telecom in 1992 and DSC Communications Corporation in 1993).

- **A new high level of cooperation was set between suppliers and carriers** - Suppliers and carriers worked cooperatively to collect and analyze data and report on results.

- **Development of a voluntary, distributed national CCS laboratory** - In carrying out each of the first several series of tests, the Internetwork Interoperability Test Plan (IITP) members volunteered their laboratories and effectively created a distributed national laboratory by the resulting interconnection of major CCS carriers and suppliers. If these interconnections could continue, those volunteering their facilities will have made a major step could toward resolving varied CCS interconnection issues or problems as they might arise in live networks.

- **Industry-generated test scripts targeting CCS network integrity** - The industry has voluntarily worked together in generating test scripts related to network interconnection, but this is the first time that the industry has worked together to develop scripts that were used specifically to identify potential internetwork weaknesses. The IITP test scripts, which were cooperatively developed, are based on real-life scenarios that may or may not have been CCS related, but have been applied to CCS. For example, the tests simulate faults like cable cuts and how they might affect a CCS network. In addition, the industry has made these scripts available publicly with the hope that they would be used on a regular basis.

  The process for developing test scripts began with suggestions from IITP participants. The participants then developed a document that included both execution plans and expected results. These publicly-available scripts (used for Phases 0, 1A, and 1B) include expected messaging, and deviations from expected messaging can easily be found when analyzing test results.

B

Knowledge of these deviations is vital toward maintenance of SS7 networks.

- **Cooperative test execution** - With one company (Bellcore) serving the central role as Hub provider and testing coordinator, the tests have been run cooperatively, successfully, and speedily. Our experience has shown that once testing begins, the technical interests and attention of the participants moves the process along smoothly and effectively. In Phase 0, for example, four intensive weeks of testing led to the discovery of several scenarios with potential for lost calls. Those scenarios have been addressed by suppliers and carriers, with affected carriers quickly notified.
- **Cooperative problem resolution** - As the analysis uncovered problems with various equipment included in the testing, the affected carriers took responsibility for working with their supplier(s) to have the issues resolved. This resolution included confirmation of the problem and sharing of the problem and its resolution by those supplier(s) with their affected customer base.
- **Test results sharing** - The SS7 Workshop saw a need for a process for sharing test results in a timely manner across the entire industry while protecting supplier-specific or carrier-specific proprietary information. They then defined a process, documented in the SS7 Workshop's "Information Sharing Guidelines" that was successfully implemented in IITP testing and served as the basis for rapid sharing of test results.
- **Cooperative venue for CCS test needs** - One side benefit to this effort is the opportunity these meetings provide for off-line discussions of testing approaches and testing needs. These off-line discussions have helped companies gain insight into how others in the industry have improved their own processes.

4.2 Original Program Objectives and Their Current Level of Compliance

This section discusses (1) the five objectives that the industry agreed were necessary for a CCS internetwork testing program and (2) how well this program, implemented through the IITP, complies with each of the objectives. The IITP process is succeeding in addressing the intent of the original objectives, but it is important to recognize that the objectives themselves were not fully met by the implemented program.

In reviewing the results of this year's effort, we recognized that a major IITP accomplishment was that it met the implicit, though unstated, objective of

Objective 6: Create and utilize an industry-wide mechanism for (1) lab-oriented, network integrity testing and (2) information sharing

B

Early on, the IITP recognized that meeting this objective was critical to the program's success. The IITP implementation fills the void in the industry for a means by which network integrity concerns can be tested in a realistic, multi-supplier, off-line environment, and then eliminated before live implementation, and by which results can be shared rapidly across the industry. The IITP recognizes that it would be beneficial to enhance the testing by including additional scenarios, including different tests and different traffic loading conditions.

The proposed objectives for the CCS Internetwork Testing program were:

Objective 1: **Facilitate identification and sharing of CCS network vulnerabilities with industry participants and stimulate Supplier and Carrier implementation of corrective actions before product deployment**

Objective 2: **Provide Carriers and Service Providers with confidence in the robustness of new software prior to network integration**

Objective 3: **Develop a library of possible faults and the appropriate responses**

Objective 4: **Provide a framework for performing post mortem analyses on event data**

Objective 5: **Provide a unique environment to enable suppliers to demonstrate product reliability and interoperability in a multi-supplier environment**[3]

In our view, the objectives set forth above have been largely but not completely met. For example, the IITP has a mechanism in place for sharing results from cooperative testing, however, there is no arrangement in place for testing all products in an internetwork environment before their deployment. In the first phases of testing, there were some isolated cases of pre-released generics being included in the test beds but, in general, most product in the test beds had been previously deployed.[4] We observed that software robustness was tested, but only to the extent of the network integrity scripts developed by the IITP in an internetwork environment (the scripts for Phases 0, 1A, and 1B did not target software robustness directly).

The IITP has developed a library of faults and responses by the nature of its test scripts. The scripts form the basis of a library that are available to the entire industry. Those scripts (1) provide ways to induce faults and then (2) detailed

4. The limited amount of lab equipment being made available for IITP precluded testing being limited to ONLY pre-released equipment.

B

expected messaging and offer a recovery strategy. The induced faults are based on real life observations of potential faults that could apply to CCS and the scripts are written such that they could be reused in other testing. The library's utility could grow by further examining the network's ability to self-correct when faults are induced and examining the effects of options available to network operators to manually recover. It would be of great benefit to have the library address each of these areas:

1. notification - through surveillance, alarms, and other means, the network operators needs to be made aware of a potentially negative condition occurring in the network. This has been addressed as conformance of events to predicted conditions.
2. containment - the ability of the network to "contain" or minimize the fault, and in so doing to isolate it, and/or the affected elements of the network, away from the whole or "well" parts of the network.
3. diagnostic ability - the ability of the network to "heal itself" in such a way so as to notify the network operator via maintenance channels or other means what has to be done to correct the fault. At a minimum, the protocol exchange should be used as a guide for this notification.
4. reconfiguration - the ability of the network to realize that a problem exists, and to reconfigure itself around the fault, including the ability to recover or return to the normal configuration after the fault has been "healed."

It is expected that tests developed and executed in 1993 will better account for the aspects detailed above.

Because major internetwork outages have not occurred in 1992, it is difficult to say conclusively that we have in place a facility to perform post mortem analysis on live network failures, not just on the scenarios and equipment under test. To meet the objective, it would be necessary, at a minimum, for lab interconnections to remain in existence after testing completes.

5. Suggestions for Moving Forward

This CCS Internetwork testing effort has been successful and its current efforts should be enhanced. For example, additional testing could account for additional and varied traffic loads. Testing could focus on recent changes to Standards and requirements, additional network integrity-affecting scenarios (such as congestion) and/or application integrity. To achieve this, it is necessary to improve the cost-effectiveness of the effort as well as to address areas not fully covered because of the nature of this testing. These areas are discussed below. Many of these suggestions have been discussed within the IITP committee and have

B

already been implemented.

5.1 IITP Participation

The cost of IITP participation is substantial, in terms of equipment, transport facilities, and human resources. While industry-wide participation in the IITP planning meetings was fairly good, a number of participants were less than enthusiastic about investing personnel, equipment, or other resources in the actual testing. This inequity needs to be addressed as the process moves forward. IITP will not succeed in the long run if some companies are asked to bear an unfair portion of the costs. Participants who cannot offer lab facilities could volunteer to contribute in some other way (e.g., purchase some of the transport facilities or provide testing personnel).[5] One alternative is to develop a mechanism for making payments that would be disbursed to more active participants.

To facilitate future testing, interconnection testing costs should continue to be borne by individual participants, although some participants have expressed desires to more equitably share those costs. The costs of the central testing facilitator, however, will most likely exceed the costs for any individual participant and should be shared more equitably. For example, for Phases 0, 1A, and 1B, the central tester provided facilities for interconnection, facilitated all discussions (including arranging for conference calls), prepared test scripts, provided staffing to execute tests, and provided resources for analyzing and reporting on results. Considerable discussion continues throughout the industry as to whether (and how) these costs can be more equitably shared.

5.2 Testing Foci

The most cost effective approach to IITP testing would be periodic "large" tests (similar to how the early IITP tests were accomplished) and further encouragement to utilize the test results obtained by participants in non-IITP bi-lateral and other types of tests. The IITP tests result in both debugged scripts and findings. Both should be subsequently used to improve IITP tests and other stand-alone or bi-lateral tests. Results from these tests should be fed back into the IITP process.

Initial IITP testing focused on CCS network integrity. This focus should continue and subsequent testing needs to account for varied traffic loads. Additional tests

5. An example of where this occurred in Phase 1 was where NYNEX provided facilities that were supported during testing by U S WEST.

B

should focus on changes to Standards and requirements, additional network integrity-affecting scenarios (such as congestion), and the inclusion of applications. The IITP group is well positioned to identify the priority of these tests/conditions (and others) as well as configurations for future testing. In addition, there remains a need to address fully intra-network, product-to-product, and stand-alone equipment modeling and testing by the industry as a whole.

5.3 Fuller Empowerment of the IITP

While the time from test planning through implementation and results reporting was fairly rapid, the IITP often found itself hindered because it could identify issues but the SS7 Workshop retained control of resolving these issues. The IITP's charter precluded them from addressing major issues relating to testing. As such, the IITP could *identify but not solve* such issues. We estimate that this may have contributed to delays of two or three months.

This concern has been alleviated by the new Mission Statement and Operating Principles agreed to by the IITP and the SS7 Workshop. In those Principles, the IITP has additional latitude to take charge of testing more fully than before.

5.4 Address the Need for an Industry Focal Point for the Test Efforts

Many participants noted the vital role of having one company provide the Hub and be central test facilitator. Although Bellcore did not have an "official" standing in the NOF or the IITP, it did voluntarily take the lead (as Hub provider) to insure that the testing and analysis progressed. It is unlikely that the testing would have been as successful had one company not performed this role. The responsibilities assumed by Bellcore include test script editing, test facility interconnection, data collection and analysis, reporting of results, and administrative support of the IITP and NOF. The industry needs to address this role and these responsibilities for future testing. Bellcore's recommendation is for the IITP to identify "a central testing facilitator" that would be viewed by test participants as unbiased and would take on the responsibilities that Bellcore assumed for early testing.

5.5 Additional Activities

The IITP has shown the usefulness of expeditiously sharing test results across the industry. Those test results are being used by the industry to improve future testing and improve other stand-alone and bi-lateral tests. They may also be used for demonstrating deficiencies in Standards or requirements.[9] The sharing of test

B

results could be expanded in several ways. While IITP test results are shared, methods for improving that process and speeding up distribution of results should be implemented. Also, until the recent changes to the IITP's Operating Principles, there was no industry-wide medium for sharing results from other (non-IITP) tests such as bi-lateral carrier testing. Because the IITP membership is primarily testers and analysts, it would appear that the IITP is best positioned to serve this purpose, and we recommend that the IITP's charter be revised to accommodate this function.

One of the original objectives agreed to across the industry was to *Provide a framework for performing post mortem analyses on event data*. The IITP testing essentially formed the basis for a distributed laboratory that could be used to provide a framework for performing post mortem analysis on events data if such a situation is needed. This distributed facility is only available as long as the leased line connections used for IITP and other testing remain available to serve this purpose. We have already seen the utility of maintaining these connections in order to achieve retests from Phase 0, and this concept could readily be extended to other purposes, including performing post mortem analyses.

5.6 Concluding Remarks

The IITP committee has taken several steps toward meeting the suggestions detailed here by (1) drafting a revised mission statement consistent with the suggestions in this paper, (2) drafting operating principles that also are consistent with the suggestions in this paper, and (3) developing tests that focus on both the message transfer part and the application layers of the protocol. Additional effort is needed to continue the testing begun in 1992 and to enhance the IITP by addressing the other suggestions in this paper.

6. For example, the IITP representatives have frequently noted their interactions with their company representatives to Standards or requirements development to assure that the tests and results can be used to identify how the implementations compare with the intent of the Standards or requirements.

B

REFERENCES

1. Proposal from Irwin Dorros, Bellcore, to all Participants at September 12, 1991 FCC meeting on Network Reliability, October 4, 1991.
2. Letter from Irwin Dorros to Richard Firestone, FCC Common Carrier Bureau, November 12, 1991.
3. *CCS Internetwork Test Proposal*, Bellcore, October 4, 1991.

B