ATIS-0100002

RELIABILITY ASPECTS OF NEXT GENERATION NETWORKS

TECHNICAL REPORT

The Alliance for Telecommunication Industry Solutions (ATIS) is a technical planning and standards development organization that is committed to rapidly developing and promoting technical and operations standards for the communications and related information technologies industry worldwide using a pragmatic, flexible and open approach. Over 1,100 participants from over 300 communications companies are active in ATIS' 22 industry committees and its Incubator Solutions Program.

< http://www.atis.org/ >

ATIS-0100002, *Reliability Aspects of Next Generation Networks*

Is an ATIS Standard developed by the **Reliability (REL)** Subcommittee under the **ATIS Network Performance, Reliability, and Quality of Service Committee (PRQC)**.

Published by

Alliance for Telecommunications Industry Solutions
1200 G Street, NW, Suite 500
Washington, DC 20005

ATIS-0100002

Technical Report on

RELIABILITY ASPECTS OF NEXT GENERATION NETWORKS

Secretariat

Alliance for Telecommunications Industry Solutions

Approved July 1, 2004

American National Standards Institute, Inc.

Abstract

This Technical Report (TR) provides initial information on the reliability and availability aspects of Next Generation Networks (NGNs). NGN-specific characteristics are discussed in terms of their relevancy to reliability-related aspects. Recommended reliability-related metric and parameter objectives are not established.

FOREWORD

This Technical Report (TR) addresses the growing interest from the telecommunications community about the reliability aspects of next generation telecommunication networks, including the services provided under failure conditions. It is intended to provide a basis for designing and operating next generation telecommunications networks to meet users' expectations regarding end-to-end network reliability.

This TR is intended for providers of telecommunications networks and services (including Internet services), and telecommunications equipment suppliers.

The Alliance for Telecommunication Industry Solutions (ATIS) serves the public through improved understanding between carriers, customers, and manufacturers. The Network Performance, Reliability, and Quality of Service Committee (PRQC) -- formerly T1A1 -- develops and recommends standards, requirements, and technical reports related to the performance, reliability, and associated security aspects of communications networks, as well as the processing of voice, audio, data, image, and video signals, and their multimedia integration. PRQC also develops and recommends positions on, and foster consistency with, standards and related subjects under consideration in other North American and international standards bodies.

Suggestions for improvement of this document are welcome. They should be sent to the Alliance for Telecommunications Industry Solutions, Network Performance, Reliability, and Quality of Service Committee, Secretariat, 1200 G Street NW, Suite 500, Washington, DC 20005.

At the time it approved this document, PRQC, which is responsible for the development of this Technical Report, had the following members:

The Reliability (REL) Subcommittee was responsible for the development of this document.

O. Avellaneda, PRQC Chair
S. Makris, PRQC Vice-Chair
F. Kaudel, PRQC Chief Editor
R. Paterson, PRQC Technical Editor
J. Bennett, PRQC Technical Editor

Active Participants:

O. Avellaneda		J. Huang
J. Bennett	S. Makris	
P. Tarapore		A. Nguyen
F. Kaudel		R. Paterson
P. Kimbrough		A. Webster
R. Patel		R. Holley

TABLE OF CONTENTS

0 EXECUTIVE SUMMARY 1

1 PURPOSE, SCOPE, & APPLICATION 1

1.1 PURPOSE 1
1.2 SCOPE 1
1.3 APPLICATION 2

2 INTRODUCTION 2

3 NORMATIVE REFERENCES 2

4 DEFINITIONS 2

5 ABBREVIATIONS & ACRONYMS 4

6 RELATED WORK 4

6.1 T1A1 TECHNICAL SUBCOMMITTEE 4
6.2 INTERNATIONAL STANDARDS WORK 4
6.3 OTHER FORUMS AND COMMITTEES 5
6.4 FEDERAL GOVERNMENT RELATED WORK 5

7 NEXT GENERATION NETWORKS OVERVIEW 5

7.1 NGN SCOPE 5
7.2 NEXT GENERATION NETWORK FUNCTIONALITY 6

8 NGN DESIGN CONSIDERATIONS 7

8.1 DESIGN CHALLENGES 7
8.2 NGN REQUIREMENTS 8
8.3 NGN DESIGN STRATEGIES 8
8.4 NGN DESIGN CONSIDERATIONS 10
8.5 DESIGN CONSIDERATION EXAMPLE 11
8.5.1 Normal Operating State 12
8.5.2 Detection and Recovery 12
8.5.3 Outage States 13

9 NGN EXAMPLES 13

9.1 RELIABILITY CONSIDERATIONS FOR VOICE OVER IP SERVICE IN NGNS 13
9.2 HYBRID VOICE OVER PACKET SWITCHES 15
9.2.1 Overview 15
9.2.2 Definitions for the Hybrid VOP/Next Generation Network Functional Elements 15
9.3 NGN SYSTEM ARCHITECTURE EXAMPLE 16
9.4 VOICE OVER PACKET SWITCHES 18
9.4.1 Overview 18
9.4.2 Definitions for the VOP/Next Generation Network Functional Elements 19

10 NGN RELIABILITY MODELING CHALLENGES 20

10.1 OVERVIEW 20
10.2 NGN RELIABILITY AND AVAILABILITY MODELS 21
10.3 FAILURE MODES 22
10.4 SOFTWARE RELIABILITY MODELS 23
10.5 MODELING SUMMARY 23

A DATA ELEMENTS FOR REPORTING CYBER AND PHYSICAL EVENTS AFFECTING TELECOMMUNICATIONS NETWORKS 24

A.1 INTRODUCTION 24
A.2 DISCUSSION 24
A.3 SUMMARY 26

B APPROACH TO SET END-TO-END RELIABILITY/AVAILABILITY REQUIREMENTS FOR NEXT GENERATION NETWORKS 27

B.1 INTRODUCTION 27
B.2 DISCUSSION 27
B.3 PROPOSAL 28
B.4 ILLUSTRATION 29
B.4.1 High Availability IP Service Use Access 29
B.5 NETWORK DESIGN REQUIREMENTS 30

C RELIABILITY OBJECTIVES RATIONALE FOR NEXT GENERATION NETWORK ELEMENTS 34

C.1 INTRODUCTION 34
C.1.1 Intent 34
C.1.2 Context 34
C.1.3 Scope 35
C.1.4 Motivation 35
C.2 NETWORK ELEMENT TYPES 36
C.2.1 Concept 36
C.2.2 Network Element Definitions 37
C.3 ILLUSTRATION 39

TABLE OF FIGURES

FIGURE 1 - NGN SCOPE 6
FIGURE 2 - NEXT GENERATION NETWORK FUNCTIONALITY 7
FIGURE 3 - NETWORK DESIGN OPTIMIZATION FOR RELIABILITY 9
FIGURE 4 - NETWORK ELEMENT REQUIREMENTS 10
FIGURE 5 - DESIGN CONSIDERATIONS FRAMEWORK 12
FIGURE 6 - NGN ARCHITECTURE (HYBRID VOICE OVER PACKET) 15
FIGURE 7 - HIGH-LEVEL SCHEMATIC OF A SAMPLE NGN ARCHITECTURE 17
FIGURE 8 - NGN ARCHITECTURE (VOICE OVER PACKET) 19

FIGURE A.1 - DATA ELEMENTS 25

FIGURE B.1 - NETWORK RELIABILITY/AVAILABILITY REQUIREMENTS 28
FIGURE B.2 - NETWORK SOLUTION OVERVIEW 29

FIGURE C.1 - NE RELIABILITY OVERVIEW 34
FIGURE C.2 - NE RELIABILITY REQUIREMENTS AND RQMS/TL9000 35
FIGURE C.3 - FAULT TOLERANCE AND REVENUE RISK 37
FIGURE C.4 - NETWORK ELEMENT TYPES 38
FIGURE C.5 - SAMPLE NETWORK 40

TABLE OF TABLES

TABLE A.1 - EXTERNAL REFERENCE INFORMATION 26

TABLE B.1 - END-TO-END NETWORK SOLUTION REQUIREMENTS 29

TABLE C.1 - NE TYPES 39
TABLE C.2 - NE RELIABILITY PERFORMANCE 39
TABLE C.3 - CUSTOMER ACCESS DOWNTIME RESULTS 40
TABLE C.4 - MATURE VS. AD HOC DEVELOPMENT PROCESSES 41

Technical Report on –

Reliability Aspects of Next Generation Networks

0 EXECUTIVE SUMMARY

The *Next Generation Network* (NGN) is a multi-service, multi-vendor, multi-provider-managed packet-based network. It must be capable of providing a wide-range of service reliability levels from mission-critical to non-critical, each with Applications that have a wide range of sensitivity to failure. These aspects present some key network design and reliability modeling challenges.

Similarly to any network, the design strategy categories are: prevention, mitigation, and masking. *Prevention* strategies prevent the occurrence of failure. Examples include security features that prevent people to cause network outages resulting in denial of service attacks and robustness features that prevent network outages due to traffic or control message overloads. *Mitigation* strategies reduce the frequency, duration and/or impact of failures. Examples include remote diagnostics that quickly isolate failures to reduce mean-time-to-repair and equipment returns, good design practices to reduce technology failure rates, graduated recovery to reduce network element downtime due to software failures, and distributed design to reduce the impact of failure modes. Lastly, *masking* strategies mask failures from disrupting service as experienced by end-users and end-devices.

Since many of these design strategies are features that must inter-operate between network elements, standardization work will be required -- such as fault management messaging, Class of Service marking, etc.

Reliability-related modeling prediction also needs to be enhanced to include the ability to predict software and procedural failure rates and to incorporate these into end-to-end Service Downtime models. It may also be useful to incorporate the affect of traffic variability impact on Service Downtime.

1 PURPOSE, SCOPE, & APPLICATION

1.1 Purpose

The purpose of this document is to provide an initial information on reliability-related aspects of Next Generation Networks (NGN), to facilitate the establishment of NGN reliability requirements.

1.2 Scope

Although techniques, parameters, and methods needed to study NGN reliability are defined, recommended parameter objectives are not established.

1.3 Application

This TR presents the telecommunications industry with a foundation for to designing and operating Next Generation Networks (NGN) to meet users' expectations regarding end-to-end network reliability.

2 INTRODUCTION

The Next Generation Network (NGN) is a multi-service, multi-vendor, multi-provider-managed packet-based network. It must be capable of providing a wide-range of service reliability levels from mission-critical to non-critical, each with applications that have a wide range of sensitivity to failure.

This document describes some preliminary perspectives and solutions for network reliability design and modeling challenges. It is organized as follows:

- Introduction to NGN
- NGN Reliability Design Considerations
- NGN Examples
- NGN Reliability/Availability Modeling Challenges
- Appendix

3 NORMATIVE REFERENCES

[1] T1.TR.70-2001, *Network Survivability Performance*.[1]

[2] GR-929-CORE, Issue 8, *Reliability and Quality Measurements for Telecommunications Systems (RQMS-Wireline)*, Telcordia Technologies, December 2002.[2]

4 DEFINITIONS

4.1 Availability: The proportion of the operating time in which an *entity* meets its in-service functional and performance requirements in its intended environment.

4.2 Failure: The occurrence of an event in which an entity's does not meet its in-service functional and performance requirements or expectations.

4.3 Failure Frequency: The rate of occurrence of failure (in time or in number of operations) of an *entity* to meet its in-service functional and performance requirements in its intended environment.

---

[1] This document is available from the Alliance for Telecommunications Industry Solutions (ATIS), 1200 G Street N.W., Suite 500, Washington, DC 20005. < https://www.atis.org/docstore/default.aspx >

[2] Telcordia documents are available from Industry Direct Sales, Telcordia, 8 Corporate Place, PYA 3A-184, Piscataway, NJ, 08854-4156, or: < http://telecom-info.telcordia.com >.

4.4 Failure Recovery Coverage: The proportion of the recoverable failure rate of fault tolerant equipment that is successfully detected and recovered.

4.5 Failure Isolation Coverage: The proportion of the failure rate of a Field Replaceable Unit (FRU) that can be isolated to that FRU for successful repair by the NE's diagnostics.

4.6 Fault Tolerance: The ability of a functional unit to function at a specified level when one or more of its components have failed (transient or hard failures).

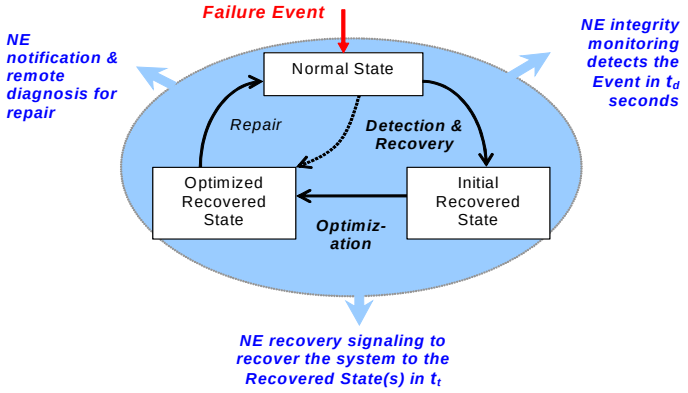
4.7 Maintainability: The ability of an *entity* to facilitate personnel to diagnose and repair network elements.

4.8 Intrinsic Mean-time-to Repair: The average time to field repair a failed FRU starting from the initiation of the repair activity to when the replacement FRU is returned to service. This metric excludes travel time and assumes spares are available (and work) in order to measure the effectiveness of the NE's diagnostics as used by the operational personnel.

4.9 Total Mean-time-to Repair: The average time to field repair a failed FRU starting from the time of the failure to when the replacement FRU is returned to service. This metric includes all travel and administrative time such as to identify and retrieve the required spare.

4.10 Mean-time-to Restore Service: The average time to restore service measured from when the service has failed to when it meets its in-service functional and performance requirements or expectations.

4.11 Network Recovery Cycle: The steps, initiated by a failure event, that a system of Network Elements execute to detect, recover, and notify for repair to return the network to its original normal operating state.



4.12 Reliability: The probability that an *entity* will complete its intended mission as required over a specified period of time in its intended environment.

4.13 Reliability-related Prediction: The computation of reliability-related metrics from design parameters and piece-part failure rate models that have been calibrated from field or life-test data.

4.14 Reliability-related Estimation: The computation of reliability-related metrics from development process verification and validation parameter results.

4.15 Service Performance Threshold: The acceptable limit of packet delay, packet jitter, and packet integrity for acceptable customer service performance.

4.16 Survivability: The ability of an *entity* to continue to meet its functional requirements during network failure events such as cyber-attacks, physical attacks, natural disasters, and traffic overloads.

5 ABBREVIATIONS & ACRONYMS

AG	Access Gateway
CATV	Cable Television
CCA	Call Connection Agent
CTU	Circuit Termination Unit
EMS	Element Manager Server
FE	Functional Element
FRU	Field Replaceable Unit
NE	Network Element
NHPP	Non-Homogeneous Poisson Process
NGN	Next Generation Networks
OAMP	Operations, Administration, Management and Provisioning
PBX	Private Branch Exchange
POTS	Plain Old Telephone Service
PSTN	Public Switched Telephone Network
PTU	Packet Termination Unit
RTS	Routing and Translation Server
SCP	Service Control Points
SG	`Signaling Gateway
SNC	Service and Network Controller
TCAP	Transaction Capabilities Application Part
TG	Trunk Gateway
VOP	Voice Over Packet

6 RELATED WORK

6.1 T1A1 Technical Subcommittee

In addition to the T1A1.2 Working Group (WG), the following T1A1 WGs is involved in work related to Internet:

- T1A1.3 WG (Performance of Networks and Services).

EDITORIAL NOTE - T1A1.2 and T1A1.3 were merged to form PRQC.

6.2 International Standards Work

The following ITU-T study groups are involved in work related to network survivability performance:

- Study Group 2 – Operational Aspects of Service Provision, Networks, and Performance (see ITU-T Recommendation E.436);
- Study Group 12 – End-to-End Transmission Performance of Networks and Terminals (see ITU-T Recommendation I.350);
- Study Group 13 – Multi-Protocol and IP-based Networks and their Interworking; and
- Study Group 15 – Optical and Other Transport Networks.

6.3 Other Forums and Committees

Forums involved in network reliability include the following (see T1.TR.70-2001):

- IETF – Internet Engineering Task Force;
- NRIC – Network Reliability and Interoperability Council;
- NRSC – Network Reliability Steering Committee;
- OIF – Optical Internetworking Forum; and
- Cable Labs (see pkt-tr-voipar-v01-001128).

6.4 Federal Government Related Work

See Appendix A on *Data Elements For Reporting Cyber And Physical Events Affecting Telecommunications Networks*.

7 NEXT GENERATION NETWORKS OVERVIEW

7.1 NGN Scope

The NGN is an edge-to-edge packet-based network that seamlessly supports data and voice services, video and multimedia services, and other advanced features (Figure 1). NGN Reliability Performance (as discussed in this document) has two perspectives: (*i*) the *service view*; and (*ii*) the *network view*. Generally, the service view will be important to both end users as well as other service providers. The network view will be most important to the owner and operator of the network. The service user experiences service outages, failed service attempts, etc., while the service provider experiences maintenance costs as well as OAMP[3] outages such as loss of the ability to diagnose. These and other key concepts are discussed in Section 6 of T1.TR.70-2001 [1].

[3] Operations, Administration, Management, and Provisioning

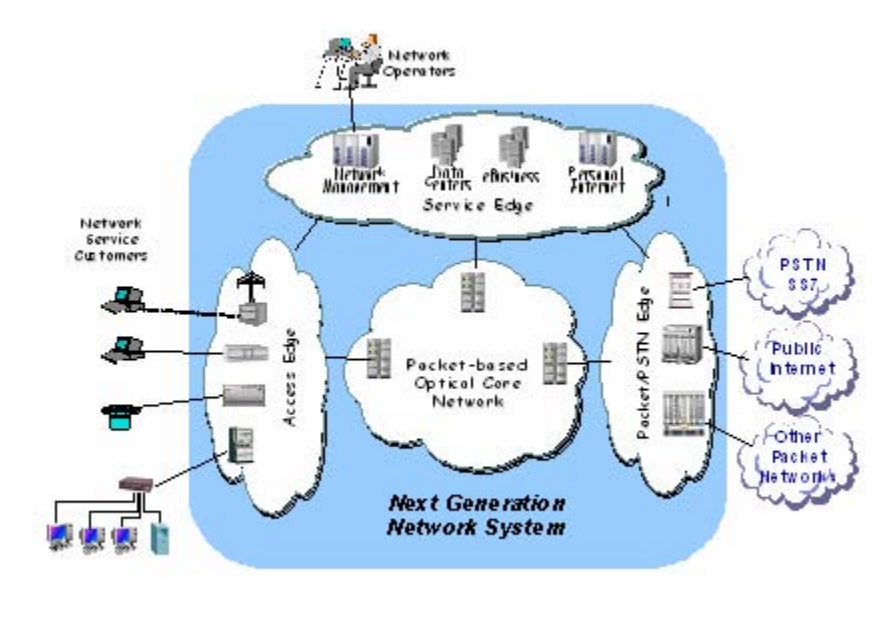


Figure 1 - NGN Scope

The architectural components are:

- *Access Edge* to interface network customers, add services functionality, and aggregate traffic to the backbone transport network.
- *Services Edge* to provide key service functionalities such as Services and Network Management, authentication, VoIP call control, *etc.*
- *Core Network* to provide transport connectivity.
- *Packet* and *PSTN Edge* to interface to the Internet and the PSTN.

7.2 Next Generation Network Functionality

The NGN functionality is depicted in three levels as shown in Figure 2: (*i*) *Content and Applications*, (*ii*) *Communications Services*, and (*iii*) *the Communication Paths* to provide multiple service and applications.

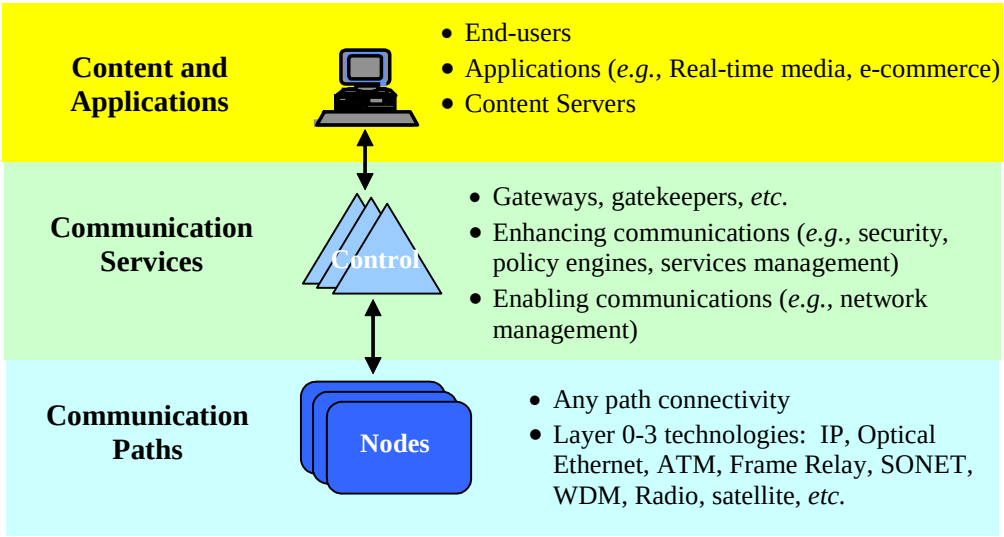


Figure 2 - Next Generation Network Functionality

These NGN levels inter-operate to provide end-users or end-devices with services and network operators with remote OAMP capabilities. The Communication Path level provides path connectivity between end-user and end-devices using Layer 0-3 technologies such as SONET, WDM, ATM, Frame Relay, Optical Ethernet and IP. The Communications Services level enhances communications by provided capabilities such as network management and security. The Content and Applications level provides the end-user applications such as voice and video.

8 NGN Design Considerations

8.1 Design Challenges

The NGN is a multi-service packet-based network that is multi-vendor supplied and multi-provider operated. This presents some key reliability-related design challenges:

- Wide range of service reliability expectations over the same network.
- Wide range of application sensitivity to failure.
- Functional, OAMP, state information, fault information, etc., inter-operability.
- Containment of failures (fault propagation causing high impacting outages).
- Non-deterministic nature of packet networks, which may lead to long protocol convergence time at the time of control plane failure.
- Increased system functionality and, in turn, hardware and software complexity resulting in lower fault detection and recovery coverage.
- Frequent software upgrades for new features and services, which may result in increased annual down time.

- Distributed VOP control requiring inter-NE co-operation to save and use state information for successful recovery.
- VOP applications and services provided by multiple individual systems, which may lower end-to-end service availability (due to concatenation of the systems along the service path).

8.2 NGN Requirements

NGN reliability-related requirements that only consider the communication path have limited value because they do not address reliability and availability as experienced by end-users or end-devices. For the service user reliability experience to be satisfactory, all three-network levels must operate together reliably as a system. This means that the failure mode "behavior" of the NGN system must be mapped to the impact on the end-user or end-device "quality of experience".

It is necessary to relate reliability-related NGN design parameters (e.g., network restoration time, port failure frequency, etc.) to the reliability-related metrics that capture the end-user or end-device experience (e.g., Service Downtime)

Objectives for the end-user metrics, such as Service Downtime, should not be standardized because these numbers are technology and implementation-specific and will improve over time based on competition. A requirement should be phrased as "*no single point of failure causing a service outage requiring a field repair*". Depending on the technology and network design, the end-user downtime to meet this requirement could vary from 0.5 to 3 minutes per year.

Because the applications vary in terms of their timeliness needs, the performance criterion that constitutes a failure varies. These thresholds also vary depending on the usage state (e.g., access vs. use). Values for these parameters should be characterized and agreed to across the industry.

8.3 NGN Design Strategies

The network architect's role is to optimize the network design to satisfy service-based reliability/availability expectations and to minimize cost.

The design strategies, shown in Figure 3, are grouped into two areas that are meant to minimize or eliminate the frequency of occurrence of the failure events that originate within the network system (prevention design strategies), and reduce the impact of the failure event on the service (mitigation/masking strategies).

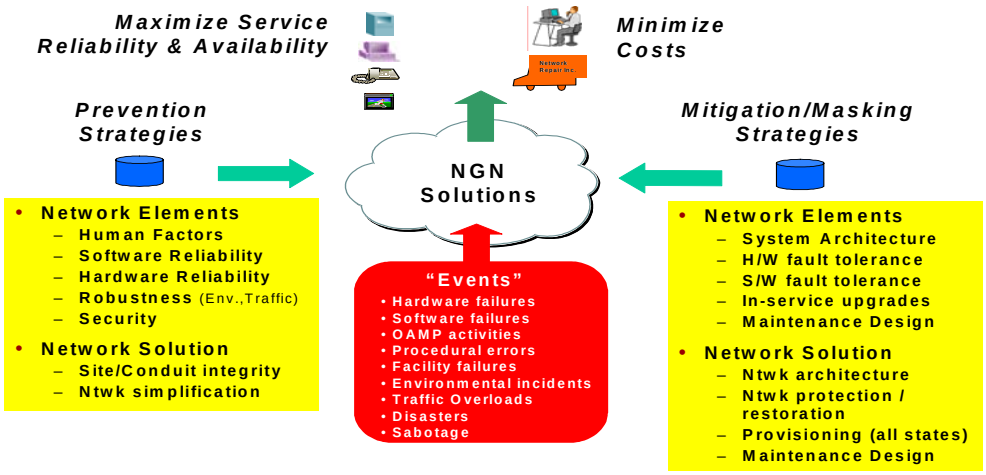


Figure 3 - Network Design Optimization for Reliability

The design strategies are selected based on how effectively they satisfy the service requirements. These requirements are set based on the criticality of the network services or Operations, Administration, Maintenance, and Provisioning (OAMP) feature; the impact of the failure event failure mode; and the business value.

The network-wide use case approach requires that reliability/availability requirements should not be specified for Network Elements (NEs) independently of the network solution.

As Figure 4 illustrates, network use case requirements that are set based on both market business drivers (top-down) and technology capabilities (bottom-up).

The solution-specific requirements result in network element options to allow for design flexibility. This flexibility allows the network designer to mitigate or mask failure modes via networking or network element (or both) design strategies -- whichever is of most value for the specific network solution. An example is 1:N port protection as a network element option.

The baseline set of requirements is independent of any specific network solution. These attributes, which are to be met for all network solutions, are ones that are most economically resolved within the product not by networking design strategies. An example is traffic overload robustness, where it is better to contain the impact within the network element rather than relying on network restoration to recover.

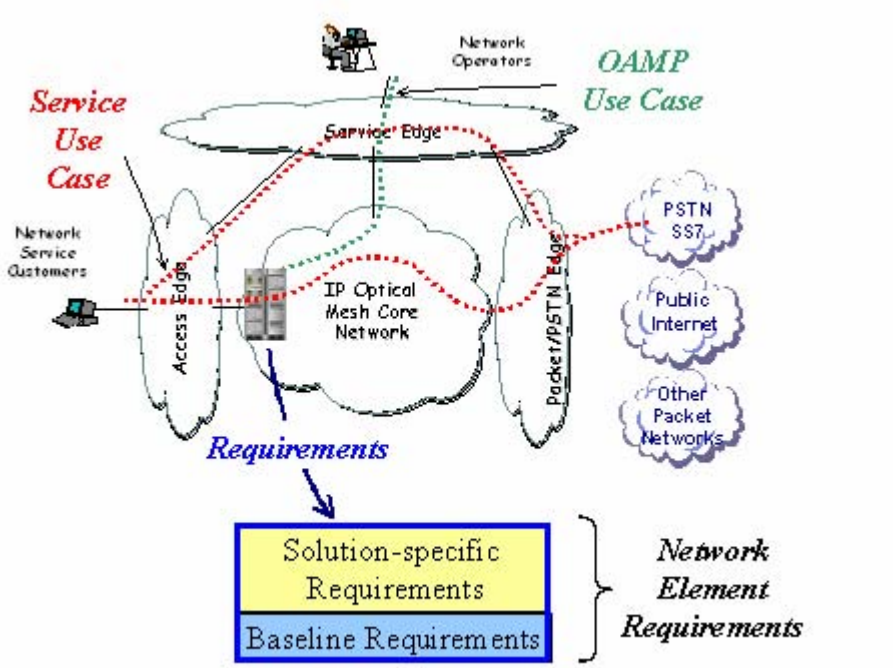


Figure 4 - Network Element Requirements

8.4 NGN Design Considerations

The key network reliability design principles for the NGN starts with the prevention strategies. The masking and mitigation strategies simply add cost to the NGN and therefore must be selected based on value.

1. Simplify the functional design to minimze the NGN's technology failure rates (e.g., increase Mean-time-between-Failures).
2. Ensure that the functional design is robust to events such as climate, ESD/EMI and traffic overloads.
3. Design partitioning to facilitate good fault isolation to reduce equipment return rates and improve mean-time-to-repair.
4. Human factors design to minimize procedural error.
5. Security features to prevent denial of service attacks.

The masking and mitigation strategies should be selected assuming good implementation quality of the functional design. Adding cost and complexity to the NGN design should not be done because of poor quality, it should be done based on the inherent reliability of the design. That is, select those areas where the failure frequency-duration-impact combination warrants the cost versus the Service Customer expectations.

1. To minimize cost of reliability and complexity of design, fault handling technologies should be selected based on:
    - Failure mode risk;
    - Bandwidth efficiency; and
    - Ability to mitigate failure mode impact on end-user services.
2. To expand the failure event scope to include all failure events, it is necessary to go beyond the widely used case-based scope. These events include:
    - Hardware and software failures.
    - Normal OAMP activities done by the network operator both remotely and on-site.
    - People — both procedural errors and acts of sabotage.
    - Traffic overloads — both bearer traffic and control messages.
    - Environmental incidents such as floods, earthquakes, etc.

Although Communication Servers must be built with the best current practices for building carrier-grade platforms with no single point of failure, the impact of catastrophic failures on the building itself where these network elements are located has to be taken into account when designing these networks. Therefore, the architecture for an NGN must include strategies to handle events beyond direct control (e.g., fires, earthquake, flooding). One possible strategy is to operate the processors that compose the Communication Server in an N+M configuration (N working servers and M backup servers), where the extra processors can take over call processing in the event of a failure of one of the other processors. Of course, the redundant processors would be located in a separate physical location.

In normal operation, the Media Gateways communicate with the processor to which they are assigned. In the event that a processor fails completely, the Media Gateways impacted would then try to communicate with a standby processor and resume processing. In parallel, the standby processor would have detected or have been informed of the failure, and would have loaded the right system configuration to assume the role of the failed processor. Because of the distributed architecture of an NGN, the Media Gateways can be physically located in several different locations, minimizing the risk of one catastrophic event cutting off service to all users. Service to end users can be restored very quickly with this architecture, much faster than the older approach -- which consisted of shipping new equipment to the affected site, sometimes in a pre-configured container, and physically rebuilding the connectivity.

8.5 Design Consideration Example

To discuss the design considerations, a generic State Diagram (Figure 5) describes the classes of states the network can exist in. For each state type and transition, there are design considerations to prevent, mitigate, or mask the failures.

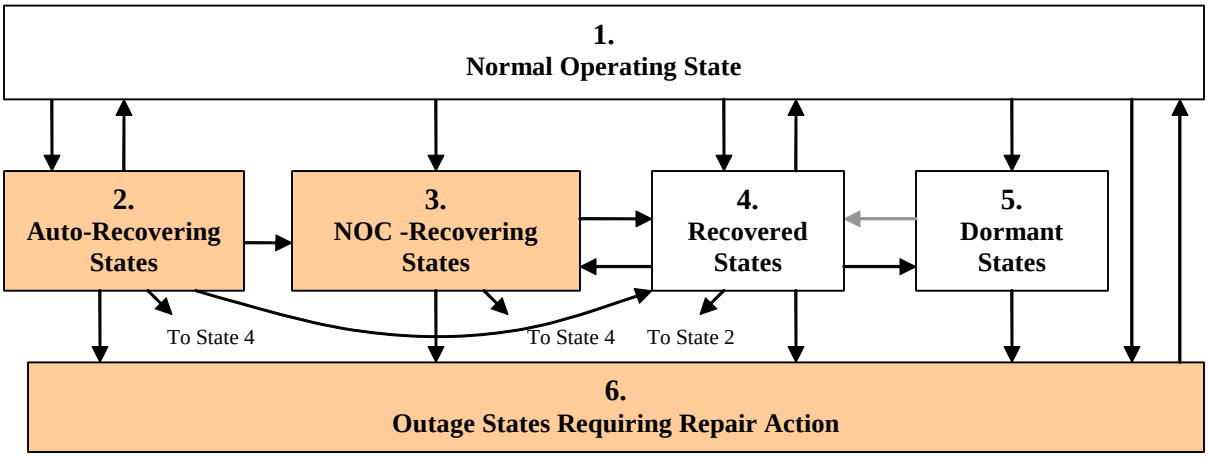


Figure 5 - Design Considerations Framework

The following sections describe the design considerations for each of the states and transitions.

8.5.1 Normal Operating State

Because the network system spends most of its time in this state, the network protection/restoration features are often overhead resources waiting to be used, thus representing a cost that is not directly generating revenue. Reserved bandwidth and static pre-provisioned back-up paths are examples. The design considerations for this state are:

- Network architecture to minimize single points of failure. (Transition 1 to 6)
- The design complexity and its ability to ensure the ongoing integrity of the back-up facilities to minimize dormant faults.
- Robustness of the network elements to the operating and traffic environments to ensure the network does not change failure states.
- Human factors design to prevent procedural errors, such as fail-safe commands.

8.5.2 Detection and Recovery

There are three generic intermediate state types:

1. *Auto-recovering States* are of two types: *Transients* or software failures are detected and automatically recovered back to the normal operating state and require no repair. (Transitions 1 to 2 and 2 to 1). *Hard faults* are where there is protection using hold-off timers. (Transitions 1 to 2 and 2 to 4). These states are service-affecting and if long enough will be considered a service outage.
2. *NOC Recovering States* are those that require the personnel at the Network Operations Center (NOC) to manual recover the network to a recovered state. (Transitions 1 to 3 and 3 to 4). The intent is to recover to the non-service-affecting state 3; however, some designs can only recover to a reduced service-affecting state.

3. *Recovered States* are non-service-affecting states requiring repair that have recovered and alarmed the failure.
4. *Dormant States* are non-service-affecting states where there are hard faults that are undetected (e.g., of a back-up resource). They are of two types: *detectable* by a scheduled background integrity test (Transitions 1 to 5 to 4) and *undetectable* (Transitions 1 to 5 to 6 or any of the recovering states).

The design considerations for these states are:

- High failure mode detection coverage for both the operational resources to eliminate single points of failure as well as back-up resources to eliminate dormant faults.
- Integrity of recovery requires that the speed of detection and recovery is fast enough to mask the impact on the higher layers and end users. Packet loss and state information, if required for successful recovery.
- Fault containment or the ability of the design strategy to limit the impact of the failure mode.
- The recovered states' network design should:
  - Ensure adequate provisioning or use Class of Service marking strategies to satisfy Service Level Agreements (SLA).
  - Robustness of the network elements to the operating and traffic environments to ensure the network does not change failure states.
- Local and remote alarms are used to isolate the network resource for fast repair.
- Human factors design to prevent procedural errors, such as fail-safe commands.

8.5.3 Outage States

In the event that the network system enters the outage state due to either a single point of failure, or due to two failure events, it is important that it is alarmed. If not the event will last for a long period as the network operators try to find out what has failed based on users' complaints.

9 NGN EXAMPLES

The following example architectures assume the continued existence of the PSTN. However, this assumption may not be true after an evolution to a multi-service packet-based network.

9.1 Reliability Considerations for Voice over IP Service in NGNs

NGNs will support a variety of communications and media services such as data, video, and voice seamlessly. Customers will demand that these networks be highly reliable as more and more traffic and services use them. Because of the historically exceptional reliability of Plain Old Telephone Service (POTS), the reliability of voice services supported by NGN necessitates special attention in order to achieve the same level of customer satisfaction.

Many NGN failures will result in reduced capacity until the network is repaired. This could result in unacceptable service performance that to the end-user could appear like poor service reliability.

It is necessary to define key metrics to quantify the reliability of Voice Over Packet (VOP) service in NGNs. VOP is a more general case of Voice over IP (VoIP). Once metrics are established, the next step will be to develop objectives based on these metrics so that high reliability can be assured.

To achieve this, the issues of VOP service reliability in NGNs should be addressed on two levels:

1. The reliability of individual network elements.
2. The reliability of the network as a whole.

Reliability should be related to loss of service, not just failure of equipment. Specifically, each level will be addressed with respect to the availability of VOP service. Reliability should take into account customer expectations of service availability and Quality of Service (QoS). The contributions of failure modes for hardware, software, and human interaction will be considered. Reliability models should incorporate repair and maintenance to represent the mitigating effects of best practices and proper network support.

In order to provide consistency and continuity, VOP service reliability standards for NGNs may take as their starting point existing standards for voice telephony. The special nature of voice services over an NGN will require re-evaluation and reinterpretation of these standards and objectives within the context of this new architecture. In particular:

- New architectures, such as NGNs, are particularly susceptible to procedural error reliability problems resulting from the learning curve of operations personnel who interact with new equipment and procedures.
- The likelihood that equipment from multiple suppliers will be needed to implement VOP service in NGNs increases the probability that failures may result from interoperability design errors between network elements.
- The substantially greater reliance on software makes VOP service for NGNs especially susceptible to failures resulting from computer viruses; such a virus could have a potentially devastating effect on a VOP service through its widespread dissemination via the network itself.
- The packetization of voice provides new service failure modes from the customer's perspective. VOP service in NGNs is susceptible to a type of reliability service degradation not seen in voice service over wire-line networks: delay variability and errors in voice transmission after call setup. In addition, packets can be misrouted or lost, creating gaps in speech. Packets may be placed out of sequence, creating confused speech or conversation without logical flow.

In order to make VOP service in NGNs a viable alternative to POTS, it is imperative that service availability not be substantially degraded. Customer familiarity with the existing POTS may require that the VOP service objectives are comparable to those of POTS.

9.2 Hybrid Voice Over Packet Switches

9.2.1 Overview

The major business challenges facing next-generation network service providers and suppliers are to build VOP networks that provide levels of reliability that meet or exceed those in the circuit-switched network. As networks converge to support data, voice, and video applications, the circuit switches are evolving to include packet functionality. This phenomenon is driving some circuit switch architectures to become a *hybrid switch*. These hybrid switches are typically configured as End or Tandem Offices, creating the need for metrics to determine reliability of these hybrid switches.

The Hybrid VOP (HVOP) architecture (see Figure 6) allows the migration of traditional telecommunication networks (circuit switch based) to Next Generation Network (Pure Packet Network). The HVOP switch typically includes Call Connect Agent, Signaling Gateway, and Service Agent, and in addition includes circuit termination units (e.g., analog/digital line and trunk unit) and packet network termination units (e.g., packet trunks).

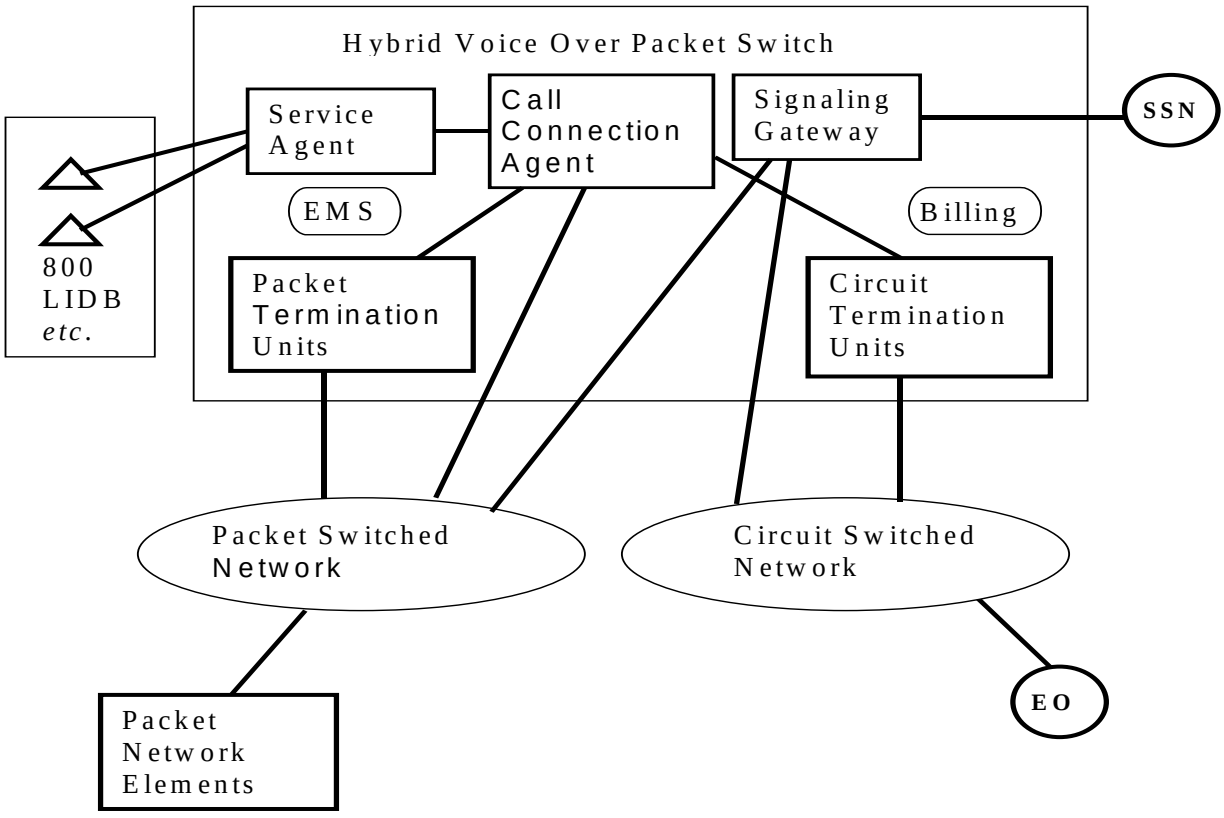


Figure 6 - NGN Architecture (Hybrid Voice over Packet)

9.2.2 Definitions for the Hybrid VOP/Next Generation Network Functional Elements

The HVOP switch combines the following Functional Elements (FEs):

1. *Call Connection Agent (CCA):* A CCA provides much of the necessary call processing functionality to support voice on the network via the circuit and packet switched access units.

CCA processes messages received from various other FEs to manage call states. A CCA communicates with other CCAs to setup and manage an end-to-end call. Although each gateway (Access Gateway, Customer Gateway, Signaling Gateway, and Trunk Gateway) is associated with a specific CCA, a CCA instructs gateways with call control commands. A CCA interacts with the Billing Servers to generate usage measurements and billing data, such as CDRs, for billing. The loss of a CCA will contribute to Total or Partial HVOP Outage.

2. *Signaling Gateway (SG):* The HVOP switch interconnects the VOP network to the PSTN signaling network. A SG terminates SS7 signaling links for circuit trunks, and Bearer Independent Call Control (BICC) signaling links for packet trunks. These signaling links themselves could be circuit or packet. A SG communicates with the CCA to support the end to end signaling for calls with the PSTN. Each SG is associated with a specific CCA. The loss of a SG will contribute to HVOP outage.

3. *Service Agent (SA):* The SA supports supplementary services and generates TCAP messages to interact with Service Control Points for vertical services (intelligent network services) such as 800 and LNP. It is initially envisioned that there would be a single SA for the entire VOP network that would interact with and through multiple CCAs.

   Note -- Currently there are no metrics associated with service agent outages.

4. *Circuit Termination Unit (CTU): A* CTU supports circuit terminations on the HVOP. These terminations include analog and digital lines and trunks, Integrated Service Digital Network (ISDN) lines, *etc.* The call processing for these terminations is provided by one or more CCAs. It does not use the capability of the packet network or packet switching NEs when the call is completed over PSTN. However, when the circuit call is routed over the packet network, a CCA will convert the call to a packet call and place the call over the packet network.

5. *Packet Termination Unit (PTU):* A PTU supports packet terminations on the HVOP (e.g., packet trunks). The call processing for these terminations is provided by one or more CCAs. It uses the capability of the packet network or packet switching NEs to complete the call. However, when the packet call is routed over the circuit network, a CCA will convert the call to a circuit call and place the call over the circuit network.

9.3 NGN System Architecture Example

Figure 7 below provides a high-level schematic of a sample NGN architecture. From a gross-functional perspective, the architectural design for a network designed to support VOP/NGN is analogous to a single very large switch. The Core Network is densely interconnected like the switching fabric at the heart of a switch. The Access Network and its attendant Customer and Access Gateways play the role of the local loop and the line concentrators. The Signaling and Trunk Gateways provide access to other switches in the PSTN. The Call Connection Agent takes on the functions of the central call processors of a switch. The Service Agent controls the connections to the Service Control Points for vertical services (Intelligent Network services) such as 800 and LNP (Local Number Portability). Thus, it has one of the roles of the Signaling Transfer Point in the Common Channel Signaling network.

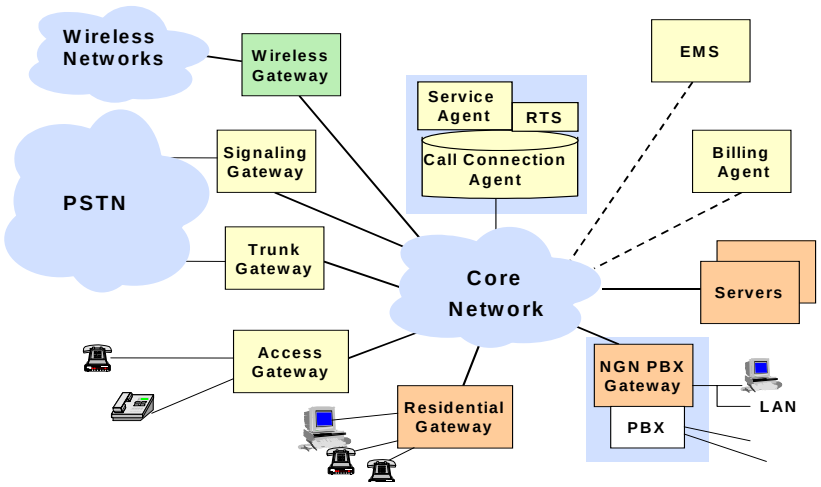


Figure 7 - High-level Schematic of a Sample NGN Architecture

The functional elements in this architecture are:

- *Core Network:* The key functional element at the heart of the VOP/NGN architecture is the Core Network. This functional element is too large to be duplicated for the purposes of reliability. However, its reliability is augmented by its robustness through the creation of a high-density path structure within the Core Network.
- *Access Network:* This functional element represents the local loop network in the VOP/NGN. There are various ways of offering access to the VOP/NGN. The Access Network could be based on the existing copper plant of Local Exchange Carriers or could use other technical options as Hybrid Fiber-Coax (e.g., CAble TV - CATV), any-rate Digital Subscriber Line (xDSL), *etc.* The reliability standards for the Access Network will be based on existing standards for the corresponding technical options (i.e., architectures) that offer access to the VOP/NGN.
- *Billing Agent:* Each VOP/NGN has multiple Billing Agents. It is not clear at this stage whether Billing Agents are dedicated to any particular part of the network or are used as a central pooled resource. In either case (although with differing consequences), the effects of failure of one or multiple Billing Agents should be modeled.
- *Call Connection Agent:* The VOP/NGN also has multiple Call Connection Agents. However, in this case, it is clearly planned that specific gateways (Access Gateways, Customer Gateways, Signaling Gateways, and Trunk Gateways) are associated with each Call Connection Agent. The failure of a Call Connection Agent would not bring down the VOP/NGN but could impose total loss of service to a substantial fraction of the customer base. Modeling the reliability of this functional element is of great importance in establishing reliability standards. It is also crucial to traffic engineering for establishing the number of Call Connection Agents in the VOP/NGN. For example, reliability considerations may require more Call Connection Agents than required to meet their normal traffic capacity engineering constraints.
- *Service Agent:* Multiple Service Agents exist for a VOP/NGN. Current VOP/NGN architectures envision one Service Agent for each Call Connection Agent. It generates Transaction Capabilities Application Part (TCAP) messages to interact with Service Control Points (SCPs). Its functional elimination or isolation would make vertical services such as 800 and LIDB services unavailable throughout the portion of the VOP/NGN served by that Call Connection Agent. Since it plays a more limited role than the Call Connection Agent, its reliability

standards are not expected to be as strict as those for the Call Connection Agent. Still, the importance of vertical services in telecommunications will still impose the necessity for high levels of reliability in the Service Agent.

- *Routing and Translation Server (RTS):* The RTS also supports the Call Connection Agent by providing translation functions for call setup. Like the Service Agent, its supportive role does not require reliability requirements as strict as those for the Call Connection Agent. However, its support of call setup makes its reliability requirements of greater import than those of the Service Agent.
- *Gateways:* Because of their position at the lowest level of the VOP/NGN architecture hierarchy, the various gateways (Access Gateways, Customer Gateways, Signaling Gateways, and Trunk Gateways) have the least import in reliability standards with respect to survivability of the network for a single failure. However, because of their multiplicity throughout the VOP/NGN, frequent (though less critical) failures can still produce customer perception of unreliable service. For this reason, it is no less important to model their characteristics and modes of failure as input into the analysis of reliability standards.

Special consideration should be given to the separate roles each type of gateway plays in a VOP/NGN. Signaling Gateways provide signaling access to the PSTN. A Signaling Gateway failure would cripple the interconnection of vertical services with the PSTN. A VOP/NGN is likely to have few Signaling Gateways so a single failure may have serious repercussions. On the other hand, in most cases, a VOP/NGN will have many Customer Gateways providing a limited effect if one fails. Still, a Customer Gateway may be assigned to provide access for a single large customer; the failure of such a gateway may have a greater impact than that of other Customer Gateways because of the focus and concentration of its effect.

- *Element Management System (EMS):* The EMS manages VOP/NGN operations. Since it does not directly support services, it has secondary importance in the reliability of VOP/NGN services.

9.4 Voice Over Packet Switches

9.4.1 Overview

This section is primarily inherited from GR-929-Core, Issue 7, [2] with modifications. The Voice over Packet Next Generation Network architecture (see Figure 8) is comprised of the following network elements:

- Service and Network Controller
- Trunk Gateway
- Access Gateway
- Packet Network & Packet Switching NEs

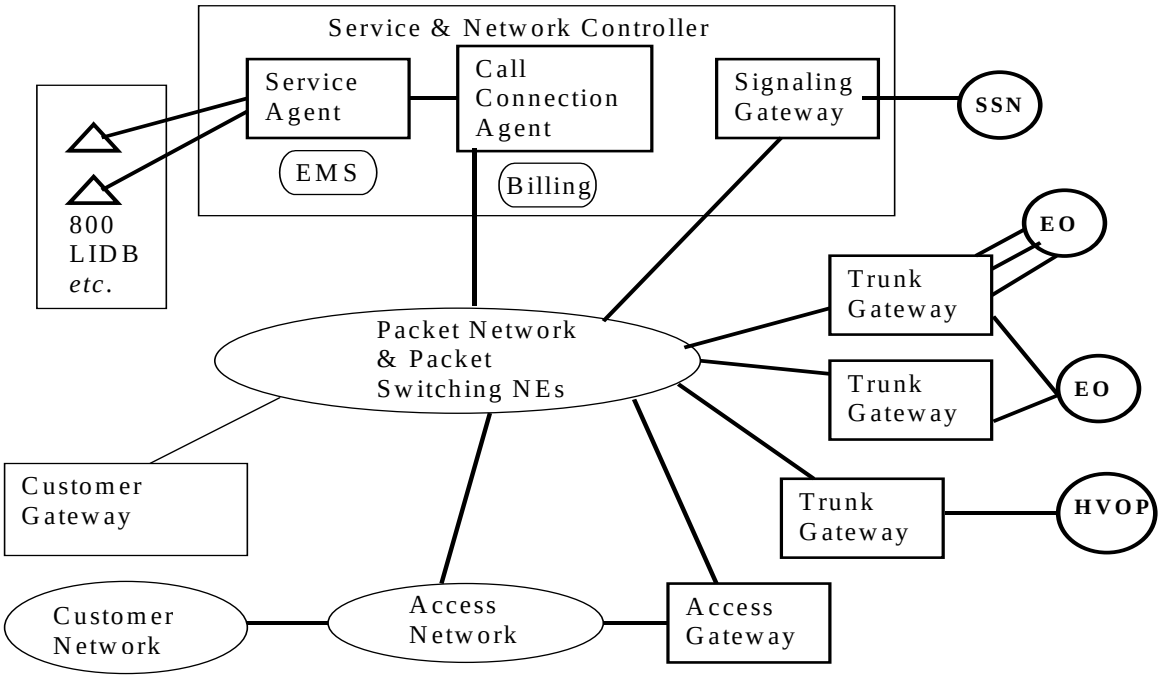


Figure 8 - NGN Architecture (Voice Over Packet)

The NGN is comprised of the following network elements:

- Service and Network Controller
- Trunk Gateway
- Access Gateway
- Packet Network & NEs.

9.4.2 Definitions for the VOP/Next Generation Network Functional Elements

Following are the definitions for the VOP NGN functional elements:

- **Service and Network Controller (SNC)** combines the following Functional Elements (FEs):
    1. *Call Connection Agent (CCA):* A CCA provides much of the necessary call processing functionality to support voice on the core network. CCA processes messages received from various other FEs to manage call states. A CCA communicates with other CCAs to setup and manage an end-to-end call. Although each gateway (Access Gateway, Customer Gateway, Signaling Gateway, and Trunk Gateway) is associated with a specific CCA, a CCA instructs gateways with call control commands. A CCA interacts with the Billing Servers to generate usage measurements and billing data, such as Call Data Records (CDRs), for billing. The loss of a CCA will contribute to Total or Partial SNC Outages.
    2. *Signaling Gateway (SG):* The SNC interconnects the VOP network to the PSTN signaling network. A SG terminates SS7 links from the PSTN CCS networks and thus provides the Message Transport Part (MTP) Level 1 and Level 2 functionality. A SG communicates with the CCA to support the end to end signaling for calls with the

PSTN. Each SG is associated with a specific CCA. The loss of a SG will contribute to Common Channel Signaling (CCS) Isolation SNC Outages.

3. *Service Agent (SA):* The SA supports supplementary services and generates TCAP messages to interact with Service Control Points for vertical services (intelligent network services) such as 800 and Local Number Portability (LNP). It is initially envisioned that there would be a single SA for the entire VOP network that would interact with and through multiple CCAs. Note: Currently, there are no metrics associated with service agent outages.

- A *Trunk Gateway (TG)* supports a trunk side interface to the PSTN and/or Packet network. The TG terminates circuit switched trunks in the PSTN and ATM virtual circuits and/or IP routed flows in the packet network and, as such, provides functions such as packetization. This FE supports circuit switched to packet switched trunks as well as packet switched to packet switched trunks. In the case of packet-to-packet switched trunks, it will not provide packetization functions. This FE does not provide the resource management functions for trunks that it terminates. However, the TG has the capability to set up and manage transport connections when instructed by the CCA. It is associated with a specific CCA that provides it with the necessary call control instructions.
- An *Access Gateway (AG)* supports the line side interface to the Packet backbone. Traditional phones and PBXs currently used for the PSTN can access the Packet backbone through this FE. As such this FE provides functions such as packetization, echo control, etc. It is associated with a specific CCA that provides the necessary call control instructions. On receiving the appropriate commands from the CCA, the AG also provides functions such as audible ringing, power ringing, miscellaneous tones, etc. It is assumed that the AG has the functionality to set up a transport connection when instructed by the CCA.
- The *Packet Network* is the network that provides connectivity to the functional elements in the VOP network. The Packet Network is commonly composed of a group of interconnected Packet Switching Network Elements (NEs). These elements may be ATM and/or IP based.
- The *Packet Switching Network Element (Packet Switching NE)* transports data and signaling messages between the Voice over Packet Switching NEs. The Packet Switching NEs may support IP routed flows and/or ATM virtual connections. The CCA uses an IP interface or an ATM interface to the Packet Switching NEs for transport of signaling and to control traffic. The following capabilities exist within the Packet Switching NEs:
  - The Packet Switching NEs support the transport of data and control traffic between the VOP NEs.
  - The Packet Switching NEs support ATM virtual circuits and/or IP routed flows
  - The Packet Switching NEs support IP and/or ATM interfaces to transport signaling messages (call control).
  - The Packet Switching NEs offer services over facilities with controlled access, i.e., appropriate security mechanisms.

10 NGN RELIABILITY MODELING CHALLENGES

10.1 Overview

Of particular concern is the effect of human interaction on reliability of individual systems and the network as a whole. Recent studies indicate that failures resulting from procedural errors in existing

voice networks are increasing. The rapid roll-out of new technologies and services to meet customer needs constantly introduces new equipment and processes into developing networks. The new equipment and the processes needed to manage them demand the consideration of a learning curve as technicians learn proper operational procedures. New architectures such as the VOP/NGN are particularly susceptible to this reliability problem. Consequently, reliability models for the VOP/NGN elements should capture the frequency and impact of procedural errors in their estimates. The models must reflect:

- Probability of error as a function of the ease-of-use and the craft-person skill level, the frequency and complexity of the task, the prevention attributes (e.g., command confirmation), and any error tolerance such as auto-image fail-back.
- Impact based on the type of NE, the NE state.

Of course, failures may result from intentional as well as unintentional human interactions with network elements. Failure modes should also include the effects of sabotage and vandalism on network elements. Robustness in network design may reduce the impacts of such failures as well as their frequency.

Besides the reliability of individual network elements, failures may result from interoperability design errors between network elements. Even when standards are established, equipment suppliers to the VOP/NGN may have incomplete or incompatible interpretations. This problem is exacerbated by the likelihood that equipment from multiple suppliers will be needed to make the VOP/NGN architecture a reality. Interoperability testing will eliminate most of these errors, but it is likely that some will remain especially in the early stages of the network's existence. Models for such errors should be developed and allowance for early reliability problems should be considered in the implementation phase of the VOP/NGN life cycle.

10.2 NGN Reliability and Availability Models

A common aspect of reliability for an individual network element is its availability. The *availability* of a system is the probability that the system performs a required function at a given instant of time. *Unavailability* (i.e., the complement of availability) is commonly expressed as the long-term fraction of time that the system fails to perform as intended. In many applications, unavailability is expressed as cumulative downtime per year, which is the long-term average amount of time (e.g., minutes) during a year that a system is unable to provide service. Unavailability can also be weighted, typically (though not exclusively) by the number of customers affected by the loss of service. In this way, reliability models may include the effects of service demands that vary by time-of-day or by geographical location.

Since a network failure rarely results in a total loss of services supported by the network, an aspect of reliability of particular import to networks is *survivability*, which quantifies the performance capabilities of a network under network failure conditions. Measures of impact of service loss on customers may be developed based on failure attributes such as duration, time of failure, and number of customers affected.

A comprehensive reliability model needs to be developed specifically for each of the functional elements in the VOP/NGN architecture. Based on this reliability model for the element, reliability standards for various components of the element may be specified. While reliability standards on

individual elements go a long way to managing overall network reliability, separate reliability standards for network segments and the network as a whole should also be established. Network reliability standards may be based on failure frequency, measurable impact attributes, or an index calculated from various impact measures. Reliability standards may establish thresholds for various measures of service loss in order to define when network failures are serious enough to be counted as a service outage.

Developing models for individual network elements is only the first step. These models must then be combined into a reliability model for the NGN as a whole. The model must have the capability to be applied at two levels: 1) the network level; and 2) the service level. It should provide predictions of reliability, availability, survivability, and effectiveness for the NGN and VOP service over the NGN.

10.3 Failure Modes

Reliability standards should consider carefully the various failure modes to be encompassed. The decision of which failure modes to include may depend on perceptions of potential customer expectations for reliability. If it is expected that customers will use the VOP/NGN as a replacement for existing wireline networks, it is probable that customers will expect reliability comparable to that delivered currently by the wireline networks. If this level of reliability is to be delivered, models for the frequency and impact of failure events on the VOP/NGN should be developed. In addition, reliability analyses should incorporate repair and maintenance models to represent the mitigating effects of best practices and proper network support. The generic standards will be developed to preserve continuity with existing standards in wireline telephony.

If the VOP/NGN delivers price or service advantages beyond those of existing wireline networks, customers may be willing to relax their reliability expectations to obtain those advantages. It is the prerogative of individual VOP/NGN service providers to decide on their level of adherence to standards to meet their perception of customer expectations. Such providers do so at their own risk.

The packetization of voice for transport over a data network provides new failure modes from the customer's perspective. In wireline voice telephony, outside of transmission quality, there is little that can go wrong from the customer's viewpoint once the call is setup. Data transport of voice packets creates a host of new possibilities. Packets can be misrouted or lost creating gaps in speech. Packets may be placed out of sequence creating confused speech or conversation without logical flow. The most likely problem would be delay of packets, which could make conversation unacceptably difficult. Such delay occurs when a portion of the network is overloaded by traffic. Assuming proper traffic engineering has been performed, such overloads have the greatest likelihood of occurrence when a portion of the network has failed.

Thus, VOP/NGNs are susceptible to a type of reliability-attributed service loss not seen in wireline networks. Reliability standards should establish thresholds for delay and loss of speech packets to identify when service quality is sufficiently poor that service may be considered lost from the customer's perspective. Reliability models for the frequency and impact of failures of network elements should be created to encompass these effects.

A VOP/NGN will support multiple services. The distributed nature of the VOP/NGN architecture allows multiple services to be supported by and shared by the same equipment. Understanding the interdependency of services on shared equipment is vital to the analysis of failure modes and the way these failure modes can impact multiple services. The importance of different services may necessitate the development of different reliability objectives on a per-service basis.

10.4 Software Reliability Models

Proper functioning of any telecommunications network places a heavy responsibility upon the software controlling its network elements. Over the years, this has become increasingly true of wireline networks, and this responsibility is expected to be even greater in a VOP/NGN. In a wireline network, no software involvement is necessary to support most calls between the completion of call setup and the initiation of call release. In contrast, a VOP/NGN must provide software support to every call throughout the duration of the call. Software should control the correct creation, routing, delivery, and sequencing of each voice packet.

Software reliability prediction models should be developed to predict failure rates from design and implementation faults in the software. A prediction of reliability is an important factor in selecting equipment for use by telecommunication service providers. In the past, such a statement concerning reliability has implied hardware reliability. Software reliability prediction models have not achieved the level of maturity established by hardware reliability prediction models.

Most software reliability prediction models are based on the premise that software failures are the result of a Non-Homogeneous Poisson Process (NHPP). With the choice of a variety of possible failure intensity functions, NHPPs provide a rich source of models for software reliability prediction. The standard use of software reliability prediction models is to predict the growth of reliability in the software as it is exposed to use in the laboratory or in the field. While useful, such models do not address the critical period when software is first used in the field. However, using additional data from prior experience, characteristics of the software, and characteristics of its development process, software reliability predictions can be made prior to general availability. Based on these principles, Telcordia GR-2813-CORE "Generic Requirements for Software Reliability Prediction" provides a starting point for developing the models needed to understand software reliability in VOP/NGNs.

The substantially greater reliance on software makes the VOP/NGN especially susceptible to failures resulting from computer viruses; such a virus could have a potentially devastating effect on the VOP/NGN through its widespread dissemination via the network itself. Reliability analyses would need to model such a virus and its effect in order to understand potential impacts on standards.

10.5 Modeling Summary

The focus of Reliability-related modeling has been on equipment reliability that feeds into system availability modeling via failure modes analysis. Because of impact of software reliability and procedural errors in NGN, prediction modeling needs to be enhanced to include these to predict end-to-end Service Downtime for NGN systems.

Annex A

A DATA ELEMENTS FOR REPORTING CYBER AND PHYSICAL EVENTS AFFECTING TELECOMMUNICATIONS NETWORKS

A.1 Introduction

Presidential Decision Directive (PDD) 63: "Protecting America's Critical Infrastructures" called for the creation of a private sector Information Sharing and Analysis Center (ISAC) to gather, analyze, appropriately sanitize and disseminate information regarding vulnerabilities, threats, intrusions, and anomalies from the private sector to both industry and the National Infrastructure Protection Center. Since the issuance of PDD-63 in May 1998, several ISACs have been established (e.g., banking and finance, telecommunications, and government).

The National Coordinating Center (NCC) for Telecommunications was designated as an ISAC for telecommunications in January 2000. The NCC-ISAC has developed a collection of automated systems and tools, collectively known as the Information Sharing and Analysis System (ISAS), to facilitate the collection, analysis, and exchange of information on vulnerabilities, threats, intrusions, and anomalies affecting the telecommunications infrastructure. To achieve full operating capability as an ISAC, a minimum set of data elements must be considered for reporting cyber and physical events affecting telecommunications networks. The following section addresses those data elements identified by the NCC-ISAC that should be considered when collecting reports on physical and/or cyber events affecting telecommunications. This set of data elements may serve as a model or starting point for other entities wishing to develop similar information sharing and analysis functions.

A.2 Discussion

Data elements that should be considered when automating collection, analysis, and dissemination processes intended to support a real-time information sharing and analysis function may be grouped into five (5) main categories:

1. Administrative information;
2. Event description;
3. Problem diagnosis;
4. Reconstitution and recovery; and
5. External reference information.

For each category, data classes are identified, from which data elements common to all event reports (with the exception of problem diagnosis) may be derived.

- *Administrative information:* Reporting organization, date and time stamps, security and proprietary classifications, and sharing constraints.

- *Event description:* Name and description of the event, severity, impact, and hardware and software involvement.
- *Problem diagnosis:* Information specific to the diagnosis of individual events (i.e., technology-specific information).
- *Reconstitution and recovery:* Restoration status, estimated restoration time, corrective actions taken, and recommendations.
- *External reference information:* Information collected from a variety of external sources (e.g., other Government agencies, private industry, open sources).

Figure A.1 provides a summary of recommended data elements for the first four (4) data categories.

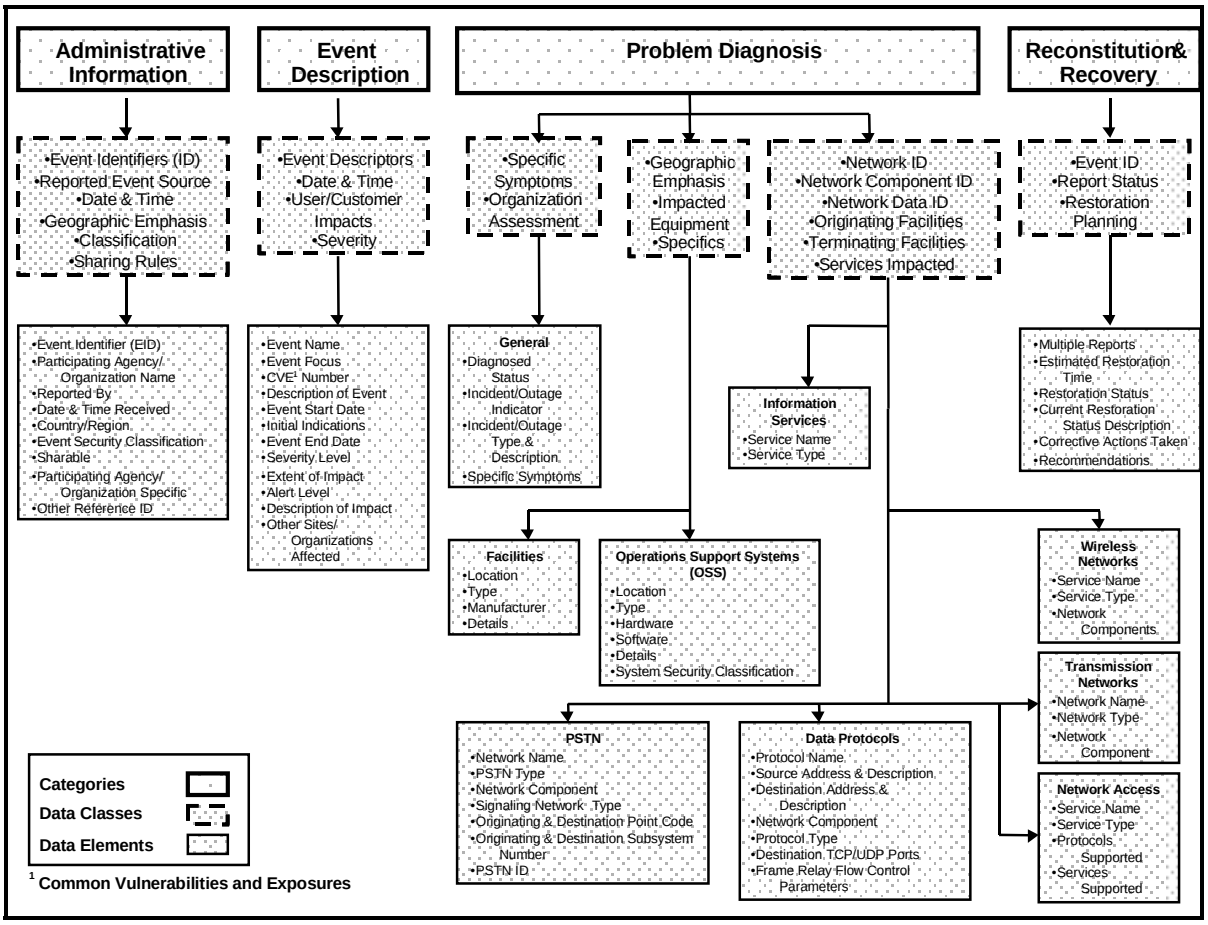


Figure A.1 - Data Elements

Finally, any effort to fulfill an information sharing and analysis function must also consider the receipt of external reference information. Table A.1 describes external reference information that can be leveraged to support data mining and advanced analyses.

Table A.1 - External Reference Information

• Open source information (e.g., periodicals/publications, listservs)
• Threat and vulnerability information (*e.g.,* advisories, hacker publications)
• Other Government information (*e.g.,* law enforcement investigative data alerts and bulletins, intelligence feeds, all-hazard feeds, outage reports)
• Ad hoc sources
• Vendor information
• Information from other ISACs
• Participant information

The correlation of events and analysis allows the NCC-ISAC to provide an indications and warning capability. To provide value and accomplish the ISAC function, the collection of data elements must facilitate analysis and make correlation activities easy to perform. Many of the data elements identified in Figure A.1 are particularly important to capture because they may be used to facilitate correlation with other events and support analysis functions.

Collecting identified data elements from the telecommunications industry may present challenges. For example, gathering the requisite data elements may be affected by the following factors:

- Availability of automated tools;
- Corporate culture;
- Multiple reporting requirements;
- Insufficient/inadequate legal protections (i.e., absence of non-disclosure agreements, sharing rules/procedures);
- Time constraints (i.e., real-time versus non-real-time); and
- Return on investment/benefit received (*e.g.,* analysis is not of sufficient value to supplier of data compared to cost expended).

Additional legal, policy, and/or operational factors may affect the collection of data today and in the future. These factors must be considered as new technologies emerge and the amount and type of data required to fulfill an information sharing and analysis function change.

A.3 Summary

This appendix provides an example of data elements that should be considered when collecting data on cyber and physical events affecting the telecommunications infrastructure. These data elements help to ensure that the data collected can yield meaningful results when analyzed and that these results will be valued by participants who are sharing information within the information sharing and analysis framework.

Annex B

B Approach to Set End-to-End Reliability/Availability Requirements for Next Generation Networks

B.1 Introduction

The Next Generation Network (NGN) is a multi-service packet-based network that will provide both wire line and wireless telephony services. Currently ILECs and network vendors are re-using large telephone switch reliability requirements and applying them to many types of network elements in Voice over IP (VoIP) and Voice over ATM (VoA) network solutions regardless of the impact of their failure modes. The issues with this approach are:

- Product requirements reflect a PSTN design strategy of highly fault tolerant products based on a large telephone switch architecture. However, packet-based products vary in size and function, deliver multiple applications, use packet-based protocols that are more tolerant to failure, and are deployed in a network rich in networking fault tolerant and architecture capabilities.
- Product-only requirements have no influence over how the network is designed so that it is possible that each network element may meet product requirements while the network may not meet end-to-end service reliability expectations of customers (or conversely over-designed).
- Product requirements have been a mixture of 'black-box' requirements (what) and 'white-box' specifications (how), thus inhibiting design innovation to satisfy the requirements.
- Product requirements are defined in terms that are not readily translated into design requirements.

B.2 Discussion

The PSTN product reliability requirements assume specific network and product architectures and technologies. System downtime of 2 minutes per year for a telephone switch equates to a network outage downtime affecting a specific group of users (~ 30,000 – 50,000). Thus, it is not appropriate to apply this system downtime requirement to all products. Downtime requirements for access networks should be specified based on failure mode impact. Product requirements can then be determined based on the product size and the network design strategy.

The PSTN requirements are set to be very stringent because of the criticality of the service and as well as high hardware failure rates of the past. For example, matched processors were required for a switch using central control in order to guarantee that large numbers of calls would not be dropped when control and memory hardware failed. The need for this design strategy diminishes as the impact and frequency of failure diminishes. As well, most packet technologies will not drop a call if the fail-over is not lighting fast…but this would result in some delay.

There is risk of over-specifying many of the VoIP products if the industry simply applies the large telephone switch requirements. For other cases, there is danger of under-specifying. For example, the PSTN per trunk downtime requirement of 12 minute per year was originally set for a DS1 trunk.

Apply it for a Gigabit Ethernet port where the impact is much more significant, and this could under-specify the requirement.

B.3 Proposal

The proposal (Figure B.1) is to specify "black-box" or outward-bound requirements (customers); linked to the "white-box" or inbound requirements (design and measurement). For the latter, these requirements are "generic, which is product independent. They are specified for failure modes, thus allowing the designer more latitude on *how* to satisfy the requirements.

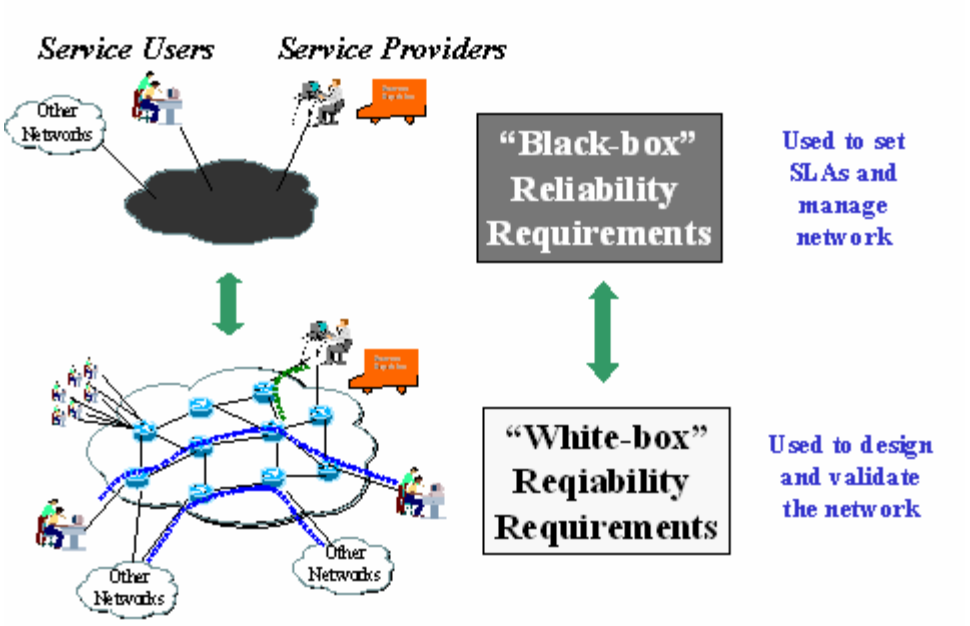


Figure B.1 - Network Reliability/Availability Requirements

The following example is used to illustrate the requirements proposal. The requirements are set for illustration purposes only.

B.4 Illustration

B.4.1 High Availability IP Service Use Access

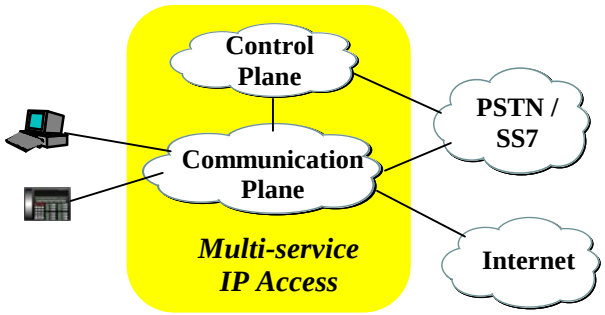


Figure B.2 - Network Solution Overview

Table B.1 - End-to-end Network Solution Requirements

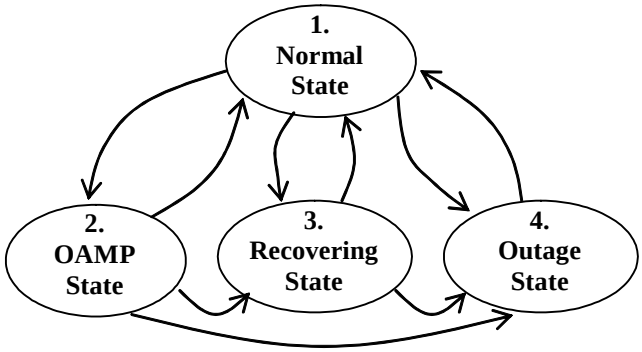
Service: Voice over IP Access	**Business Driver:** Best-in-class service reliability to win market share.	
Network Solution: Access to the PSTN for voice using Succession.		
Service Reliability		
Metric	**Objective**	**Units**
Individual subscriber voice service downtime	15	minutes per year
Individual subscriber defective calls	35	per 10^6
Critical downtime (specific group of > 30,000 < 50,000 users)	2	minutes per year
Major downtime (specific group of > 10,000 < 30,000 users)	5	minutes per year
Minor downtime (specific group of > 1000 < 10,000 users)	10	minutes per year
OAMP Reliability		
Metric	**Objective**	**Units**
Loss of Billing downtime	3	minutes per year
Loss of diagnosability (NOC to any network element)	30	minutes per year

Conditions:

1. The outage criteria for multi-user service outages is where users cannot initiate new service sessions or established sessions for periods > 10 seconds.
2. The outage criteria for OAMP outages is where operators cannot operate a feature or an alarm display delay for periods > 30 seconds.
3. The individual subscriber outage criteria is where the user cannot initiate new service sessions or the establish session for periods > 10 seconds.
4. These requirements are to be met for unattended equipment assuming an MTTR of 4 hours, including travel for the useful-life period (after 3 months from cut-over) and for 24x7.
5. The requirements include planned and unplanned causes attributed to the network vendor's equipment: all hardware and software failures, normal OAMP activities and cable cuts of 0.2/100km/yr.
6. The planned OAMP activities are assumed to be two per year per network element.

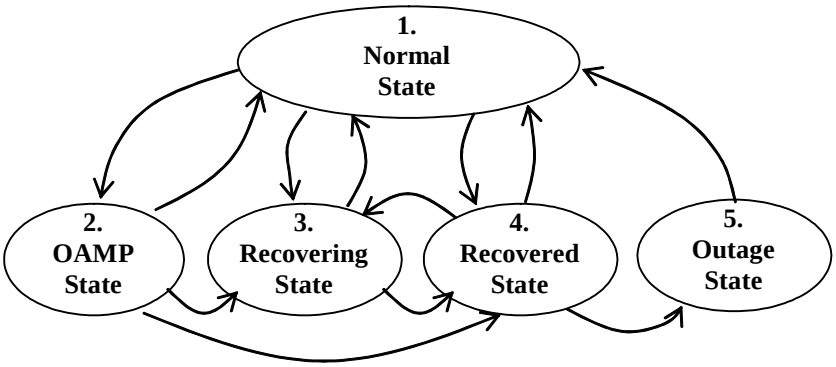
B.5 Network Design Requirements

Failure Mode: Affecting < 1000 subscribers



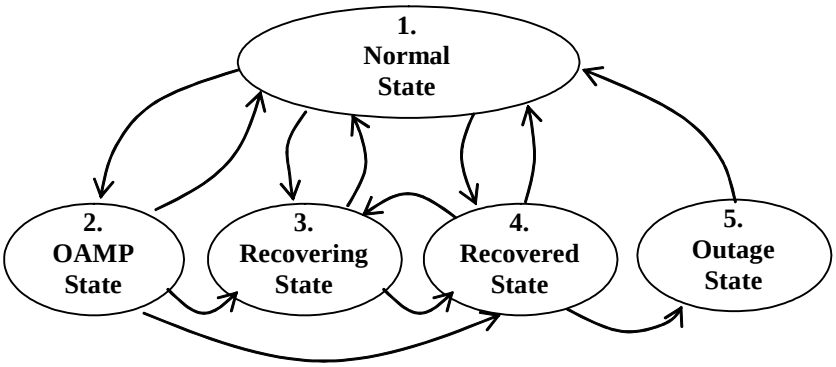
State / Transition	Design Requirements
State 1	User-initiated self test with hardware & software failure coverage >90%. No impact on service from management commands & queries.
State 2	Software upgrade impacts subscribers for < 90 seconds. Software patch application impacts subscribers for < 90 seconds. Hardware upgrades impact subscribers for < 15 minutes.
State 1 to 3	Software failure rate average < 0.01 / year. 99% software failure detection.
State 3	Recovery < 90 seconds. New and existing service sessions impacted.
State 3 to 1	100% of detected software failures return successfully. Failure event logged.
State 1 to 4	Hardware failure rate < 0.2 per year. No procedural or software failures.
State 4	90% of hardware failures isolated to the replaceable unit.
State 4 to 1	90% of repair actions < 30 minutes.

Failure Mode: Affecting 1000-10,000 subscribers



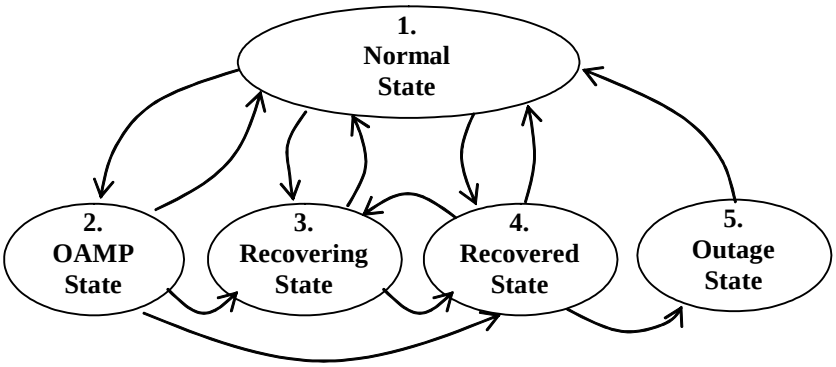
State / Transition	Design Requirements
State 1	Hardware protection minimizes capital costs. Automatic non-service-affecting background tests at >90% coverage. No impact on service from management commands & queries. Recovers without impact on established service for traffic overloads > twice specified capacity.
State 2	Software upgrade impacts subscribers for < 30 seconds. Failed software load insertions < 1%. Automatic recovery to previous software release. Hardware upgrades impact subscribers for < 30 seconds.
State 1 to 2 to1	OAMP commands are fail-safe to ensure no procedural-caused outage.
State 1 to 3	99% software failure detection, frequency < 0.15 per year.
State 3	80% of software failure rate automatically recovers < 30 seconds. 95% of software failures recover < 5 minutes. New and existing service sessions impacted during recovery
State 3 to 1	100% of detected software failures return successfully. Failure event logged.
State 1 to 4	All common hardware duplicated with 95% of the hardware failure rate recovers in less than 90 seconds.
State 4	Performance meets specified QoS requirements. 90% of hardware failures isolated to the replaceable unit without impact on service.
State 4 to 5	100% detection and alarming of hardware failures.
State 5	90% of hardware failures isolated to the replaceable unit.
State 5 to 1	90% of repair actions < 30 minutes.

Failure Mode: Affecting 10,000-30,000 subscribers



State / Transition	Design Requirements
State 1	Hardware protection minimizes capital costs. Automatic non-service-affecting background tests at >90% coverage. No impact on service from management commands & queries. Recovers without impact on established service for traffic overloads > twice specified capacity.
State 2	Software upgrade impacts subscribers for < 30 seconds. Failed software load insertions < 1%. Automatic recovery to previous software release. Hardware upgrades impact subscribers for < 30 seconds.
State 1 to 2 to1	OAMP commands are fail-safe to ensure no procedural-caused outage.
State 1 to 3	99% software failure detection, frequency < 0.15 per year.
State 3	80% of software failure rate automatically recovers < 30 seconds. 95% of software failures recover < 5 minutes. New and existing service sessions impacted during recovery.
State 3 to 1	100% of detected software failures return successfully. Failure event logged.
State 1 to 4	All common hardware duplicated with 99% of the hardware failure rate recovers in less than 10 seconds.
State 4	Performance meets specified QoS requirements. 90% of hardware failures isolated to the replaceable unit without impact on service.
State 4 to 5	100% detection and alarming of hardware failures.
State 5	90% of hardware failures isolated to the replaceable unit.
State 5 to 1	90% of repair actions < 30 minutes.

Failure Mode: Affecting 30,000-50,000 subscribers



State / Transition	Design Requirements
State 1	Hardware protection minimizes capital costs. Automatic non-service-affecting background tests at >90% coverage. No impact on service from management commands & queries. Recovers without impact on established service for traffic overloads > twice specified capacity.
State 2	Software upgrade impacts subscribers for < 10 seconds. Failed software load insertions < 1%. Automatic recovery to previous software release. Hardware upgrades impact subscribers for < 10 seconds.
State 1 to 3	99% software failure detection, frequency < 0.05 per year.
State 3	80% of software failure rate automatically recovers < 10 seconds. 95% of software failures recover < 3 minutes. New and existing service sessions impacted during recovery.
State 3 to 1	100% of detected software failures return successfully. Failure event logged.
State 1 to 4	All common hardware duplicated with 99.9% of the hardware failure rate recovers in less than 1 second without impact on new and existing services.
State 4	Performance meets QoS requirements. 90% of hardware failures isolated to the replaceable unit.
State 4 to 5	100% detection and alarming of hardware failures.
State 5	90% of hardware failures isolated to the replaceable unit.
State 5 to 1	90% of repair actions < 30 minutes.

Annex C

C RELIABILITY OBJECTIVES RATIONALE FOR NEXT GENERATION NETWORK ELEMENTS

C.1 Introduction

C.1.1 Intent

Provide the background and rationale for a reliability standard for Next Generation networks elements used in access networks.

C.1.2 Context

Consistent, well-implemented Network Element (NE) reliability features are fundamental to the fault tolerant networks to which they are deployed. These features are both internal to the element (intra) and external, between neighboring elements (inter).

The proposed standard is to be used to specify design requirements so that:

- Vendors can consistently design-in key reliability attributes; and
- Carriers can audit key aspects of the design to verify design compliance and minimize introduction risk.

The standard is also used to align RQMS field performance targets to ensure consistency between input to design and improvement to existing NE via field tracking programs (Figure C.1).

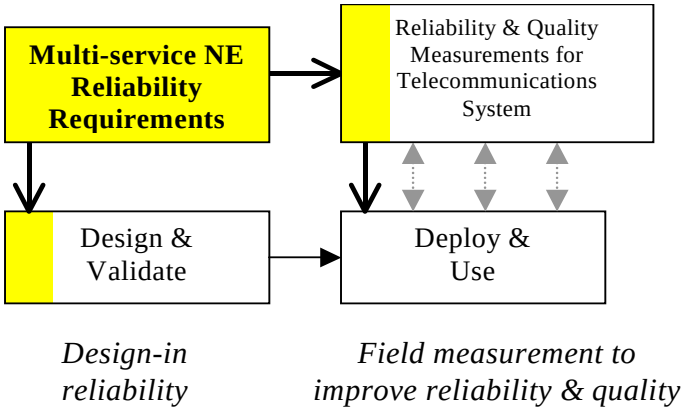


Figure C.1 - NE Reliability Overview

C.1.3 Scope

The proposed NE Reliability standard covers NE reliability measures addressed by the RQMS as well as other metrics in order to cover all end-to-end NE failure modes. In addition, the standard covers key aspects of the NE reliability development program required to achieve them.

Figure C.2 contrasts the scope of the proposed standard and the RQMS/TL9000.

The RQMS/TL9000 focus is a set of NE reliability and quality measurements used for field tracking in order to drive corrective and preventive programs. It also defines the underlying quality system (process requirements) used to develop, deploy, and support the NE. However, the RQMS performance measures do not cover the complete scope required to design reliable NE's and networks. It addresses the more critical service-affecting outages and NE field quality (predominantly software field quality).

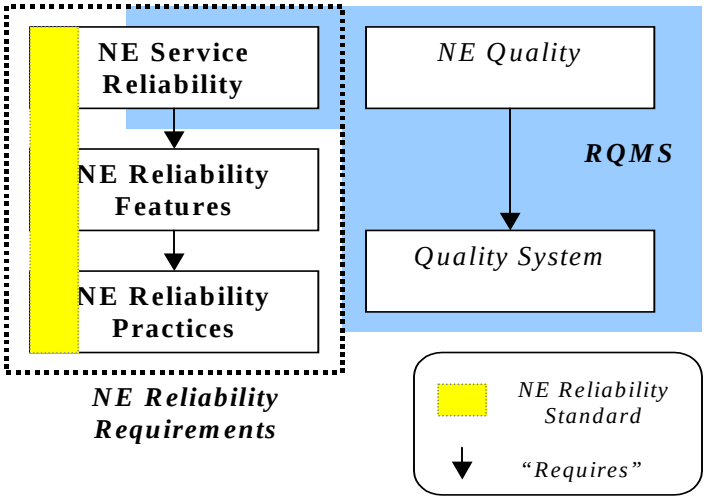


Figure C.2 - NE Reliability Requirements and RQMS/TL9000

C.1.4 Motivation

The PSTN Network Element (NE) switching reliability requirements have been dominated by those for large TDM switches in the context of the PSTN architecture, TDM technologies and voice application that is considered "mission-critical. Fault tolerance adds cost to network elements; therefore, selective application is required to ensure the investment meets service reliability/availability expectations at minimum cost. Too stringent requirements for the NE size and function may result in over-designed, costly network elements making NEs unnecessarily complex. Conversely, less stringent requirements may result in under-designed network elements requiring excessive costly networking to meet end-to-end service downtime expectations.

The drivers for a revision of network element reliability/availability requirements for the next generation network are:

- *Multi-service, packet-based network*: The service applications range from mission-critical to non-critical services each with different customer reliability expectations, and from real-time

interactive to non-real time non-interactive each with different thresholds of failure. This drives different NE reliability feature requirements.

- *Technology failure rates continue to decrease*: Both hardware and software failure rates continue to decrease reducing the value for fault tolerance. When the LSSGR Section 12 requirements were set, hardware failure rates on a functional basis were two orders of magnitude higher. This drove requirements for hardware duplication in the peripherals that can be achieved with today's technologies without duplication.

- *Network Element size continues to increase*: With more hardware integration, the size and therefore the impact of system outages is getting bigger, thus increasing the revenue risk for Service Providers.

- *More degrees of design freedom to protect service via networking*: The network designer has a broader range of network architectures and protection/restoration technologies to mitigate or mask the frequency, duration, and impact of network element failure modes.

- *Network designers need reliability-optimized NE's that they can depend on*: In recent years, NE requirements have been driven by the RQMS, whose focus is to specify the critical failure modes and software quality metrics that are readily measurable in the field. Post-introduction tracking has driven "intra-NE" quality and reliability. These metrics do not cover all NE reliability aspects required to design reliable NEs and networks -- such as Input/Output (I/O) ports and networking features. A more comprehensive set of reliability requirements are needed as input into design, to ensure both improved NE and network reliability at introduction.

C.2 Network Element Types

C.2.1 Concept

This proposal defines different levels of NE fault tolerance based on the "revenue risk" of their failure modes. This is similar to the PSTN where PSTN products' level of redundancy varies depending on product role, size complexity and failure mode impact.

Figure C.3 illustrates the concept as applied to a Next Generation access network. The dotted line represents the NE total system downtime of for a "basic" NE (no hardware duplication – only auto-detect and recover from transient failures). As a result, the downtime increases as the complexity and size of the NE increases. The solid (green) line represents the PSTN downtime profile users have grown to expect.

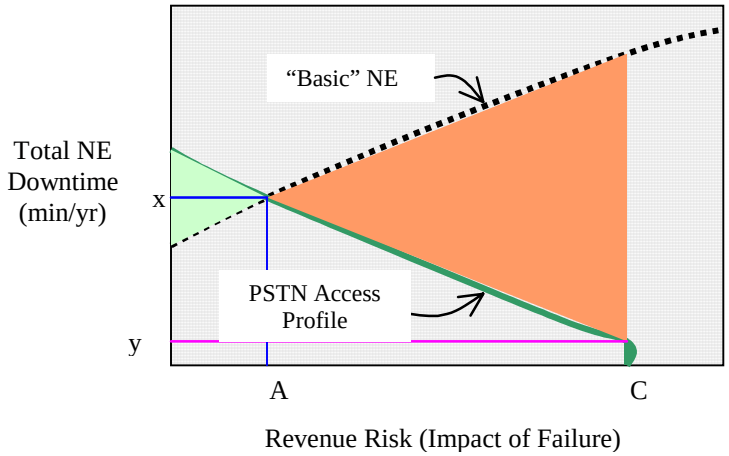


Figure C.3 - Fault Tolerance and Revenue Risk

The intersection at failure impact "A" represents the point where fault tolerance is required in order to meet customer expectations. As the revenue risk increases after A, there is a need for increasing levels of fault tolerance. For the PSTN "y" was 2 minutes per year and "C" was typically 50,000 subscribers.

To better illustrate the concept, consider an edge NE that provides L3 routing for 6 customer ports that is aggregated to a single 30Gbps Router that interfaces to the core network.

For the edge router, the system failure mode affects six customers at 15 minutes per year. The impact of its downtime is 90 customer-minutes per year. Assuming an average revenue loss of $5K per minute per customer, the revenue risk is $450K per year per NE and for the solution; it is $450M per year. The 30Gbps Router's system downtime is 5 minutes per year and without network redundancy its system outage would affect 6,000 customers resulting in a customer impact of 30,000 customer-minutes per year or $150M per year. The Solution cost to reduce the small router's revenue risk by $200M by providing carrier-grade duplication is $10M – a 20:1 return on investment. For the Terabit router the solution cost to reduce the revenue risk by $145M is only $1M - 145:1 return on investment.

C.2.2 Network Element Definitions

Figure C.4 illustrates the three types of NE's and their location in the network: Low Revenue Risk (LRR), Medium Revenue Risk (MRR), and High Revenue Risk (HRR). All types share a common set of reliability and maintainability capabilities and level of quality. However, they differ by the increasing levels of fault tolerance, both intra- and inter- NE (e.g., network protection).

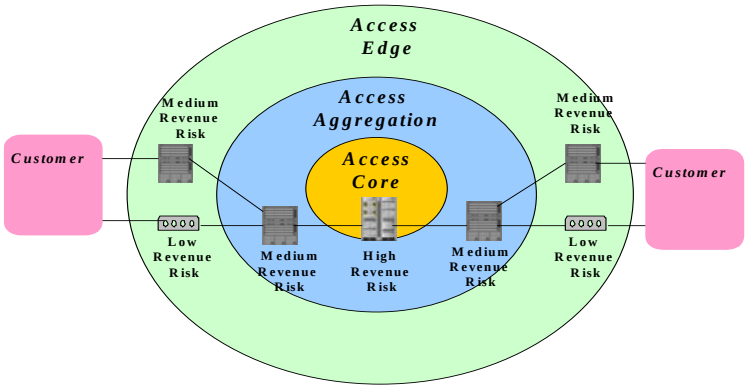


Figure C.4 - Network Element Types

LRRs typically are used at the access network edge and employ basic fault tolerance, MRRs are used at the edge and at the various aggregation levels of the access network and because of their increased revenue risk have increased fault tolerance. The HRRs, typically used to interface to the backbone core, require the highest level of fault tolerance.

It is anticipated that these three levels are sufficient to provide the network designer with enough flexibility to optimize network designs for end-to-end reliability performance.

Table C.1 summarizes the key attributes for the NE types.

Table C.1 - NE Types

Attribute	**Low Revenue Risk**	**Medium Revenue Risk**	**High Revenue Risk**
Access Network Application	Edge NEs for access networks	Edge and first level aggregation for access networks	Core NE in access networks or where networking is not possible for service protection
Requirements Drivers	Relative high volume and low revenue impact of failures drives low cost design strategies	Moderate volume and revenue impact of failures warrants added fault tolerance investment to mitigate revenue risk	Low volume and high revenue impact of failures warrants significant fault tolerance investment to mitigate revenue risk
Intra-NE Fault Tolerance	External power & auto-software failure recovery	System hardware duplication requiring re-start to recovery	No impact hardware duplication with graduated software recovery
Hardware & software reliability Fault Management	Common for all NE types		

C.3 Illustration

To illustrate the application of using the NE types to design an access network, an Optical Ethernet Solution is presented. The design must provide 100BT Ethernet services to multi-and single tenant buildings and offer a range of customer access availability for the Optical Ethernet service. Also Network outages greater than 100 customers should be less than 0.5 minutes per year (99.999% availability). The reliability performance of the three types of NE's are:

Table C.2 - NE Reliability Performance

Metric	Objective			
	LRR	MRR	HRR	Units
Total NE Outage Downtime	15	2	0.5	Minutes per year per NE
Unscheduled	12	1	0.5	
Scheduled	3	1	0.0	

The network design comprises customer premises Optical Ethernet devices that present 100BT ports to customer equipment. These devices are either LLR or MRR NE's depending on the number of customers or amount of bandwidth in the building. The first level of aggregation uses MRR-level L2 switches. Layer 2 highly resilient collector rings are used to collect the local traffic and transport it to either its intra-ring destination or to the Core via two HRR-level switches to meet the single or multiple ring downtime objective of 0.5 minutes per year.

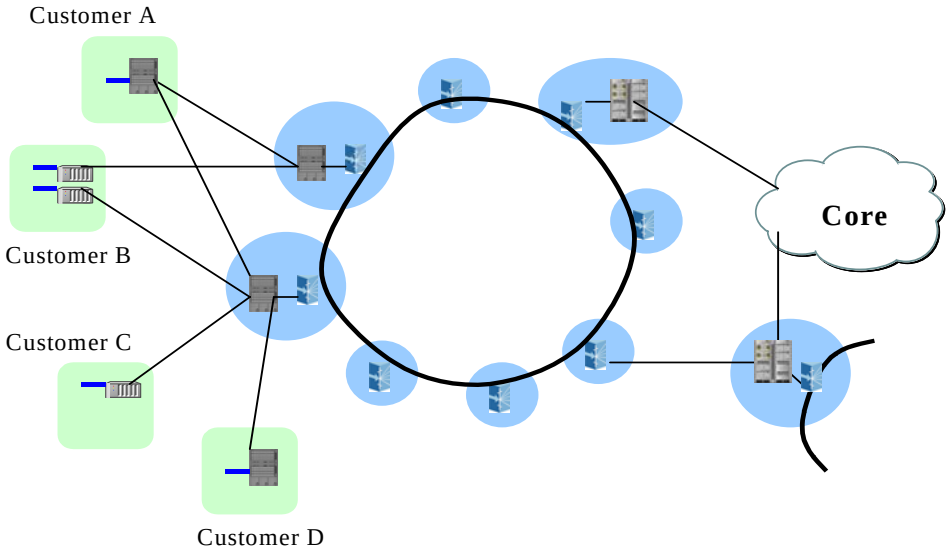


Figure C.5 - Sample Network

The following table summarizes the predictions for the various customers:

Table C.3 - Customer Access Downtime Results

	Service Downtime (min/yr)	**Service Failure Rate** (/10^6)
Customer A	7.2	14.9
Customer B	1.3	2.7
Customer C	25.7	53.7
Customer D	15.7	32.1

The predictions assume that the Vendor has the process capabilities to ensure quality implementation of the reliability features. To illustrate the wide variation that implementation quality can have, Table C.4 compares expected field performance metrics for a mature and ad hoc development practices.

Table C.4 - Mature vs. Ad hoc Development Processes

Reliability Metric	Objective	Mature Practices	Ad hoc Practices
LRR NE Total Downtime	<15	10	55
MRR NE Total Downtime	<2	1.5	18
HRR NE Total Downtime	<0.5	0.5	16
Customer A Access Downtime	<5	7.2	68
Customer B Access Downtime	<5	1.3	28
Customer C Access Downtime	<30	25.7	125
Customer D Access Downtime	<30	15.7	97

NOTE -- Downtimes in “minutes per year.”

The results in Table C.4 can be used to set customer SLAs and for field tracking.