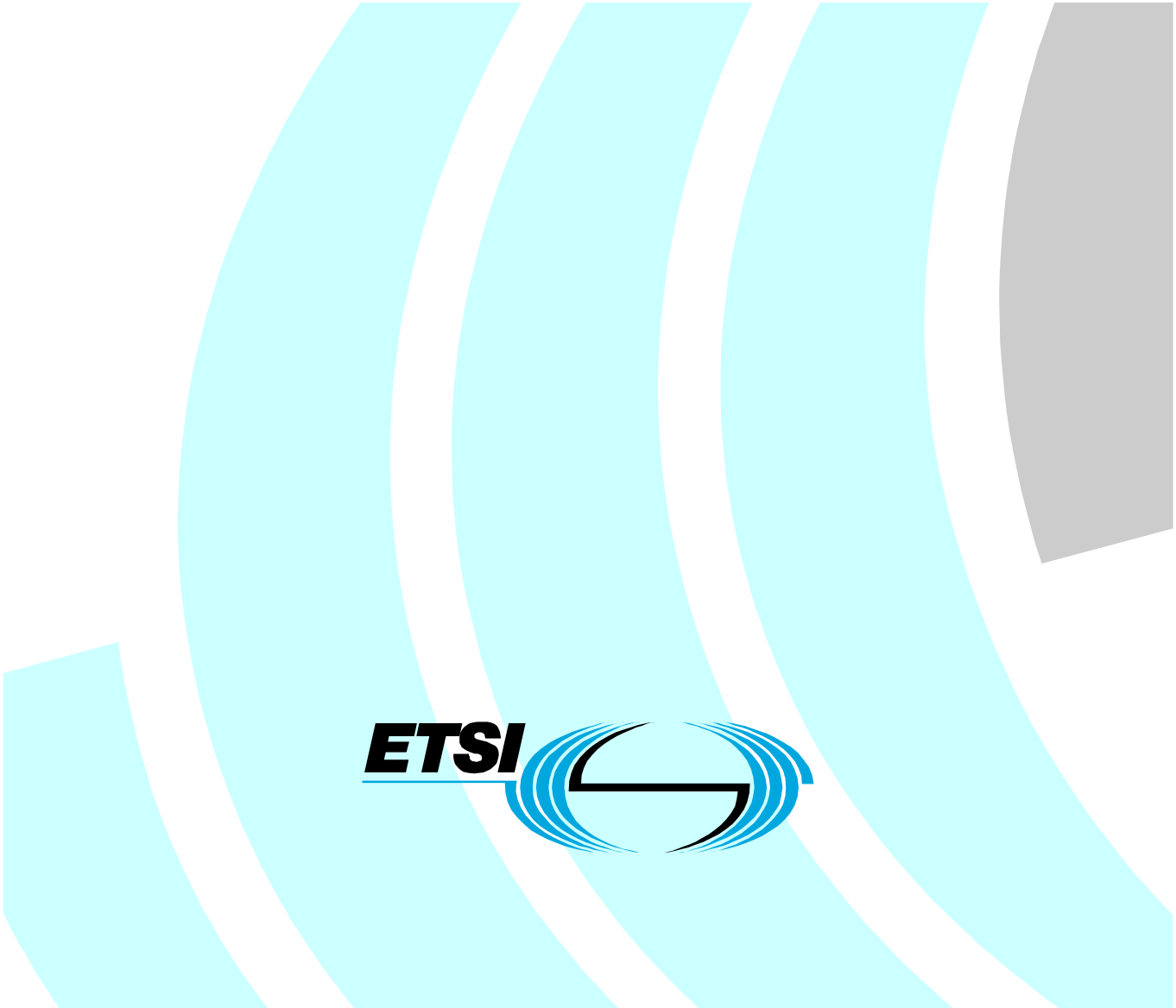
ETSI TR 101 971 V1.1.1 (2003-05)

Technical Report

Access and Terminals (AT); IP Cable Services for Multimedia Broadband Cable Networks; Availability and Reliability



Reference
DTR/AT-020025

Keywords
access, broadband, cable, IP, VoIP, availability, SLA

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://webapp.etsi.org/IPR/home.asp).

All published ETSI deliverables shall include information which directs the reader to the above source of information.

Foreword

This Technical Report (TR) has been produced by ETSI Technical Committee Access and Terminals (AT).

Introduction

The present document addresses reliability/availability of IP-based cable communications networks, including the services provided under failure conditions. It provides a basis for designing and operating such networks to meet user expectations regarding network reliability and service availability.

Network providers need to know that what they are building will deliver the services reliability performance required by end users. Network service providers specify network availability within their own network domains, but end-user services are delivered across multiple domains. If the public carrier networks are to fulfill their promise of service convergence, then a set of reliability metrics and terminology are needed that are common across the industry for which individual network services reliability requirements can be specified.

The intended audience of the present document includes providers of cable communications networks and services (including Internet services), as well as suppliers of equipment and support systems. Network-provider personnel - including designers, planners, traffic engineers, and individuals in charge of operations, administration, maintenance, and management - can use the present document to enhance the performance and survivability of their networks. Equipment and support system suppliers can use the present document to guide the design and building of equipment to improve network survivability performance.

The present document draws heavily on the prior work of ANSI accredited T1 in the context of telecommunications networks (T1 Technical Report 70 [1]).

Clause 2 lists the references, and clause 3 the definitions, symbols and abbreviations. Clause 4 defines an IP network survivability framework. Clause 5 summarizes the formal standards organization involvement with network reliability/availability issues. Clause 6 discusses the service and Network views of IP network reliability performance. Clause 7 describes the network design considerations for survivability. Clause 8 describes and proposes development of a set of guides and metrics for IP based networks and services. Annexes provide further background of work in formal standards organizations.

1 Scope

The present document concerns availability and reliability modeling for IP cable communication networks. Availability and reliability parameters for cable access networks are addressed in the context of end-to-end performance.

The document focuses on the design considerations of IP based networks for survivability. It provides guides for operational measurement and improvement of the reliability/availability of IP based networks and services. It also discusses how to use metrics for the reliability/availability clauses of Service Level Agreements (SLAs). It applies these techniques to cable communications networks. The carrier and data network industries, both service and equipment providers, are familiar with Service Level Agreement (SLA) and Quality of Service (QoS) objectives. The present document provides common analysis that both parties will understand and can use to improve interworking and performance for all end users.

2 References

For the purposes of this Technical Report (TR) the following references apply:

[1] T1 TR.PP.70: "A Reliability/Availability Framework for IP-based Networks and Services".

[2] ITU-T Recommendation E.436: "Customer Affecting Incidents and blocking Defects Per Million".

[3] Void.

[4] ITU-T Recommendation I.350: "General aspects of quality of service and network performance in digital networks, including ISDNs".

[5] Void.

[6] Jim W.Roberts: "Traffic Theory and the Internet" IEEE Communications Magazine, January 2001, pp. 94-99.

[7] T1.TR.11: "Switched Exchange-Access Network Traffic Availability Performance".

[8] Telecordia GR-929-CORE: "Reliability and Quality Measurements For Telecommunications Systems (RQMS-Wireline)".

[9] Telecordia Technologies SR-332: "Reliability Prediction Procedure for Electronic Equipment".

[10] Telecordia (Bellcore) Special Report SR-TSY-001171: "Methods and Procedures for System Reliability Analysis".

[11] Telecordia GR-2813-CORE: "Generic Requirements for Software Reliability Prediction".

[12] Telecordia SR-TSY-001547: "The Analysis and Use of Software reliability and Quality Data".

[13] T1.TR.55: "Reliability and Survivability Aspects of the Interactions Between the Internet and the Public Telecommunications Network".

[14] T1.TR.68: "Enhanced Network Survivability Performance".

[15] Void.

[16] Nader Mehravari: "Queueing Theory".

[17] Jose A. Rueda: "Telecommunication Traffic".

[18] ETSI TR 101 963: "Access and Terminals (AT); Report on the Requirements of European Cable Industry for Implementation of IPCablecom Technologies; Identification of high level requirements and establishment of priorities".

[19] IETF RFC 3272: "Overview and Principles of Internet Traffic Engineering", D. Awduche, A. Chiu, A. Elwalid, I. Widjaja, X. Xiao. .

[20] Atiquzzaman, Mohammed: "Traffic Management and Switching for Multimedia", IEEE Communications Magazine, Vol. 37, January 1999, pp. 30.

[21] Paxson, Vern and Sally Floyd: "Why We Don't Know How To Simulate The Internet" Proceedings of the 1997 Winter Simulation Conference, pp. 1037-1044.

[22] Frost, Victor S. and Melamed, Benjamin:"Traffic Modeling For Telecommunications Networks" IEEE Communications Magazine, March 1994, pp. 70-81.

[23] Floyd, Sally and Paxson, Vern:"Difficulties in Simulating the Internet", IEEE/ACM Transactions on Networking, February 2001.

[24] Awduche, Daniel O.: "MPLS and Traffic Engineering in IP Networks", IEEE Communications Magazine, Vol. 37, No 12, December 1999, pp. 42-47.

[25] Void.

[26] Cáeres, Ramón, Duffield, Nick, Feldmann, Anja, Friedmann, John D., Greenberg, Albert, Greer, Rick, Johnson, Theodore, Kalmanek, Charles R., Krishnamurthy, Balachander, Lavelle, Dianne, Mishra, Partho P. Rexford, Jennifer, Ramakrishnan, K.K., True, Frederick D., and van der Merwe, Jacobus E.: "Network Traffic Measurements and Experiments: Measurement and Analysis of IP Network Usage and Behavior", IEEE Communications Magazine, May 2000, pp. 144-151.

[27] Finsiel, Luca Deri, and Suin, Stefano: "Network Traffic Measurements and Experiments: Effective Traffic Measurement Using ntop", IEEE Communications Magazine, May 2000, pp. 138-143.

[28] Geng-Sheng, Kuo: "Multiprotocol Label Switching", IEEE Communications Magazine, Vol. 37, No. 12, December 1999, pp. 36.

[29] Ghanwani, Anoop, Jamoussi, Bilel, Fedyk, Don, Ashwood-Smith, Peter, Li, Li, and Feldman, Nancy: "Traffic Engineering Standards in IP Networks Using MPLS", IEEE Communications Magazine, Vol 37, No 12, December 1999, pp. 49-53.

[30] Keshav, S., An Engineering Approach to Computer Networking: "ATM Networks, the Internet, and the Telephone Network", Addison-Wesley, Inc., Reading, Massachusetts, 1997, Chapter 2.

[31] Newman, David, Network Computing, "Internet Traffic Management: From Chaos, Order", Vol. 11, No. 11, June 12, 2000, pp. 85-94.

[32] Paxon, Vern, and Floyd, Sally: "Wide Area Traffic: The Failure of Poisson Modeling", IEEE/ACM Transactions on Networking, Vol. 3, No. 3, June 1995, pp. 226-244.

[33] Thompson, K., and Miller, G.J.: "Wide-Area Internet Traffic Pattern", IEEE/IEE Electronic library on-line Nov./Dec. 1997, pp. 10-23.

[34] Zheng, Bing and Atiquzzaman, Mohammed, IEEE Communications Magazine: "Traffic Management of Multimedia over ATM Networks", Vol. 37, January 1999, pp. 33-38.

[35] ETSI TS 101 909-2: "Digital Broadband Cable Access to the Public Telecommunications Network; IP Multimedia Time Critical Services; Part 2: Architectural framework for the delivery of time critical services over cable Television networks using cable modems".

[36] ITU-T Recommendation J.112: "Transmission systems for interactive cable television services".

[37] ITU-T Recommendation E.106: "Description of an International Emergency Preference Scheme (IEPS)", March 2000.

[38] COST 253 ED (98) 002: "Analysis and Modelling of Traffic in Modern Data Communications Networks", G. Babic, B. Vandalore, R. Jain, Ohio State University, Department of Computer and Information Science.

3 Definitions and abbreviations

Also see clause 8.2.

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

access: function required to initiate or request a service

accuracy: degree of conformity of a measured or calculated value to its actual or specified value

alternate routing: routing of a call or message over a substitute route when a primary route is unavailable for immediate use

billing downtime: proportion of time the billing system is either recording incorrect billing data or losing billing

NOTE: The unit of measure is "minutes per year".

call attempt: in a telecommunications system, a demand by a user for a connection to another user

NOTE: In telephone traffic analysis, call attempts are counted during a specific time frame. The call-attempt count includes all completed, overflowed, abandoned, and lost calls.

capital outlay: initial network solution investment required to meet the service requirements of the service users

connectivity: for nodes (or links), the minimum number of nodes (or links) whose removal results in losing all paths that can be used to transfer information from a source to a sink

dead-on-arrival: average percentage of defective delivered hardware, between receipt and solution cut-over

disengagement: function required to terminate access to a service

Downtime Performance Measurement (DPM): an outage downtime metric is the expected long-term average sum, over one operating year, of the time durations of events that prevent a user from requesting or receiving services

NOTE: A failure that causes service interruption contributes to the outage downtime of that service. Outage downtime is usually expressed in terms of minutes of outage per year. See Telecordia GR-929-CORE [8].

duration: amount of time from the onset (start time) of a service outage until its end

end user: person or group of persons making or receiving service request(s)

NOTE: For certain services, identification of the "end user" is not obvious. An example is the 800-type Service. Is the end user the person placing the call, or the person or company receiving and paying for the call? Both parties have an interest in the call attempt's completion, and are end users.)

failure rate (λ): average number of transitions from the available state to the unavailable state per unit available time

fault isolation: percentage of the network element's failure rate that can be isolated to a specified number of hardware repairable units

fault tolerance: extent to which a functional unit will continue to operate at a defined performance level even though one or more of its components has failed

grade of service (traffic): probability of a call being blocked or delayed more than a specified interval, expressed as a decimal fraction

NOTE: Grade of service may be applied to the busy hour or to some other specified period or set of traffic conditions.

IP-based service: end user service that is provided, at least in part, over an IP-based network

layer: in telecommunications networks and open systems architecture, a group of related functions that are performed in a given level in a hierarchy of groups of related functions

maintainability: ability of an item under stated conditions of use, to be retained in, or restored to, a state in which it can perform a required function, when maintenance is performed under given conditions, and using stated procedures and resources

maintenance controlling downtime: proportion of time when a network element cannot be controlled remotely to conduct maintenance activities

NOTE: The unit of measure is "minutes per year".

maintenance costs: costs for planned and unplanned maintenance actions required to ensure that the Service Level Agreements (SLA) are met for each and all of the network services

NOTE: The unit of measure is maintenance costs per unit of service per year.

network availability: probability of success of network functions performed by a network over a specified time interval

NOTE: Network availability is affected by both network congestion due to element unavailability associated with outages, *etc.* and network overload due to insufficient capacity for the volume of service requests associated with traffic engineering, demand surges, etc.

network element: generic term referring to any element residing on a network

network failure: complete or partial failure of a component or components of a network because of malfunction or natural or human-caused disasters

NOTE: Partial failures include degradation.

network outage: one or more service outages instigated by the same network failure

network performance: the level at which a network fulfills its function

network reliability: probability that a network will perform its required function for a specified interval under stated conditions

network restoration: automatic or manual methods to return a network to its normal function in response to a network failure

network service: set of functionalities that a network solution provides to users

network solution: two or more network elements that work as a system to deliver network services to users

network survivability: the (a) ability of a network to maintain or restore an acceptable level of performance during network failures by applying various restoration techniques, and (b) mitigation or prevention of service outages from network failures by applying preventative techniques

network users: end-users and other network owners that use the services of the network

node restoration time: amount of time that it takes to reroute all affected traffic to its original destination, as a result of a "node" failure

path restoration time: amount of time that it takes to reroute all affected traffic to its original destination, as a result of an equipment or facility failure

performance parameter: quality, usually quantified by a numerical value, which quality characterizes a particular aspect, capability, or attribute of a system

NOTE: Examples of performance parameters are jitter, mean time between failures, throughput, and delay.

recurring costs: ongoing costs to own, operate, and maintain the network solution

repairability: percentage of repair actions completed within a designated time *"t_r"*. *"t_r"* is measured from the time the craft person initiates the repair until the system is returned to the pre-failure state

reliability: probability that a functional unit will perform its required function for a specified interval under stated conditions

revenue: income generated from the services satisfying the needs of the service users

service: set of functions or communications capabilities performed by the network at the request of the end user

service attempt: specific instance of an end user attempt to invoke a given service transaction

service availability: state or condition that occurs when the performance of all of a set of selected performance parameters is deemed acceptable

NOTE: The performance of a specific parameter is deemed acceptable if its performance is greater (or lesser) than that of a pre-specified threshold. The entirety of these selected parameters and their thresholds is called the availability function. An availability parameter and its threshold is called an outage criterion. The failure of one or more of these parameters results in a transition to the unavailable state. The available state is re-entered when all parameters are once again functioning acceptably.

service denial: average proportion of service sessions by an individual user that are not successful

service outage: state of a service when (a) a network failure impairs or prevents the initiation of new requests for service, (b) continued use of the service is impaired or not possible, or (c) a certain service falls outside prescribed limits

service outage downtime: proportion of time when "n" users are without the network service or when the network service is of unacceptable quality for duration longer than "t_o" seconds, where "t_o" seconds is the user tolerance threshold for outage

NOTE: The unit of measure is minutes per year. The service impact expressed as "n" users is categorized into network-wide, catastrophic, major, and minor, depending on the number of users impacted.

service reliability: probability that a service will operate without failure in its intended environment over a specified period of time

service request: event in which a user places a demand for a service

service transaction: specific capability provided by the Service (e.g. Dial-Up Modem Session)

service users: end-users and other network owners that use the services of the network

speed: category of service reliability success criterion based on factors associated with time and timing in a service

transaction: basic unit of service or service session

unavailability: expression of the degree to which a system, subsystem, or equipment is not operable and not in a committable state at the start of a mission, when the mission is called for at an unknown (i.e. random) time

NOTE 1: The conditions determining operability and committability must be specified.

NOTE 2: Expressed mathematically, unavailability is 1 minus the availability.

NOTE 3: Unavailability may also be expressed mathematically as the ratio of the total time a functional unit is not capable of being used during a given interval to the length of the interval (e.g. if the unit is not capable of being used for 68 hours a week, the unavailability is 68/168).

user service downtime: average proportion of time that an individual user cannot access and use the network service because it is either unavailable or of unacceptable performance quality for durations longer than "t_o" seconds, where "t_o" seconds is the user tolerance threshold for outage

NOTE: The unit of measure is minutes per year.

user service premature disconnect: average proportion of user service sessions that are disconnected prematurely

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

ARMA	Autoregressive Moving Average
ATIS	Alliance for Telecommunications Industry Solutions
ATM	Asynchronous Transfer Mode
BER	Bit Error Rate
BGP	Border Gateway Protocol
B-ISDN	Broadband-ISDN
CCS	Common Channel Signaling
CIP	Critical Infrastructure Protection
CMS	Call Management Server
CoS	Class of Service
CS	Call Server
DCS	Digital Cross-connect System
CQR	Communications Quality and Reliability
DPM	Defects Per Million
DPM	Downtime Performance Measurement
EC	Exchange Carrier (local)
EMI	ElectroMagnetic Interference
ESD	ElectroStatic Discharge
FCC	Federal Communications Commission
FIFO	First In First Out
FTP	File Transfer Protocol
GII	Global Information Infrastructure
GUI	Graphical User Interface
GW	GateWay
HFC	Hybrid Fibre Coax
IC	Interexchange Carrier
ICMP	Internet Control Message Protocol
IEMS	International Emergency Multimedia Service
IEPS	International Emergency Preference Scheme
IETF	Internet Engineering Task Force
IOAM&P	Internetwork Operations, Administration, Maintenance and Provisioning
IP	Internet Protocol
IPs	Intelligent Peripherals
ISDN	Integrated Services Digital Network
ISP	Internet Service Provider
ITU	International Telecommunication Union
ITU-T	ITU-Telecommunications standardization sector
KLOC	Kilo-Lines-of-Code
LAN	Local Area Network
LIFO	Last In First Out
MAC	Media Access control
MG	Media Gateway
MPLS	Multi Protocol Label Switching
MTBF	Mean Time Between Failures
MTTR	Mean Time To Repair
NGN	Next Generation Network
NRC	Network Reliability Council
NRIC	Network Reliability and Interoperability Council
NRSC	Network Reliability Steering Committee
NSTAC	National Security Telecommunications Advisory Committee
OA&M	Operations, Administration and Maintenance
OAM&P	Operations, Administration, Management, and Provisioning
OSPF	Open Shortest Path First
POT	Point Of Termination
PSTN	Public Switched Telecommunications Network
PTN	Public Telecommunications Network
QoS	Quality of Service

QTES	Quantized TES
R	Router
RBOC	Regional Bell Operating Company
RPR	Resilient Packet Ring
SDH	Synchronous Digital Hierarchy
SG	Signaling Gateway
SLA	Service Level Agreement
SONET	Synchronous Optical NETwork
SP	Service Provider
SS7	Signaling System 7
TCP	Transmission Control Protocol
TEWG	Engineering Working Group
TDM	Time-Division Multiplexing
TMF	Telecommunication Management Forum
TMN	Telecommunication Management Network
TE	Traffic Engineering
TES	Transform Expand Sample
TMF	Telecommunications Management Forum
TSP	Transport Service Provider
US	United States
VC	Virtual Channel
VoIP	Voice over IP
WAN	Wide Area Network
WDM	Wavelength Division Multiplexing
WG	Working Group

4 IP network survivability framework

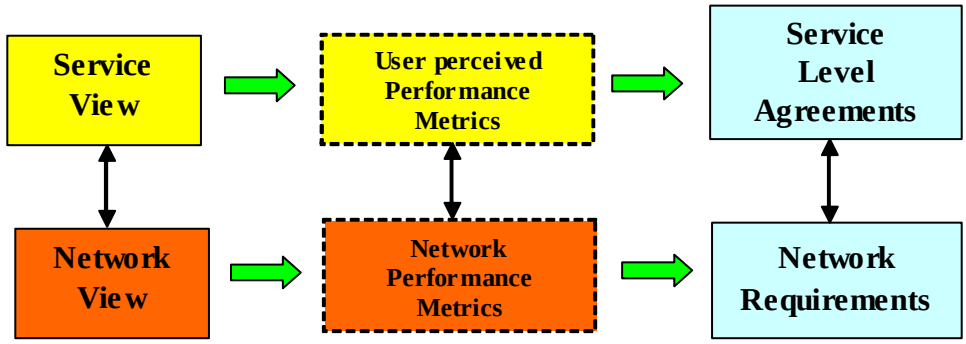


Figure 4.1: IP network survivability framework

Service view clause describes those attributes of importance to the service users. It includes the concept of service outages based upon a given service. For example, a 30 second network outage may result in a VoIP failure, but go unnoticed for email.

Network view clause deals with those attributes of importance to network owners and network suppliers. Attributes such as hardware and software reliability, protocols, redundancy, contribute to both satisfying the Service View attributes as well as the cost to own, operate, and maintain the network.

User perceived performance metrics include existing and new metrics used to define a user's experience for various services. There is mapping from the network performance metrics to grades of service provided on IP networks.

Network performance metrics include metrics taken from ITU-T SG13, T1A1.3, etc., as well as reliability metrics generated by T1A1.2. They cover networking, network element, operations, and supplier-support attributes.

Service Level Agreements (SLAs) can utilize the metrics from the corresponding clauses of the present document.

Network requirements contain information for network design.

5 Standards Organization Relationships to Network Reliability/Availability Issues

ITU-T Recommendation I.350 (SG 13) [4] addresses the upper part of figure 5.1, namely the relationships of the service performance matrices. A service connection has three phases:

1. *Access* (successfully connecting the customer to the network),
2. *Transfer* (connection is made and intelligence is going across the network), and
3. *Disengagement* (disconnect the customer from the network).

A service connection also has three performance characteristics: *speed*, *accuracy*, and *dependability*. The multiple layers of 3x3 matrices indicate that multiple services will be impacted by these same characteristics. The service availability function controls the flow from the service available state to the service unavailable state. The linear time chart to the right in figure 5.1 indicates changes of state over time.

ITU-T SG2 and Committee T1 address traffic engineering, the subject of annex B. The lower left part of figure 5.1 breaks available time into three components related to traffic engineering. Provisioning for a Grade of Service, offered traffic, and system capacity. ITU-T SG2 work includes recovery during emergency situations, for which the technique described in the present document are applicable.

ITU-T SG4 addresses the equipment reliability portion (i.e. the lower right part) of figure 5.1. It shows the flow from Reliability to Maintainability to Maintenance Support.

ITU-T SG16 addresses multimedia systems, including consideration of emergency situations.

Further detail of these activities is given in annex A.

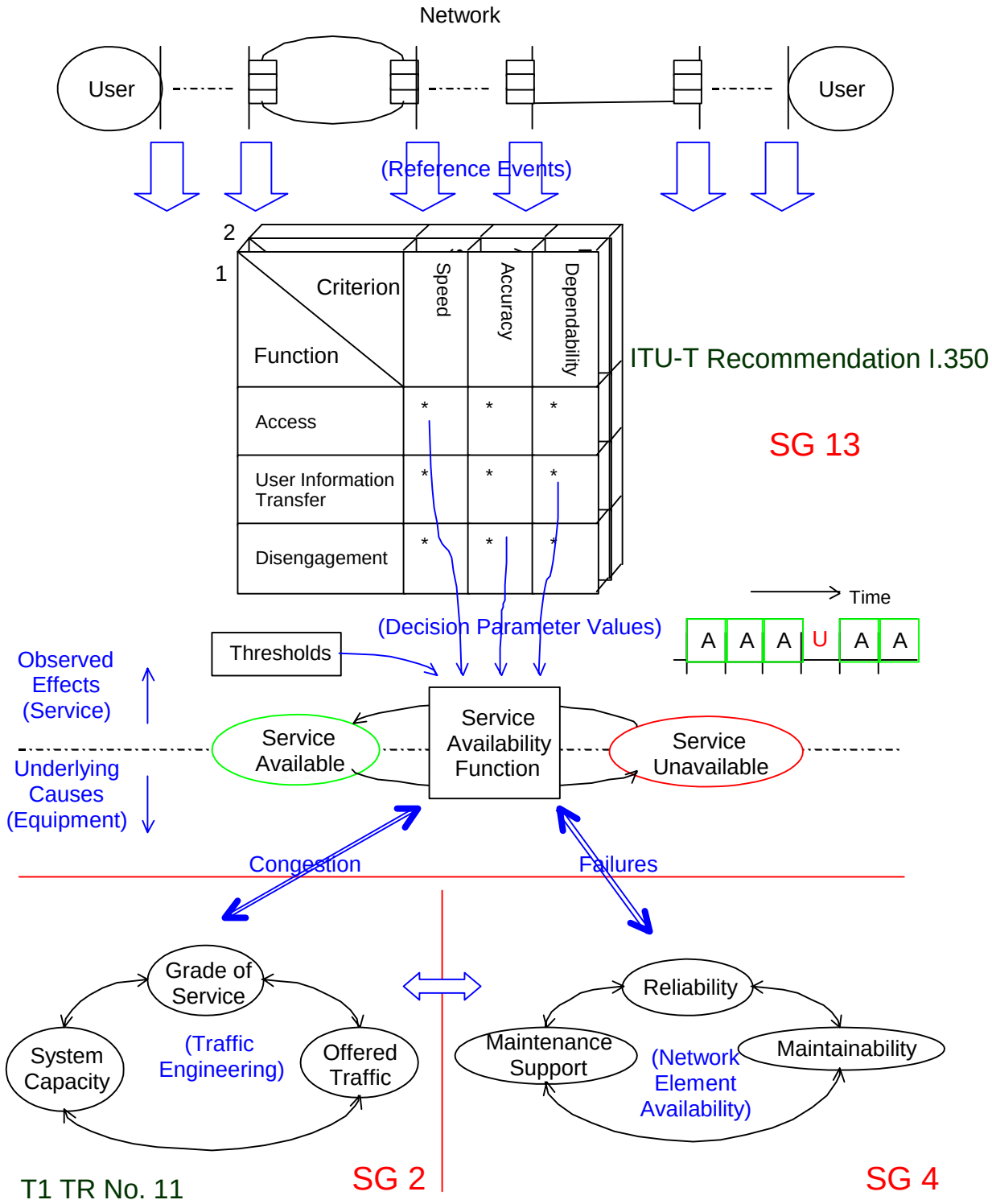


Figure 5.1: Service availability, network element availability, and traffic engineering

6 Key concepts

IP Network Reliability Performance (as discussed in the present 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 outages such as loss of the ability to diagnose. These and other key concepts are discussed in this clause.

6.1 Service view

The service view drives the network reliability and availability requirements. Service users experience network failure modes as service failures or as unacceptable service performance while trying to access and use a service. There are four (4) key attributes that need to be considered:

1) *Service criticality:* Services range from mission-critical ones through to non-critical services such as residential email. Service customers are willing to pay more for higher service reliability especially when the service is critical to the service customers' business or when it is a life-line.

2) *Service failure impact:* The impact refers to the number of service users or amount of bandwidth impacted. Obviously, requirements are more stringent as the impact increases.

3) *Service failure duration:* The length of time the service is down or is experiencing unacceptable degraded performance is a critical attribute. Services vary in their failure thresholds to both packet delay and packet loss. Real-time interactive services such as Voice over IP fail or cause the user to experience unacceptable performance at lower packet delays and loss duration than does non real-time, non interactive ones such as email. Users' tolerance to performance characteristics also differs.

4) *Service failure rate:* The frequency of service failure that is acceptable to users varies depending on service criticality, failure impact and failure duration. A monthly failure that causes one user not to be able to access and send email that lasts 30 minutes is more acceptable than a monthly failure where a stock exchange is down for 30 minutes.

While users have different tolerance to differing degrees of each of these attributes, so do individual network elements. Often it is not the failure event that results in the user being adversely affected, but rather certain network elements response to these failure events.

6.2 Network view

The network needs to satisfy two views: the service view to meet service users' expectations and the network owner view to satisfy the network owners' costs and Operations, Administration, Maintenance and Provisioning (OAM&P) requirements. The network failure mode behavior when technology fails, when people cause a procedural error or when there is an environmental incident needs to be translated to both points of view. A good network design optimizes service reliability to meet requirements of specific market segments, with the cost to own and operate the network.

6.3 Causal attributes

The causal attributes are technology failures such as hardware and software failures, OAM&P activities (e.g. software upgrades), environmental incidents (e.g.an earthquake and traffic overloads such as control messages), and procedural errors. The IP Network is designed and operated to both mitigate and mask the causal attributes from the Service User and Service Provider. The network attributes are categorized into networking, network element and operations.

6.4 Service characteristics

Figure 6.1 is a representation of service characteristics, breaking out the service availability function over time into three service categories: *Successful Performance*, *Incorrect Performance*, and *Non-Performance.* Depending on the network design, service can even be superior when customers receive performance beyond acceptable, but we will consider this to be successful performance because the additional performance adds no utility to the end user.

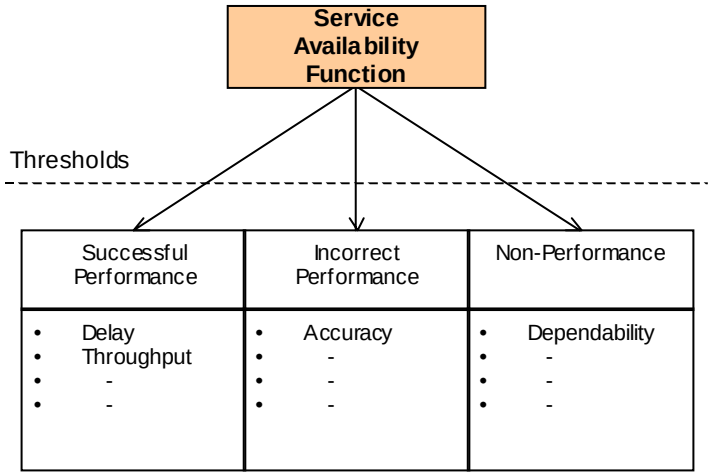


Figure 6.1: Breakout of the Service Availability Function

The horizontal bar graph of figure 6.2 shows the normal operating state, network failure state (reduced capacity), and service availability affected state. The majority of the time, the system is in the normal operating state. 8 766 hours represents 365 ¼ days (an average year).

The vertical flow chart relates application services, service infrastructure, and transport infrastructure, as well as their impact on users. Depending upon the severity or sequence of failures within the network (vertical flow chart), the condition of the network (horizontal bar graph) may move from left to right until the failures are noticed by the user or avoided by mitigating/masking techniques.

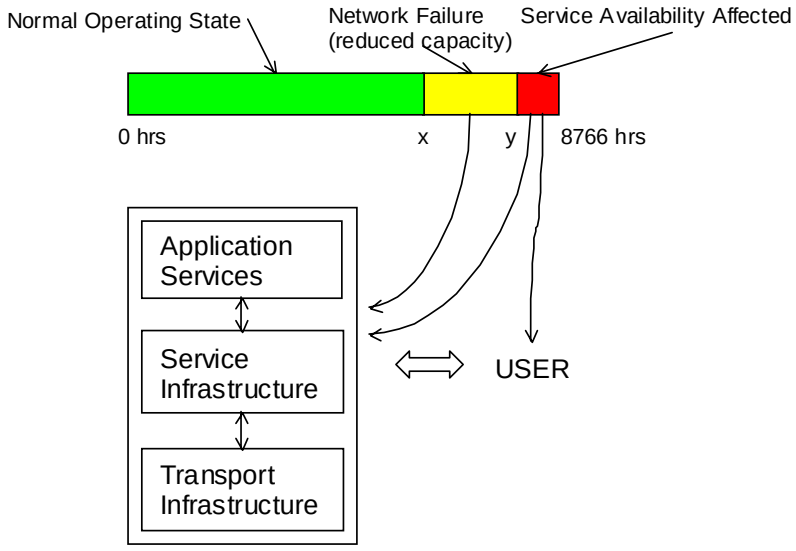


Figure 6.2: System state and user impact

6.5 Network outages versus service outages

Network outages are loss of network resources due to failures, acts of nature, or operational activities. The loss of a network resource can impact services, reduce the available bandwidth or simply result in the loss of network protection. The loss of network resources may also be transient and have no impact on the network that warrants action by the network provider. Any network outage will have an impact on the provider, except perhaps for transient software failures due to known faults. A network outage may not have an affect on service users, or at least some of the effects may be masked from the end users by the design of the network and method of interconnection.

Service outages are defined depending on the criticality of the service. If the service is viewed as mission-critical then an outage is defined independent of the user experiencing the outage. It is viewed that the user depends on the service as a life-line and they may have to use it at any time. Typically, in this case the service experiences an outage when the user(s) cannot use the service for periods of greater than 30 s. For less critical services, the period may vary and the user may have to experience the service outage. Service outages are defined depending on the service criticality.

Additionally, outages can be considered, based on traffic types being carried on the service. Booth service criticality and traffic types can be considered together.

Network outages, such as network node or link failures may or may not have an impact on a network service. For example, if a core router fails due to a catastrophic hardware failure causing the network to restore around the node in 60 s (see note), then the service is down for 60 s though the core router is unavailable to the network for the time to travel to the site and repair the fault. Typically the Mean Time To Repair (MTTR) is expected to be on average 4 hours. In this example the network outage of the node is 4 hours and the service outage is 60 s. However, if the recovered state has not been properly provisioned such that the service experiences unacceptable performance for the 4 hour period, then the service outage would be considered 4 hours not 60 s. If the service restoration time becomes less than 1 second then the service outage is zero and the network node outage is 4 hours (assuming adequate provisioning for the recovered state).

NOTE: Some network devices (i.e. alternate routing facilities) can switch in 60 milliseconds or less; thus, the user may experience only an error in transmission, and no loss of either service or network capability.

6.6 Service and operations dependability

This clause describes the hierarchy of attributes or metrics used to organize and set reliability and maintainability requirements for the public carrier IP network. The primary attributes (observable effects) are separated from the secondary attributes (causes) to facilitate solution flexibility. This flexibility is required in order to meet the wide range of services and operations dependability requirements.

The primary attributes describe the observed attributes as seen by network end-users and operators independent of solution technology. The secondary parameters are those that represent the underlying networking, network element and support causes. The reference Network Reliability Model describes the relationship between the primary and secondary attributes.

The following provides an overview of the components. Clause 8 defines the attribute metrics.

The primary attributes start with the business criteria: revenue, capital outlay and recurring costs based on the market segment and type of services provided. These are used to determine the service dependability and operations dependability requirements. These requirements will vary depending on the market segment, service type and network function. Thus, Voice over IP (VoIP) residential access provided by a cable company with certain operations practices and skills would have different requirements than for a service provider delivering Voice over ATM for business customers. The requirements will be different but the metrics and terminology should be the same.

Service dependability is the delivered quality and in-service reliability of the *service* from the service users' perspective. The pre-service quality attributes are defective service and late service, while the in-service reliability attributes (and examples of failure impacts) are described in the ITU-T Recommendation I.350 matrix [4] (see figure 6.3).

In-Service Reliability	
Access	Failed service attempts Service downtime
Information Transfer	Dropped connections Failed transfers
Disconnect	Failed user disconnects

Figure 6.3: ITU-T Recommendation I.350 Matrix (User)

Operations Dependability is the pre-service quality and in-service reliability and maintainability of the *solution* from the Service Providers' perspective. Similarly, the pre-service quality is delivered quality of the Solution. The OAM reliability is the reliability of the operator's functions, and thus the ITU-T Recommendation I.350 [4] matrix applies (see figure 6.4). OAM dependability also includes maintainability attributes such as fault isolation and repairability.

OAM Reliability (Operator)	
Access	Failed OAM attempts OAM downtime
Transfer	Dropped connections Lost OAM
Disconnect	Failed operator disconnects

Figure 6.4: ITU-T Recommendation I.350 Matrix (Operator)

The secondary attributes are categorized into networking, product and supplier support attributes. They describe solution design attributes such as network restoration time and product software failure rates, and supplier support attributes such as responsiveness. Refer to clause 8 for a more comprehensive description of the attributes.

The reference reliability model describes the behavior of the IP network solution for all events, and relates the primary and secondary attributes. Any secondary attribute can be varied to determine the impact on a primary attributes. However, to do so, the definition of failure for the primary attributes must be defined. IP based networks transport multiple applications. The applications see network failures as delay and packet loss. The end points of an IP communication path, both users and devices vary in their tolerance to delay and packet loss. The failure threshold criteria are essential to relate the service users' and network operator's requirements to the dependability attributes of the network solution.

For example, for a VoIP service downtime of 15 minutes per year, applicable packet loss and delay threshold needs must be specified to define what constitutes an outage. This outage definition may be, for the Access and Information Transfer transaction functions, delays of greater than 10 s and packet loss greater than 10 %. These thresholds are set based on user tolerance to delay and media quality as well as technology limitations. Figure 6.5 illustrates this relationship using the ITU-T Recommendation I.350 [4] matrix. The algebraic terms shown in the figure are not used elsewhere in the present document, and are merely included for completeness.

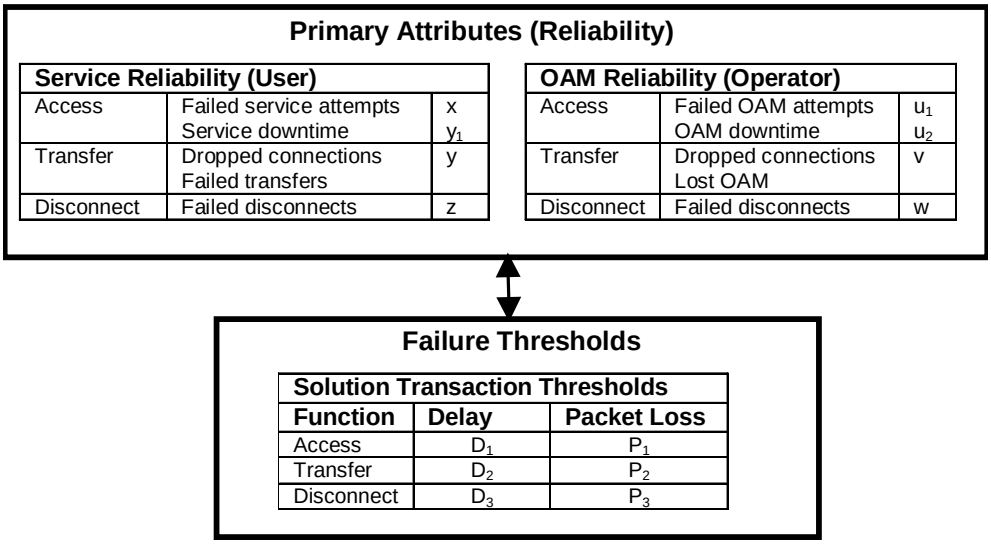


Figure 6.5: Failure thresholds

7 Network design considerations for survivability

Figure 7.1 illustrates the design considerations for network survivability. The considerations are grouped into prevention and mitigation/masking strategies. Prevention strategies either prevent the occurrence or reduce the frequency of occurrence of network node and link failures due to technology failures, environmental incidents, procedural errors, and traffic overloads. When the prevention strategies are not sufficient to satisfy the market expectations of service reliability/availability, then mitigation and masking strategies are used. These include network protection, hardware duplication, automatic software failure recovery, diverse routing, and site duplication. These latter strategies should be selectively applied to minimize costs.

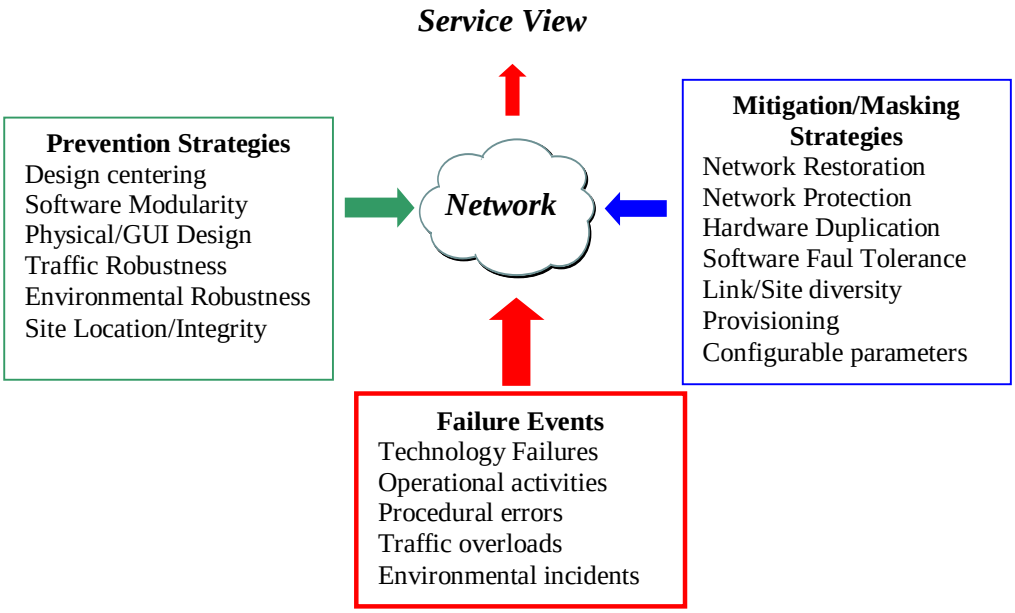


Figure 7.1: Network design considerations for survivability

Figure 7.2 depicts a process for iteratively analyzing a network to optimize its design. It starts with the proposed functional network architecture where reliability objectives are set based on the market segment business drivers. Failure mode analysis design walk throughs are done to identify rogue failure modes. A prediction model is built to compare the predicted reliability of the proposed architecture against the objectives as well as to quantify the impact of the rogue failure modes on service and maintenance reliability. The network can be optimized to maximize service reliability and minimize maintenance costs by drawing from any of the prevention, mitigation and masking design strategies.

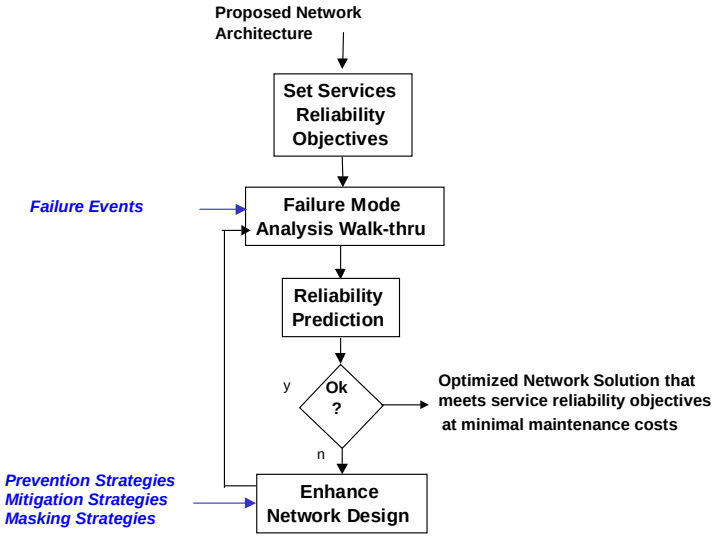


Figure 7.2: Network reliability design analysis flowchart

7.1 Reference network architecture

Figures 7.3 and 7.4 provide a description of a user-to-user connection on an IP network (this connection is also known as a hypothetical reference path in ITU-T Recommendation Y.1541).

NOTE: When restoration needs to be done at the physical layer underlying the architecture of figure 7.3, consideration must also be given to the overlying layers (i.e. engineered IP paths).

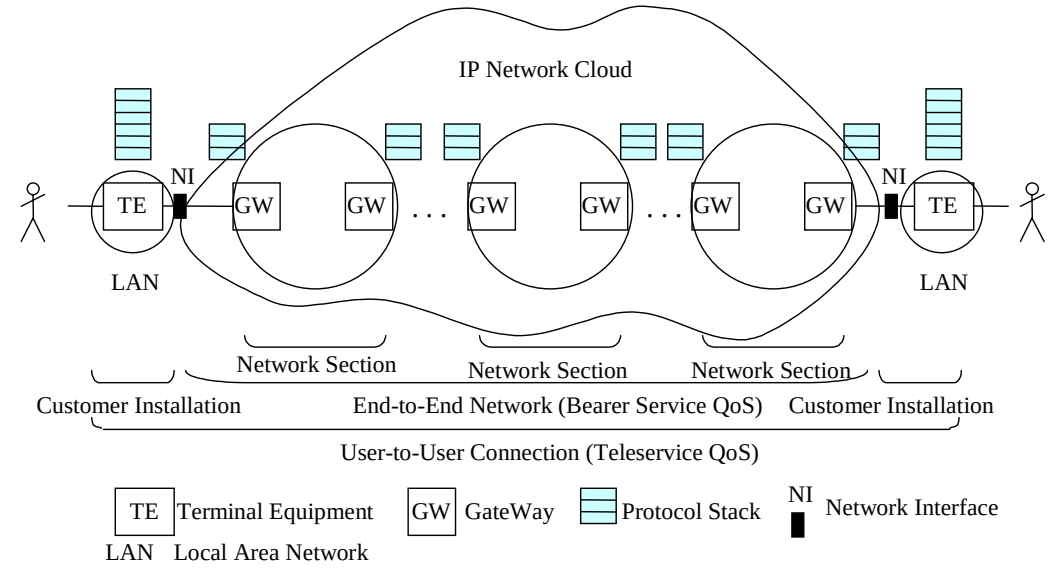


Figure 7.3: User-to-User connection on an IP network

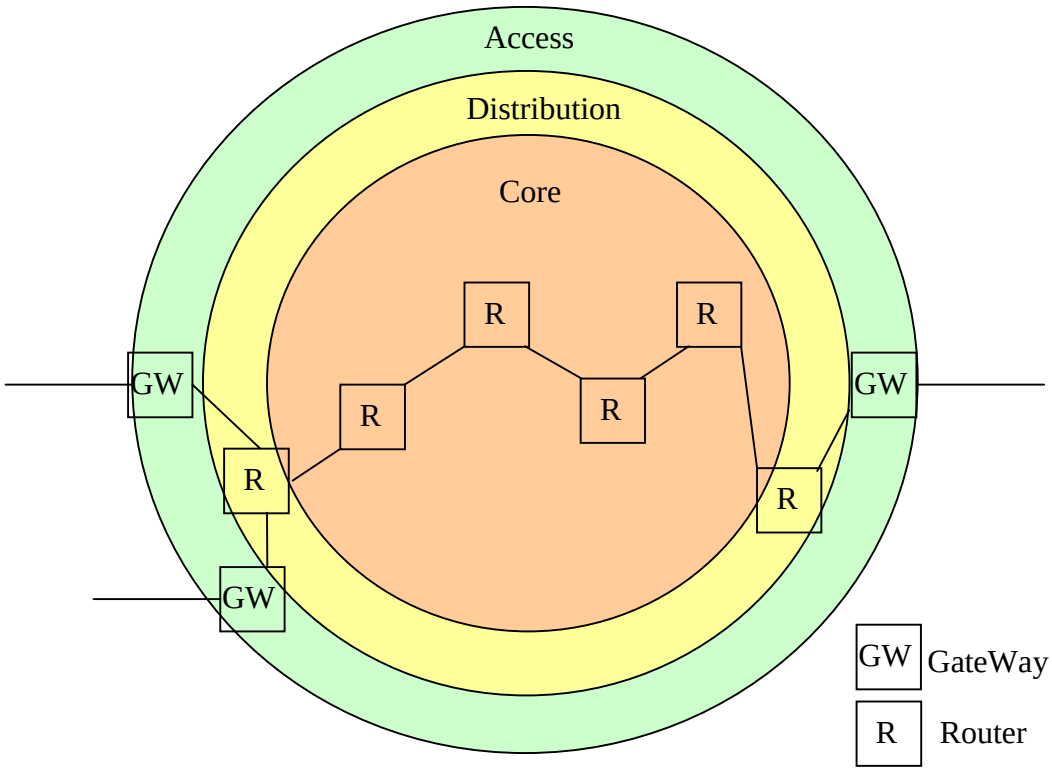


Figure 7.4: Role of IP nodes in a network clause

The intent of reference network architecture figure 7.5 is to provide a reference for the application of metrics and solution approaches. The Reference Network Architecture describes both an IP multi-service network as well as a hybrid VoIP network that is integrated into the PSTN. It illustrates both access and backbone networks with some reference end-to-end paths. The solution approaches, such as nodal and link protection, restoration and architectural details are not shown.

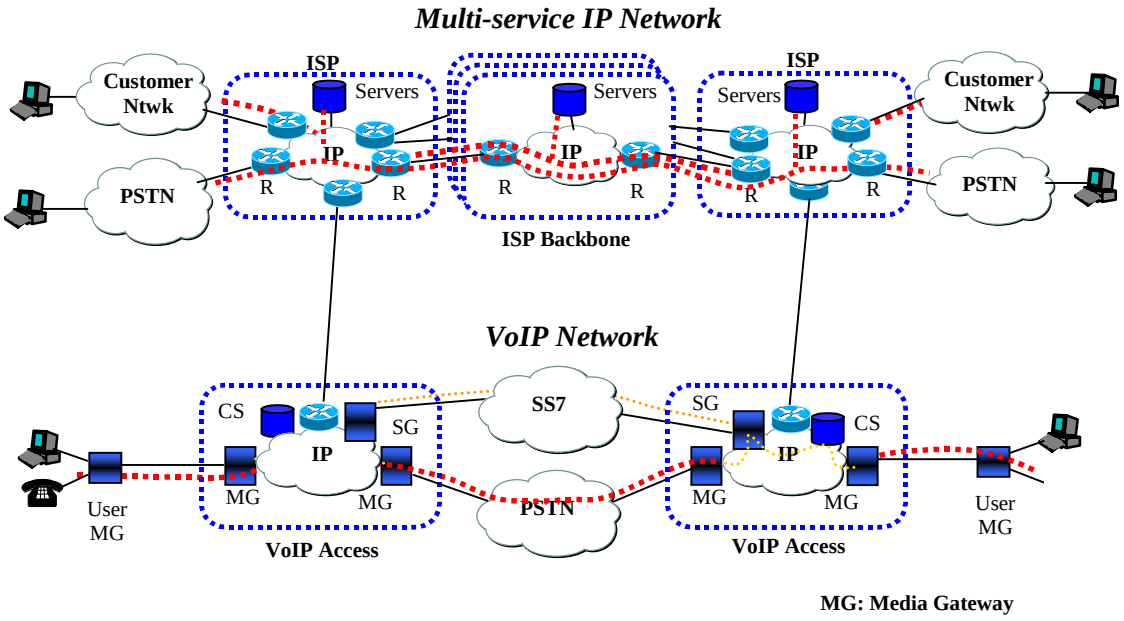


Figure 7.5: Reference networks

For example, for a port-to-port path across the reference network there are metrics (e.g. port-to-port service downtime), there are causes of failure (e.g. router outage) and solutions to mitigate the failures (e.g. Fast OSPF restoration) to achieve a reliability/availability Service Level Agreement (SLA) e.g. 99,9 % port-to-port availability [4].

7.2 Traffic analysis issues in IP based networks

Traffic analysis techniques are very important to the characterization and definition of network reliability and availability. The spread of IP based networks and services has led to a need for tools to better assess the survivability, reliability, and availability of these networks, particularly as IP infrastructures become more widely used in supporting telephony and other real-time services.

While the need for traffic engineering techniques suitable for IP-based networks is great, the subject is still very much in the realm of research. Compounding the problem of characterizing the nature of IP traffic is the fact that the Internet is constantly changing, and at a rapid pace.

Traffic engineering has always been used for PSTN planning and continues to be used today. Network simulation is used by network planners to more closely predict the performance of their networks. Simulations can be designed to characterize a network with or without explicit details of the expected traffic, although the usefulness of the results obtained will depend upon the accuracy of the input parameters and the assumptions made.

Much has been written recently about the self-similar (or fractal) nature of packet switched traffic on the Internet [6]. This research is promising and certain conclusions can be drawn and utilized in traffic engineering and management. However, in the absence of definitive data on IP traffic, network planners can, without erring to a large degree, fall back on the traditional traffic analysis methods of circuit switched networks [7] as long as they can assume an aggregation of flows.

A full treatment of traffic engineering issues is not in the scope of the present document. Some useful information has been collected in the following appendices to help IP-based network planners assess availability and reliability.

Annex A contains a review of the relevant standards work.

Annex B contains historical background information on traffic engineering related to circuit-switched networks.

Annex C contains a discussion of traffic issues related to IP networks.

Annex D addresses monitoring network metrics in IP based networks with a focus on delay.

7.3 Causes of service outages

The key causes of IP service outages are listed below along with each of their root causes.

7.3.1 Hardware failures

- Single points of failure.
- High failure rates due to new unproven technology, poorly centered and highly stressed circuit designs, uncontrolled operating environment, insufficient equipment cooling, insufficient ElectroStatic Discharge (ESD) protection.
- Poor fault detection coverage.
- Slow network restoration.
- Unreliable network restoration.
- Lack of sufficient protection from ElectroMagnetic Interference (EMI) and power line noise.
- Immature processes resulting in design and manufacturing defects.
- No physical link diversity.

7.3.2 Software failures

- Unstructured, overly complex and large amounts of poorly documented code.
- Processor speed.
- Poor fault detection coverage and slow software recovery.
- Slow network restoration.
- Unreliable network restoration.
- Immature processes resulting in design and load build defects.

7.3.3 OAMP activities

- GUI and physical design that facilitates human error.
- Inadequate training or procedures resulting in human error.
- Network elements not designed for in-service upgrades.

7.3.4 Environmental incidents

- Environmentally high risk site location.
- Poor building design or location of equipment in the building.
- Inadequate training or procedures resulting in human error.
- No site diversity.

NOTE: Environmental incidents include: temperature, humidity, electrical storms, floods, office vibrations, earthquakes, power line noise, EMI, and ESD.

7.3.5 Traffic overloads (bearer and control message traffic)

- Lack of overload controls.
- Immature development processes resulting inadequate overload controls.
- Poor load balancing by protocols.

7.4 IP protection and restoration technologies

The following lists some of the IP-based network restoration/protection technologies, their application and restoration times.

Table 7.1: IP-based Network Restoration/Protection Technologies

Restoration and Protection Name	Network Application Area	Network Area	Restoration Time
Border Gateway Protocol (BGP-4)	Paths between private and public Internet network peering points	WAN, Core	3 min to 10 min.
Open Shortest Path First (OSPF)	Autonomous system Layer 3 paths	Metro, WAN, Core	10s to 40 s (node) 0,5 s to 10 s (link)
Multi Protocol Label Switching (MPLS) Explicit Source Routing	Autonomous system Layer 2/3 paths	WAN, Core	< 0,5-3 s
Equal Cost Multi-Path (ECMP)	Intra-autonomous system Layer 3 path	WAN, Core	200 ms to 500 ms
Routing Information Protocol	Intra-autonomous system Layer 3 node	LAN, WAN	3 min to 5 min.
ATM PNNI	Paths between private and public ATM network peering points	Metro, WAN, Core	1 s to 10 s
Spanning Tree Protocol	Bridges	LAN, Metro, WAN	30 s to 40 s
ATM/Frame Relay Automatic Protection Switching I.630 or Smart SVCs	Layer 2 PVCs (Permanent Virtual Circuits)	WAN, Core	1 s to 5 s
SONET Automatic Protection Switching	Layer 1 facility protection	Metro, WAN, Core	50 ms
WDM Automatic Protection Switching (e.g. Optical Shared Protection Ring)	Layer 0 facility protection	Metro, WAN, Core	500 ms
WDM Mesh Restoration	Layer 0	Metro, WAN, Core	500 ms to 20 min.

8 Guides and metrics

The lack of industry consistency for IP network reliability makes it virtually impossible for network providers to know if what they are building will deliver the services reliability performance required by end users. This is further complicated by the fact that network service providers specify network availability within their own network domains, so that end users' services which are delivered across multiple domains are virtually impossible to guarantee. If the future public carrier network is to fulfill its promise of services convergence, then the industry needs a set of reliability metrics and terminology that are common across the network for which individual service reliability requirements can be specified.

This clause describes and proposes development of a set of guides and metrics for IP based networks and services. These guides and metrics will provide a complementary approach to the top down framework prescribed in the present document. They will serve as a basis for processes aimed at monitoring and improving reliability, and verifying the levels of reliability intended by the top down process.

8.1 Guides for operational measurement and improvement of the reliability/availability of IP-based networks and services

There is an immediate need for a standardized methodology for measuring the reliability/availability of IP based networks and services that will allow end users, service providers, and equipment providers to communicate effectively regarding their IP service reliability expectations and capabilities. Overall simplicity and ease of understanding, as well as broad applicability should characterize this methodology.

Expression of service reliability/availability to an end user should be meaningful, in that it relates directly to the user experience, and should not be vague or overly complex. A standard measurement would enable consumers to make better comparisons and more informed choices when selecting services or service capabilities, such as QoS class. Use of a standard measurement by equipment manufacturers and network operators assures that their network and system performance planning is driven by a parameter known to be visible to users.

Additionally, the rapid pace of technological change and time-to-market drivers make collaboration between equipment and service providers essential to the delivery of services that meet user expectations for reliability/availability. This collaboration depends on a common understanding of the reliability/availability requirements of the service and establishment of appropriate objectives. A standard measurement methodology that captures the interrelationship of service and network reliability/availability can minimize the time needed to resolve issues that are complicated when disparate approaches are employed by individual firms.

8.1.1 The DPM parameter and its advantages

The rapid evolution of IP networks requires a standardized methodology to evaluate IP network reliability in terms of actual customer impact of outages. This can be done using the concept of a defect, normalized to a defined rate - Defects Per Million (DPM) [2], which is a useful complement to traditional reliability measures that have been used in the past as scaling conversions for very small numbers (e.g. FITS, Failures In 10^9 operating hours).

NOTE: Defects Per Million (DPM) is not related to Downtime Performance Measurement (DPM) as defined in GR-929-CORE [8].

This clause is not intended to advocate DPM as a solution, but rather to guide those who choose to use DPM. Also, this clause is not intended to be a complete description of how to apply DPM, only to provide an example of guidance.

The DPM is, for a given reporting period, the number of units that failed to meet expectations (defects) divided by the total number of units multiplied by one million. DPM is thus the number of defects per million units.

DPM is compatible with traditional measures of reliability/availability that are commonly used and easily understood. It is also very adaptable and can be applied to measurement data from various sources. It can be used to evaluate the reliability/availability of complex services, systems, and networks. DPM is successfully used in voice networks, where it is defined as the number of blocked calls per one million calls averaged over one year. This definition can be directly extended to transaction oriented services in IP based networks, such as email, by replacing call with a specific transaction. Extension of DPM to IP based services where a transaction is not clearly defined or cannot be measured could be non-trivial.

The value of the DPM methodology is realized by defining units and defects that directly relate to user's expectations (e.g. for voice service the unit would most logically be a call). The more direct this relationship, the more useful and meaningful the results. DPM enables establishment of goals and monitoring of progress towards those goals, and has been successfully used to drive significant reliability/availability improvements in voice networks.

Care should be taken, however, in relating defect definitions and measurements to other types of analysis.

EXAMPLE: Those using the impact, duration and frequency of failure events.

8.1.1.1 Measuring the reliability/availability of IP-based networks and services through defects per million

DPM is a generic measurement normalization of (bad # / total #) where DPM/1,000,000 = (bad # / total #). When applying DPM, the question is what should be the units of the counted terms. The associated question is can we always define reliability and availability requirements in this general framework?

The trick is to translate service conditions into measurable network conditions, and associate the thresholds of one with the translated thresholds of another. While some of this translation is network design specific, we can provide a framework for making this translation, and we can translate that which is unrelated to the network design.

8.1.1.1.1 Session: a service perspective

Any failure may or may not lead to a customer impact, and a lot of this connection has to do with the service session, the transaction, the protocol, and the tolerance of the end user. Take a service perspective: any use of a service is initiated, continues, and is terminated. Call this complete use of service a *session*. A session then can be made of several transactions in which information is transferred one way, source to destination.

During some service sessions, some transactions may be repeated without affecting service, and some transactions can be incomplete without affecting service. A transaction can be made of multiple IP packets. Packets can be repeated, or even lost in some applications, without significant effect to the transaction. This depends on whether the underlying protocols manage these issues, and whether the services and customers are tolerant to the conditions that result. However, excessive repeating or dropped transactions can affect any service.

Session type defines specific effects to packets, transactions, and sessions that will determine a failed session (service attempt). For example, based on the type of service, say a phone call, the requirements of the service and user determines that a certain number of dropped packets will affect a transaction (a garbled "hello"), but may not affect the session in any noticeable way. Yet another number of dropped packets will affect the transaction and the session in a way users notice (noise, or no communication). The transaction type, in association with the service, may also define a failed session. For example, in a telephone call, a failed call setup transaction may cause sufficient delay in the initiation, and cause the user to decide to retry; this would then be a failed session.

QoS/SLA/CoS can also define some of the tolerances to failure. And some services are not tolerant to some network failures because of general customer expectations beyond QoS/SLA/CoS, or because interfacing equipment is not tolerant to some network conditions.

Figure 8.1 depicts the relationships between conditions in the network and how they can propagate to a customer impact. Figure 8.2 illustrates the ideas noted above, and the detail that drives movement across each arrow in figure 8.1.

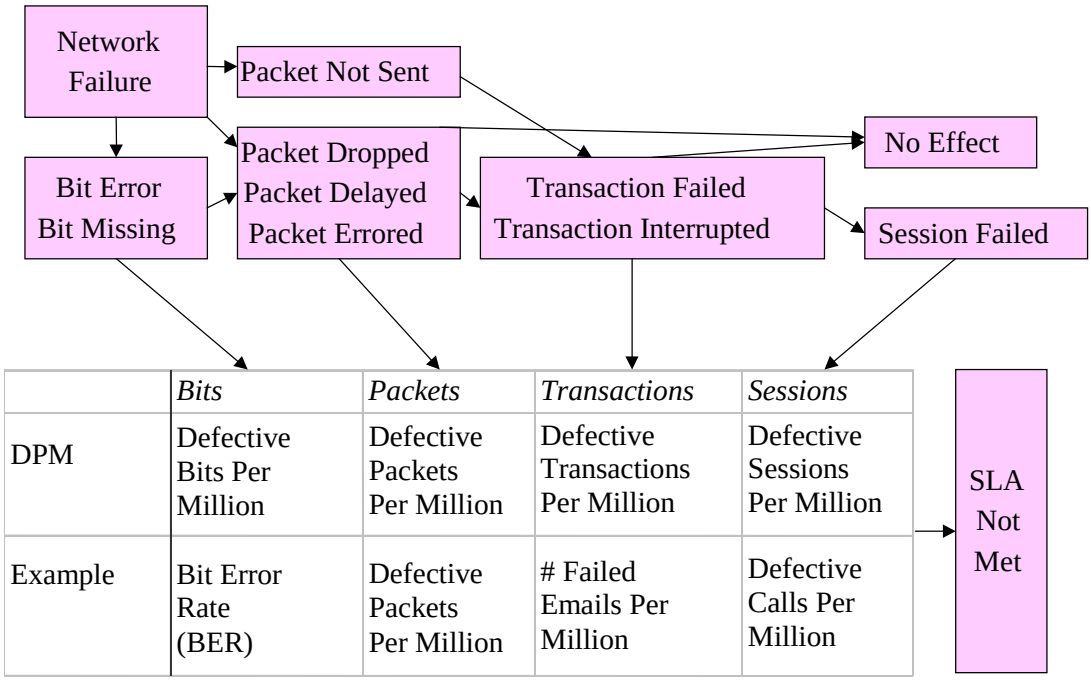


Figure 8.1: The flow from a network failure to a session failure, and failure to meet a SLA

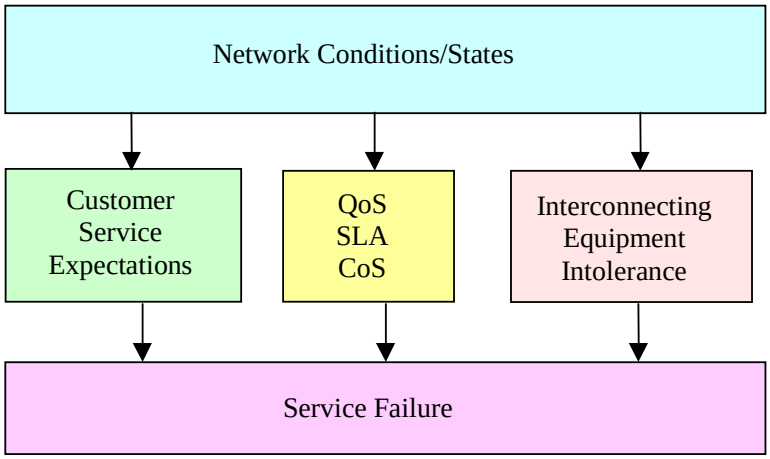


Figure 8.2: The flow gate process that determines how a network condition or state translates into service failure, but also can be generalized into any condition translating into a fault condition of bits, packets, transactions or sessions

8.1.1.1.2 Examples

In each example, you can trace the flow of condition to customer impact through figure 8.1.

VoIP example: Some network condition (possibly some network failure, or maybe even just congestion) would cause a delayed packet. These delayed packets could then affect one or more transactions (could be someone speaking a sentence, or could be a call setup message) in the form of unacceptably large transaction delay. This can then lead to a failed session, or a failed call.

Modem over VoIP example: Some network condition causes an IP gateway to stop communicating with the local call server, so that server assumes a lost trunk condition with the IP gateway and disconnects. This causes the connection to reset, which causes the modem to disconnect. This becomes a failed session, and requires the user to reconnect.

8.1.2 Measuring the reliability/availability of IP-based networks and services using Defects Per Million (DPM): IP based network examples

In these examples, the reliability/availability of IP Backbone Access Facilities and the IP Backbone Network are being measured. The portions of the network that are measured can be varied depending on the particular situation (e.g. ownership, control).

NOTE: References to *port* in this example refer to access ports (i.e. customer connections).

The Access Router is in the IP Backbone Network and its failure would be observed as an outage of all IP access ports connected to it. The failure of a single IP Backbone Router would not be observed as an outage of IP ports unless an Access Router was isolated (e.g. due to lack of redundancy, simultaneous facility failure). In this instance, the failure(s) would be observed as an outage of all IP ports on the isolated Access Router. See figure 8.3.

8.1.2.1 IP backbone network DPM

- *Units*: Each unit is 1 Port-Hour. For each customer connection, or access port, into the IP Backbone there are 24 daily port-hours available.
- *Formula*: DPM = ((sum (Total Down Port-Hours)/sum (Total Available Port-Hours)) x 1 000 000 for the reported time period, e.g. daily.
- *Definitions*:
  - *Total Available Port-Hours* is the active access port count times the number of hours in the reported time period, e.g. (sum(daily active port count x 24)).
  - *Total Down Port-Hours* is the total number of hours that access ports were down as a result of outages within the IP backbone network, including failures of facilities interconnecting IP backbone equipment, in the reported time period.

EXAMPLE: Daily IP Backbone Network DPM for a network with 10 000 active access ports that experiences a single failure - an Access Router with 100 access ports fails for 30 minutes.

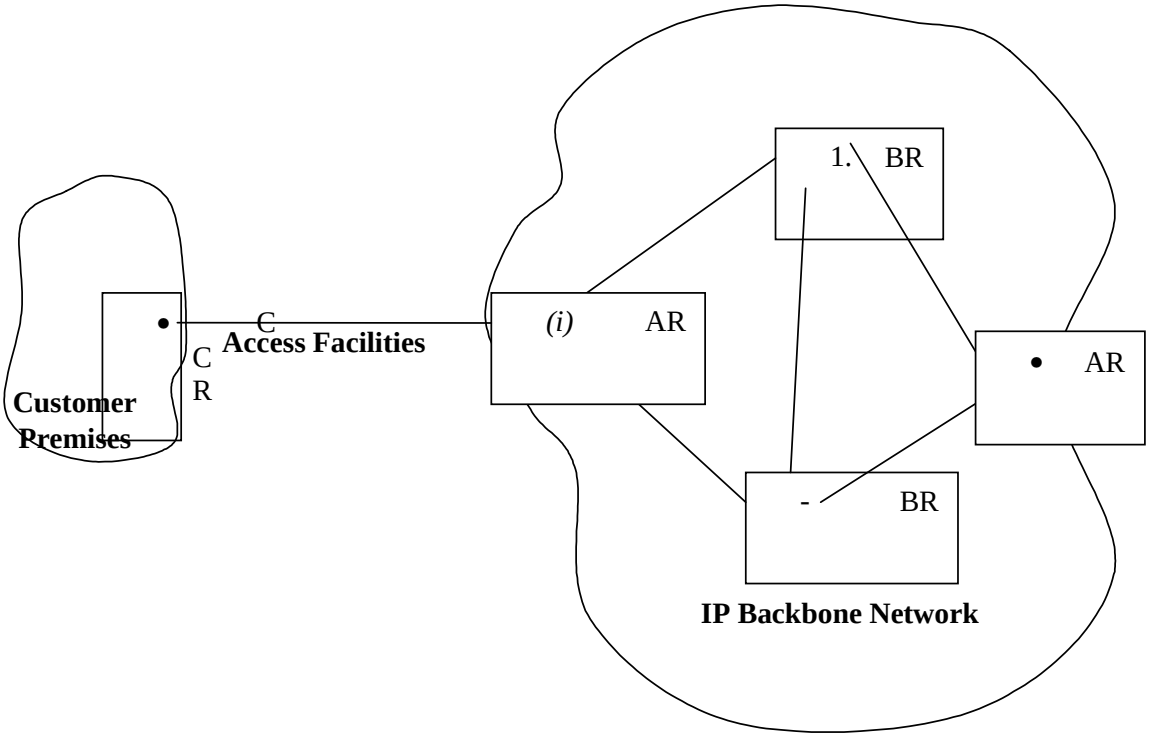
- Total Available Port-Hours = 10 000 x 24 = 240 000
- Total Down Port-Hours = 100 x 0,5 = 50
- Daily DPM = (50/240 000) x 1 000 000 = 208

8.1.2.2 Access Facilities DPM

- *Units*: Each unit is 1 Port-Hour. For each customer connection, or access port, into the IP Backbone there are 24 daily port-hours available.
- *Formula*: DPM = ((sum (Total Down Port-Hours)/sum (Total Available Port-Hours)) x 1 000 000 for the reported time period (e.g. daily).
- *Definitions*:
  - *Total Available Port-Hours* is the active access port count times the number of hours in the reported time period, e.g. (sum(daily active port count x 24)).
  - *Total Down Port-Hours* is the total number of hours that access ports were down as a result of outages within the IP Backbone Access Facilities, which include all facilities between the customer demarcation point and the IP Backbone Demarcation Point, in the reported time period.

EXAMPLE: Daily IP Backbone Access DPM for a network with 10 000 active access ports that experiences a single failure - an Access Facility connected to 10 access ports fails for 90 min.

- Total Available Port-Hours = 10 000 x 24 = 240 000
- Total Down Port-Hours = 10 x 1,5 = 15
- Daily DPM = (15/240 000) x 1 000 000 = 63



CR: Customer Router
AR: Access Router
BR: Backbone Router

Figure 8.3: Example IP-based network

8.1.3 DPM usage considerations

Care should be taken in relating defect definitions and measurements to other types of analysis, for example, those using the impact, duration and frequency of failure events.

DPM is a quality-based unit of measure that can be applied to a broad range of existing metrics:

- System downtime of 3 minutes per year is equivalent to 5,7 defective minutes per million offered minutes of service, or 5,7 DPM.
- Weighted port downtime of 12 Mbit/s minutes per year is equivalent to 22,8 defective Mbit/s minutes per million of offered Mbit/s minutes or 22,8 DPM.
- Ineffective call attempts and dropped calls are already expressed per million.

The use of DPM in multiple ways as described in these bullet items makes it imperative that the user understands the origins of the DPM metric. DPM from different network or service types may not be comparable or additive if the measurement units providing the basis of the DPM calculation are not the same. Using the examples above, a customer, seeing 5,7 DPM quoted for one network and 22,8 DPM quoted for another network, might be led to believe that the two measures are comparable. However, if the 5,7 DPM quoted is based on system downtime while the 22,8 DPM quoted is based on weighted port downtime, no direct comparison can be made.

The DPM approach uses a broad definition of defect to cover error, defect, and failure. For example, designers make errors; the resultant software has defects, which may fail to cause system outages. The traditional approach measures software quality in defects per Kilo-Lines-of-Code (KLOC), software reliability in failures per year, and system downtime in minutes per year. The DPM approach converts all metric units to defects per million. Its value is that it usually results in numbers of manageable size, and helps foster a quality improvement culture. DPM is calculated based on measured data from the field or, during development, based on design reliability analysis and prediction. An example of the current approach is weighted bandwidth DPM. DPM is therefore an integrated measure involving frequency, duration, and impact. The advantage is that it allows for simple tracking. However, individual contributions are *masked*. Thus, DPM could stay constant while independent variables may range beyond acceptable limits.

The following example illustrates this limitation. Figure 8.4 depicts a Service Provider's IP network that provides bandwidth to a customer network, which in turn provides Voice over IP (VoIP) and data services to end users.

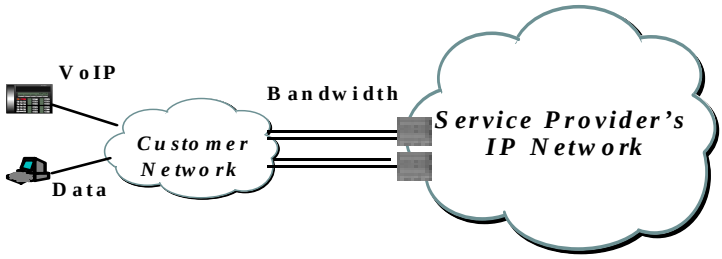


Figure 8.4: DPM limitation illustration

In this example, the Service Provider supplies the Customer Network with 10 Gbit/s of bandwidth using ten 1 Gb/s Ethernet ports distributed over two network elements. For Year I, the total DPM (73,2) is calculated from table 8.1. In Year I there were no outages for which all 10 ports failed. However, there were failures that resulted in the loss of 5 Gbit/s for five minutes, and six failures resulting in the loss of 1 Gbit/s for 60 minutes.

Table 8.1: Year I

Failure Mode Impact	Number of Failures	Failure Duration (minutes)	DPM Contribution	End-user Service Impact
10 ports down (10 Gbit/s)	0	0	0	None
5 ports down (5 Gbit/s)	1	5	4,8	Unacceptable QoS and service denials for 5 minutes for VoIP
1 port down (1 Gbit/s)	6	60	68,4	Unacceptable QoS and service denials 6 times that lasted 30 s as the links recovered for both VoIP and Data services
Total DPM 73,2				

The 5 port failure caused the customer's service users of VoIP to experience service denials and unacceptable subjective QoS for five minutes. The six single port outages caused service denials and unacceptable subjective QoS for 30 s for each event as the links recovered.

In Year II, there were 3 single port failures, no 5 port failures, and one 10 port failure that took 30 minutes to repair. The resultant total DPM for Year II showed a marginal DPM improvement to 72,2. However, in Year I the customer's users did not experience any service downtime, while in Year II all of the customer's service subscribers experienced a 30 minutes outage. If the SLA between the Provider and the Customer was 75 DPM, then for both years the SLA had been met. However, if the customer's SLA with the service subscribers was 100 % availability, then for Year II this SLA would not have been met.

Table 8.2: Year II

Failure Mode Impact	Number of Failures	Failure Duration (minutes)	DPM Contribution	End-user Service Impact
10 ports down (10 Gbit/s)	1	20	38,0	All service subscribers experience a 30 minutes outage
5 ports down (5 Gbit/s)	0	0	0	None
1 port down (1 Gbit/s)	3	60	34,2	Unacceptable QoS and service denials 3 times that lasted 30 s as the links recovered for both VoIP and Data services
Total DPM 72,2				

As we can see from the previous example, the application of DPM for ports provides limited insight into the impact of its individual contributors on the service as experienced by the users. Hence, one DPM measure, by itself, *cannot* sufficiently capture reliability management from both a service provider's perspective as well as from a customer's perspective. DPM serves as a useful tool in managing network element reliability. However, customer SLA's need to be written with additional reliability measures (e.g. service transaction DPMs), which can drive DPM objectives for network element reliability. In this example, a strict customer SLA requirement would drive the design such that all 10 ports cannot fail at the same time.

8.2 Reliability/availability SLA types

Several types of SLAs are considered below:

EXAMPLE: SLAs between an ISP (Internet Service Provider) and a service user, and between a TSP (Transport Service Provider) and an ISP.

For the former, the ISP is providing a wide range of services to end-users, and for the latter the TSP is providing transport of packets across a backbone network.

The following clauses list and define a set of metrics appropriate for different types of SLA.

8.2.1 ISP to user reliability/availability SLA metrics

Service activation/change time: The time to activate a service or a service change measured from receipt of the request to when service/service change is ready for successful use (functions as specified).

Service restoration ratio: The percentage of service restorations that are successfully completed by the service provider in less than "t_r" minutes, where t_r is the time to restore the service.

Response time: The time to respond to a query measured from the acceptance of the query to the time that a plan is communicated to respond to the query.

User service outage downtime: The average proportion of time over the specified service interval that an individual user cannot use the network service because it is either unavailable or of unacceptable QoS for durations longer than "t_o" seconds, where "t_o" seconds is the user tolerance threshold for the service outage.

User service denial frequency: The percentage of service access attempts by an individual user that is not successful. A failed attempt is one where the access delay is longer than "t_d" seconds, where "t_d" seconds is the user tolerance to access delay for that service.

User service disconnect frequency: The percent of user service sessions that are disconnected prematurely. A premature disconnect is one where the service session has been disconnected and has to be re-established when the network is ready to do so.

Failed service transaction request: The percentage of service sessions where information transaction requests are not successful the first time. A failed information transfer is one that takes longer than "t_i" seconds, where "t_i" seconds is the user threshold for delay of the service transaction or arrives corrupted and therefore needs to be re-sent.

User service failed termination: The percentage of service termination attempts by a user that is not successful. A failed termination attempt is one that takes longer than "t_t" seconds, where "t_t" seconds is the user threshold for service termination delay.

8.2.2 ISP to ISP metrics

Service activation/change time: The percent of service/service change requests that are completed within "t_a" minutes, measured from the receipt of the requests to when services/service changes are ready for successful use (functions as specified).

Service restoration ratio: The percentage of service restorations that are successfully completed by the service provider in less than "t_r" minutes.

Response time: The percentage of queries that are responded to within "t_r" minutes, measured from acceptance of the query to the time that a plan is communicated to respond to the query.

Service outage downtime: The average proportion of time over the specified service time where all ISP transport service is either unavailable or of unacceptable performance quality for periods longer than "t_o" seconds, where "t_o" seconds is service outage threshold.

Service outage failure rate: The average number of outage incidents over the specified service time where all ISP transport service is either unavailable or of unacceptable performance quality for periods greater than "t_f", where "t_f" is service failure threshold.

Service degradation downtime: The average proportion of time over the specified service time that a specified percentage of bandwidth is either unavailable or of unacceptable performance quality for periods greater than "t_o" seconds, where "t_o" seconds is service failure threshold.

Service degradation failure rate: The average number of degradation incidents over the specified service time that a specified percentage of bandwidth is either unavailable or of unacceptable performance quality for periods greater than "t_f" seconds, where "t_f" seconds is service failure threshold.

8.2.3 TSP to ISP reliability/availability SLA metrics

Service activation/change time: The percent of service/service change requests that are completed within "t_a" minutes, measured from the receipt of the requests to when services/service changes are ready for successful use (functions as specified).

Service restoration ratio: The percentage of service restorations that are successfully completed by the service provider in less than "t_r" minutes.

Response time: The percentage of queries that are responded to within "t_r" minutes, measured from acceptance of the query to the time that a plan is communicated to respond to the query.

Service outage downtime: The average proportion of time over the specified service time where all ISP transport service is either unavailable or of unacceptable performance quality for periods longer than "t_o" seconds, where "t_o" seconds is service outage threshold.

Service outage failure rate: The average number of outage incidents over the specified service time where **all** ISP transport service is either unavailable or of unacceptable performance quality for periods greater than "t_f", where "t_f" is service failure threshold.

Service degradation downtime: The average proportion of time over the specified service time that a specified percentage of bandwidth is either unavailable or of unacceptable performance quality for periods greater than "t_o" seconds, where "t_o" seconds is service failure threshold.

Service degradation failure rate: The average number of degradation incidents over the specified service time that a specified percentage of bandwidth is either unavailable or of unacceptable performance quality for periods greater than "t_f" seconds, where "t_f" seconds is service failure threshold.

8.2.4 ISP to supplier metrics

Dead-on-arrival: The average percentage of defective hardware delivered hardware, between receipt and Solution cut-over.

Software release insertion aborts: The average percentage of software release insertions that need to be aborted because of software defects.

Maintenance costs: The costs for planned and unplanned maintenance actions required to ensure that the SLAs are met for each and all of the network services. The unit of measure is maintenance costs per unit of service per year.

Network upgrade cost: The average cost to the network service provider for upgrading the network to the next network element version. The unit of measure is cost per network element per upgrade.

Spares inventory costs: The cost of the spare network element equipment required to meet the network services reliability requirements.

Maintenance controlling downtime: The proportion of time when a network element cannot be controlled remotely to conduct maintenance activities. The unit of measure is "minutes per year".

SLA monitoring downtime: The proportion of time the SLA monitoring system is either measuring incorrectly or is not available for any measurements. The unit of measure is "minutes per year".

Billing downtime: The proportion of time the billing system is either recording incorrect billing data or losing billing. The unit of measure is "minutes per year".

Support availability: The amount of time the network supplier's support services are available to the network service provider. The unit of measure is hours per year.

Support responsiveness: The percentage of successful supplier responses that occur within time "t_s", where "t_s" is measured from the time network supplier is notified to when the problem is corrected to the satisfaction of the network service provider.

Problem resolution: The percentage of successfully corrected network problems by the network supplier.

8.2.5 Network attributes and metrics

Network element outage failure rate: The frequency of network element outages of greater than "t_o" second durations, where "t_o" seconds is sufficient to cause a network service outage. The metric is applied for all service impacts from partial to complete network element outages. The unit of measure is "failures per year".

Network element service interruption failure rate: The frequency of network element outages that are greater than "t_i" second, where "t_i" seconds is sufficient to cause a network service to be prematurely interrupted. The unit of measure is "failures per year".

Network element outage downtime: The amount of time a network element is unable to perform its network function(s) for durations greater than "t_o" second durations, where "t_o" seconds causes a network service outage. The metric is applied for all service impacts from partial to complete product outages. The unit of measure is "minutes per year".

Unplanned maintenance actions: The average number of unplanned maintenance actions due to hard and transient technology failures. The unit of measure is "maintenance actions per unit of bandwidth per year".

Fault isolation: The percentage of the network element's failure rate that can be isolated to a specified number of hardware repairable units.

Repairability: Percentage of repair actions completed within a designated time "t_r". The metric "t_r" is measured from the time the craft person initiates the repair until the system is returned to the pre-failure state.

Path restoration time: As a result of an equipment or facility failure in the solution, the amount of time that it takes to reroute all affected user "units" of traffic to its original destination.

Node restoration time: As a result of a "node" failure in the solution, the amount of time that it takes to reroute all affected user "unit" of traffic to its original destination.

Solution restoration coverage: The percentage of network element failures in the solution that are successfully detected and recovered by the network.

Network protection capacity reduction time: The proportion of time that the network is operating in simplex mode (i.e. misleading the user to believe that he is being protected when he is not). The unit of measure is "minutes per year".

Network reachability: The percentage of the end-to-end paths with connectivity for a specific user.

8.3 Prediction analysis modeling

8.3.1 Design guide for IP based network reliability prediction and analysis

Mitigation of failure rates is achieved by the use of mature technologies and good design practices. To further improve solution reliability, masking design approaches such as network element redundancy or network link protection are used.

Network design requires architectures that ensure reachability, restoration/protection for network recovery from failures and adequate provisioning. These three design elements must be defined for both the network solution's "nominal state" (e.g. where there are no failures) as well as for its various failed or recovered states. For example, it is important to ensure that when a Router fails and recovers to a state where all its previous paths are re-routed through alternate ones, that all recovered paths will provide adequate bandwidth and reachability. If not, then the recovered states could cause significantly degraded performance.

Current reliability evaluation methods are focused on products (e.g. network elements), and hardware reliability. Telecordia has specified two methodologies: (i) SR-332 [9] describes device-level reliability predictions, and (ii) SR-TSY-001171 [10] describes how to transform device failure rates into product reliability performance predictions. These methods need to be extended to include networks, multi-services and software [12], [13]. Once extended, methods would have to be standardized across the industry so that network service providers can compare network solutions and the risks and parameter sensitivities of different network solution options.

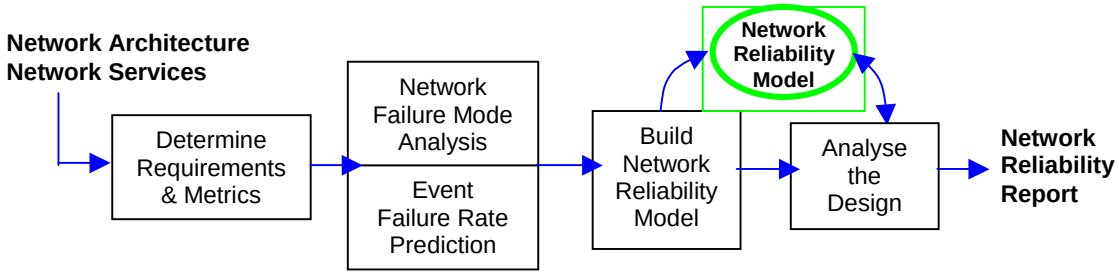


Figure 8.5: Network reliability prediction and analysis

The following proposal describes how to build a network reliability model to predict the various primary and secondary attributes for the various "events" (see figure 8.5).

The key enhancement is the Network Failure Modes Analysis. For each failure mode, the impact on the network service, both during and after recovery, is determined. This requires knowledge of the failure thresholds of the service applications. The following provides an overview of the methodology steps.

Step 1: Requirements and metrics determination

Service and operations reliability requirements need to be set for each of the network services. Factors to be considered when setting the requirements are:

- User expectations of service-reliability and willingness to pay.
- Potential revenue services.
- Cost of providing the service reliability.

- Impact on the number of users caused by various classes of network failure.
- Regulatory requirements.

The requirements need to be expressed in metrics that are defined in the context of the network. We propose two types of service reliability metrics: path metrics and impact metrics. The path metrics define the service reliability (e.g. downtime, ineffective attempts, dropped connection) between two points in the network. The calculation includes any event in the network that would impact the metric for that path. This means that a failure of a router somewhere else in the network, (not in the direct path defined in the routing table) would be included in the calculation if its failure impacts the service reliability of the specified path.

Impact metrics calculate the service reliability that impacts a specific group of users. Requirements would be more stringent for failure modes impacting 30 000 users versus 1 000 users. These metrics replace the product specific metric called system or partial system outage downtime. The new approach ensures that the metric is architecture independent. This metric is calculated considering a specific group of users or bandwidth, not for any group of users or bandwidth. This ensures that the metric is not inherently network size dependent. However, as described for the path metrics, the impact metrics must consider any network failure that impacts the specific group of users.

Besides service reliability, operations reliability and maintenance metrics and requirements need to be defined. Operations reliability metrics for such as loss of billing, loss of diagnosibility and loss of management control should apply the same approach as described for the service reliability metrics. The maintenance metrics calculate the sum of all hardware and software failures that either cause a maintenance action or a return. These metrics are measured as a frequency per subscriber or per unit of bandwidth.

Step 2a: Network failure modes analysis

The next step is to do "walk-throughs" of the network architecture, and for each of the metrics, conduct a failure mode analysis. For each event, the following must be determined:

- Detection mechanism: time and impact on the *service reliability metric* during detection.
- Recovery mechanism: time and impact on the *service reliability metric* during recovery.
- Recovery state: protection resource and impact on the *service reliability metric* until repaired to the normal state (this includes the impact of the repair action).
- How the network management system is notified for repair.

The events should include hardware failures, software failures and OAM activities of product upgrades and network re-configuration.

Step 2b: Network failure rate prediction

For each of the "failure-events" defined in the failure mode analysis, failure rate predictions are calculated. They should be estimated based on the following approaches:

- *Hardware:* SR-332 failure rate prediction methods for units and devices. The methods incorporating laboratory and field data should be used when the data are available [9].
- *Software:* Design complexity tool correlated to controlled laboratory test data or field data.
- *OAM activities:* For planned activities, use the average anticipated frequency of planned upgrades and a probability factor of human error correlated to field or laboratory data. For unplanned activities, use the predicted hardware and software failures (calculated as indicated in 1 and 2 above) that require a repair action. The human error factor is applied here as well.

Step 3: Network reliability model construction

There are two types of models: service/operations reliability and maintenance actions. The reliability model is used to calculate the service reliability performance of service downtime, service denials, dropped connections, etc., as well as the operations reliability performance. Since IP networks are fully or partially meshed, and their network elements employ fault tolerance, a Markov model is constructed from the failure mode analysis results. The Markov model simply describes the failed states of the network and the transitions between the states are either the failure mode failure rates calculated in Step 2b or the recovery and repair "rates" determined in Step 2a. This method extends SR-TSY-001171 [10] to the network level. For consistency and repeatability, common notation needs to be devised and agreed upon across the industry.

The maintenance action prediction model is simply the sum of all the events that require either a planned or unplanned maintenance action. The maintenance model considers repairs for both service-affecting events as well as non-service-affecting events. The model requires an assumed configuration of the entire network. Configurations should be done for typical and worst case configurations.

Step 4: Network solution design analysis

When the models are validated, they are used to vary the secondary parameters to determine the impact on the primary parameters. There are two objectives:

1) identify opportunities to optimize the design to meet the service and operations reliability requirements at minimal ongoing maintenance costs;

2) identify the critical secondary parameters to understand the primary parameters' sensitivity to them.

Network Solution Design Enhancement

From the previous analysis, critical areas are identified where the network design contributes significantly to the service failures and outages. Topology, provisioning, restoration, and protection enhancements are made to mitigate the critical areas. Table 8.3 lists various failure causes and suggested solution strategies.

Table 8.3: Solution Strategies

Failure cause	Solution strategy
Hardware Failures	Device integration Well-centered designs Proven technology Hardware redundancy Distributed functional partitioning Network restoration/protection Multi-homing
Software Failures	Development process maturity Graduated software failure restoration Software fault tolerance Distributed functional partitioning Multi-homing Network restoration/protection
Facility Failures	Buried and conduit-protected Signage to prevent accidental cuts Physical link diversity Network restoration/protection Multi-homing
Environmental Incidents	Site location / building integrity Network Element environmental robustness Site duplication
Traffic Overloads	Traffic overload filtering Buffer design Link/node provisioning for both nominal and recovered states

Step 5: Results reporting

The reliability report should contain the following:

- An overview of the network architecture required to meet the requirements.
- A summary of the predictions compared to the requirements.
- A list of prediction modeling assumptions.
- Attachments that describe the network reliability models.
- Attachments that describe the parameter sensitivities.

8.4 How to use the metrics

8.4.1 Reliability/availability SLA proposal

Current SLAs, used to make legally binding service contracts with service customers, consider a wide range of Quality of Service attributes such as delay, throughput, utilization and packet loss. However, they are not equally rich in service reliability attributes such as service denial, service failure, and service downtime. SLAs specify network availability. They do not address the complete reliability "experience" from an end user's perspective. Further, the monitoring of reliability attributes is problematic. These attributes exhibit statistical variability and hence "point-estimates" are not representative for small measurement windows.

8.4.1.1 Terminology

In the present document the following terms are used as defined:

- *Service Failure Rate*, the frequency of service failure, is used to describe service reliability.
- *Service Downtime* is used to describe service availability.

These terms each require a definition of service failure:

- *Service Failure Threshold* is the service user's threshold between unacceptable and acceptable QoS.

Thus, a *reliability/availability-SLA* is a contractual agreement between service providers and service users that specifies the service reliability and service availability performance that the network solution provides.

8.4.1.2 Service *vs.* network solution reliability/availability

The applications that are provided by IP network service offerings experience network outages as packet delay and loss. Therefore network outages impact differently depending on the type of service as well as the extent and duration of the network outage. Service reliability attributes such as service denial, service failure rate, premature service disconnection, and service downtime are service failures that depend on the network outage duration and frequency, as well as whether or not the user is using the network at the time of the network failure.

Users' tolerance to service impairments depend on a multitude of human factors that vary depending on the service type, service criticality, and the user's willingness to pay for the service. Because service features vary in their robustness to network delay and packet loss, the reliability/availability requirements vary for multi-service IP based networks.

To illustrate this point, figure 8.6 depicts two curves that describe the outage frequency profiles versus the duration of outages. Network unavailability is the area under the curves. A service with real time interactive features such as voice would experience an unacceptably higher service failure rate and service downtime using Network B than when using Network A. However, a service such as Web Browsing over TCP and where both the users and the application are more tolerant to delay, Network B would provide acceptable service reliability.

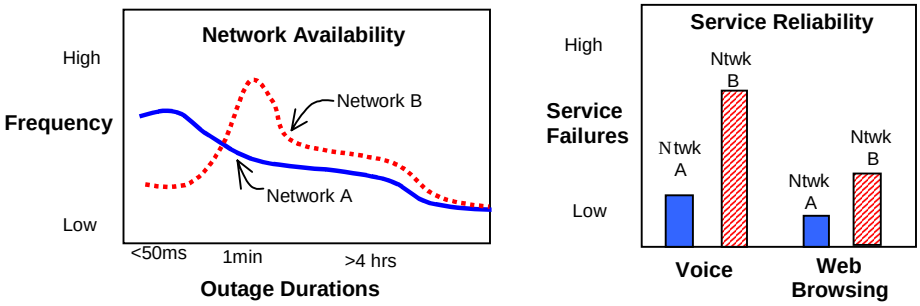


Figure 8.6: Network availability *vs.* service reliability

8.4.1.3 Reliability/Availability SLA Framework

8.4.1.3.1 Introduction

Most of the reliability/availability SLA requirements will be driven by the market. The challenge for the Service Provider is to set best-in-class reliability/availability SLAs, yet minimize the cost to own, operate and maintain the Network Solution. This means that reliability/availability SLAs are a set of requirements that are based on business trade-offs that are centered on optimizing the Network Solution to maximize revenues and minimize costs.

For some level of consistency across the industry, a standard set of reliability/availability SLA metrics is required. The following framework is a proposed template that is used to specify consistent reliability/availability SLAs. To illustrate how to use the framework a typical set of reliability/availability SLAs are defined. Note that this proposal does not recommend that the actual values of the reliability/availability SLAs become industry standards, but rather they are competitive attributes as part of any service offering.

8.4.1.3.2 Reliability/availability-SLA process

The following is a set of steps (see figure 8.7) used to specify reliability/availability-SLAs:

1) Propose an initial set of metrics depending on service type.

2) Propose initial set of reliability/availability SLA requirements and agreement conditions based on:

   a) User Tolerance to failure and downtime.

   b) Impact of service failure and downtime.

   c) Regulatory requirements.

   d) Competitors' offers, current and anticipated..

3) Assess the business risk of initial set of requirements:

   e) Range of revenue/market share potentials, assumptions and risks.

   f) Range of network solution costs, assumptions and risks.

4) Define reliability/availability SLAs and associated network solution reliability, availability and maintainability requirements to satisfy the reliability/availability SLAs.

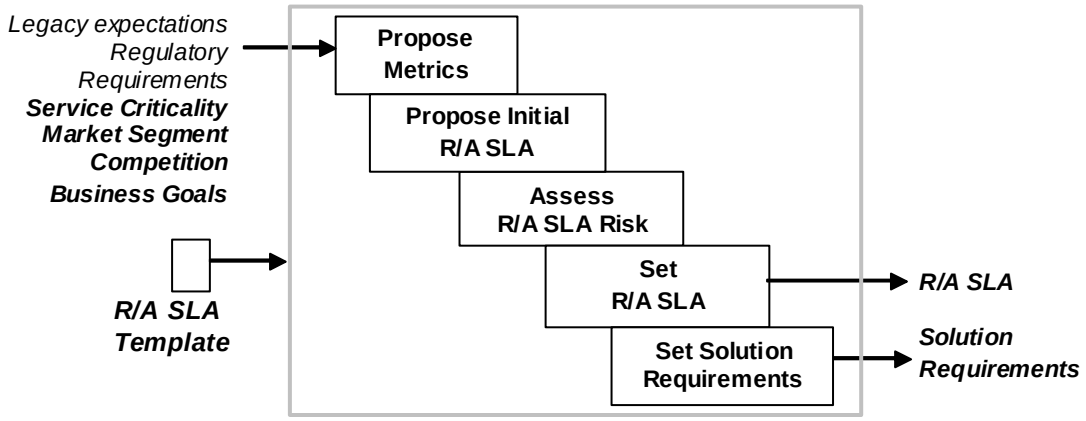


Figure 8.7: Reliability/availability SLA process steps

8.4.1.3.3 Reliability/availability SLA template

The following template lists the key clauses of an reliability/availability SLA: *Conditions, Categories, and Metrics*. Not all template metrics are used for all services and in all markets. They represent the set of metrics from which the Service Provider chooses based on business considerations.

8.4.1.3.4 Reliability/availability SLA conditions

The reliability/availability SLA requirements shall be met subject to the following conditions:

1) *Service Period* is the period of total calendar time that the reliability/availability SLA applies (e.g. 24/7 or excluding a specified maintenance window).

2) *Measurement Conditions* defines the measurement method and statistical parameters used to determine compliance/non-compliance. This is required to minimize compliance/non-compliance decision errors due to statistical variability.

3) *Types of Causes* specifies types of events that contribute to the reliability/availability SLA impairment. The following should be considered and addressed:

   a) Equipment coverage (e.g. Service Provider's only).

   b) Event types: hardware, software failures, OAM&P activities, traffic overloads, environmental and sabotage.

   c) Event causes: service provider attributed versus user attributed.

8.4.1.3.5 Reliability/availability SLA categories

The service class hierarchy is dynamic depending on the service type and the market segment. The proposal is to combine in various ways and in varying degrees two independent attributes of a service:

1) *Service Criticality:* categorizes the criticality of the service from the users' perspectives. The criticality drives the requirements for service failure rate, service failure duration and service failure impact.

2) *Service Feature Traffic Types:* categorizes the nature of the time dependency of the service feature (drives the user service failure thresholds).

Table 8.4 summarizes the main categories of reliability/availability SLAs.

Table 8.4: Reliability/availability SLA category

R/A SLA Category	Traffic Type	Service Criticality	Description	Examples
A1	Real-time interactive	Mission-critical	For real-time interactive services where service outages are not tolerated because of the severity of impact.	Voice for 911, hospitals, airports, national security, emergency services, stock market, etc.
A2		Critical	For real-time interactive services where high service availability is expected: a low level of service downtime can be tolerated.	Uni-access residential voice, interactive video for businesses, etc.
A3		Non-critical	For real-time interactive services where service failures and outages are tolerated.	Multi-access residential voice, residential e-gaming, etc.
B1	Non-real-time interactive	Mission-critical	For non-real time interactive services where service outages are not tolerated. Because of the severity of impact.	Interactive transaction processing for big accounts for the stock market, banking, etc.
B2		Critical	For non-real-time interactive services where high service availability is expected: a low level of service downtime can be tolerated.	Interactive transaction processing for small to medium e-commerce transactions, etc.
B3		Non-critical	For non-real-time interactive services where service failures and outages are tolerated.	Residential Web browsing, Telnet, etc.
C1	Non-real time non-interactive	Mission-critical	For non-real time non-interactive services where service outages are not tolerated. Because of the severity of impact.	Email, FTP, etc. for hospitals, stock market, banking transactions.
C2		Critical	For non-real-time non-interactive services where high service availability is expected: a low level of service downtime can be tolerated.	Critical email, FTP, etc. for business communications, etc.
C3		Non-critical	For non-real-time non-interactive services where service failures and outages are tolerated.	Non-critical email, FTP, etc. for residential communications, etc.

8.4.1.3.6 Sample reliability/availability SLAs

To illustrate the template the following lists sample reliability/availability SLAs between an ISP and a service user or group of service users. Note that these numbers should not be viewed as proposed industry standards.

Category A1 **Type: ISP to Service User** EXAMPLE: Voice over IP service for a Stock Exchange.	
Metric	**Requirement**
Service Activation/Change Time	< 24 hours
Service Restoration	< 30 minutes 100 % of the outage incidents.
Problem Response Time	< 5 minutes 95 % of outage incidents.
Catastrophic Service Outage (e.g. > 90 % of users impacted)	0 minutes per year for periods greater than 10 s, averaged over one year.
Major Service Outage Downtime (e.g. 10-90 % users impacted)	Averages < 0,5 minutes per year for periods greater than 10 s, averaged over one year.
Minor Service Outage Downtime (e.g. < 10 % of users impacted)	Averages < 1 minute per year for periods greater than 10 s, averaged over one year.
User Service Downtime	Averages < 5 minutes per year for periods greater than 10 s, averaged over one year.
User Service Access Failure Rate	Averages < 10 per 10^6 user attempts per year where it takes longer than 5 s to access the service.
User Service Information Transfer Failure Rate	Averages < 10 per 10^6 user-minutes per year where latency is greater than 50 ms
User Service Premature Disconnect	Averages < 10 per 10^6 user-sessions per year.
Conditions: This agreement shall be met for 24/7 or the Service Provider shall give the customer 3 months free service. Failures or impairments attributed to the customer or equipment not owned by the Service Provider are not considered.	

Category A2 ***Type: ISP to Service User*** EXAMPLE: Voice over IP service for residential access.	
Metric	**Requirement**
Service Activation/Change Time	< 24 hours
Service Restoration	< 240 minutes 100 % of the outage incidents.
Problem Response Time	< 30 minutes 95 % of outage incidents.
User Service Downtime	Averages < 15 minutes per year for periods greater than 30 s, averaged over one year.
User Service Access Failure Rate	Averages < 50 per 10^6 user attempts per year where it takes longer than 10 s to access the service.
User Service Information Transfer Failure Rate	Averages < 50 per 10^6 user-minutes per year where latency is greater than 50 ms
User Service Premature Disconnect	Averages < 50 per 10^6 user-sessions per year.
Conditions: This agreement shall be met for 24/7 or the Service Provider shall give the customer 3 months free service. Failures or impairments attributed to the customer or equipment not owned by the Service Provider are not considered.	

Category A3 **Type: ISP to Service User** EXAMPLE: IP e-gaming service for residential users.	
Metric	**Requirement**
Service Activation/Change Time	< 24 hours
Service Restoration	< 240 minutes for 100 % of the outage incidents.
Problem Response Time	< 60 minutes for 95 % of outage incidents.
Individual User Service Access Failure Rate	Averages < 1 per 1 000 user attempts per year where it takes longer than 5 s to access the service.
Individual User Service Information Transfer Failure Rate	Averages < 1 per 1 000 user-sessions per year where latency is greater than 200 ms
Individual User Service Premature Disconnect	Averages < 1 per 1 000 user-sessions per year.
Conditions: This agreement shall be met for 24/7 excluding 2 hours per month for server enhancements that will occur at pre-defined intervals with 1 week notice or the Service Provider shall give the customer 3 months free service. Failures or impairments attributed to the customer or equipment not owned by the Service Provider are not considered.	

Category B2 ***Type: ISP to Service User*** EXAMPLE: e-commerce transaction with customer..	
Metric	**Requirement**
Service Activation/Change Time	< 24 hours
Service Restoration	< 240 minutes 100 % of the outage incidents.
Problem Response Time	< 30 minutes 95 % of outage incidents.
Business to any client Service Downtime	Averages < 15 minutes per year for periods greater than 10 s, averaged over one year.
Client Service Access Failure Rate	Averages < 50 per 10^6 user attempts per year where it takes longer than 10 s to access the service.
Business to client Information Transfer Failure Rate	Averages < 50 per 10^6 user-minutes per year where latency is greater than 5 s
Business-to-client Premature Service Disconnect	Averages < 50 per 10^6 user-sessions per year.
Conditions: This agreement shall be met for 24/7 or the Service Provider shall give the customer 3 months free service. Failures or impairments attributed to the customer or equipment not owned by the Service Provider are not considered.	

Category C3 **Type: ISP to Service User** EXAMPLE: Email service for residential users.	
Metric	**Requirement**
Service Activation/Change Time	< 24 hours
Service Restoration	< 240 minutes for 100 % of the outage incidents.
Problem Response Time	< 60 minutes for 95 % of outage incidents.
User Service Access Failure Rate	Averages < 1 per 100 user attempts per year where it takes longer than 5 s to access the service.
User Service Information Transfer Failure Rate	Averages < 1 per 1 000 Emails that do not arrive to the destination within 120 minutes.
User Service Premature Disconnect	Averages < 1 per 100 user-sessions per year.
Conditions: This agreement shall be met for 24/7 excluding 2 hours per month for server enhancements that will occur at pre-defined intervals with 1 week notice or the Service Provider shall give the customer 3 months free service. Failures or impairments attributed to the customer or equipment not owned by the Service Provider are not considered.	

8.5 Guides

8.5.1 Supplier compliance guide

To de-risk the introduction of a network solution, the ISP should be involved throughout the supplier's development and introduction lifecycle of the solution. The following lists this involvement:

- The Service Provider should review the supplier's network reliability, availability and maintenance predictions. These predictions should include both the network-wide metrics as well as the network element's contribution to them. The suppliers should include the details of the prediction models, methodology, assumptions and provide sensitivity analysis of critical parameters and show how the critical parameters are under adequate control. The predictions should address the appropriate *ISP to supplier* metrics defined clause 8.2.4.
- The Service Provider works with the supplier to customize the spares inventory plan.
- The Service Provider should review the solution's test results and track the supplier's action plans on outstanding issues.
- The Service Provider works with the supplier to define the customer acceptance test plan including reliability readiness criteria.
- The Service Provider works with the supplier to define and execute a field study plan to track field reliability performance *vs.* requirements and action plans on outstanding issues.
- The Service Provider should review the supplier's process improvement plans and their status.

8.5.2 Service solution reliability/availability SLA guide

Most reliability/availability SLA requirements will be driven by market competition rather than industry wide agreed requirements. The challenge for the Service Provider is to set best-in-class reliability/availability SLAs, yet minimize the cost of operations and maintenance. This means that reliability/availability SLAs are a set of requirements that are based on business trade-offs that are centered on optimizing the network solution to maximize revenues and to minimize costs.

Currently there are only two common reliability SLA metrics: *Service Restoration Time* and *Network Availability*, though end users care also about the frequency of service denials and service interruptions.

Network Availability is, in the most part, not consistently nor rigorously defined. In the SLA cases where it is, the ISP specifies an ingress port to egress port availability across the ISP network. A failure criterion is also defined (e.g. durations greater than 1 minute), as well as a time period (e.g. averaged over one month). All ISPs define what equipment and what types of failure events are not included (e.g. not the customer premises equipment, not acts of God such as floods). Typically the defined compensation for an outage is for every hour lost the ISP will pay for one day service cost- not the cost of the outage on the service customer's business. As well, most ISPs only write reliability SLAs for their own network. There are a few exceptions where the ISP negotiates SLA agreements with other ISPs and, based on these, sets a network wide SLA for their customers. For many reliability SLAs, Network Availability is the average across the network, so if a particular customer experiences an outage compensation is not given if the average for the network over the specified time period is below that defined in the SLA.

It is proposed to use the metrics and metric definitions defined in clause 8.3. The following is a set of steps used to set reliability/availability SLAs.

1) Propose an initial set of metrics depending on service type, selected from those defined in clause 8.2, *ISP-to-User and ISP-to-ISP*.
2) Propose reliability/availability SLA requirements and agreement conditions based on:
    a) User tolerance to failure and downtime and willingness to pay.
    b) Impact (e.g. number of users or amount of bandwidth) of service failure and downtime.
    c) Regulatory requirements.
    d) Competitors' offers- both current and anticipated.

3) Assess the business risk of initial set of requirements:

   a) Range of revenue/market share potentials, assumptions and risks.

   b) Range of Network Solution costs, assumptions and risks.

4) Set reliability/availability SLA requirements and associated network solution reliability, availability and maintainability requirements to satisfy the reliability/availability SLAs.

The reliability/availability SLA conditions should address all of the following:

1) *Service Period* is the period of total calendar time that the reliability/availability SLA applies (e.g. 24/7 or excluding a specified maintenance window).

2) *Measurement Conditions* defines the measurement method and statistical parameters used to determine compliance/non-compliance. This is required to minimize compliance/non-compliance decision errors due to statistical variance.

3) *Types of Causes* specifies types of events that contribute to the reliability/availability SLA impairment. The following should be considered and addressed:

   a) Equipment coverage (e.g. Service Provider's only).

   b) Event types: hardware, software failures, OAM&P activities, traffic overloads, environmental, and sabotage.

   c) Event causes: service provider attributed verses user attributed.

8.5.3 Network solution reliability/availability measurement guide

Network wide reliability metrics for a solution are not directly measured but are calculated from the individual failure modes of links and nodes that can be directly observed or measured.

The network wide metrics are calculated either based on each specific network configuration or for a set of specified reference networks. The latter is preferable because it would require less specific network knowledge and provide more readily comparable results. The measured network failure modes are classified and averaged based on the population size (nodes and links) and used in the metric calculations. Predictions are also calculated from the predicted rates for the failure modes. A network reliability field performance report compares the actual network metric performance versus that predicted.

The metrics should be selected from those defined in clause 8.2.

The collected failure mode data used to calculate the network:

1) Determine the Network Element component that failed.

2) Time of failure (preferable time to failure).

3) Failure impact: amount of bandwidth or the number of users impacted.

4) Duration of the outage on subscriber service and/or on bandwidth.

5) Trouble report response time if required.

Also collect all network equipment failure occurrences and times that require a maintenance repair action.

The following network architecture information is required:

1) Network Elements: types and quantities.

2) Network ports: types and quantities.

3) Logic and physical topology including diversity information.

4) Link distances and conduit medium.

5) Link and node protection and restoration.

9 Application to cable networks

The TS 101 909 series of Technical Specifications address inter-operability of Network Elements for IP cable communications (*IPCablecom*). These specifications target the implementation over cable access networks of VoIP, with QoS equivalent to that of the PSTN [19], [38]. Therefore they relate to conveyance over cable access networks of real-time interactive traffic for a critical service, i.e. category A2 of table 8.4. IP backbones, other traffic types, and other service levels may be subjects for further study.

The following clause 9.1 reproduces from the architectural framework specification [37] the clause that describes the administrative architecture. Cable access uses cable modems to ITU-T Recommendation J.112 [36] working over a Hybrid Fibre Coax (HFC) network in order to interconnect Multimedia Terminal Adapters (MTAs) on the customer's premises to a Call Management Server (CMS).

Then clause 9.2 reviews the metrics relevant to PSTN equivalent VoIP service.

9.1 IPCablecom zones and domains

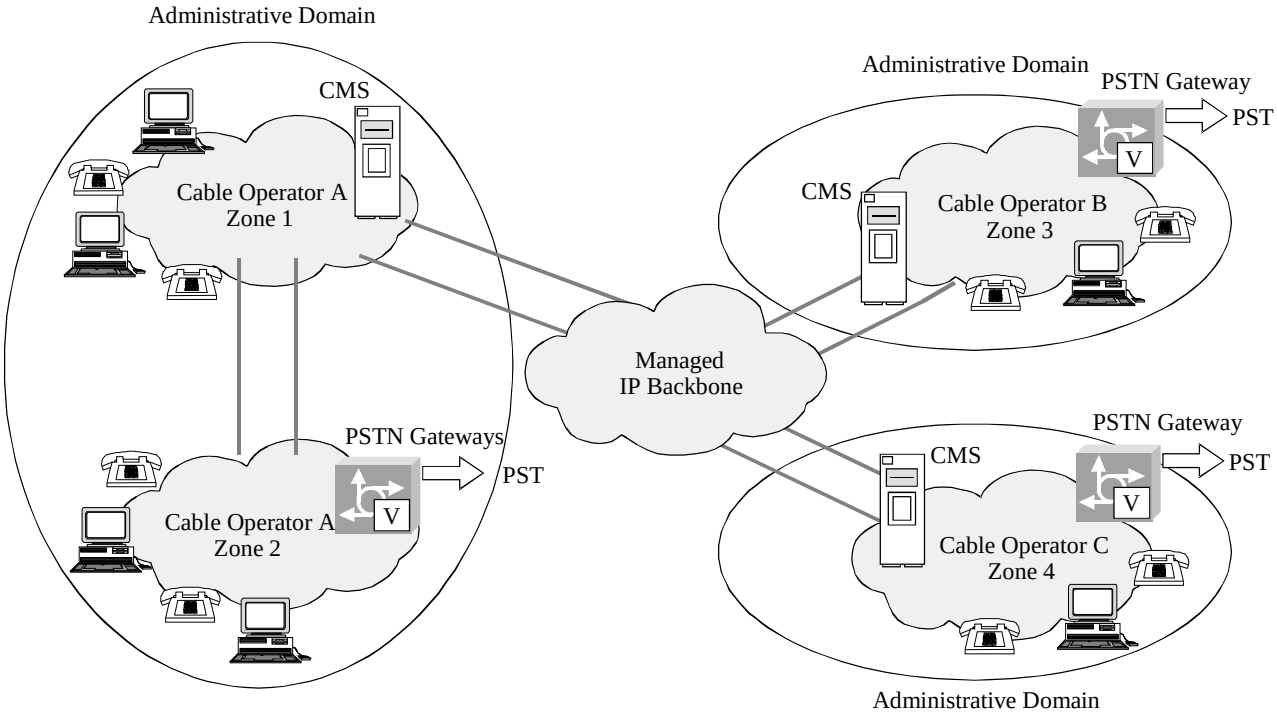


Figure 9.1: Zones and administrative domains

An IPCablecom zone consists of the set of MTAs in one or more J.112 HFC access networks that are managed by a single functional CMS as shown in figure 9.1. Interfaces between functional components within a single zone are defined in the IPCablecom specifications. Interfaces between zones (e.g. CMS-CMS) have not been defined and will be addressed in future phases of the IPCablecom architecture.

An IPCablecom domain is made up of one or more IPCablecom zones that are operated and managed by a single administrative entity. An IPCablecom domain may also be referred to as an administrative domain. Interfaces between domains have not been defined in IPCablecom and are for further study.

9.2 Applying the reliability/availability metrics and SLAs to IPCablecom

For VoIP with performance equivalent to the PSTN, metrics were presented in 8.4.1.3.6 in the table entitled Category A2. That table focussed on the specific case of an SLA between Service Provider and Service User. Note that the metrics given were examples only, as it is only the methodology that could be sutable for standardization, and not the specific metrics and example values.

Similar tables can be generated for SLAs between Service Provider and any other party, as was explained in clause 8.2. In particular, SLAs between Service Providers will relate to some of the boundaries between the administrative domains shown in figure 9.1. In this case, each of the relevant metrics, such as those listed in clause 8.2.2, needs to be derived from the value used in the Service provider/User SLA. The method for deriving consistent values for all of the Service Providers involved depends on the metric. For example, query Response Time may be solely the concern of the Service Provider facing the User, but Service Outage Downtime needs to be subdivided between all of the Service Providers that may be involved in providing the user with VoIP service.

Annex A:
Related work of other standards organizations

This annex identifies standards work that can be used to assist in the specification and analysis of network reliability and availability of IP-based networks. Although they address primarily circuit-switched networks, many of the techniques will be of use in IP based networks.

A.1 ITU-T Study Group 2 (operational aspects of service provision, networks and performance)

Study Group 2 addresses the overall operation of telecommunication networks. This work addresses: (i) various design alternatives for survivable networks, and (ii) parameters for exchanging network performance results among administrations (including customer affecting incidents and blocking defects per million). See ITU-T Recommendation E.436 [2].

The ITU-T Study Group 2 is also writing the E.TE Series of Draft Recommendations, which are relevant to IP Network Reliability. The E.TE Series of Recommendation describes, analyzes, and recommends Traffic Engineering (TE) methods which control a network's response to traffic demands and other stimuli, such as link failures or node failures. The functions discussed and recommendations made are consistent with the definition of TE employed by the Traffic Engineering Working Group (TEWG) within the Internet Engineering Task Force (IETF): "Internet Traffic Engineering is concerned with the performance optimization of operational networks. It encompasses the measurement, modeling, characterization, and control of Internet traffic, and the application of techniques to achieve specific performance objectives, including the reliable and expeditious movement of traffic through the network, the efficient utilization of network resources, and the planning of network capacity".

ITU-T Recommendation E.106 describes an International Emergency Preference Scheme for telecommunications services that will support recovery activities during crisis situations [37].

A.2 ITU-T Study Group 4 (telecommunication management, including TMN)

Study Group 4 is responsible for studies relating to the management of telecommunication services, networks, and equipment using the Telecommunication Management Network (TMN) framework. Additionally, they are responsible for other telecommunication management studies relating to designations, transport-related operations procedures, and test and measurement techniques and instrumentation. Study Group 4 is the Lead Study Group on TMN.

Study Group 4 is studying the restoration of failed international exchanges, and transmission systems. They are also working on Draft Recommendation M.ieps, "Service management functions across the X-interface for IEPS communications over internet-based multimedia services". IEPS stands for International Emergency Preference Scheme. Several Questions are relevant to IP Network reliability.

A.3 ITU-T Study Group 12 (end-to-end transmission performance of networks and terminals)

Study Group 12 is responsible for guidance on the end-to-end transmission performance of networks, terminals, and their interactions in relation to the perceived quality and acceptance by users of text, speech, and image applications. As Lead ITU-T Study Group on QoS and Performance, Study Group 12 provides leadership for the ITU-T in dealing with QoS-related issues. This leadership involves providing a roadmap for QoS activities that can be used to identify and resolve QoS-related issues across Study Groups. The measurement of QoS is important to the measurement and specification of network reliability/availability performance. QoS parameters are needed for the establishment of SLAs.

A.4 ITU-T Study Group 13 (multi-protocol and IP-based networks and their internetworking)

Study Group 13 is responsible for studies involving internetworking of heterogeneous networks encompassing multiple domains, multiple protocols and innovative technologies with a goal to deliver high-quality, reliable networking. Specific aspects are architecture, interworking and adaptation, end-to-end considerations, routing and requirements for transport.

Study Group 13 is also the Lead Study Group for IP related matters, B-ISDN, Global Information Infrastructure and satellite matters.

A.5 ITU-T Study Group 15 (optical and other transport networks)

Study Group 15 is the focal point in ITU-T for studies on optical and other transport networks, systems and equipment. This encompasses the development of transmission layer related standards for the access, metropolitan and long haul clauses of communication networks.

Study Group 15 is addressing transmission system requirements, including the protection requirements for Synchronous Digital Hierarchy (SDH) rings, and restoration requirements for Digital Cross-connect Systems (DCSs).

Study Group 15 is the Lead Study Group on access network transport and the Lead Study Group on optical technology. One important Recommendation in progress is G.8080 which covers automatic switched optical networks. They provide the capability to automatically establish optical connections (i.e. optical information transmission paths) using signaling methods similar to those used in today's circuit-switched networks.

A.6 ITU-T Study Group 16 (multimedia services, systems and terminals)

Study Group 16 is responsible for studies relating to multimedia service definition and multimedia systems, including the associated terminals, modems, protocols and signal processing. It is the Lead Study Group on multimedia services, systems and terminals and on e-business and e-commerce.

Study Group 16's work on ITU-T Recommendation F.706, "International Emergency Multimedia Services" and several questions in Study Group 16 are relevant to IP Network Reliability:

A.7 TMF (Telecommunications Management Forum)

The TMF has produced an SLA-Management-Handbook that is very pertinent to the work on Network Reliability/Availability [4]. See clause 8.3 of the present document for information on SLAs.

For more information see http://www.tmforum.org/

A.8 ETSI TIPHON (Telecommunications and Internet Protocol Harmonization Over Networks)

ETSI TIPHON's objective is to support the market for voice communication and related voiceband communication (such as facsimile) between users. It will ensure that users connected to IP based networks can communicate with users in Switched Circuit Networks (SCN - such as PSTN /ISDN and GSM), and *vice versa*.

- Working Group 02 develops reference architecture models and interfaces. These are important for defining and measuring network reliability.
- Working Group 05 defines Quality of Service classes and develops measurement methodologies. These can be used in the development of SLAs.

A.9 IETF (Internet Engineering Task Force)

The IETF is concerned with almost all aspects of IP-based networks and services. Many of their working groups have relevance to Reliability/Availability of IP based networks and services.

For more information see http://www.ietf.org.

A.10 IEEE (Institute of Electrical and Electronic Engineering)

802.17 is a relatively new working group under IEEE 802, which is tasked with developing a Resilient Packet Ring (RPR) Media Access Control (MAC) layer. This MAC will offer a both a competing technology to traditional 802.3 Ethernet and a way of extending Ethernet-based services out from the LAN to the MAN network.

RPR proposes to bring SONET-like reliability and OAMP monitoring with a packet-based Ethernet extension to a dual counter-rotating fiber ring topology. RPR proposes to improve fiber BW utilization while supporting both SONET/SDH and best effort connectionless packet data transport. There are RPR vendors already contemplating offering circuit-emulation services at OC-3 to OC-48 speeds without using the frame structure of SONET in order to be more bandwidth efficient, to better support bursty packet data and to push LAN services out to the MAN.

The Technical Committee on Communications Quality and Reliability (CQR) focuses on and advocates worldwide communications and reliability on behalf of, and within, the IEEE Communications Society. CQR serves as the catalyst for global awareness and the exchange of information relative to technical and management-related aspects of communications quality and reliability.

A.11 T1

T1 TR No. 55 [13] addresses the important topic of the Internet and its interactions with the public telecommunications network as it relates to reliability and survivability. Two main categories of reliability solutions are explored: network engineering and network architecture. Besides the important solutions offered in the body of the report, the appendices contain a selection of very useful information on the Internet. These include the major findings Internet Study Team of the Network Reliability Steering Committee of the American Alliance for Telecommunications Industry Solutions (ATIS), a description of the major Internet governing and standards bodies, a brief description of internet routing and transmission technologies, as well as discussions of QoS, availability, and current trends.

T1 TR No. 68 [14] combines, updates, enhances, and supercedes the Committee T1 Technical Reports Nos. 24 and 24A. The present document resolves some of the issues and questions left for further study from the previous reports.

Annex B:
Background - Traffic engineering

This annex surveys traditional traffic analysis methods developed for circuit-switched networks. Most of this annex is based on references [16], [17], [18].

B.1 Traffic analysis methods

Models, queuing theory, and analysis tools are all essential components in the current examination of traffic engineering. The following paragraphs summarize each of these components.

Models of traffic volumes have provided an understanding of probabilities of circuit availability and lost calls since the early days of telephony. A historical lineup of the principal models is shown below:

Year	Model Name and/or Inventor
1903	Rorty Model developed by Malcolm Rorty (later refined by Edward Molina)
1909	A.K. Erlang developed Erlang B and Erlang C models (used thru late 1970's)
1918	Engset model by T. Engset
1920	Molina developed a model used by AT&T in the 1920's ("Poisson process")
1920's	Retrial Model
1970's	Erlang C model is still used
1980	Retrial Model is enhanced by H. Jacobsen
---	Equivalent Random Theory Model

A discussion of the salient characteristics of the principal models is provided below.

B.1.1 Malcolm rorty model

This model, developed in 1903, began the study of traffic and congestion in the calling processes. Later, Edward Molina refined Rorty's traffic model, which is based on the following premises:

- An average holding time is the minimum time a call is held in the traffic-conveyance system, regardless of whether or not a call is blocked.
- If the quantity of calls exceeds the capability of the resource to handle that quantity, blocking occurs.

B.1.2 The Erlang B and Erlang C Models

These models were based on the following premises:

- Erlang B Model determines that calls that arrive at the system when all the traffic-carrying resources are in use are cleared from the system and do not return. In practice, "cleared" can mean rerouted to a traffic facility with available capacity.
- There can be an infinite number of sources of traffic; when the number of sources is finite, the predicted number of servers from the Erlang B model is too high to be practicable.
  In recent years, three enhanced models have evolved from the Erlang B model:
  - The Engset model.
  - The Equivalent Random Theory model.
  - The Retrial model.
- The Erlang C Model is based on the premise that calls that arrive at the traffic-carrying system when all the resources are in use are placed in an infinitely long (first-in, first out) queue, from which calls cannot be removed or abandoned until they are served by the system.

- In the Erlang C model, exponential arrivals and exponential holding times are assumed.
- The Erlang C Model has been adjusted to reflect the facts that:
  - Queued calls do not wait indefinitely for service.
  - Finite queues in real equipment make a significant difference in the probabilities.
- The Erlang C Model was used to derive a set of Erlang C Infinite Queuing tables, namely:
  - CCS capacity tables.
  - Probability of Delay tables.
  - Tables of Average Delay of Delayed Calls in Multiples of Holding Times.
  - Server Occupancy tables.
- The set of Erlang C Finite Queuing tables consists of tables like the four tables of the Infinite Queuing case, with the addition of a Queue Length Table.

B.1.3 The Engset model

This model, developed in 1918, is based on the probability that a call is blocked given a certain number of servers and sources. A recursive of the formula can be used to generate tables of probabilities of blocked calls.

B.1.4 The Molina model

The Molina model predicts the probability that a call is blocked in a system that neither reroutes nor queues. This model assumes that the user will retry at a later time. The holding times are not fully considered, as in Poisson's work, and the results are similar to Poisson's. This Molina-Poisson model is known as the Poisson process.

B.1.5 The retrial model

This model was first developed by R. Wilkinson and then later enhanced by H. Jacobsen. The model is based on the premise that when calls are blocked, the callers do not give up, but they hang up and try again. It was developed as an attempt to account for the discrepancy between reality and the Poisson model. The model assumes that:

- New calls arrive following an exponential interarrival time distribution,
- Blocked calls are retried, and
- Completed calls leave the system.

B.1.6 The equivalent random theory model

This model is based on the precept that for every peaked traffic load there is an equivalent random traffic load that yields the same quantity of overflow traffic when it is offered to a specific number of trunks. This model is used for determining the last-choice route in networks with alternate routing capabilities.

B.2 Queuing theory

Queuing theory is a branch of applied probability theory. Different types of probability distributions are used to mathematically model the behavior of customer interarrival times and the customer service times. Queuing theory shares many of the same models of traffic analysis as described in the Models clause above. A queue, or waiting line, is developed when the service facility cannot service all the units requiring service. An accurate representation of such a system requires a detailed characterization of the parameters and processes.

Queuing theory concepts, like their corresponding models, have applications in many disciplines including telephone system traffic. Initially, capacity is assumed infinite. However, in real life, loss systems have been used to model the behavior of many dial-up telephone systems and telephone switching equipment. Queuing systems with a positive but finite length have been deployed to characterize the performance of various computing and telecommunications systems where the finite queue models the finite amount of memory or buffer present in such real-world systems.

Queuing theory is important in studying both circuit switching and packet switching communications networks because the theory and its associated tools allow estimations of waiting time before achieving access to the server and waiting time before delivery of buffered message units. In packet switching networks, for example, where messages are divided into small units called "packets", the small message packets arrive at several intermediate nodes on their way to their ultimate destination. At each intermediate node the packets are stored in buffered memory before they are processed and forwarded to their proper link when the transmission facilities become available. The waiting time in question depends on such things as processing power/speed of the node, speed of the transmission link, size or length of the packets, traffic volume, etc. The estimation of this waiting time, along with a study of the queue length, is an important measure/descriptor of capacity, quality of service, and system performance of data transmission networks.

Queuing disciplines such as First In First Out (FIFO), Last In First Out (LIFO), and Priority, offer another level of detail to the system under analysis. Queuing Systems with Priority allow preferred or high-priority customers to be given service before others. For example, in packet-switched computer communications network using such a Priority Queueing System, packets containing voice or video signals may be given precedence over packets containing no real-time information. Of course, with each additional level of detail like inclusion of priority, the mathematical analysis in the models becomes much more complicated.

There are many performance tradeoffs in a given queuing system.

EXAMPLE: If one designed a system with a great many servers available (to reduce waiting time or eliminate queues), the system would be so large that the servers would likely be idle a large percentage of the time, resulting in a waste of resources and unnecessary expense. If, on the other hand, almost all customers are obligated to join long queues where all servers are busy much of the time, there would likely be customer dissatisfaction and probably lost customers, which again has undesirable economical consequences. Queueing theory and its analytical tools provide the designer with the necessary equipment to analyze the system and to ensure that the proper levels of resources are provided in the system design while avoiding undue cost. Simulation of such queuing systems then leads into various analysis tools that are available and that are discussed in the next clause.

One useful and intuitive formula from queueing theory is Little's Theorem, which states that the average arrival rate of customers to a queuing system times the average time spent in that system equals the average number of customers in the system. This result is extremely general in its application. A corresponding result relates the average number in queue with the average arrival rate and average time in queue.

B.3 Analysis tools

Analysis tools (e.g. software modeling and simulation packages) are essential in modern traffic engineering. This is especially important for computer networks, because the variety of sources and the characteristics of multimedia communication on these networks complicate resource allocation. Traffic characterization techniques for computer networks can be classified into the following categories: autoregressive moving average (ARMA) models, Bernoulli process models, Markov chain models, neural network models, self-similar models, spectral characterization, autoregressive modular models such as Transform Expand Sample (TES) and Quantized TES (QTES) models, traffic flow models, and wavelet models. The traffic descriptors are the mean, peak, and sustained rates, burst length, and cell-loss ratio. These values capture only the first-order statistics, and a need has been identified for descriptors that provide more information in order to describe highly correlated and bursty traffic.

Commercial networking software based on modeling and simulation technology is available to analyze traffic flow, communication systems, network performance and thus survivability. Such software can be used to design and optimize networks, communications equipment, and applications identifying possible congestion conditions that may result in a network degradation and/or failure.

All these modeling and queuing techniques combine to give us analysis tools that can be used to approximate the traffic flow of a network. As in all engineering efforts, there are tradeoffs of time and cost with accuracy and complexity. Even the best of models make assumptions, sometimes gross assumptions, and it is imperative to understand the limitations of each model. It is also important to understand the proposed system accurately. With a good understanding of both of these key components, one can model a proposed system accurately. Understanding the proposed system and the limitations of the models allows for an accurate simulation. Ultimately, the model is limited by the analyst's understanding of the system.

Annex C:
Traffic analysis over IP based networks

This annex provides perspectives on the traffic engineering problems inherent in packet-based networks. The focus is on traffic analysis aspects relevant to reliability, availability, and survivability. As traffic engineering is a critical step in the reliable delivery of telecommunication services, so traffic analysis techniques are important to the characterization and definition of network reliability and availability performance. The spread of IP-based networks and services has led to a need for better tools for assessing the survivability, reliability, and availability of these networks, particularly as IP infrastructures become more widely used in supporting telephony and other real-time services. While it has sometimes been assumed that IP networks will provide an inferior service for telephony, this assumption is perhaps only valid in limited applications (e.g. "best effort" service applied to telephony). As protocols that include resource reservation or other priority mechanisms are developed, implemented, and standardized, it is expected that services provided over IP networks will provide a quality of service equivalent to that provided by circuit-switched telephony (e.g. see [19], [38]).

From a reliability, survivability, and availability standpoint, IP-based networks could potentially offer superior performance because of their greater flexibility in routing and other factors. The problems of specifying and measuring survivability, reliability, and availability performance are being addressed by T1A1.2. This annex discusses aspects of this problem and introduces some tools for addressing the analysis of traffic on IP networks.

The goal of traffic engineering is to optimize performance of a network while efficiently utilizing resources. The IETF Traffic Engineering Working Group has produced a valuable document [20] which covers many aspects of the problem. In the present discussion, performance aspects relevant to reliability, availability, and survivability are the focus. The premise is that if the performance provided to users in a particular application falls below a certain threshold (due to network failures or traffic congestion or a combination of the two), then the network is no longer considered available for that application.

Traffic characteristics, analytical traffic models, and computer simulation models are the primary components of modern traffic engineering. Characteristics of data traffic play a crucial role in the development of both analytical and computer simulation models. Analytical methods and techniques continue to develop to address Internet Protocol (IP) and other packet-based networks. These continue to be topics of considerable research, with definitive solutions remaining elusive. Nevertheless, with realistic traffic characteristics and reasonable analytical methods, new computer simulations can be developed and used to design efficient networks and to accurately predict network performance. Traffic engineering studies can also facilitate improvements to network protocols, topologies, and routing and switching hardware, eventually leading to better user services.

The nature and characteristics of packet network traffic have changed dramatically, both quantitatively and qualitatively, over the past decade. Quantitatively, the amount of network traffic has increased by several orders of magnitude. Qualitatively, the number of new network applications has greatly increased. This has changed the statistical properties of packet network traffic. Most noticeable are changes in the types of traffic generated by new network applications such as World Wide Web and newsgroups, which are quite different from the traditional IP applications of File Transfer Protocol (FTP) and e-mail. These traffic profiles also differ radically from voice telephony traffic over circuit-switched networks, from which old classical traffic models were developed - although "streaming" applications with traffic characteristics more similar to conventional telephony services have also emerged.

The rapidly evolving Internet now provides voice over IP, video distribution, video teleconferencing, and various other interactive services as well. New services with different (and potentially more demanding) traffic characteristics are likely to appear.

This contribution provides a brief overview of different traffic models relevant to IP networks, starting with *neoclassical* Poisson-type models. It then summarizes more recent developments such as packet train models and long-memory (self similar) models. It discusses the importance of computer simulation in IP network traffic analysis.

C.1 Traffic characteristics

Traditional traffic engineering was based on the statistical behavior of large numbers of voice calls over the public switched telephone network. Voice call statistics are inapplicable to IP or other packet networks - at least at a micro level. Data calls over such networks typically are of much longer duration, and have different call rates and traffic flow characteristics, than PSTN voice calls.

Stochastic models of packet traffic used in the past were often Markovian in nature. Those traffic models, herein referred to as *neoclassical* models, assumed a Poisson (independent) arrival rate and exponential message length. Data source models with those characteristics were used in the analysis and modeling of early ARPANET [21]. These traffic models are useful, but cannot be relied upon exclusively.

Perhaps the most useful, for our purposes, among the other commonly used traffic models are packet-train models and self-similar models. These models can be employed either as part of an analytical model, or to drive a discrete-event computer simulation. A recurrent theme relating to traffic in broadband networks is the traffic "burstiness" exhibited by key services such as compressed video, file transfer, etc. Burstiness is present in a traffic process if the arrival points appear to form clusters, tending to give rise to runs of several relatively short interarrival times followed by a relatively long one. Packet transmission often exhibits bursty statistical behavior.

C.2 Packet trains

The concept of "packet-trains" was introduced in 1986 [28]. Packet train models assume that a group of packets enter and travel through a network together like the cars in a railroad train. This reflects one of the prominent features in packet network traffic, namely its long-range dependency. This dependency is found in both local area and wide-area networks. In addition, traffic in local-area networks is self-similar or fractal (see below), a characteristic usually not found in wide-area network traffic.

The packet train model can be contrasted with a *car* model, in which each vehicle is independent and may take a different route at each interclause. Even if all of the cars are going to the same destination, they make independent decisions at interchanges (e.g. routers). In a packet network, this results in increased overhead, since all intermediate nodes (routers, gateways, or bridges) must make this decision for all packets. In a train-type model, the first packet in the train may make the routing decision and all other packets of that train follow. This model applies only when we look at the packets coming or going to a single node. (Unlike the Poisson processes, trains are not additive. The sum of a number of trains is not a train.)

To allow analytical modeling with a simplified train model, usage of a two-state Markov model has been suggested. The source can be either in generation (train) state or idle (inter-train) state. The transitions between these states are memoryless (Markovian). The duration of the two states is exponentially distributed, with inter-train arrival times usually of the order of several seconds and inter-car times inside the trains on the order of a few milliseconds.

C.3 Self-similar modeling

Recent studies of high-quality, high-resolution traffic measurements have revealed a new phenomenon with potentially important consequences to modeling, design, and control of broadband networks. These studies included an analysis of hundreds of millions of observed packets over an Ethernet LAN in a research and development environment, and millions of frames of data generated by video services. In these studies, packet traffic appears to be statistically self-similar. A self-similar or fractal phenomenon exhibits structural similarities across a wide range of time scales. In the case of packet traffic, self-similarity is manifested in the absence of a natural burst length: at every time scale, ranging from a few milliseconds to minutes and hours, similar-looking traffic bursts are evident. Self-similar stochastic models include fractional Gaussian noise and fractional ARIMA (autoregressive integrated moving average) processes, [28] page 78.

A relevant observation is made in Atiquzzaman: "Previous traffic models for data, such as Markovian models, are generally not applicable to model multimedia traffic. Researchers have reported long and short range dependencies in multimedia traffic over networks, resulting in self similarities in the traffic" [22].

The longer-term correlations characteristic of the packet arrivals in aggregated Internet traffic are well described by self-similar or fractal processes. This might appear counter-intuitive to those familiar with traditional network theory. The standard modeling framework, often Poisson or Markovian, predicts that longer-term correlations should rapidly die out, and consequently that traffic observed on large time scales should appear smooth. However, empirical data argues strongly that these correlations remain non-negligible over a large range of time scales [23].

Longer-term means time scales from hundreds of milliseconds to tens of minutes. On shorter-time scales, effects due to network transport protocols, which impart a great deal of structure on the timing of consecutive packets, are believed to dominate these traffic correlations. On longer-time scales, non-stationary effects such as diurnal traffic patterns become significant [23].

In principle, self-similar traffic correlations can lead to significant reductions in the effective deployment of buffers imbedded in Internet routers, absorbing the transient increases in traffic load. However, the network community is not united on the practical impact of self-similarity. One conducting Internet simulations must not a priori assume that its effects can be ignored. How to incorporate self-similarity into traffic models for simulation is still an issue. Accurate synthesis is still a problem. A number of algorithms exist for synthesizing exact or approximate sample paths for different forms of self-similar processes. However, these only solve how to generate a specific instance of a set of longer-term traffic correlations.

The next step is how to go from the pure correlational structure (in terms of a time series of packet arrivals per unit time) to the details of exactly when within each unit of time each individual packet arrives. Once addressed there are still difficulties in packet-level simulation versus source-level simulation [23].

In the absence of definitive data on IP traffic, network planners can, without erring to a large degree, fall back on the traditional traffic analysis methods of circuit switched networks [7] as long as they can assume an aggregation of flows. In other words, the self-similarity of IP traffic can be ignored for many applications of traffic analysis.

C.4 Rare event simulations

Another aspect of modern traffic engineering relates to "rare events". With the improved reliability of telecommunications networks, rare event simulations have become an increasingly important ingredient of the quality-of-service metrics. A typical example is cell loss in ATM systems, making rare-event simulation quite useful [20]. Other rare events that are simulated are node and link failures.

C.5 Conclusions

The utilization of standard analytical traffic models based upon self-similar traffic characteristics and assuming the presence of packet-train traffic should allow computer simulations to yield the most relevant results for the optimization of availability and survivability performance. When these models are not available, models based upon the PSTN can yield useful results. In either case, the task of simulating the Internet is "an immensely challenging undertaking" [20]. Traffic characteristics and analytical models need to reflect quantitative and qualitative changes in communication networks to become realistic, accurate, and useful. As characteristics and models become more accurate, the traffic simulation and prediction models that use them as a foundation become more accurate. As we are often reminded, the predicted performance of a network is only as good as the model on which it is based. Still, since the network environment is so large and complex, computer simulation may provide the best (perhaps the only) realistic prediction of network performance - particularly of reliability and survivability performance. For additional information, see [26] to [36].

Annex D:
Monitoring network metrics in IP based networks

Network reliability/availability metrics are defined to enable suppliers, service providers, and customers to determine the degree to which their needs are met. A key element of any reliability program is the capability to monitor a network in order to obtain values for those metrics deemed important. Monitoring can be performed with respect to a variety of network quality of service metrics including delay, availability, packet loss, and jitter. The discussion here focuses on *delay*. Two basic techniques for monitoring IP-based networks are *data gathering monitoring* and *remote monitoring*. This annex discusses attributes of these monitoring methods.

D.1 Data gathering monitoring

Data gathering monitoring uses time stamps on packets to determine delays over network segments. Gathering agents are installed on all routers, servers, or gateways of interest in the network. Gatherers are hierarchically organized, sending network transaction data to other gatherers for further aggregation. Gatherers collect data passively; collection has little or no effect on network traffic. Gathering agents (i) collect Simple Network Management Protocol (SNMP) data from routers, servers, or gateways, and (ii) send burst data at pre-determined off-peak hours to central database information from network elements.

Since the actual network session data are collected at the individual network elements, the data gathering approach can be very accurate subject to the cost of analyzing the data. However, attaining this accuracy requires tight synchronization of clocks in disparate parts of the network to eliminate potential bias in delay measures. Real-time reporting is not possible because data collected from various gathering points need to be combined, processed, and analyzed. Data gathering may be performed using hard or soft probes installed in network elements. This is a disadvantage since service providers often balk at such intrusive methods.

D.2 Remote Monitoring

Another effective alternative is remote monitoring. Unlike the previous method, remote monitoring is based on Internet Control Message Protocol (ICMP) ping probes to determine the network reliability/availability metrics (e.g. delay, jitter, packet loss, and availability of network segments). This introduces some minor additional traffic, which should have little or no effect on congestion. The major advantage of this approach is that it does not require any data gathering agents within the network. Moreover, this approach can provide near real-time reports on metrics being tracked. In addition, this method does not require SNMP, which is not available on all systems.

Figure D.1 provides an example of the application of remote monitoring. M_1, M_2, M_3, and M_4 are monitoring sites outside the IP network cloud. The objects inside the cloud are routers. L is a line defining the hop between the two routers of interest, A and B.

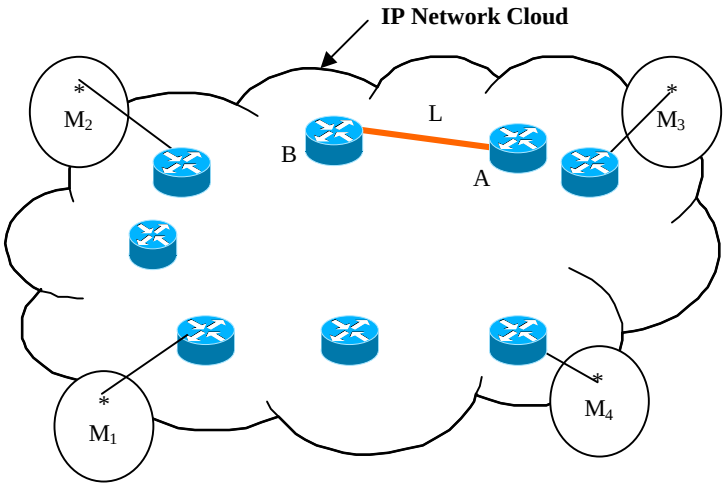


Figure D.1: Example of remote monitoring application

To measure the delay between these two points, a monitoring site sends a ping to point A and another ping to point B via point A. The delay and other metrics are obtained using the following data:

- ICMP ping data from the monitoring site to point A.
- ICMP ping data from the monitoring site to point B via point A.

Ad-hoc solutions based on this data are known to have undesirable properties and accuracy problems. For example, let T_A and T_B the mean delay data obtained from steps 1 and 2 above. Then, the naive estimate of delay contribution of the segment L from A to B is the difference, $T_B - T_A$. Jitter nature of IP traffic can lead to enormous variability in this estimate. For example, as much as 40 % of the time, this difference could be negative, which does not make sense, and is a mere artifact of delay subtraction. This estimate can also become a very large number, another artifact.

So, the second key element in remote monitoring is careful analysis of data. This includes:

- decomposition of delay data into queuing, propagation and processing delays,
- modeling of delay data, and
- the use of appropriate statistical techniques to filter noise in the raw data to produce realistic delay estimates.

Figure D.2 provides an example of estimates obtained by this approach. The vertical bars demonstrate the variability in the naive estimate obtained by simple subtraction. The line through the data shows the reduction in variability using statistical methods.

The accuracy of the estimate given by the remote monitoring method improves as the monitoring station is closer to the hop and as the length of the hop increases. This method does not suffer from the synchronization accuracy of computer clocks, because the time stamps are taken from the same computer.

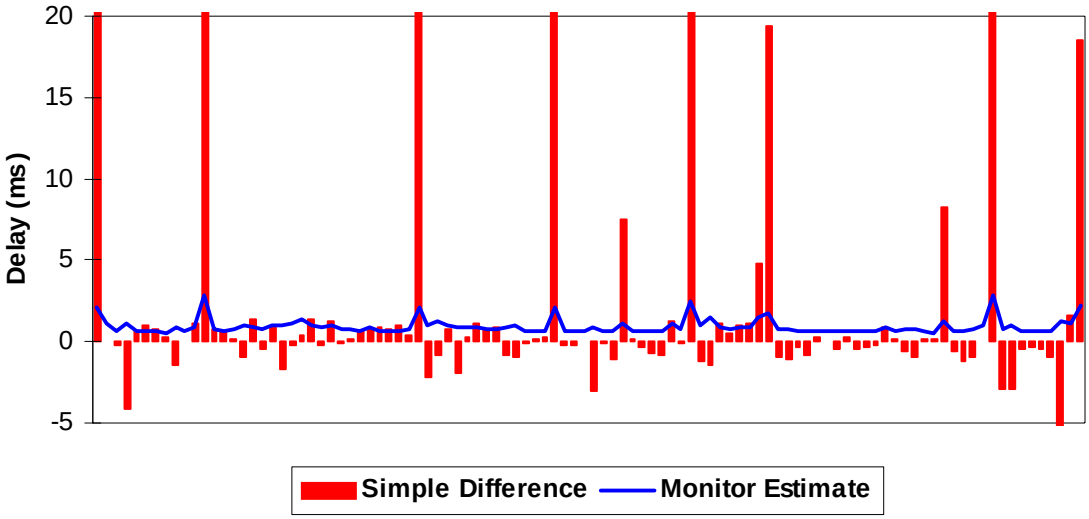


Figure D.2: Filter process example in remote monitoring

Annex E: Bibliography

- SLA Management Handbook, Telemanagement Forum, GB-917: "Evaluation Version 0.8" November 2000.
- Kihong Park and Walter Willinger: "Self-Similar Network Traffic and Performance Evaluation".
- John G. Webster (ed.): "Wiley Encyclopedia of Electrical and Electronics Engineering -Telecommunications Traffic", Vol. 21 (1999).
- Bellamy, John: "Digital Telephony", Second Edition, John Wiley & Sons, Inc., Copyright 1991, New York, Chapter 9.
- ITU-T Recommendation G.8080/Y.1304: "Architecture for the automatic switched optical networks (ASON)", Nov. 2001.
- ITU-T Recommendation Y.1541: "Network performance objectives for IP-based services ".
- ITU-T Recommendation F.706: "Service definition".
- IEEE 802.17: "Resilient Packet Ring Working Group".

History

Document history		
V1.1.1	May 2003	Publication