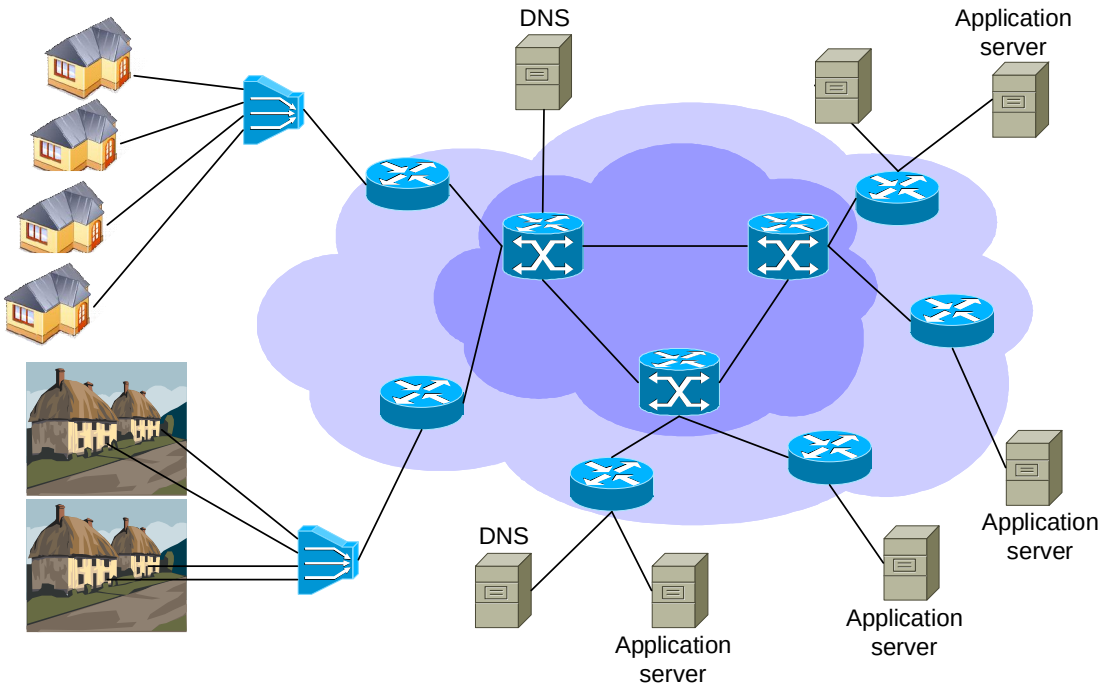


# Cost to Build Dependable All-IP Networks

Authors Pertti Raatikainen

Confidentiality Public

| Report's title | |
|---|---|
| Cost to Build Dependable All-IP Networks | |
| Customer, contact person, address | Order reference |
| | |
| Project name | Project number/Short name |
| IP verkkojen luotettavuus II | 13674 / IPLU II |
| Author(s) | Pages |
| Pertti Raatikainen | 30 |
| Keywords | Report identification code |
| IP network, reliability, dependability, cost | VTT-R-09852-07 |

Summary

This report studies methods to enhance dependability of an all-IP network and discusses the capital and operational expenses caused by the use of those methods. At first, different perspectives to the dependability of a packet switched network are identified and goals of each viewpoint are compiled. Then a layered model for dependable communication is introduced and methods to increase dependability on the given layers are discussed. Finally, simple formulas are given to estimate additional Capex and Opex, caused by the different methods.

Methods to be used on the various dependability layers are categorized to redundancy, network control, design activity, OAM activity and purchasing activity methods. Some other methods are also discussed. The redundancy methods, e.g. duplication of network equipment, are considered cost sensitive causing usually clear increase of Capex and Opex. The network control methods may require purchase of new devices, training of personnel and hiring of new employees thus leading to clear increase in Capex and Opex. Some other control methods may require only activation of an existing feature in the network devices, thus causing no additional expenses.

Design and purchasing activities are found to cause no additional expenses, because proper design and purchasing processes should already cover all that is needed to maintain high dependability. However, sharpening of the existing design and purchasing processes may be needed. OAM activities to increase dependability may require only modifications to the existing OAM practices, causing practically no extra expenses, or there may be need for new OAM equipment, training and new personnel in which case Capex and Opex go up clearly.

Other discussed methods (topology, location of networking devices, agreements, history and alternative technology), may produce substantial increase in Capex and/or Opex. The use of resilient ring and mesh topologies is an example of Capex intensive methods. Agreements to increase dependability are a good example of Opex intensive methods. The highest cost increase is faced with the alternative technology option. It offers the best solution to avoid shortcomings of the IP networks, but within a short time frame results in the highest cost.

| Confidentiality | Public |
|---|---|

Espoo, 20.12.2007
Signatures

VTT's contact address
Vuorimiehentie 3, Espoo, PL 1000, 02044-VTT, Finland

Distribution (customer and VTT)
IPLU II project partners

# Preface

This report has been produced by VTT as part of the IPLU II (Dependability of All-IP Networks II) project. The report summarizes the outcome of the discussions on and study of the cost to introduce additional technology to all-IP networks in order to enhance their dependability to the level available in conventional telecommunications networks. IPLU II has been funded by Tekes, BaseN Oy, Digita Oy, Elisa Oyj, Finnet Oy, Fortum Oyj, F-Secure Oyj, Ministry of Transport and Communications, National Emergency Supply Agency of Finland, Nokia Siemens Networks Oy, TDC Song Oy, TeliaSonera Oyj and VTT. Additionally, Scientific Computing Ltd. (CSC) has provided information on its network for specified case studies. The steering group of IPLU II has been composed of members of all the project partners.

The author would like to express his gratitude to the partners for their valuable contributions to the report.

Espoo 20.12.2007

Authors Pertti Raatikainen

# Contents

# Acronyms

| | |
|---|---|
| **ADLS** | Asymmetric Digital Subscriber Line |
| **BGP** | Boarder Gateway Protocol |
| **CoS** | Class of Service |
| **DDoS** | Dynamic Denial of Service |
| **DNS** | Domain Name System |
| **EAPS** | Ethernet Automatic Protection Switching |
| **ICMP** | Internet Control Message Protocol |
| **IETF** | Internet Engineering Task Force |
| **IP** | Internet Protocol |
| **OAM** | Operations, Administration and Maintenance |
| **MPLS** | Multi-Protocol Label Switching |
| **QoS** | Quality of Service |
| **RSTP** | Rapid Spanning Tree Protocol |
| **SLA** | Service Level Agreement |
| **STP** | Spanning Tree Protocol |
| **TCP** | Transmission Control Protocol |
| **VLAN** | Virtual Local Area Network |
| **VPN** | Virtual Private Network |
| **WiMax** | Wireless Interoperability for Microwave Access |

# 1 Introduction

Packet switched technologies, i.e., networks that are based on the Internet Protocol (IP), are gradually replacing the old-established circuit-switched telecommunications infrastructure. While the IP networks enable lowered networking cost, they tend to offer less reliable transfer of data than the conventional networks. Additionally, the IP networks introduce a number of disagreeable features, some of which are threatening reliability and security of communication. An example of such threats is spoofing, which incorporates techniques that are used to gain unauthorized access to computers. Another example covers techniques, such as DDoS and DNS pollution, which aim at disturbing and paralyzing the Domain Name System (DNS). DNS provides the IP networks with essential functionality to run smoothly.

Since reliability, or more broadly dependability, of communication is a cornerstone in data communications, additional measures are needed to raise the reliability of the all-IP networks to an acceptable level. Due to the various actors, such as end-users, network operators and different sorts of service providers, which deploy and utilize the communications networks, there are different perspectives to the reliability. The end-user wants seamless and constant connections to the networks and services at the subscribed access rate, while the operator wants to maximize its revenue by keeping the network's running cost as low as possible. Therefore, the measures to increase reliability depend on the viewpoint.

Regardless of the standpoint, it is clear that something additional needs to be included in the network or at least something needs to be changed to obtain enhanced dependability. All additions and changes imply more investment in the network, either in the technology, in the infrastructure or in the personnel. When investing, the question always is whether the investment pays back and, in case it does so, how long will it take.

This report studies solutions to overcome the known dependability shortcomings of the all-IP networks and discusses their impact on network's capital and operational expenses. The survey has a technological emphasis although other viewpoints are also considered. Chapter 2 discusses the different viewpoints to and layers of dependability, chapter 3 defines the goals and requirements for dependable communications, chapter 4 surveys the different methods to increase the dependability and chapter 5 studies the cost of the different dependability enhancement methods. Chapter 6 gives the concluding remarks.

# 2 Layered view to dependability

A dependable network carries data from the source to the destination without losses or duplications and within a pre-calculable time period. When assessing the dependability of a communications network, we can identify different aspects that can be divided basically into technological and non-technological ones. In the next chapters, we introduce different non-technological viewpoints, however linking them to the technology behind them.

## 2.1 Layered IP concept

Let's look at the IP network concept more closely. An IP network is composed of physical devices, such as routers, switches and different sorts of servers, carrier paths (i.e. links) between the devices and protocols that take care of the transport of information between applications residing in the devices (see Figure 1). In the IP networking concept, all these are considered to form different layers [1]. Due to the layered structure, faults on lower layers reflect to upper layers and, therefore, faults on the lower layers can cause larger disturbance on network performance than respective faults on the upper layers. For example, break-down of an application (server) normally affects only those users that can have access to and utilize the application. Break-down of a router may collapse connections of a much larger group of users. So, it might be concluded that the lower layers should be designed to be more reliable than the upper ones.

However, this is only one way of looking at the dependability. It may happen that an application has a large group of users and the server in question runs several applications. If there are no redundant facilities available then the break-down of an application (software) or a server may have a large impact. On the other hand, a link cut or router break-down may affect only a limited number of users if there are redundant network facilities available and the IP rerouting capability is exploited. Thus the simple technological viewpoint is not enough for our purposes and we have to consider also non-technological viewpoints. For the purpose of this discussion we consider operational, business and regulation viewpoints.

The operational viewpoint reflects the technology and related functions, which are discussed further in section 2.3. The business viewpoint can be divided into the following sub-viewpoints: network operator, access/transport service provider, application provider, end-user and end-user application. For the purposes of further discussion, we define the business viewpoints as follows. The end-user is a domestic or business user that subscribes a connection to the Internet from an access operator and accesses end-user services (i.e. applications) provided by the application providers. The access/transport service provider offers transport capacity for the end-users as well as for the application providers and possibly for other access/transport service providers. The network operator owns and operates the physical network and provides transport facilities for the access/transport operators. The regulation viewpoint covers all authorities that set guidelines for the operational and business activities, i.e., regulate and supervise the whole value chain of the communications networking. These include competition legislation,

consumer protection, recommendations and regulations to build and maintain communications networks, etc.

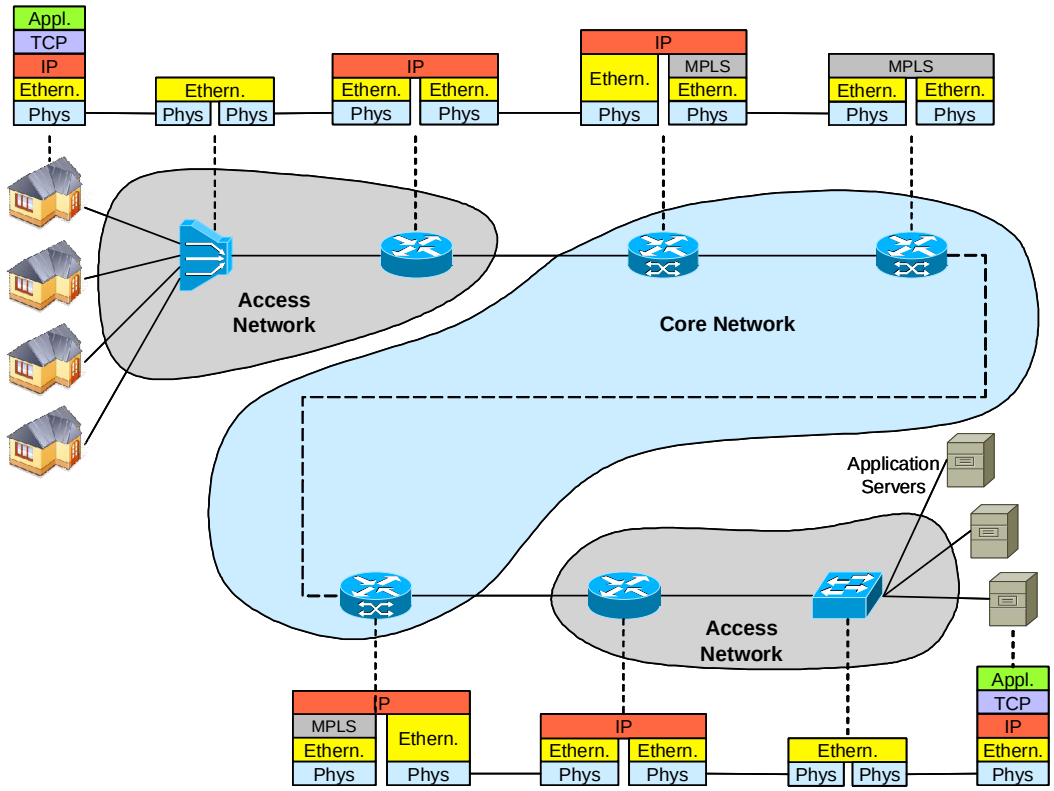


*Figure 1. An example IP network configuration.*

## 2.2 Goals for a dependable network

There are different groups that exploit the communications networks and therefore it is not easy to draw up general goals for a dependable network covering interests of all involved parties. The business perspectives, listed in section 2.1, give a good picture of the various exploitation levels. Since the business viewpoints also reflect the operational perspectives, the business viewpoints are used here in identifying objectives of a dependable network.

From an end-user **application**'s point of view, a dependable network should guarantee required bit rate, low enough delay and sufficiently bounded delay variation for an application to run smoothly. Some applications may also require access to additional facilities in the network, such as name servers and authentication servers.

From an **end-user**'s perspective, a dependable network should provide unbreakable access to the network resources at the subscribed bit rate so that the applications can be utilized as expected. The end-user is not aware of the actual status of the network or the application servers and in the case of failures cannot make difference between the network failures and application failures. Thus the

end-user experiences the obtained quality that can simply be categorized as good, adequate or poor.

Public **authorities** form a special user group that has more rigorous requirements for the network and offered services than the other users. Access to the network and service applications should be available also during exceptional conditions, such as major accidents or natural catastrophes. The quality of the communication may decline, but it should be maintained although at a lowered quality level, e.g., rich video information may be replaced by voice or text communication when the bit rates decrease and/or bit-error-ratios increase. The overall target is to have networking resources available to run society's critical functions at all conditions.

An **application provider** is satisfied if the customers (end-users) can have access to the provider's service applications and related supporting facilities, such as authentication and billing services provided by the network or by some other operator/provider. These guarantee that the provider is able to invoice the customers for the usage of the services, which enables smooth running of the provider's business.

Since an **access/transport service provider** sells the transport capacity that it has purchased from the network operator, it is important that the purchased physical transport capacity, defined in a relevant Service Level Agreement (SLA), is available and its quality is in line with the SLA. This guarantees that the access/transport service provider is capable of fulfilling the end-user contracts. Lowered transport quality and breaks in the access/transport services may result in compensations for the customers.

From a **network operator**'s point of view, a dependable network runs and can be operated in a predefined and efficient way. Network resources, e.g., transport capacity and supporting functionality, can be provisioned quickly while fulfilling the SLA requirements. In the case of faults or malfunctions, corrective actions can be carried out promptly and in a planned way.

One additional viewpoint that needs to be considered is the regulatory perspectives. The communications networking business is more or less regulated and the role of the regulator is to draw up rules, specifications, recommendations and regulations covering the network, its usage and activities around it. Additionally, the regulator supervises that the given instructions are obeyed by all related parties. As a whole, the regulator's work supports the objectives of some viewpoints and limits the objectives of some other viewpoints.

## 2.3 Layers of dependability

When combining the operational, business and regulatory perspectives, the dependability of an all-IP network can be viewed as a layered structure resembling that of the IP protocol stack. As shown in Figure 2, we can identify five successive layers: *network and its facilities*, *network operations*, *access and transport services*, *end-user services* and *end-user experience* layer. These represent the different operational viewpoints. The business and regulatory perspectives are placed parallel to the layered structure indicating which layer(s) each of the business aspects and regulatory authorities are related to. Notice,

however, that more than one business aspect may be linked to a single actor, e.g., a network operator may act also as an access operator and service provider thus representing several viewpoints at a time.

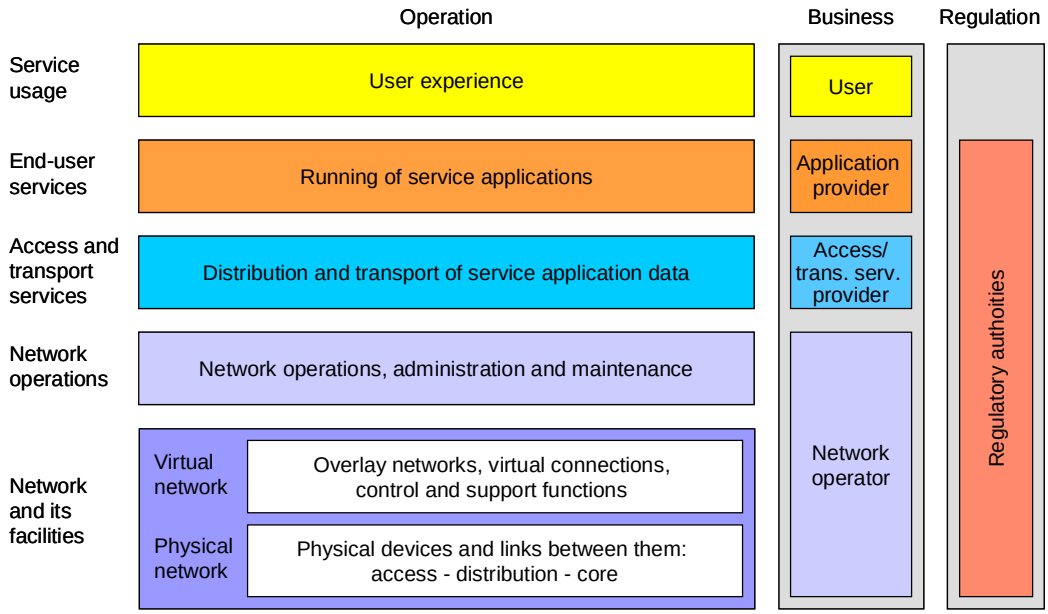


*Figure 2. Layered view to dependability of an all-IP network.*

The lowest, *network and its facilities*, layer represents the physical network and is divided into two sub-layers. The lower sub-layer represents the *physical network* covering transport links, all the physical devices and related software. The upper sub-layer represents the *virtual network* that is composed of overlay networks, virtual connections and related supporting functions.

The second layer is a control layer, here named as the *network operations* layer. Its major function is to control the physical network, i.e., the *network and its facilities* layer. This layer provides for the network operator means to run the network, e.g., to control and provision the network resources, supervise network's performance (e.g. bit-error-ratio, packet-loss-rate and delay performance) and carry out maintenance actions.

The third, *access and transport services*, layer represents activities related to connecting end-users to the Internet and carrying user and application data across the network. Access/transport providers are the key players on this layer.

The forth layer represents the *end-user services*, i.e., the various applications that the user can access and run through the network. From the business perspective, it is the application providers that act on this layer.

The fifth layer is the *service usage* layer that represents the user experience, e.g., service availability, accessibility, confidentiality and ease of use.

Dependability of the above layers can be studied separately, although many functions and activities on the different layers are closely related to those of the

adjacent layers. When considering that the different layers map to different business aspect, it is more straightforward to study the layers separately. Notice, however, that more than one business aspect may be linked to a single actor, e.g., a network operator may act also as an access operator and service provider thus representing several viewpoints at a time. The following chapter discusses the requirements of dependable communication using the layered approach.

# 3 Requirements for dependable communication

Requirements for dependable communications can be reviewed from the different business perspectives described in section 2.1. However, the business perspectives map to the defined dependability layers, which in turn reflect the related technology. Therefore, the requirements for dependable communications are here surveyed in layers by using mostly technological measures and terminology.

The foremost requirements of the different dependability layer:

The *network and its facilities* layer:
- adequate network resources (e.g. bandwidth and routing/switching capacity)
- good transport quality (i.e. low bit-error-ratio, low packet-loss-rate, accurate timing, low delay and bounded delay variation)
- fault tolerant hardware and software solutions
- powerful network devices, i.e., capacity to process the offered load
- minimization of disturbances, e.g., downtimes and outages
- automatic and fast recovery from faults (and malfunctions)
- ability to minimize harmful and/or malicious use of network resources
- ease of installation, update and upgrade

The *network operations* layer:
- fast and resilient control operations
- fast and versatile allocation of network resources
- resilient installation and configuration of network devices
- steady routines for fast recovery from network failures
- automatic and fast recovery from faults (and malfunctions)
- controllability of maintenance
- ease of network management, incl. software updates
- detection and prevention of harmful network usage (and traffic)

The *access/transport services* layer:
- secure and reliable access to network
- secure connections between end-points and secure access to applications
- secure and reliable transfer of data
- reliable authentication, authorization and accounting of users
- removal of harmful/disturbing users
- removal of disturbing traffic

The *end-user services* layer:
- service availability and accessibility
- service usability
- authentication, authorization and accounting of users
- security of service usage
- prevention of malicious use
- detection and removal of abuse

The *service usage* layer:
- services available when they are needed
- services run smoothly and reliably
- security of the used services

Some layers have equally named requirements, such as the security, authentication and authorization related requirements on the access/transport services layer and end-user services layer. Although the names may be the same, the measures in question are layer specific and are performed independently.

# 4 Methods to increase dependability

Several methods can be applied on each dependability layer in maintaining and increasing dependability. Since there are similarities between the methods used on the different layers, they are here categorized in the following way:

- redundancy
- control of network resources and functions
- design activities
- operation, administration and maintenance activities
- purchasing activities
- other methods

## 4.1 Redundancy

Redundancy implies that there are reserve resources/facilities available that can be mobilized when the active resources are no more functioning in the expected way. Redundancy methods apply to the *end-user services* layer and the layers below. In case of the *network and its facilities* layer, physical links, network devices, supporting servers and even software modules can be redundant. Equally important facilities to be duplicated are the cooling/heating systems, power supplies and the physical premises where the networking devices reside. The *network operations* layer can have redundant OAM devices, software as well as redundant personnel. The *access/transport services* layer may offer redundant access facilities (such as WiMax in parallel with ADSL), redundant or over-provisioned transport facilities between known end-points and duplicated authentication servers. The *end-user services* layer may introduce duplicated servers and software to maintain service availability.

## 4.2 Control of network resources and functions

By controlling the available network resources and functions it is possible to alleviate or remove existing performance bottlenecks or proactively prevent the system from getting into hazardous states. On the *network and its facilities* layer, this means, for example, rerouting of traffic to avoid congested or damaged links or network nodes. On the *network operations* layer, operations activities may be balanced between several servers to avoid overloading hotspot OAM servers. The *access/transport services* layer may limit the access to the network or limit the available/offered bit rates to guarantee that all users get served and transport delays stay within the promised limits. On the *end-user services* layer, the customer traffic may be directed to less loaded servers to guarantee smooth service for selected customers or to maximize the number of served customers.

Configuration problems of the network devices, protocols and other software have caused a lot of headache in the IP networks. Proper training of maintenance and installation personnel would help to avoid most of the problems. However, this

does not always help. One such problematic area is the configuration of edge routers that interact with corresponding routers of the neighbouring operators. Operators should be able to agree upon common configuration parameters to guarantee that the traffic runs smoothly with the quality promised to the end-user. Boarder Gateway Protocol (BGP) plays a key role in exchange of routing information and operators usually have different path selection criteria, network policies and rule-sets that are used by BGP in making routing decisions [2]. This causes interoperability problems and may cause end-user traffic to experience varying QoS performance when passing through different operators' networks.

Another area of control, which affects the dependability and is getting a more emphasized role in the IP based networks, is detection and prevention of harmful traffic. To prevent harmful traffic from causing problems, special devices and software should be implemented in the network to monitor and supervise the entering and bypassing traffic. This would work effectively if the networks carried only specially formulated IP packets and the network devices were able to check validity of the traffic [3]. The ingress routers could also implement policies and rule-sets to block and discard unorthodoxy traffic as well as implement connection admission control mechanisms to prevent unauthorized access to the network.

## 4.3 Design activities

A lot can be done to increase dependability during the design phase of a communications network. Major problems can be avoided by exchanging information between the parties that are responsible for the different dependability layers (Figure 2). The service provider needs to communicate with the customers to estimate the demand for their service applications and in this way to prepare for changes in volume of the service usage, e.g., by strengthening the server capacity. The access/transport provider needs to communicate with the service providers to know where the access and transport services are needed and to estimate the bandwidth and delay requirements as well as the need for other supporting functionality. The network operator, which manages the *network and its facilities* layer and the *network operations* layer, needs to communicate with the access/transport providers to know where to build the transport capacity and what sort of capacity is needed (to comply with the required QoS).

The network operator needs to communicate also with parties that do not directly utilize the network, but have a crucial role in ascertaining that the network runs reliably. Among such parties are the network equipment manufacturers, electricity companies, regulators and public institutions, such as construction office or land use planning office. Equipment manufactures can help to understand better the possibilities of the existing technology and thus to build the required network functionally in an optimal way. Since networking equipment need electricity to run, it is natural that the network operator discusses with the electricity companies about the availability of the electricity to the network operator's premises.

Public institutions sometimes own and operate facilities that are useful for network operators in building the physical network and, especially, in establishing disjoint redundant transport paths. Examples of such institutions are the public gas companies and road offices. Public construction office can usually help in finding

the right cable paths and owners of those paths. Communication with the regulators ascertains that the network is build based on the official security and reliability principles, e.g., a mobile network uses only those frequencies that are allocated to the operator or an Internet access provider allocates only those IP addresses for its customers that have been allocated for the provider by the regional Internet registry authority.

In the network planning phase, the planning engineers should contact several other departments inside the operator's organization, e.g., the maintenance, installation, purchasing and marketing departments. The maintenance and installation departments can possibly help to define easy-to-use networking and testing equipment that are compatible with the existing device set. The purchasing and operations departments can help to identify solutions and related equipment that offer the lowest cost to the operator. The marketing department can give guidelines, based on the market studies, where and what network resources to design and build.

## 4.4 OAM activities

The OAM activities play a significant role in everyday reliability of a communications network. Incompletely carried out OAM activities can severely degrade performance of a network and lead to serious service breaks. Processes that involve human actions are the most vulnerable points of OAM. Examples of such activities are configurations of network devices, device updates and repair activities. The key issues in enhancing reliability of the OAM activities is adequacy and training of the OAM personnel, OAM tools as well as coordination of the OAM processes. For example, if there is need to reconfigure some network devices and it is known that software of the same devices needs to be updated, then those activities should be coordinated to take place during the same service break to minimize disturbance caused to the network's performance.

In order to prepare for network failures and to minimize the number and length of service breaks, one should make sure that essential spare parts, service tools and skilful personnel are at hand and will be available also in the future. This presumes that the OAM personnel are in contact with the company's other departments, such as network planning, purchasing and installation departments. Smooth operation requires also that the operator/provider takes care of constant communication with external actors that directly affect the operator's/provider's business, such as other network operators and service providers, equipment manufactures and electricity suppliers. Regulators and other authorities should not be forgotten.

## 4.5 Purchasing activities

One important matter that affects the overall dependability of a communications network is the purchasing process. When networking equipment and software are purchased or when contract agreements to build networks or to hire transport capacity are made, it is crucial that the purchasing party fully understands what sort of quality it needs and what sort of quality is offered. This has a direct impact, e.g., on the contents of the signed SLAs.

A network operator's purchasing department needs to communicate at least with departments responsible for network operations, maintenance and installation to guarantee that the purchased items are compatible with the existing facilities and practices and they fit into the required quality framework. Disparity with the existing facilities might mean extra adapters between the existing and new network facilities, new OAM tools, additional training of the personnel and in the worst case extra personnel. On the other hand, communication with the equipment manufactures and vendors is equally important to keep up with the development of the networking devices. Factor that need to be clarified and which affect the purchasing decisions are updating possibilities, future development and backward compatibility of the devices as well as test and measurement possibilities, expected lifetime of the products, etc.

An access/transport provider's purchasing department should communicate with the sales office to be aware of the contents of SLAs that are made between the provider and its customers. Thereby the purchasing department gains required information to prepare for SLA negotiations with the network operators. An access/transport provider may also need network devices and therefore the provider has to discuss with the network operator and equipment manufactures to guarantee compatibility with the operator's devices. In order to verify the obtained QoS, the access/transport provider and network operator need to agree upon the methods how to verify the obtained QoS. Likewise, an application provider needs to be aware of transport service's quality to be able to make contracts with the end-users.

## 4.6 Other methods

As was discussed in the previous chapters, dependability of an IP network can be viewed from various perspectives and next some additional viewpoints and related measures to improve dependability are highlighted. Measures to be discussed include network topology, location of links and network devices/premises, contracts/agreements in enhancing dependability, lessons learned from the history and alternative technologies.

**Network topology**

Network's reliability and robustness against link and network node failures can be improved by topological means on the *network and its facilities* layer. Tree-and-branch type of topologies should be avoided and replaced with ring shape or mesh topologies. Rings and especially two-way double rings can employ fast protection switching in restoring damaged transport paths. Mesh and partial mesh networks are more versatile and include capabilities to restore several lost paths simultaneously by utilizing protection switching. If Ethernet transport is deployed along with Spanning Tree Protocol (STP), direct loops will be blocked by STP thus preventing the use of protection rings [4]. Additionally, STP or its faster version Rapid Spanning Tree Protocol (RSTP) does not meet convergence times necessary to maintain connections of the legacy services, such as telephony [5]. If the Virtual Private Network (VPN) option is allowed, logical protection rings can be established with the help of VPNs [6]. VPNs along with Ethernet Automatic

Protection Switching (EAPS) may offer faster operation. EAPS is used to create a fault tolerant topology by configuring a primary and secondary path for each VLAN [7][8].

The physical topology lays the foundation for the logical topology, which is more resilient and supports more versatile connections than the physical one, e.g., allowing division of a link's transport capacity into numerous lower bit rate channels. Virtual paths and LANs, e.g., light-wave paths, ATM connections, MPLS paths or Ethernet VLANs, may span over large geographical areas and failures in the network nodes' control plane may destroy the logical connections and even the logical topology. If this happens, the connected end-user devices cannot communicate any more although the physical topology and transport network is functioning well. Depending on the technology used for establishing the logical topology, there are different ways to restore the virtual and physical topology. However, the restoration delay may be too long to maintain the application layer connections and sessions.

When carrying circuit emulated legacy services, the one-way delay should be within a few hundred milliseconds (ms). In the case of telephony, the one-way delay should not exceed the 200 ms limit. Most of the packet switched services can cope with much longer delays, but the underlying TCP sessions may be terminated if the sender does not receive acknowledgement packets within a preset expiration time period [1]. In case the network deploys a layer 2 virtual topology, link and node failures imply that the IP layer has to reroute packets of all affected application sessions even if the restored physical and logical connections go via the same network nodes (i.e. routers) as before the failure. This adds up to the overall restoration delay possibly causing timers of the TCP and application sessions to expire. Thus the sessions in question are terminated and end-users experience a service break. In order to avoid unnecessary service breaks upon recovering from link or network node failures, faster protection switching and restoration schemes are needed in the all-IP networks.

**Location of networking facilities**

When building a network, care should be taken in choosing the physical locations of cables and networking equipment. Cables and primary network nodes should be located such that disjoint protection paths can really be established. Important network equipment, such as primary routers, should be located in robust and fireproof premises that provide the operator with additional protection against natural catastrophes, vandalism, intentional or unintentional obstruction of the network devices and prevent outsiders to intrude into the device premises. The physical location of the network facilities should also allow ease of maintenance.

**Agreements to enhance dependability**

Network operators and service providers can prepare for smaller and larger area network breakdowns by making backup agreements with other operators and providers. To succeed in maintaining network connectivity, a separate contingency plan, which distinguishes system originated and externally caused breaks as well as solves possible interoperability problems of the different

operators' network devices, is needed. Protective paths and device locations should be disjoint with the operator's own paths and device locations, to have effective protection, especially, against externally caused disturbance. However, disjoint paths are quite often difficult to arrange in practical networks.

**Lessons learned from the history**

Historical data can also help in enhancing dependability. If, for example, it is known that floodwater covers some geographical area every now and then, it is natural to avoid such places when locating cables and networking devices. Previous experience can guide in deciding when to install additional transport capacity to cope with the growing traffic and maintain QoS on required level. For example, growth of network load can be estimated based on the network statistics and overrun of a certain loading level may trigger upgrade of transport capacity or prevention of lower priority traffic from entering the network.

Measurement data can indicate an approaching fault and possibly the location of the fault. For example, increasing bit-error-ratio may indicate failure of an interface card. Increase in packet-loss-rate and/or in number of retransmitted packets may indicate an approaching failure of a router or that the growing traffic load is exceeding the router's capacity. Router logs may be used to track possible configuration errors of the network devices and even to pinpoint the falsely configured registers.

Previous observations about network breakdowns help to see which network devises are essentially important to protect against failures, e.g., by installing backup devices, software or links. Analysis of the past breakdowns can help to build the networks in such a way that new breaks do not cause avalanche effects, e.g., collapsed network domains are isolated and the disturbance is prevented from travelling to other parts of the network.

**Alternative technological solutions**

Due to the shortcomings of the IP technology, constant enhancements are required to fix the IP networks to meet the needs of the present day and future communications. It is not yet known does this repairing of the deficiencies ever pay back and lead to better and well functioning IP networks. What is clear is that the networks will become complex to run and, therefore, alternative approaches should also be considered. But what are the alternatives? When looking at the near future, there does not seem to be any relevant candidate. However, next some thoughts are given about a more dependable packet switched network.

At first, we have to contemplate the essential points that make the IP networks so uncertain. The basic problems are uncertainty to carry packets to intended destinations and security limitations. The first problem comes from the IP concepts inherent feature that IP packets are transmitted when they are ready to be sent. No connection establishment is needed and, thus, there is no guarantee that the path from the source to destination is available at all. Even if the path exists, failures in network nodes may cause the packets to take wrong routes or may cause the packets to be deleted. It is up to the upper protocol layers to recover

from the IP layer's faults, although the IP concept's Internet Control Message Protocol (ICMP) informs the IP layer about existing problems.

The security problem can be seen on various levels in the IP networks. Network devices and software can be disturbed and manipulated, user traffic can be spoofed to capture user data and identity, and user equipment can be taken over for different DDoS attack purposes. Worms and viruses that disturb or paralyze end-user devices can be spread quite easily in the Internet. This is the case also for spyware, which collect personal information and interfere with user control of the computer in various ways, e.g., installing additional software, redirecting Web browser activity, diverting advertising revenue to a third party or copying user files and sending them to unauthorized destinations.

There are solutions (software and hardware) to tackle the security problems, but due to the basic properties of the IP technology, malicious and illegal use takes new forms and continues. To put an end to this and solve the uncertainty of routing, a completely different packet switching concept is needed. The concept should include at least the following properties:

- connection admission control
- authentication of users and user traffic
- user profiles based on the SLAs
- traffic shaping and policing
- efficient support of mobility
- separation of network address from user name
- routing based on user names and location information
- fast protection and restoration capabilities of lost or damaged connections

# 5 Cost of dependability

The cost of a method to increase dependability can be estimated based on the previous knowledge of the equipment, software and labour expenses as well as on the knowledge of the amount of work needed to carry out required actions. If the aforementioned information is available, one has to estimate the number of devices and/or software modules that need to be purchased and the amount work to install and run them. If the method entails permanent increase in operational workload then the amount of additional labour should also be assessed. If several methods are applied simultaneously, the total supplementary cost is the sum of the costs of the separate methods.

In the following, simplified formulas to calculate the extra costs are derived. Then expenses of the methods, listed in chapter 4, are discussed and relevant references to the formulas are made. Finally, an example calculation is given.

## 5.1 Formulas for cost estimation

When assessing the cost of a specific method, we have to distinguish between the capital expenditure (Capex) and operational expenditure (Opex) caused by the use of the method. For simplicity, here Capex includes the direct cost of a product and Opex includes expenses that are caused by installing and putting the product into operation and keeping it in operational use (i.e. normal running, maintenance and repair costs).

When purchasing additional pieces of a product, the total price follows linearly the unit price. If the number of additional units is large, the price per unit may decline, because vendors tend to give price compensation due to large volumes. Thus the expense ($P_c$) to buy $n$ pieces of a product can be calculated from

$$P_c = n\,(1-\varepsilon)\,P_{unit} \tag{1}$$

where $\varepsilon$ is the relative discount ($0 \leq \varepsilon < 1$) and $P_{unit}$ is the unit price of the product.

The discount depends quite often on the number of the purchased units and increases step by step as a function of $n$. Thus (1) converts to

$$P_c = n\,(1-\min\{\varepsilon_m, \mathit{floor}[n/n_{dv}]\varepsilon\})\,P_{unit} \tag{2}$$

where $n_{dv}$ is the threshold value (i.e. the number of product units) that triggers the increase of the discount, $\varepsilon$ is the step size of the discount and $\varepsilon_m$ is the maximum obtainable relative discount value.

The installation work includes operations such as mounting, software loading and configuration. The cost ($P_i$) to install $n$ pieces of a product is given by

$$P_i = n\,P_{inst} \tag{3}$$

where $P_{inst}$ represents the installation cost of one unit of a product. $P_{inst}$ may be calculated from the known labour unit prices by estimating the number of time units (e.g. hours or months) that are needed to carry out the installation work.

The workload to operate the additional product units is usually directly proportional to the known workload to run one unit of the product. However, the operational cost increases in steps, because even a small increase in the workload may generate the need to hire an additional employee to operate the products. Therefore, the cost increase is constant for a known number of additional product units and jumps to a new level when this number is exceeded. Thus the expense ($P_r$) to run $n$ additional units of a product can be given by

$$P_r = floor[n/n_{tv}]\ p_{o\_unit}\ T_o \quad (4)$$

where $n_{tv}$ indicates the threshold value (i.e. the number of product units) that triggers the jump in the workload, $p_{o\_unit}$ represents the cost to operate $n_{tv}$ units of the product for the duration of one time unit (e.g. a month or a year) and $T_o$ gives the observation period in the given time units. When $n_{tv}$ = 1, the work load is linear to the number of the product units.

If the installation and/or operation phase of a product requires training of the personnel, the training should be considered in the cost calculations. Training can introduce a fixed cost increase or the cost may depend on the number of persons involved and time taken for the training. In the latter case, the training expense ($P_{tr}$) is give by

$$P_{tr} = m\ p_{tr\_unit}\ T_{tr} \quad (5)$$

where $m$ is the number of trainees, $p_{tr\_unit}$ is the known trainee cost per time unit and $T_{tr}$ is the training period in the given time units (e.g. a day or a month).

The total Opex for $n$ units of a product is the sum of the installation, operation and training costs and it can be estimated by the following formula

$$P_o = n\ P_{inst} + floor[n/n_{tv}]\ p_{o\_unit}\ T_o + m\ p_{tr\_unit}\ T_{tr} \quad (6)$$

where the variables are as explained above.

Provided that the training concerns only the additional new employees then (6) can be rewritten in the form

$$P_o = n\ P_{inst} + floor[n/n_{tv}]\{p_{o\_unit}\ T_o + p_{tr\_unit}\ T_{tr}\} \quad (7)$$

The total additional cost ($P_T$) caused by a method to increase an all-IP network's dependability for some period of time is

$$P_T = P_c + P_o \quad (8)$$

If several methods are applied simultaneously, the total increase of Capex and Opex is obtained by summing up the additional expenses of all the methods, i.e.,

$$P_C = \sum_{k=1}^{N} P_c^k \quad (9)$$

$$P_O = \sum_{k=1}^{N} P_o^k \quad (10)$$

where $P_c^k$ is the additional Capex and $P_o^k$ the additional Opex caused by method $k$ and $N$ is the total number of applied methods.

## 5.2 Cost of redundancy

The redundancy on the *network and its facilities* layer usually means installation of multiple network devices or transport links. Copies of software modules can also be installed into multiple network devices. The cost of the other backup facilities, such as additional premises and power supplies, quite often introduce liner dependence on the number of the installed items. Larger number of redundant products is normally compensated for by lower unit cost and therefore equation (2) applies for Capex calculations for most of the redundant methods.

Opex increases quite linearly in respect of the number of redundant products. Cost to run the products usually dominates Opex, but there are cases when either installation or training may dominate. An example of such a case is duplication of a transport link. The physical cable does not cause much training or running costs, but the cable laying-out cost is normally high and no much compensation in the laying-out cost is to be expected. However, even in cases like this, Opex increases quite linearly in respect of the number of redundant products and equation (6) applies.

On the *network operations* layer and *access/transport services* layer redundant methods focus on additional devices, software and other items that benefit from unit price compensations due to large quantities of the purchased items. The installation cost is usually minor compared to the overall running cost of the products. Therefore, the increase of Capex is close to liner in respect of the number of the additional items and equation (2) can be applied. Likewise, the increase of Opex is linear to the number of the redundant products and equation (6) can be applied. The same conclusions are valid also for Opex and Capex calculations on the *end-user services* layer.

## 5.3 Cost of enhanced control

Control of the available network resources and functions to enhance network dependability usually implies additional work to exploit capabilities of the existing network devices. This is the case when the devices need to be reconfigured to allow desired new features, e.g., firewall or BGP configurations. The use of some capabilities requires only enabling the existing feature in the device and thus the workload is minimal. An example of such a case is enabling load balancing features of servers in server farm applications or in OAM applications. Another example is enabling policing and traffic shaping functionality in ingress routers and switches. More work is needed to manipulate

the policing and traffic shaping parameters. The cost to carry out these kinds of activities is directly proportional to the additional work and quite often this work can be considered to be part of the everyday operations. Therefore, the above mentioned and similar enhancements can be concluded to cause no additional Capex or Opex.

In case the devices need to be updated to have required capabilities, the question is about purchasing update software or replacing obsolete devices with modern ones. An example is prevention of harmful usage of network resources by monitoring and blocking undesired traffic and users, which nowadays requires special monitoring devices and/or software. The cost to increase dependability in this way is composed of the device cost, update and training costs and additional work to run the devices. Thus equation (2) applies for additional Capex and (6) for additional Opex calculations.

## 5.4 Cost of design activities

Design activities aiming at a more dependable network may require more work than otherwise would be necessary. However, it is difficult to see whether this work really causes additional expenses to the network operator. In order to operate the network properly and ascertain that the network fulfils common recommendations, the operator has to cooperate anyway with external parties, such as equipment manufacturers, electricity companies, regulators and public institutions, which have direct impact on the operator's business. Smooth running of the business also requires constant communication with the customers and actors that enable the business, e.g., an access provider needs to communicate with the transport network operators and a service provider with access/transport providers. Internal cooperation and communication with other departments within the actor's own organization should be self-evident. So, it can be concluded that design activities that aim at improved dependability do not raise Capex or Opex.

## 5.5 Cost of OAM activities

As was stated in section 4.4, the major issues in enhancing reliability by means of OAM are the adequate number OAM personnel and training of them, up-to-date OAM tools and coordination of the OAM processes. The OAM tools evolve constantly, which means that there is continuous need for OAM tool updates and training of the personnel. It may also happen that the new and more efficient OAM practices cannot be carried out without increasing the number of OAM personnel. Thus OAM can be seen to contribute to additional Capex and Opex constantly, especially when trying to enhance dependability, and equations (2) and (6) apply for cost increase calculations.

Capex is increased when preparing for network device failures by storing service and spare parts. The storing activity requires additional work to maintain the stocks and may also require additional storage space, which further increases Capex and Opex. Provided that the operator takes care of the prepare activities in any case then required service tools and personnel do not cause additional expenditure. Activities to purchase the spare parts cannot either be considered to cause additional expenditure, because the components need to be purchased

anyway, when new ones are needed. Thus, equations (2) can be applied for additional Capex and (6) for Opex calculations caused by the prepare activities.

## 5.6 Cost of purchasing activities

The purchasing activities should inherently support dependability of networks and there should not be any need for additional and costly operations. However, as was stated in section 4.5, poorly organized purchasing activities may lead to additional Capex and Opex thus cutting the operator's revenues. If this is the cases, raise of professional skills and change of purchasing practices are needed. Training of the purchasing personnel and adoption of new and more efficient practices increase Opex temporarily, but pays back in the future. Since the writer of this report thinks that each operator/provides should have up-to-date purchasing skills from the very beginning, it is hard to see that purchasing activities cause any increase of Capex or Opex.

## 5.7 Cost of other methods

The cost of the other methods in improving the dependability of an all-IP network depends on the applied method. As for the topological methods, physical double rings and mesh networks are usually more expensive to establish than the more straightforward tree-and-branch topologies. There is no much difference in the operational cost, but the increase of cable cost is proportional to the amount of additional installed cable. If disjoint cable paths are required then Capex and Opex increase can be outstanding due to the excessive amount of cable laying-out and equations (2) and (6) apply. The use of logical topologies in increasing dependability is clearly less expensive and may result in only moderate dependability increase. Exploitation of the logical topologies may require additional training of the personnel thus increasing Opex and equation (6) applies.

Careful planning of the locations of the networking facilities should be an integral part of normal operation. However, it is not always feasible to locate the networking facilities, such as cables and network equipment, in optimal locations, because that may entail substantial increase in Capex and Opex. However, equations (2) and (6) apply in calculating the extra expenses.

Agreements as a method to increase dependability may not be the first thing that comes into mind. Nonetheless, in today's highly commercialized world, agreements defining responsibilities and possible sanctions encourage provider to ascertaining that the quality of their services is at the required level. Experts capable of negotiating SLAs and other relevant agreements are needed and quite often these people are highly paid specialists. Therefore, agreement based increase of dependability can be seen to increase Opex permanently and a modified version of equation (5), i.e.,

$$P_o = m_a P_{a\_unit} T \tag{11}$$

applies for additional cost calculations. Here, $m_a$ gives the number of the additional negotiation persons, $P_{a\_unit}$ is the unit cost of one negotiation person and $T$ is the observation time period (e.g. months or years).

The lessons learned from the history can help in avoiding various kinds of problems as was discussed in section 4.6. The use of the historical data does not cause any additional cost as such. If interpretation of the data requires additional processing, manual or computer based, then the operator is faced with additional expenses. Manual processing increases Opex and computer based processing, if additional software and/or devices are needed, Capex and Opex. Training of the personnel to manage the new processing tools increases Opex further. As a conclusion equation (2) and (6) still apply for additional Capex and Opex calculations, respectively.

In section 4.6 it was also discussed about alternative technologies to increase dependability. The alternative solutions referred to a new packet switching concept, specially tailored to support reliable and secure communications. Although this would solve the problems of the IP networks, it is the most expensive solution for the time being. The existing network infrastructure should be replaced by the new one and the expenses would be very high. However, when considering the technical development it is likely that the IP technology will be replaced by some other technology, but this may take some time. If there is interest to estimate the cost of a new technology, equation (2) can still be used for Capex and (6) for Opex calculations.

## 5.8 Calculation example

In order to have a more concrete view of the additional cost that has to be paid for increasing dependability of an all-IP network, an example case is given to illustrate how the deduced equations work.

**Fictitious example of a redundant method**

A network operator purchases redundant routers to increase dependability of the core network. It is assumed that the operator benefits from price reduction, because the same devices have been purchased previously and the vendor gives some price compensation due to the large router volumes. The installation cost follows directly the number of the installed routers and no training is required. The operational workload depends on the number of the routers and a new operations person is supposed to be needed for each $n_{tv}$ routers. Training of the new persons is assumed to be part of the normal operations work. Equation (2) is used for calculating the Capex increase and (6) for calculating the Opex increase.

Figure 3 illustrates how Capex and Figure 4 how Opex develops as a function of the number of redundant routers. Separate curves are drawn for different parameter values. Table 1 gives the used parameter values for curves in Figure 3 and Table 2 the parameter values for curves in Figure 4.

*Table 1. Parameter values for curves in Fig. 3*

| | $\varepsilon_m$ | $\varepsilon$ | $n_{dv}$ | $P_{unit}$ [€] |
|---|---|---|---|---|
| $P_c1$ | 0.25 | 0.05 | 2 | 15 000 |
| $P_c2$ | 0.25 | 0.05 | 5 | 15 000 |
| $P_c3$ | 0.40 | 0.05 | 2 | 15 000 |
| $P_c4$ | 0.40 | 0.05 | 5 | 15 000 |

Figure 3 shows how the maximum obtainable discount value $\varepsilon_m$ and threshold value $n_{dv}$ (that triggers the increase of the discount) affect Capex. When comparing curves $P_c1$ and $P_c2$ (or curves $P_c3$ and $P_c4$), it can be seen that smaller values of $n_{dv}$ yield lower Capex increase up to the point at which the number of routers result in the maximum discount value for curves representing the larger $n_{dv}$ values. Beyond that point the curves having the same $\varepsilon_m$ value give equal Capex increase for each additional number of routers. Smaller discount step size $\varepsilon$ also results in lower Capex increase. Likewise, higher maximum obtainable discount value $\varepsilon_m$ yields permanently lower Capex increase as can be observed by comparing curves $P_c1$ and $P_c3$ (or curves $P_c2$ and $P_c4$).

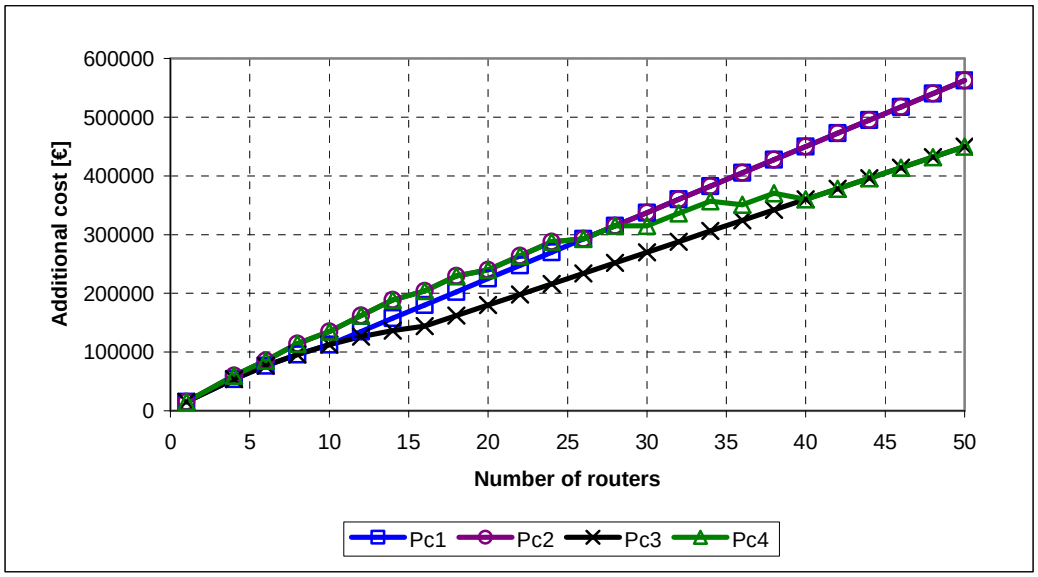


*Figure 3. Example Capex increase as a function of the number of additional routers.*

Figure 4 shows how $n_{tv}$, the threshold number of product units that triggers the jump in the operational workload, affects Opex. Curves $P_o1$ and $P_o2$ illustrate one year and curves $P_o3$ and $P_o4$ two years Opex increase. Larger values of $n_{tv}$ result in lower Opex increase, which is natural because large $n_{tv}$ values indicate that a single operations person is capable of maintaining a larger number of devices.

*Table 2. Parameter values for curves in Fig. 4.*

| | $m = n_{tv}$ | $p_{o\_unit}$ [€] | $T_o = T_{tr}$ [months] | $p_{tr\_unit}$ | $P_{inst}$ |
|---|---|---|---|---|---|
| $P_o1$ | 10 | 10 000 | 12 | 5 000 | 0 |
| $P_o2$ | 20 | 10 000 | 12 | 5 000 | 0 |
| $P_o3$ | 10 | 10 000 | 24 | 5 000 | 0 |
| $P_o4$ | 20 | 10 000 | 24 | 5 000 | 0 |

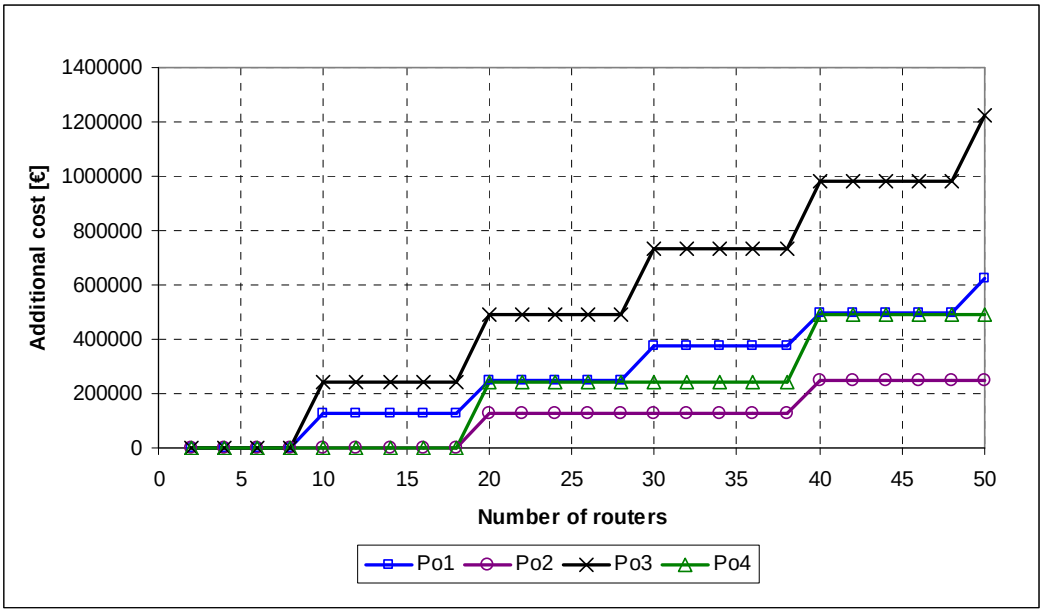


*Figure 4. Example Opex increase as a function of the number of additional routers.*

# 6 Conclusions

This report studies methods to enhance dependability of an all-IP network and discusses the capital and operational expenses caused by the use of them. At first, different perspectives to the dependability of a packet switched network are identified and goals of each viewpoint are compiled. Based on the technical structure of the IP networks and the identified viewpoints, a layered model for dependable communication is introduced. After that, methods to increase dependability on the given layers are discussed and simple formulas are provided to estimate the additional Capex and Opex, caused by the separate methods.

The means that can be applied on the different dependability layers are here categorized to redundancy, network control, design activity, OAM activity and purchasing activity based methods. Additionally, some other methods are discussed. The redundancy based methods, such as duplication of network equipment, which is often used in conventional telecommunications networks, are considered cost sensitive causing usually clear increase of Capex and Opex. As for the network control based methods, it is not so straightforward to say whether they increase expenses or not. Some of them may require only activation of an existing feature in the network devices, thus causing no additional expenses. Some other means may require purchase of new and up-to-date devices, training of personnel and even hiring of new employees, thus leading to clear increase in Capex and Opex.

There does not seem to be need for additional design and purchasing activities to enhance dependability, because proper design processes and purchasing processes should already cover all that is needed to maintain high dependability. The only thing that may be needed is sharpening of the existing design and purchasing processes. Therefore, these activities cannot be seen to cause additional Capex or Opex. OAM activities to obtain more dependable networks may turn out to be costly. On one hand, increase of dependability may require only modifications to the existing OAM practices causing practically no extra expenses. On the other hand, there may be need for new OAM equipment, training and new personnel in which case Capex and Opex go up clearly.

Other discussed methods (topology, location of networking devices, agreements, history and alternative technology), may produce substantial increase in Capex and/or Opex. Examples of Capex intensive methods are the use of resilient ring and mesh topologies that guarantee disjoint redundant paths or the secure location of network devices to ensure protection against natural catastrophes, vandalism and intrusion into the device premises. Agreements as a means to increase dependability are an example of methods that cause mainly increase in Opex due to additional highly paid professionals. Exploitation of historic data may raise Capex and Opex depending on how the data is utilized. The highest cost increase is faced with the alternative technology option. It offers the best way to avoid shortcomings of the IP networks, but within a short time frame results in the highest cost. Table 3 summarizes the effect of the given dependability enhancement methods on Capex and Opex. Small “x” indicates minor effect, large

"X" moderate or considerable effect, large bold "**X**" substantial effect and "-" negligible effect.

*Table 3. Summary of cost increase effect of the listed enhancement method.*

| Method | Capex increase | Opex increase | Note |
|---|---|---|---|
| Redundancy | **X** | X | Usually larger impact on Capex than Opex |
| Enhanced control | x | X | Usually minor impact on Capex and lager on Opex |
| Design activities | - | - | May require sharpening of processes |
| OAM activities | x or X | x or X | Cost effect is activity dependant - may have substantial or minimal effect on Capex and Opex |
| Purchasing activities | - | - | May require sharpening of processes |
| Network topology | - or **X** | X | Logical topology method usually increases only Opex, physical topology method has large impact on Capex |
| Location of network facilities | x, X or **X** | X | May have substantial effect on Capex |
| Agreements | - | X | Opex increase caused by highly-paid personnel |
| Lessons learned from the history | x | x | Minor effect on Capex or Opex |
| Alternative technology | **X** | **X** | Highest Capex and Opex increase in short time-scale |

Since the target of this report was to open structured discussion about the cost to enhance dependability of the all-IP networks, the financial impact of the different enhancement methods is studied only based on the expenses caused by them. The pay-back time or benefits of the different methods to the operator's business are not discussed. More information on the real operator business is needed to evaluate the entire financial effects of the different methods. One objective could be to find out which enhancement methods offer the best "cost-to-dependability increase" ratio. This information could be used in giving preferences to the methods when selecting them for practical use. The next phase of the project will study in more detail some of the addressed enhancement methods and their financial impacts.

# References

[1] Stevens W. R., “TCP/IP Illustrated – The protocols”, Volume 1, Addison-Wesley Professional Computing Series.

[2] B., Pelsser C., Swinnen L. Quoitin, Bonaventure O., Uhlig S., “Interdomain Traffic Engineering with BGP”, IEEE Communications Magazine, May 2003, pp. 122-128.

[3] Kurtansky P., B. Stiller, D. Singh, S. Zander, A. Cuevas, J. Jähnert, J. Zhou, “Extensions of AAA for Future IP Networks”, WCNC 2004, IEEE Communications Society, pp.

[4] http://www.alliedtelesyn.com/media/pdf/epsr_wp.pdf, “Ethernet Protection Switched Rings Creating the Survivable Ethernet Network”, White Paper, Allied Telesyn.

[5] http://miau.gau.hu/miau/94/rstp.pdf, Abuguba S. Moldovan I., “Verification of RSTP convergence and scalability by measurements and simulations”.

[6] http://www.nortel.com/solutions/optical/collateral/56046.25-0414-03.pdf, “Implementing Ethernet VPNs using Resilient Packet Ring”, Positioning Paper, Nortel Networks.

[7] RFC3619, Extreme Networks' Ethernet Automatic Protection Switching (EAPS) - Version 1, IETF.

[8] ITU-T G.8031/Y.1342, Ethernet Protection Switching