Project Number: IST-1999-11387

Project Title: Layers Interworking in Optical Networks (LION)

Deliverable Type: (P/R/L/I)* R

CEC Deliverable Number: IST-1999-11387/SIRTI/LION_D10

Contractual Date of Delivery to the CEC: month 11 of Year1

Actual Date of Delivery to the CEC: 15 / 01 / 2001

Title of Deliverable: Multilayer resilient network planning and evaluation: preliminary results

Workpackage contributing to the Deliverable: WP3

Nature of the Deliverable: **(P/R/S/T/O)**** R

Author(s): LION

Abstract:

The goal of this Deliverable D10 is the following: *“ Using planning tools as available by consortium partners and on the basis of preliminary results from WP1 and WP2, some initial results from the first networks planning case studies will be presented and discussed”.*

The Deliverable is based on the results of WP3 activities obtained from the work done. The main results of this Deliverable have been obtained using the planning tools available in the LION Consortium.

The preliminary results coming from the planned case studies are reported and analysed in terms of amount of planned resources and costs and some first indications and guidelines are gathered for each of the case studies planned. These initial results could also constitute an initial basis in order to pursue and identify a more suitable multi-layer resilient planning methodology.

Keyword list: network requirements, network scenarios, network case studies, Optical Transport Network, IP, MPLS, SDH, WDM, network architecture, network survivability, single layer network planning, multilayer network planning, metropolitan context, long distance context, planning tools.

* Type: P-public, R-restricted, L-limited, I-internal

** Nature: P-prototype, R-report, S-specification, T-tool, O-other

Status and Version:	Draft, Version 2.01	
Date of issue:	09 January 2001	
Distribution:	Project Internal	
Author(s):	Roberto Leone	Sirti S.p.A.
	Luigi Piergiovanni	Sirti S.p.A.
	Marco Quagliotti	Cselt S.p.A.
	Fausto Saluta	Cselt S.p.A.
	Julio Moyano	UPC
	Salvatore Spadaro	UPC
	Josep Solé-Pareta	UPC
	Didier Colle	IMEC – Ghent University
	Sophie De Maesschalck	IMEC – Ghent University
	Adelbert Groebbens	IMEC - Ghent University
	Ilse Lievens	IMEC – Ghent University
Checked by:		

Summary

1 Introduction

1.1 Purpose and Scope

The goal of this Deliverable D10 is the following: *“ Using planning tools as available by consortium partners and on the basis of preliminary results from WP1 and WP2, some initial results from the first networks planning case studies will be presented and discussed”.*

The Deliverable is based on the results of WP3 activities obtained from the work done. The main results of this Deliverable have been obtained using the planning tools available in the LION Consortium.

The preliminary results coming from the planned case studies are reported and analysed in terms of amount of planned resources and costs and some first indications and guidelines are gathered for each of the case studies planned. These initial results could also constitute an initial basis in order to pursue and identify a more suitable multi-layer resilient planning methodology.

1.2 Reference Material

1.2.1 Reference Documents

[WP3_T2] Roberto Leone et al., “Network scenarios and case studies propositions”, LION WP3 Task 2 Document , October 2000

[WP3_M1] Marco Qualgliotti et al., “Specification of functionalities of available planning and simulation tools”, LION Milestone WP3-M1, September 2000

[PNC] Didier Colle, et. al., “MPLS Recovery Mechanisms for IP-over-WDM networks”, special issue on 'IP over WDM and Optical Packet Switching' of ‘Photonic Network Communications’ Magazine, Vol.3, No.1, January, 2001, to be published

[ONM] Didier Colle et al., “Porting MPLS-recovery techniques to the MPλS paradigm”, submitted to Optical Networks Magazine, special issue on Protection and Survivability in Optical Networks

[1] “A Method for Setting an Alternative Label Switched Paths to Handle Fast Reroute”, work in progress, internet-draft March 2000: http://infonet.aist-nara.ac.jp/member/nori-d/mlr/id/draft-haskin-mpls-fast-reroute-03.txt

[2] Makam et al., “Framework for MPLS based recovery”, work in progress, internet-draft March 2000: http://search.ietf.org/internet-drafts/draft-makam-mpls-recovery-frmwrk-00.txt

[3] Makam et al., “Protection/Restoration of MPLS networks”, work in progress, internet-draft October 1999: http://search.ietf.org/internet-drafts/draft-makam-mpls-protection-00.txt

[4] Changcheng Huang et al., “A Path Protection/Restoration Mechanism for MPLS Networks”, work in progress, internet-draft March 2000: http://search.ietf.org/internet-drafts/draft-chang-mpls-path-protection-00.txt

[5] P. Van Heuven, et al., “Recovery in IP based networks using MPLS, Proc. of IEEE” Workshop on IP-oriented Operations & Management, Cracow, Poland, September 2000

[6] George Swallow, “MPLS Advantages for Traffic Engineering”, IEEE Communications Magazine, Vol. 37, No. 12, (December 1999), pp. 54-57.

[WPG1_DISC] Answers from Discussion Meeting, April 13th-14th 2000

[WP1_M1] Milestone WP1 M1: “Network Requirements”

[WP1_M2] Milestone WP1 M2: “Network Scenarios and Guidelines for the Testbed Configuration”

[WP1_D6] LION Project, “Network Scenarios and Requirements” – Deliverable 6, 30 October 2000

[WP2_M1] Milestone WP2 M1: “First indications of Failure Scenarios and Resilience Strategies”

[WP2_D7] Deliverable WP2 D7: “Failure Scenarios of Resilience in multi-layer networks”

[EUR_P918] EURESCOM Project P918-GI (Integration of IP over Optical Networks: Networking and Management), "IP over WDM Transport, and Routing" Deliverable 1, October 1999.

[EUR_P709] EURESCOM Project P709 (Planning of Optical Network), "Overview on modelling techniques, optimisation algorithms and planning tools". Volume 3 of 9 – Deliverable 3, March 2000.

[PANEL_D4b] Part B of Deliverable D4 of the PANEL project: "D4: Software Testbed Description; Part B: Planning"

[A1] L. Kleinrock "Queueing Systems", vol. II, J. Wiley & Sons, 1976

1.2.2 Abbreviations

ADM	Add Drop Multiplexer
APS	Automatic Protection Switching
ASON	Automatically Switched Optical Network
ATM	Asynchronous Transfer Mode
BSHR	Bidirectional Self Healing Ring
DPT	Dynamic Packet Transport
DWDM	Dense Wavelength Division Multiplexing
DXC	Digital cross Connect
EDFA	Erbium Doped Fiber Amplifier
FDM	Frequency Division Multiplexing; is used as a synonym for DWDM
FEC	Forward Equivalent Class (in context of MPLS)
FEC	Forward Error Correction
FR	Frame Relay
GbE	Gigabit Ethernet
HDLC	High-level Data Link Control
HEC	Header Error Correction
HO	Higher Order
IETF	Internet Engineering Task Force
IGP	Interior Gateway Protocol
IP	Internet Protocol
IPS	Intelligent Protection Switching
ISP	Internet Service Provider
ITU	International Telecommunication Union
LAN	Local Area Network
MAN	Metropolitan Area Network
MAPOS	Multiple Access Protocol Over SONET
MPLS	Multi-Protocol Label Switching
MSP	Multiplex Section Protection
MPλS	Multi-Protocol Lambda Switching
MS	Multiplex Section
MSP	Multiplex Section Protection
MTBF	MeanTime Between Failure
NE	Network Element
NHRP	Next Hop Resolution Protocol
NNI	Network to Node Interface

NSP	Network Service Provider
O/E/O	Opto-Electro-Optical
OA&M	Operation Administration & Maintenance
OADM	Optical Add Drop Multiplexer
OCh	Optical Channel
OTN	Optical Transport Network
OXC	Optical cross Connect
POS	Packet Over SONET/SDH
PPP	Point-to-Point Protocol
PVC	Permanent Virtual Circuit
QoS	Quality-of-Service
RS	Regenerator Section
SAP	Service Access Point
SDH	Synchronous Digital Hierarchy
SDL	Simple Data Link
SLA	Service Level Agreement
SONET	Synchronous Optical NETwork
SRP	Spatial Reuse Protocol
SRP-fa	Spatial Reuse Protocol – fairness algorithm
STM	Synchronous Transfer Module
SVC	Switched Virtual Circuit
TDM	Time Division Multiplexing
TMN	Telecommunication Management Network
VC	Virtual Container (SDH context)
WAN	Wide Area Network
WDM	Wavelength Division Multiplexing

1.2.3 Definitions

1.2.4 Deliverable History

Version	Date	Authors	Comment
0.1	15 November 2000	LION WP3	Initial document structure
1.00	23 November 2000	LION WP3	Draft friendly released to Cselt for the metropolitan Scenario 1 / case study 1 assessment and planning.
1.01	01 December 2000	LION WP3	Draft released to WP3 partners for check.
1.02	13 December 2000	LION WP3	Draft released to WP3 partners for check.
1.03	18 December 2000	LION WP3	Draft sent to partners for check
2.00	04 January 2001	LION WP3	Draft sent to partners for check. Remarks from Imec detailed list were included.
2.01	09 January 2001	LION WP3	Draft sent to partners for check
2.01	10 January 2001	LION WP3	Final document

1.3 General framework

This paragraph aims to describe the general framework in which we can find and deploy proper scenarios and case studies. Due to the ongoing evolution in telecommunications worldwide, it was agreed within WPG 1 to consider the following network architecture:

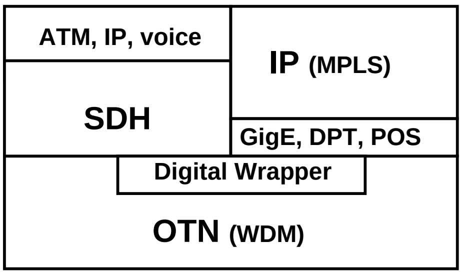


Figure 1-1: Network architecture to be considered

Based on the proposed architectural solutions, we have abstracted some main scenarios. In this selection phase, the policy was trying to follow the most probable evolutionary and migratory trace. Inside each scenario, also the case studies are proposed following an probable evolutionary trace.

1.4 Document overview

The document is structured as follows:

Section 1, the present one, gives a general overview of the document describing its purpose and scope, the general framework and its organization.

In **Section 2** a general description is given of the Scenarios and Case studies that will be planned.

In **Section 3** an overview is given on planning and simulation tools as available to LION Project participants.

In **Section 4** some preliminary results coming from plannings are given for some particular scenarios and case studies.

In **Section 5** some first indications and guidelines are given, referred to the specific cases as planned.

2 Description of the Scenarios and case studies

2.1 Introduction

The exemplary networks has been defined assuming the following criteria, based on a three level classification, from the higher to the lower level: *Context, Scenario and Case study*. Thus the same *context* could have many alternative *scenarios* and for each *scenario* we could define one or more *case studies*.

Context defines the geographical environment and the requirement of the network at the highest (IP) level. Traffic requirements are between a given set of network sites at IP level (routers, content servers) and they can be defined separately for each class of application/service.

Scenario identifies the technological solution chosen for the network. More precisely It involves the multi-layer protocol stack specification. (IP over SDH over WDM, for instance).

Case Study is the third key to define a network to be studied and implies the detail on architecture and topology. For example it defines if the topology is a ring or a mesh and chooses the type of apparatus employed at each level (for example add drop multiplexers or cross connects).

Two *contexts*, a metropolitan network located in Milan and a long haul Italian nationwide backbone network, have defined and presented in the deliverable. For each context a number of scenarios have been defined, taking also into account a migration perspective from a multilayer network structure (e.g. with SDH as a in-beetween layer) towards more integrated solutions (e.g. IP directly on WDM). Inside each scenario, some significant case studies are in their turn presented, taking into account a same evolutionary perspective (e.g. technology enhancements progressively extended from the central to the peripheral rings).

2.2 Metropolitan Context

In this section the network proposed is a metropolitan IP network. Although the example is abstracted from Milan reality, we can suppose that many other big European cities are living a similar evolution. New operators are deploying new metro IP networks with the aim to offer IP high bandwidth access to customers, both residential and business.

For the metropolitan network a number of case studies, grouped into three scenarios, have defined. A number of services are considered belonging both to elastic (web browsing, message exchange) and straeaming with stringent delay requirements (audio-ToIP- and video streaming).

2.2.1 Network description

2.2.1.1 The Client network

In this section it is described the client network that we will consider as over-standing the transport layer. In the following, we skip a general description of the Internet architecture and partitioning. The focus will be on a particular IP subnetwork, an example about a sub-network an operator or a service provider is requested to build and to manage for making its busisness.

We will main concentrate on a core (regional or backbone) IP network. This kind of networks are typically meshed and constituted by high-capacity routers, that aggregate and route great quantities of traffic coming from or going to the access routers, or directed to other interconnected IP networks.

The IP network portion we consider is shown in Figure 2-1. It is composed by 13 nodes (10 routers and 3 servers) interconnected by 20 logical links. We consider that in this network there is a single server that manages http and mail service, another single server to manage telephone traffic and another server to manage video on demand service. The connections between nodes are to be considered like logical connections of OSI level 3. Please note that even though the transport network is structured on two or more levels (peripheral versus central rings), the logical network is "flat". In other words, all the routers belong to he same hierarchical level: they can be logically connected together without any hierarchical rules and they all participate to the same autonomous system and run the same IGP (Interior Gateway Protocol) routing process.

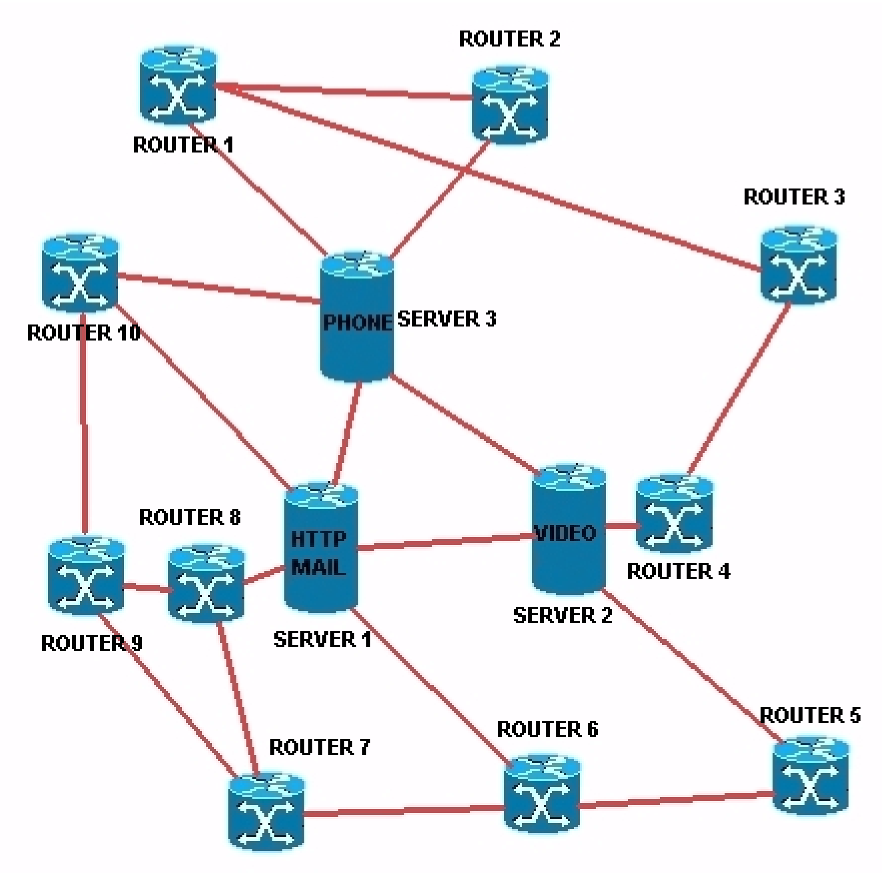


Figure 2-1: IP client network

2.2.1.2 The Transport network

The scenarios and the related case studies that will be shown in this document, are based on the same transport infrastructure, as assumed and shown in Figure 2-2. In the figure it is represented a metropolitan or a geographical high density environment administrated with a **two level** structure; level one is created with transit nodes. In level two some interconnection nodes are used. The transit nodes are grouped in such a way that each group refers to a particular interconnection node.

A ring topology is the transport solution normally used for the transit nodes. The ring or the mesh solution is used for the interconnection nodes. These usual topology solutions are reproduced in our case studies.

This transport infrastructure is characterized by the transport technologies the Operator decides to use to interconnect the IP routers. In the following sections we consider some significant scenarios in this sense (IP over SDH over WDM, IP directly over WDM, and so on).

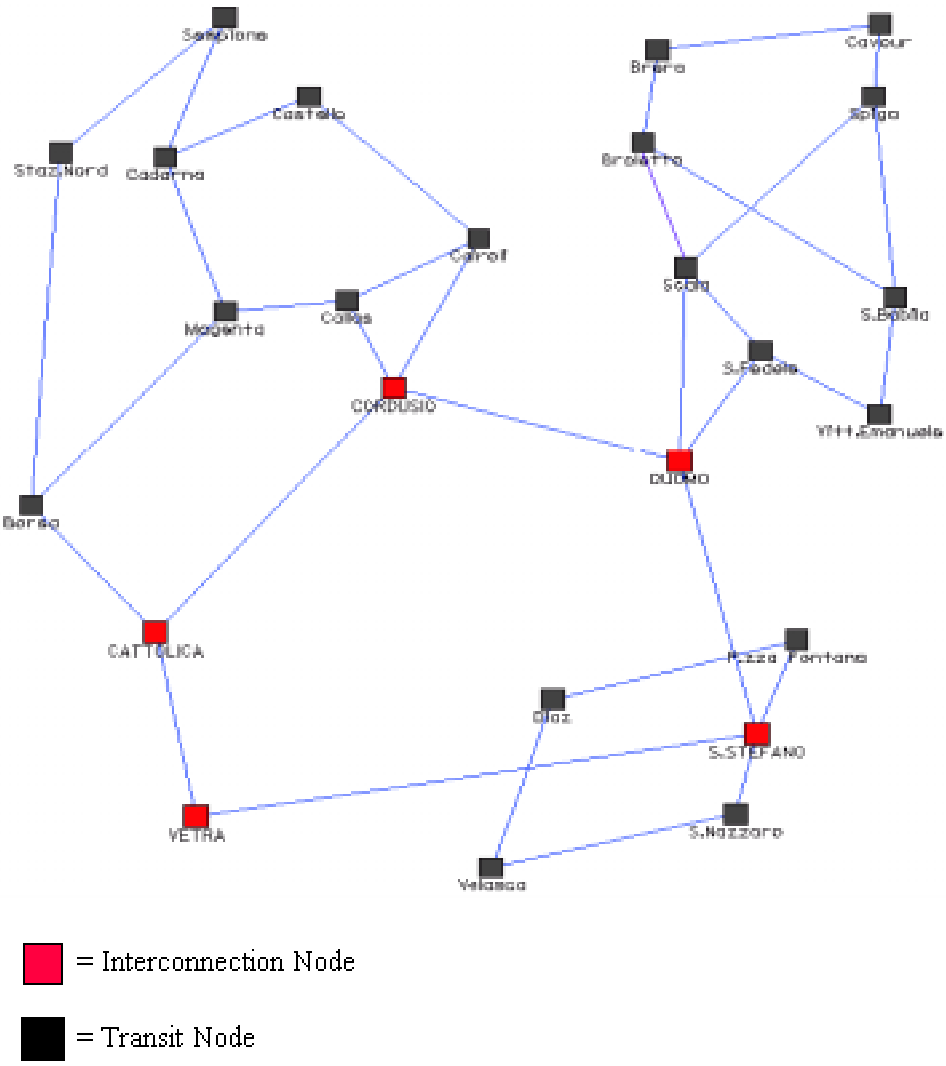


Figure 2-2: Transport network

2.2.2 Services description.

2.2.2.1 Generalities

The following services will be considered:

Web browsing

HTTP based router to router service (like video conferences or interactive archives consultation)

E-mail service

Server mediated telephony

Low Quality Video on demand

High Quality Video on demand

The http service can be considered as a bi-directional asymmetric flow, from the router to the server (upstream) and from the server to the router at which the user is connected (downstream).

The http based service can be considered composed by asymmetric bi-directional router to router flows.

On the contrary e-mail is a server-mediated service, infact an e-mail flow is composed by two parts, the first from the origin router to the server, and the second from the server to the destination router .

The Phone service is more interesting to analyze, because it is composed by two components: signaling and the data flow. In this paragraph we will consider the signaling like a server mediated service, and data like a direct router to router flows.

Considering the Video on demand service, it may be considered like a bi-directional asymmetric service, because the downstream throughput is greater than the upstream one.

The services considered are the most common IP-based applications used, and in our service modeling only some parameters will be take into account.

2.2.2.2 Services requirements

Web browsing service is composed by two “block transfer” typology contributes , the service request and the service supplying. QoS requirements imply a loose limited delay in end to end transfer.

For the service supplying (downstream flows) the supposition shown in Table 2-1 can be done. The service request (upstream flows) in nearly a tenth of the downstream one, so the bit rate in bit per second is 395 bit/s (see again Table 2-1).

Service	Web browsing
Bit rate	3950 bit/s
Directionality	Server to user
Typology	Block transfer
QoS requirements	Loosely limited delay
Mean packet size	410 byte

Service	Web browsing request
Bit rate	395 bit/s
Directionality	User to server
Typology	Block transfer
QoS requirements	Loosely limited delay
Mean packet size	410 byte

Table 2-1: Services requirements – Web browsing

For the **http** based services we can consider the same bit rate of the previous service, but the directionality is user to user (router to router). Also for this service, the flows can be divided into two classes, service request (from the router that asks for a service to the router that supplies the services) and service supplying.

Service	Http based request
Bit rate	4000 bit/s
Directionality	User to user
Typology	Block transfer
QoS requirements	Loosely limited delay
Mean packet size	410 byte

Service	Http based supplying
Bit rate	400 bit/s
Directionality	User to user
Typology	Block transfer
QoS requirements	Loosely limited delay
Mean packet size	410 byte

Table 2-2: Services requirements – Http based services

For the **e-mail** service the following suppositions can be done: this service is a “user to user” service with the traditional best effort QoS requirements

The message generation frequency is nearly 0.00199 message/second

The mean message dimension is nearly 93360 bit.

We can suppose that, when a customer uses e-mail service, the bit rate per second is nearly **186 bit/sec**.

Service	**Mail**
Bit rate	186 bit/s
Directionality	User to Server to user
Typology	Block transfer
QoS requirements	None
Mean packet size	500 byte

Table 2-3: Services requirements – E-mail

For the **telephony** service, we can do the following supposition: **Telephone** service can de separate into two contribution : signaling and real voice traffic. In this case study we will analyze only voice traffic, and it is a user to user service of a streaming typology. A bandwidth must be granted per session. The packet delay must be limited.

We consider the G.726 codify

The bit rate for this kind of service is bi-directional

The bit rate is nearly 22400 bit/sec

We can suppose that, when a customer uses telephony service, the bit rate per second is nearly **22400 bit/s**. For the phone service, as well as for its **signaling**, we can do the suppositions reported in Table 2-4.

Service	**Phone**
Bit rate	22400 bit/s
Directionality	User to user
Typology	Stream
QoS requirements	Delay, jitter
Mean packet size	80 byte

Service	Phone signaling
Bit rate	Not considered
Directionality	User to server to user
Typology	Block transfer
QoS requirements	--

Table 2-4: Services requirements – Phone service

For the **video on demand (low quality)** service we can do the following supposition:

it is a bi-directional asymmetric service of a streaming typology in downstream and of a block transfer typology in upstream. The packet delay and jitter must be limited.

The bit rate for this kind of service in nearly **10 Kbit/s** in upstream and nearly **1 Mbit/s** in downstream.

Service	Video on Demand type 1 (low quality)
Bandwidth upstream	10 kbit/s (mean)
Bandwidth downstream	1 Mbit/s (mean = peak)
Directionality	Bi-directional asymmetrical
Typology	Downstream: streaming, Upstream: block transfer
QoS requirements	Packet delay (50 ms), Jitter (25 ms)
Mean packet size	1500 byte

Table 2-5: Services requirements – VoD (low quality)

For the **video on demand (high quality)** service we can do the following supposition:

it is a bi-directional asymmetric service of a streaming typology in downstream and of a block transfer typology in upstream. The packet delay and jitter must be limited.

The bit rate is asymmetrical

The bit rate for this kind of service in nearly **20 Kbit/s** in upstream and nearly **4 Mbit/s** in downstream.

Service	Video on Demand type 2 (high quality)
Bandwidth upstream	20 kbit/s (mean)

Bandwidth downstream	4 Mbit/s (mean = peak)
Directionality	Bi-directional asymmetrical
Typology	Downstream: streaming, upstream: block transfer
QoS requirements	Packet delay (20 ms), Jitter (10 ms)
Mean packet size	1500 byte

Table 2-6: Services requirements – VoD (high quality)

2.2.2.3 Customer use assumptions.

The goal of this paragraph is to do some assumptions in order to estimate the traffic flows for the IP network described above. In this part of the study it isn't important to know which type of transport network exists under the client layer, being the IP traffic flows independent from the transport technology used.

The first assumption we do is that IP routers and servers can be considered as traffic flows origins or destinations for the IP network portion we consider. Servers can also act as transit elements.

To estimate the traffic flows intensity, let's assume to divide the customers area in some parts; each part can represent a city zone or a geographical zone. In the Figure 2-3 it is shown a possible customer area divided into 11 parts.

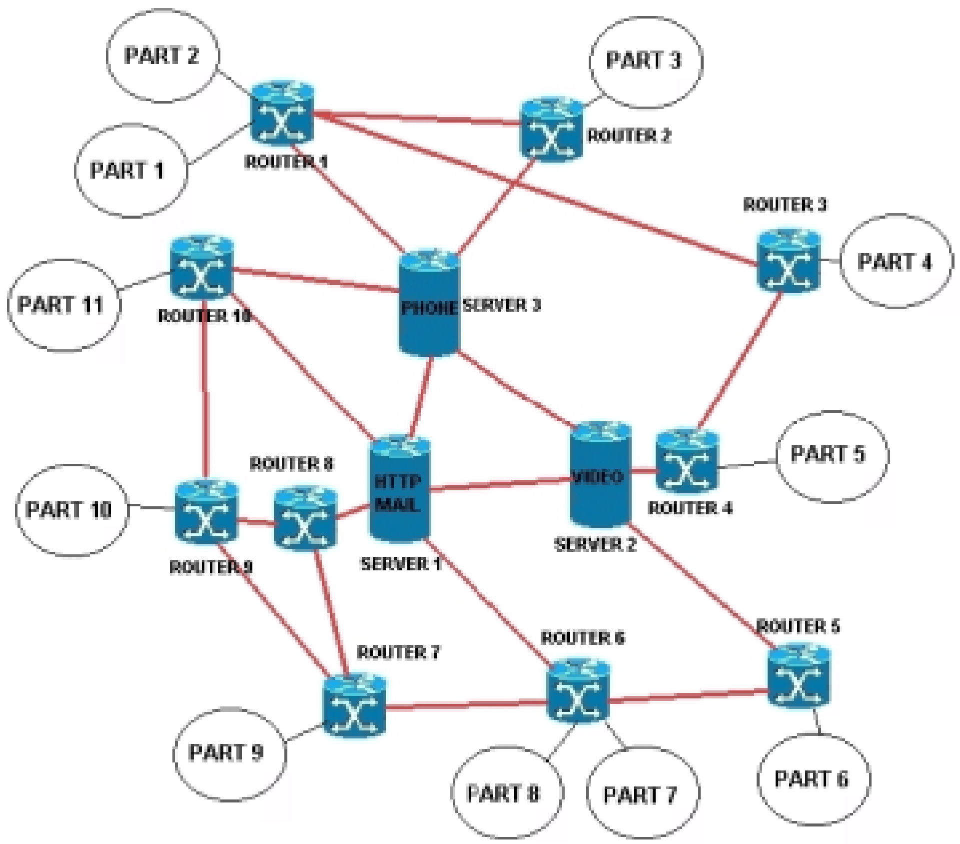


Figure 2-3: IP users distribution

Each part is served by an IP router and the same IP equipment can serve more than one part. On the contrary, a part can't be served by more than one router.

Some hypothesis about the density of the parts previously described are necessary to estimate the traffic flows. We have also to think about how many (in percentage) customers in every part use the described services. Then we have to do some hypothesis on the penetration of every service.

In the [WP3_T2] document some assumptions are done, considering that to justify the use of WDM technology, the density must be high enough to produce great traffic flows. Services available for the considered part are also reported.

2.2.2.4 IP Traffic flows estimations.

See Appendix M_2

2.2.3 Scenarios and case studies.

2.2.3.1 Scenario 1: IP over SDH over WDM

Architectural aspects

Listening how many of ISPs talk nowadays, in short time, public networks may shift from the current architectural answer (IP over ATM over SDH over WDM) to IP over SDH over WDM.

IP directly over SDH using PPP or HDLC framing and encapsulation provides a robust, reliable, bandwidth-efficient solution for the transport of IP packets from 155 Mbps to 2.4 Gbps rates. Extensions to these specifications will be necessary to extend the transmission range up to 9.8 Gbps. The SDL (Simplified data link) could be such an extension, being it a new encapsulation method and a very low-overhead alternative to HDLC.

IP over SDH/SONET technology is being deployed today in IP backbone networks to provide efficient, cost-effective, high-speed transport between fast routers.

More information concerning integration over optical networks through a SDH layer can be found in [EUR-P918].

IP over SDH over WDM is then a very strategic solution for incumbent operators that own a well established SDH network platform.

Resilience aspects

It is obvious the need to plan and build network architectures providing with the capability to recover failure situations in short time. Protection or restoration mechanisms must be quick enough to avoid that outages **could spread to the upper layers**, causing heavy re-configurations and long out-of-service times.

IP over SONET/SDH technology is being deployed today in IP backbone networks to provide efficient, cost-effective, high-speed transport between fast routers. Packet over SONET (POS) is nowadays a prevailed technology for transferring IP traffic above a SONET network. The IP routers with PoS interfaces can receive and send appropriate protection signals to connecting ADMs to detect failure states. The protection capabilities of the POS solution are similar to that of the SDH, allowing restoration with 50 msec.

The synchronous digital hierarchy **(SDH)** was introduced towards the end of the 1980s and SDH networks are widely deployed. Many different approaches have been proposed for designed a survivable SDH networks and a lot of research work has been done in the area. SDH allows fast restoration within 50 ms. Two types of protection are available in SDH and depending on the topology of the network (ring or mesh) different schema can be used.

Finally **WDM**, is the server layer that carries all the above mention client layer. The flexibility of the protection/restoration mechanism of the OTN is of vital importance since the disruption of a fiber carrying Terabits of traffic affects thousand of connection. Many ideas of the SDH protection has be shifted and adopted by the OTN, thus OTN has capabilities similar to the SDH. MPλS, which is similar to the MPLS, allows protection schemes similar to the MPLS. Moreover, the introduction of the MPλS allows new fiber-based restoration scheme which aggregates (stacks) all the wavelengths of one link into a larger optical LSP.

2.2.3.1.1 Case studies

IP to transport Interconnections

In the case studies for the Scenario 1, we suppose that the IP routers are connected with the peripheral rings (the used technology is always IP over SDH over WDM). We suppose that the servers are directly connected with the interconnections (red ones) nodes,

In the following Figure 2-4, all the interconnections between the IP level and the transport (SDH, SDH+WDM) level are shown.

We introduce three different solutions based on the probable evolution of the network solutions.

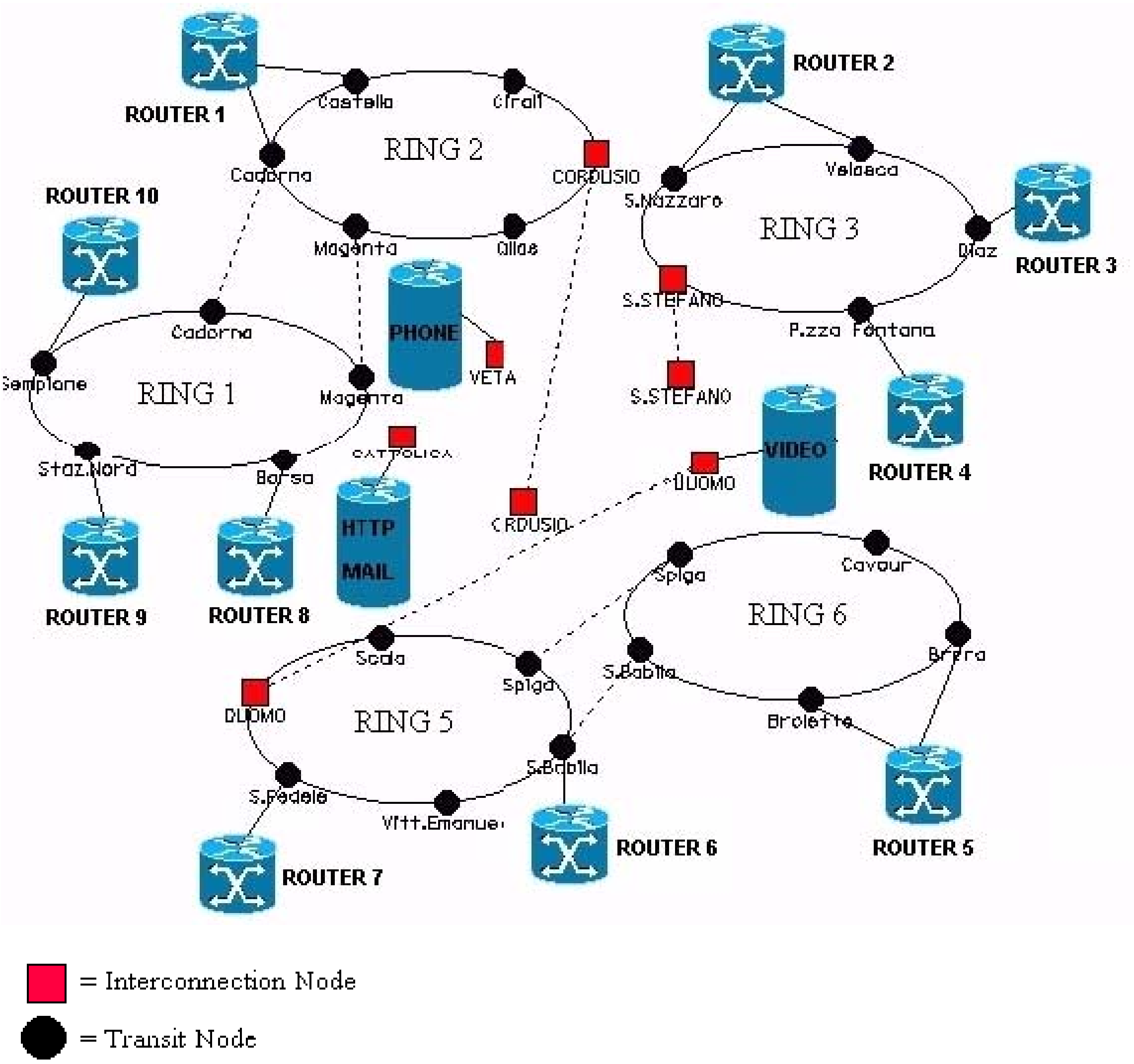


Figure 2-4: Scenario 1 – IP to transport level interconnections

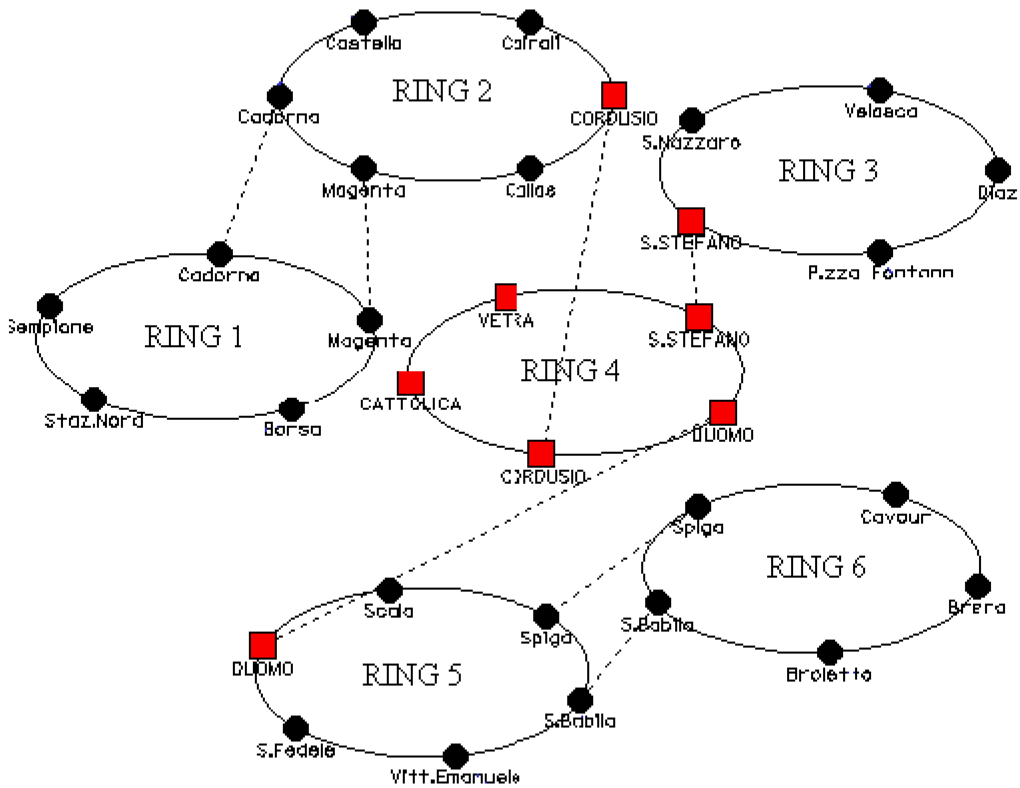
Table M_2-17 (see sub-appendix M_2.2) reports an estimation of the costs of the IP level connections. The weight is given by the number of rings to be run along the underlying transport network as configured for the scenario 1.

Case study 1: (ADM + WDM point-to-point) in the central ring

In this first case study, interconnection nodes are sites in which the operator can place add-drop multiplex (ADM) and WDM point-to-point equipment. In transit nodes only ADM equipments can be placed.

Then, a WDM point-to-point solution is analyzed for the RING_4 and a simple SDH solution is used for the other peripheral rings. In a transit node the operator can place only an ADM equipment, so the structure is simple; for example if we suppose to use on a particular ring the STM-4 system, (622 Mbps), in the transit node we will find an ADM-4 equipment. A detailed description of the structure of an Interconnection node, in which we can find both ADM and WDM equipment, is given in the Appendix M_1 of this document .

Traffic and service requirements are those described in Section 2.2.2 .



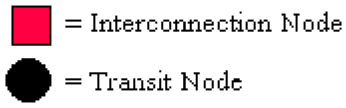


Figure 2-5: Pure SDH in the peripheral rings. SDH over WDM in the central ring

In the [WP3_T2] document a table lists the kinds of equipment the operator can put in each node.

The WDM ring will be implemented with five point-to-point connections.

Case study 2: (ADM + WDM point-to-point) all over

For this second case study, we suppose the evolution of the network will bring Operators to extend the ADM + WDM p-t-p solution from the central ring to the whole infrastructure.

Traffic and service requirements are those described in Section 2.2.2 .

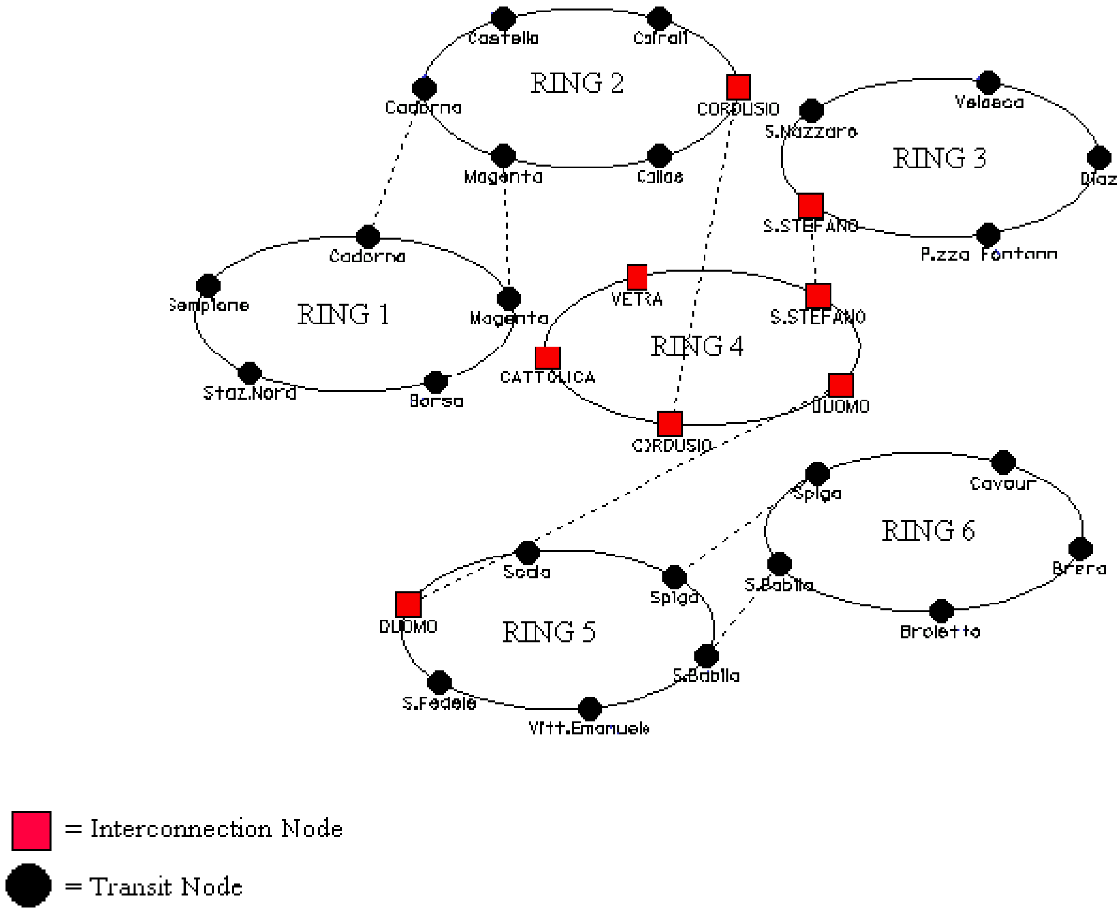


Figure 2-6: IP over SDH over WDM all over the network

Case study 3: OADM central ring

This case study will represent an intermediate step in the network evolution, preceding the complete introduction of an entire IP over WDM network. In this solution we can hypothise ADM and WDM ptp in the peripheral rings and a central ring composed by OADM equipment

Traffic and service requirements are those described in Section 2.2.2 .

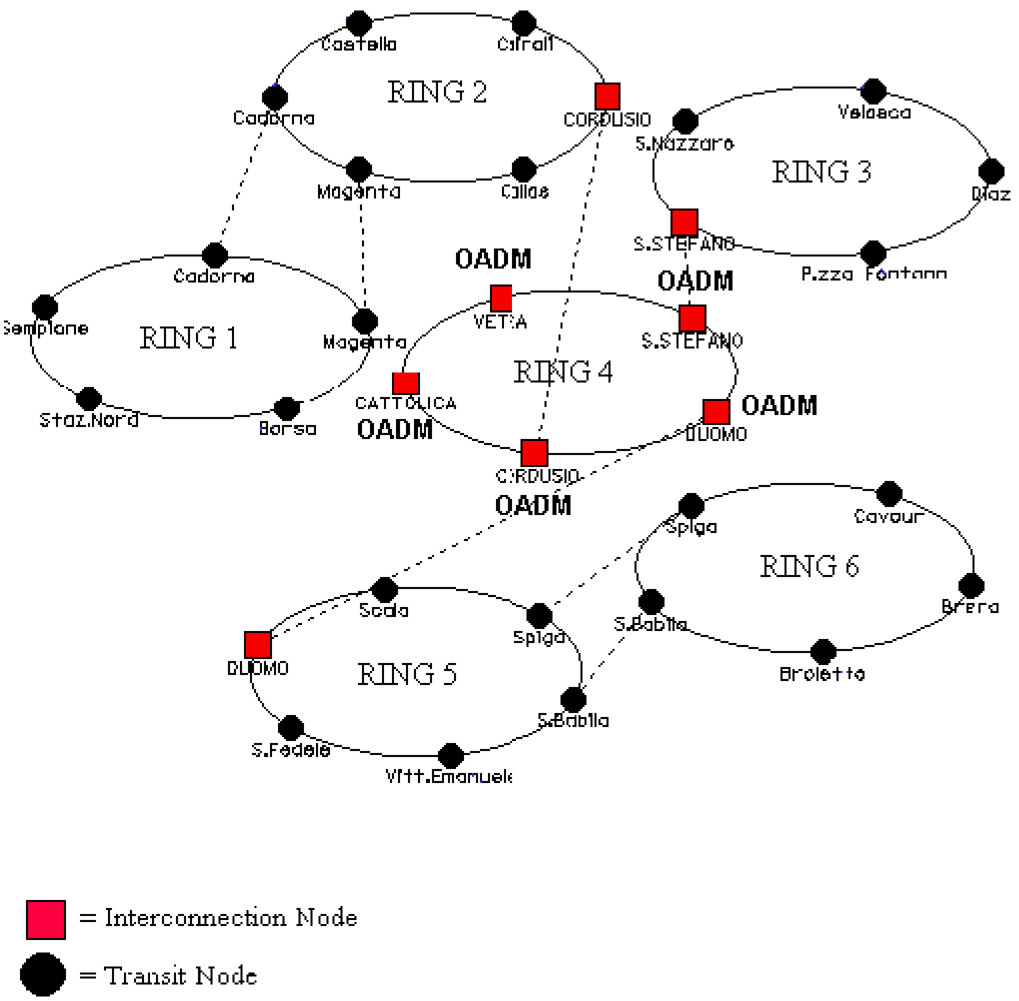


Figure 2-7: IP over SDH over WDM at the peripheral. IP over WDM in the central ring.

2.2.3.2 Scenario 2: IP over WDM

Architectural aspects

Considering the exponential growth of Internet traffic, combined with the vast bandwidth possibilities offered by WDM, the IP over WDM scenario may become very important in future.

In the medium to long term, WDM will be used to route traffic on individual wavelengths in all levels of the network, significantly increasing flexibility, leading to an *optical networking.* This transition will create an optical layer (a new networking layer) in which wavelength channels are processed and routed by all optical equipment. This will involve the deployment of optical add-drop multiplexers, enabling WDM ring architectures to be built. In the longer term this will also require the deployment of optical cross-connects to reconfigure and re-route individual wavelength channels.

“Pure” IP over WDM can be envisaged, in medium and longer terms, as the more advanced scenario for all the Operators. It could also represent, a winning short term choice, for the incoming operators (newcomers).

Resilience aspects

To combine these two technologies residing in layer 1 and layer 3 of the TCP/IP stack, one or more intermediate technologies (layer 2 or 2.5) may be needed, such as an MPLS-platform (or possibly MPλS) for traffic engineering or network resilience.

The **IP** layer at the top has a limited protection functionality in the sense that the only mechanism for a pure IP network to recover from a failure is rerouting. OSPF, IS-IS, EGP can reroute the traffic in case of a failure but the time needed for the algorithm to converge is in the order of seconds. Thus, rerouting time compared to the 50ms of the SDH recovery is extremely poor especially in the case of real time applications. However, with the introduction of the MPLS, which can be considered as a layer between layers 2 and 3, IP can support more elaborate mechanism.

MPLS allows fast protection switching in a way similar to the ATM, occupying resources along a backup path only when needed. This way of working combines the advantages of protection (fast recovery) and restoration (capacity efficiency). Survivability in the IP layer using MPLS is an area of research interest in many consortiums and institutes.

WDM is the server layer that carries the entire above mentioned client layer. The flexibility of the protection/restoration mechanism of the OTN is of vital importance since the disruption of a fiber carrying Terabits of traffic affects thousand of connection. Many ideas of the SDH protection has be shifted and adopted by the OTN, thus OTN has capabilities similar to the SDH. MPλS, which is similar to the MPLS, allows protection schemes similar to the MPLS. Moreover, the introduction of the MPλS allows new fiber-based restoration scheme which aggregates (stacks) all the wavelengths of one link into a larger optical LSP.

2.2.3.2.1 Case studies

IP to transport Interconnections

In the case studies for the Scenario 2, we present a different interconnection solution. The number of the external rings is now reduced from five to three rings. The IP routers are still connected to the peripheral rings, while now one of the two servers is connected to one of the peripheral rings.

In the following Figure 2-8, all the interconnections between the IP level and the transport (pure WDM everywhere) level are shown.

We then introduce two different solutions based on the probable evolution based on the more advanced network solutions.

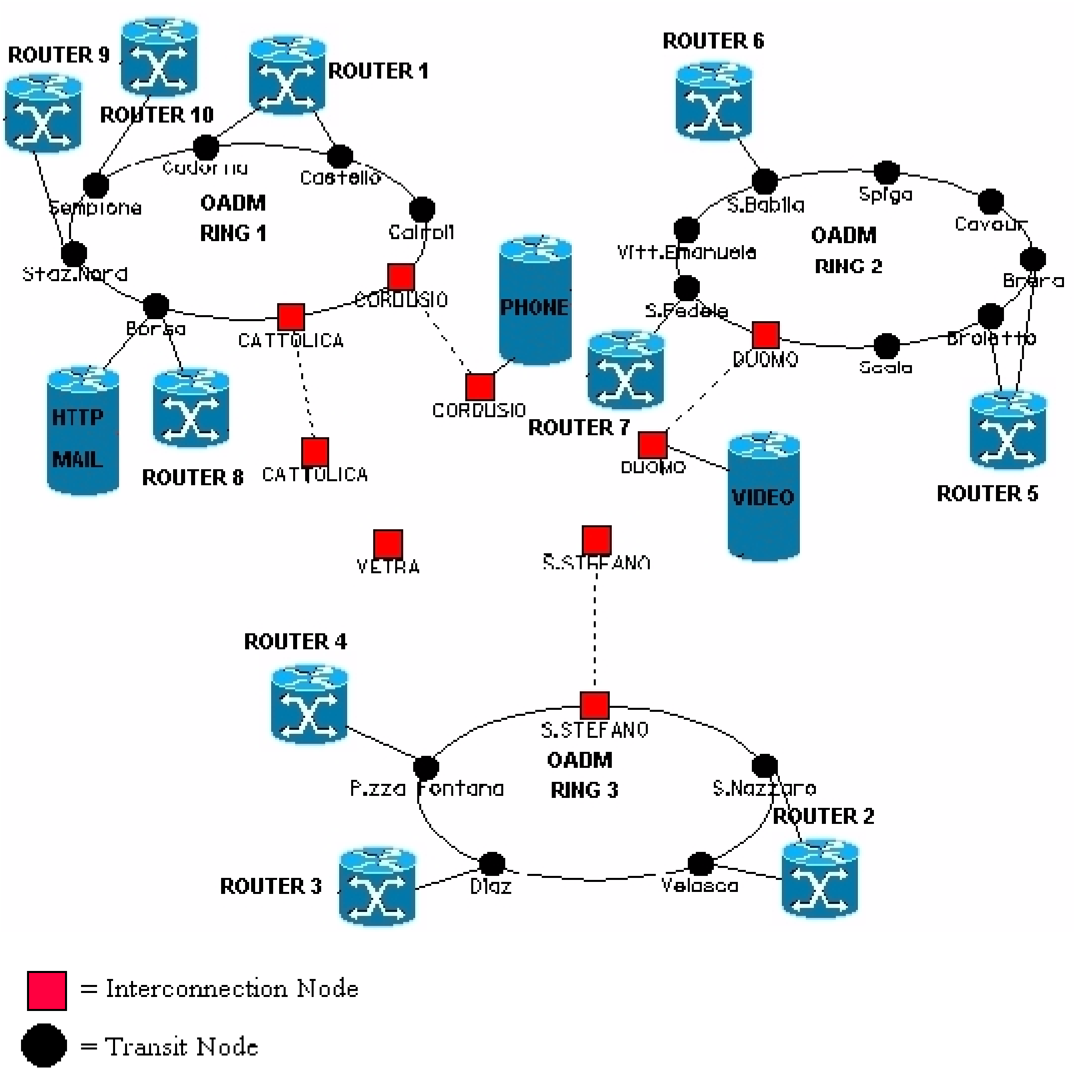


Figure 2-8: Scenario 2 – IP to transport level interconnections

Table M_2-18 (see sub-appendix M_2.2) reports an estimation of the costs of the IP level connections. The weight is given by the number of rings to be run along the underlying transport network as configured for the scenario 2.

Case study 1: IP over WDM – ring solution

In order to shift from point-to-point connections to the multipoint-to-multipoint ones (in the optical layer), more sophisticated full optical equipment has to be employed, such as reconfigurable OADMs and OXCs. These systems provide protection, restoration and performance monitoring mechanisms performed at the optical layer level, assuring the survivability of the optical network.

In this case study, we propose to study a network architecture, which combines only OADM rings, such as that depicted in Figure 2-9. The peripheral rings could be considered as belonging to regional or metropolitan networks. The central one, of greater dimensions, could be considered as a backbone ring.

Traffic and service requirements are those described in Section 2.2.2 .

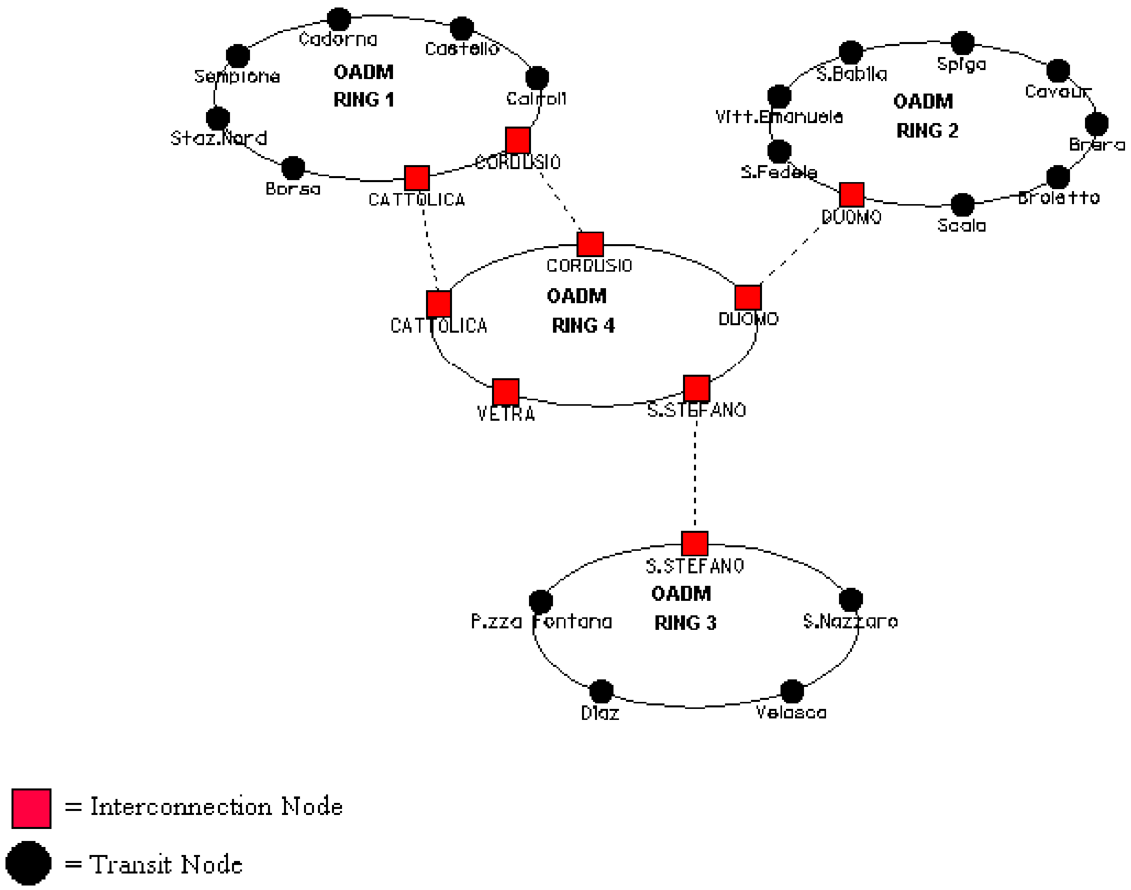


Figure 2-9: IP over WDM all over the network

Case study 2: IP over WDM – central mesh solution

In the longer term, besides the deployment of OADM rings, it is also expected the deployment of Optical Cross connects (OXC) equipment, to reconfigure and re-route individual wavelength channels in the network.

We then propose to study a network topology, which combines peripheral OADM rings and a meshed OXC network as a backbone, such as that depicted in the following Figure 2-10.

Traffic and service requirements are those described in Section 2.2.2 .

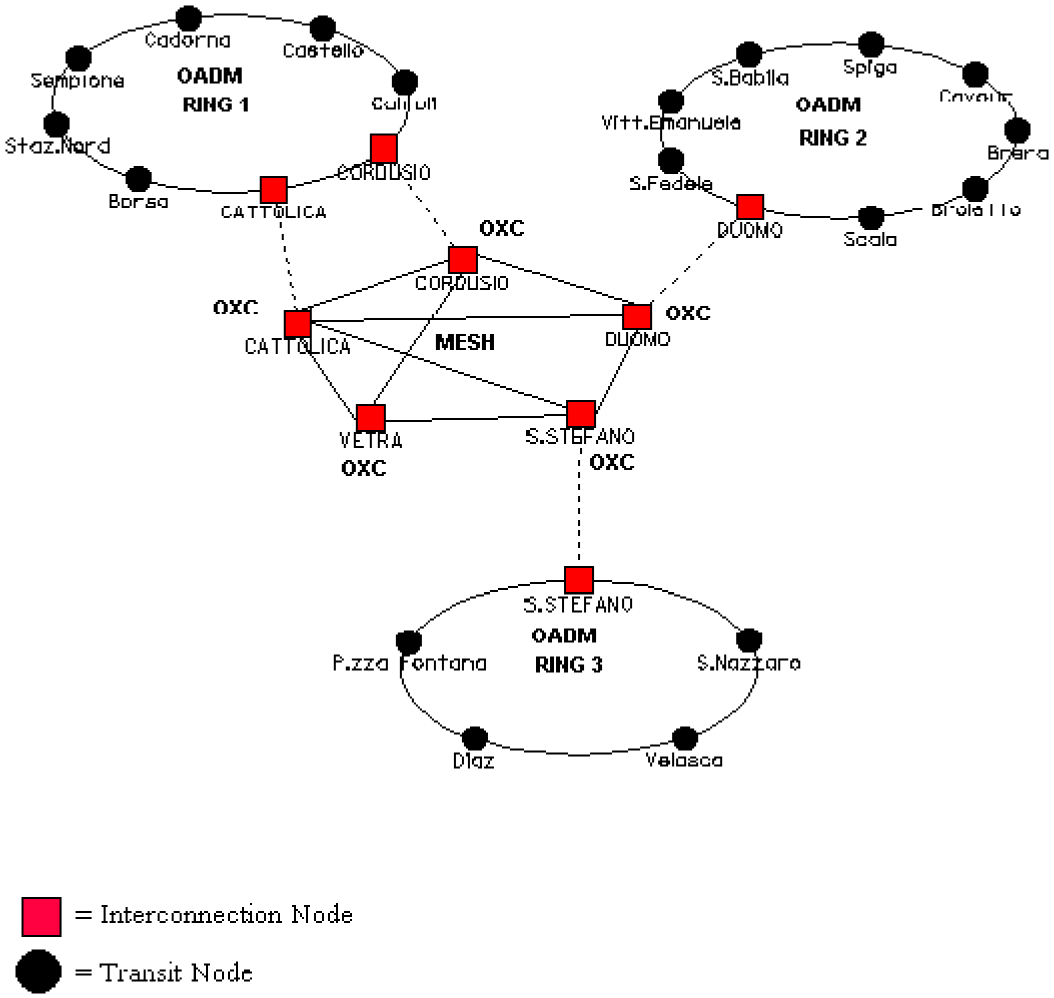


Figure 2-10: IP over WDM all over the network

2.2.3.3 Scenario 3: IP over DPT/SRP over WDM

Architectural aspects

Another interesting scenario, specifically for the metropolitan context, is that based on the Dynamic Packet Transport technique and the Spatial Reuse Protocol (DPT/SRP). An overview of the DPT solution and its SRP protocol can be found in [WP1-M1].

The purpose of this new scenario is to propose a data optimised solution due to the limitations of SDH rings when carrying data traffic (IP traffic). This new scenario (IP over DPT/SRP) eliminates the high cost of SDH multiplexing equipment (ADMs), exploits the price/performance offered by data networking equipment, and overcomes the limitations that TDM/circuit-based architectures imposed on data communications.

In particular, it is proposed to evaluate the capabilities of the IP packet transport solution based on DPT/SRP in comparison with those of the scenario 1 (IP over SDH over WDM).

Resilience aspects

The SRP layer utilises a protocol known as Intelligent Protection Switching (IPS) to provide the ability of the SRP ring (DPT ring) to recover from events and faults such as fiber cuts or node failures.

IPS is analogous to the self-healing properties of SONET/SDH (APS) but the wrapping of traffic onto the alternate fiber is done without the need to allocate protection bandwidth providing service restoration times within 50 msec. This wrapping is transparent to layer 3 routing protocols. IPS monitors and handles events at layer 1, 2 and 3 instead of just layer 1 events.

The IPS protocol maintains a protection switching event hierarchy that handles concurrent multiple events (e.g. signal fail and signal degrade events) without partitioning the ring into separate sub-rings.

At the WDM layer, the protection/restoration mechanisms are those described in the previous scenarios.

2.2.3.3.1 Case studies

IP to transport Interconnections

In the case studies for the Scenario 3, we present a slight modification respect the Scenario 2 interconnection solution. The number of the external rings is still three and the IP routers are connected to the peripheral rings, while now the http/mail server is again connected to an interconnection node.

In the following Figure 2-11, all the interconnections between the IP level and the transport level are shown (DPT peripheral rings and WDM in the interconnection nodes).

Although the SRP protocol is physical media (layer 1) independent, at present it is not clear how DPT and WDM technologies can interwork properly. Therefore, within this scenario, only DPT over dark fiber is considered as case study.

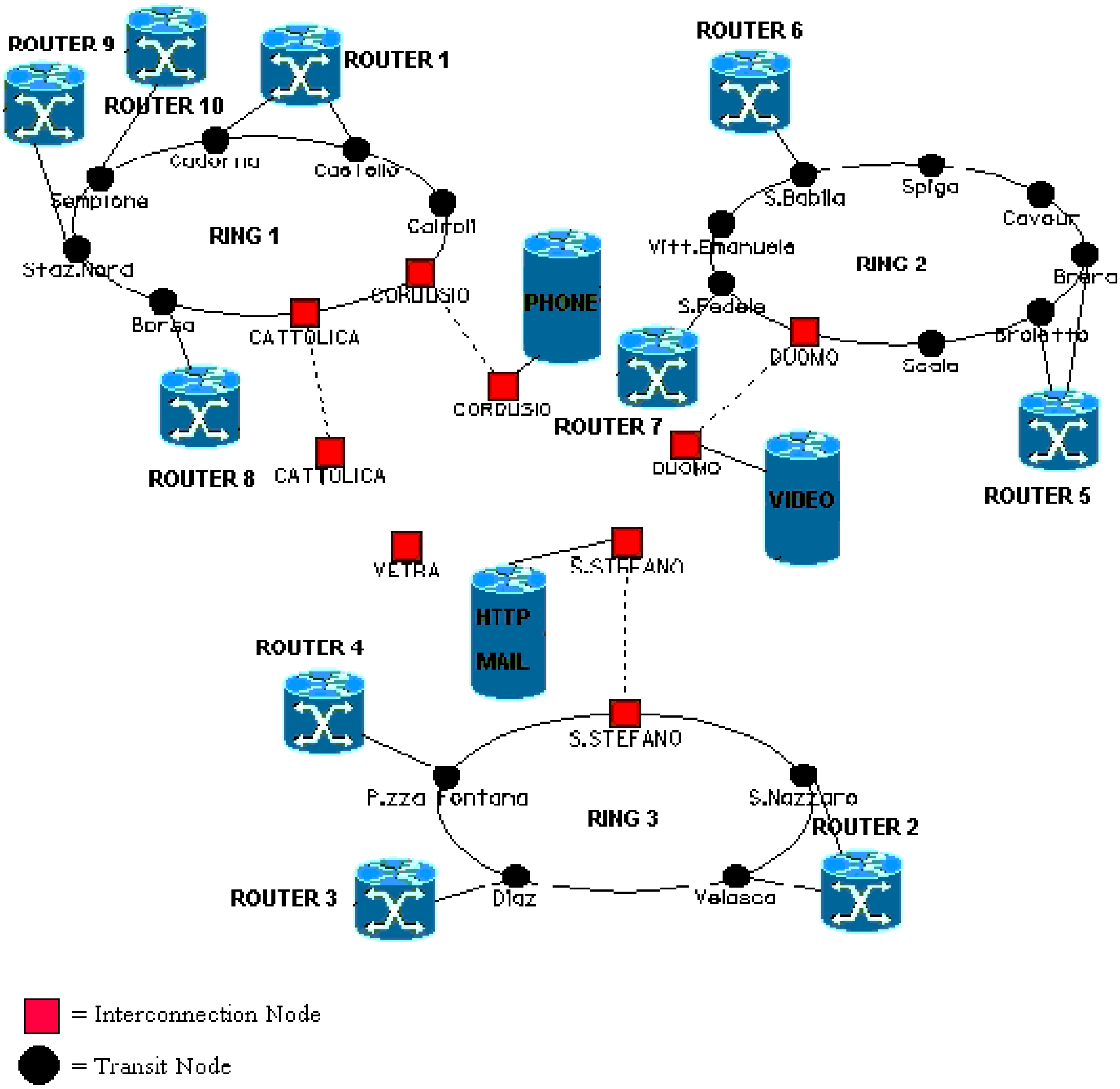


Figure 2-11: Scenario 3 – IP to transport level interconnections

Case study 1: IP over DPT/SRP

The SRP protocol is layer 1 (media) independent and can be used over a variety of underlying technologies such as SONET/SDH, WDM, dark fiber, or mixed environments [WP1-M1]. Since this solution pretends to eliminate the SDH equipment, we suggest interconnecting the IP/DPT routers directly to the fiber (dark fiber), and using conventional PoS/WDM equipment for the central ring to interconnect the servers, as shown in the Figure 2-12 below.

Traffic and service requirements are those described in Section 2.2.2 .

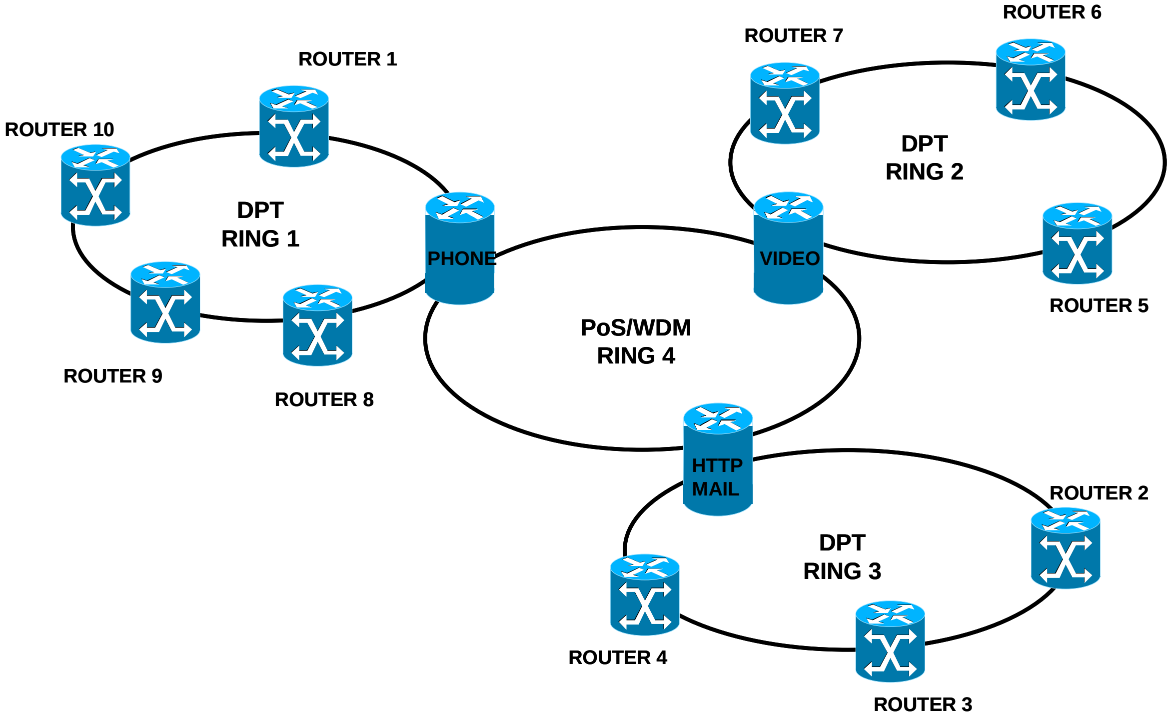


Figure 2-12: IP/DPT in the peripheral rings. PoS/WDM in the central ring

2.3 Long distance Context

A long distance IP optical backbone network example is now proposed. The purpose is to provide an alternative context to the metropolitan IP network previously proposed.

Just in order to give a geographical reference to the network we suppose that the network is deployed (or, better, to be deployed) on the Italian territory.

The proposed network could be a National backbone for both an incumbent or a newcomer operator. In any case the proposed network doesn't represent an actual or planned network and in particular It doesn't reflect the structure of the Telecom Italia IP backbone. That is true for both the transport/Physical network and the logical/IP layer.

The structure of this part of the document reproduces that one followed for the metropolitan context. Firstly, we introduce the network at IP layer, the services supposed to be transported on it with their characterization and relative parameters and architectural and networking implications. Then the transport network infrastructure (in other words the transmission node sites and the graph of available fibers) is described. The logical (IP) and physical (fibers) environments are shared by both the scenarios studies proposed: an IP over SDH over WDM reference network solution and an IP directly over WDM alternative.

Appendix LD_1 include traffic matrices, distances and list of fibres.

2.3.1 Network description

2.3.1.1 The Client network

The client network has fourteen Point of Presence (sites) in the major Italian cities.

The fourteen sites are:

Rome and Milan, international sites, connected towards the big Internet and other great Italian and European IP networks through peering agreement. International sites are connected with a big server farms for delivering web and video contents.

Two other principal National sites, Naples and Bologna with strategic function in content (web and video) delivering and for voice traffic exchanging. They are supposed connected to small video and web server farms and to voice gateway for exchanging voice traffic with other voice operators

Ten other national backbone PoP sites that collect IP traffic from regional access portions of the network.

Within international sites a couple of Multi-Gigabit Routers are installed, mainly for redundancy purposes. In the other sites we suppose that a single Multi-Gigabit Router is installed.

International links towards Big Internet starts from each Multi gigabit routers of the international sites. So there are in total four logical connections from the network to the Big Internet.

The four core sites are connected through a full mesh. In particular Naples is connected to both the routers of Rome (RM1 and RM2), to both the routers of Milan (MI1 and MI2) and to the router of Bologna too. The same is true for Bologna. Rome and Milan is connected together through a couple of link (MI1 is connected with RM1 and MI2 is connected with RM2, so two links join the two international sites). Within the PoP Multi Gigabit Routers, Server farms, voice gateway and call server exchange traffic through a high capacity VLAN (for example employing the Gigabit Ethernet switching technology). The other ten national sites are connected to the core in such a way the load in the two Gigarouter of the international site is more or less balanced. In particular Turin and Genoa is connected to MI1 and Bologna, Florence Venice and Trento is connected to MI2 and Bologna; Cagliari e Palermo is connected to RM1 and Naples, Bari and Pescara are connected to RM2 and Naples. This topology assures that the downloading of contents from a server (everyone it is located within the core) is always assured with at most two hops (logical/IP links) and even in presence of single failures (except when a failure occurs in the node where the request has been originated). In addition user-to-user traffic can be exchanged on the backbone with at most three hops even in presence of single failures of link or nodes (except when a failure occur in the one of the two termination node).

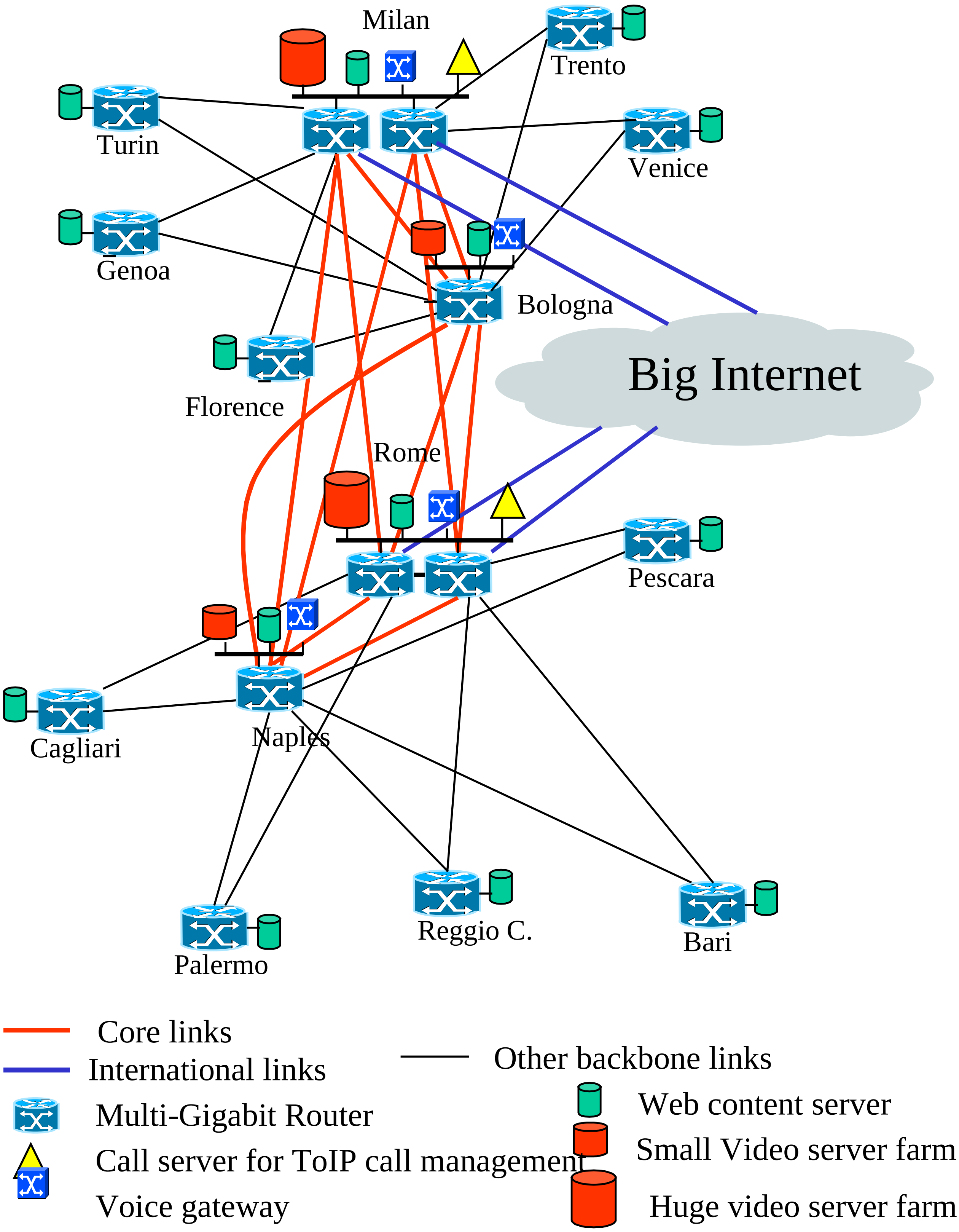


Figure 2-13: IP client network

2.3.1.2 The Transport network

Figure 2-14 depicts the Physical infrastructure in terms of available transmission sites and available fibers. Sites for transmission nodes (sites in which the fiber are terminated and where SDH and WDM equipment can be located) are assumed to be the same of the ones that hosts IP layer equipment. It is assumed that on each edge of the physical topology a couple of fibers is available.

In the [WP3_T2] document a proper table reports sites (air) distances and the list of the couple of fibers.

Figure 214: Transport network

2.3.2 Services description

2.3.2.1 Generalities

In the long distance Italian backbone the following representative services will be considered:

Web browsing

Telephony over IP (ToIP)

E-mail service

Video on Demand (or something like that)

Among that set of service Thelephony over IP and video o demand are Real Time services, Web browsing is a Near Real time service while E-mail is Best Effort.

2.3.2.2 Services requirements

Web browsing

The web content browsing service is assumed to be non-symmetrical. The ratio between the download and upload rate is approximately 10. The bit rate in downstream is supposed higher than today typical (residential) user profile. A high amount of traffic is downloaded from international links. A simple model that takes into account both the number of user supposed contemporarily active served by a PoP (a city) and the probability that the desired content is present in a server attached on a POP is used to derive the traffic matrix. All the PoP can be sites where web content can be retrieved but Rome and Milan are supposed to have significant higher requests because they are the most important Italian sites (from commercial and economical point of view) and in addition they are connected to the big internet for retrieving materials from the rest of the world. In Figure 2-13 the presence of web servers is represented by the green cylinders present in all the sites.

Appendix LD_1 include the traffic matrices for WEB traffic, separated for upload component (request messages and acknowledgements) and download component (packets flows carrying the contents).

The main parameters for the web service are the following one. Packet size and QoS service could be used for dimensioning network resources.

Service	Web browsing
Bit rate upstream (mean)	4.2 Kbit/s
Bit rate downstream (mean)	50 Kbit/s
Typology	Block transfer
Block size (downstream)	30297 bytes
Packet size (upstream)	82 bytes
Packet size (downstream)	710 bytes

QoS requirements	Maximum mean delay in transfering blocks (web page objects). Approximately 5 s

Table 2-7: Services requirements – Web browsing

Telephony over IP/ToIP

Thelephony is supposed symmetrical service with information packet flows directly exchanged between end users. (No intermediate server is supposed active for the packets including the voice samples belonging to the calls). Signalling traffic , exchanged between nodes in not considered

As the telephone traffic can be exchanged between a couple of users attached both to the IP network (more precisely, not directly to the backbone nodes but to the access portion of the network) or a user connected to the IP network and a user connected to an external telephone network (fixed or mobile) two kind of traffic are considered.

We will refer to them as IN-NET and OUT-NET components. From the total traffic exchanged by the customers attached to the backbone the OUT-NET and IN-Net components are calculated considering that a fixed percentage of the whole traffic is OUT-NET traffic (40%).

The IN-NET component, exchanged between IP users give origin to a complete matrix (14×14) that represent the native inter-POP ToIP traffic.

Traffic matrix for IN-NET component is derived taking into account distances between the nodes ()

The OUT-NET component give origin to a matrix between the 14 sites and the four nodes in which a voice gateway is located.

For each backbone node a fixed percentage of OUT-NET traffic is assumed exchanged with its two reference Voice gateways: the principal Voice Gateway (60%, Milan for the North and Rome for the South) and the secondary Voice Gateway (40%, Bologna for the North and Naples for the South).

Service	**ToIP**
Bit rate bi-directional	18 Kbit/s
Typology	streaming
Packet size	816 bytes
QoS requirements	Maximum mean delay in transfering packets: Approximately 50 ms

Table 2-8: Services requirements – ToIP

Video on Demand service

Video on Demand is modeled as uni-directional service. The download flow is supposed to be a constant bit rate stream with stringent delay requirements while the bandwidth upstream carrying the signalling packets are supposed to be negligible.

As introduced in the description of the IP layer of the network four main sites are connected to server farms containing video programs. The most requested items are supposed mirrored in the fourth sites but there are also a quota of the programs that have to be downloaded necessarily from a specific server.

The model to derive the traffic matrix is simple. It takes into account the number of simultaneous flows that the users attached to a given node are downloading and assumes that a certain percentage of those flows deriving from the four national video server sites. In particular a 60% of the flows is derived from the nearest big server (Rome o Milan), the 20 % from the other big server site (Milan or Rome) and 15% are got from the nearest small server site (Naples or Bologna) and 5% from the other small server site (Bologna or Naples).

Following is a table collecting all the information regarding the requirements of the service.

Service	**VoD**
Bit rate downstream	4 Mbit/s
Bit rate upstream	0 Mbit/s
Typology	streaming
Packet size	816 bytes
QoS requirements	Maximum mean delay in transferring packets equivalent to play-out buffer capacity Approximately 200 ms

Table 2-9: Services requirements – Video on Demand

E-mail service

The E-mail service models the traffic exchanged among E-mail server that are assumed to be present in every POP of the network depicted in Figure 2-13. External E-mail servers are also assumed to be present in the Big Internet and exchanging traffic with the E-mail servers within the considered network. The percentage of traffic received from external servers set to 20%.

The service is clearly block transfer and is assumed to be uni-directional without any backward acknowledge.

The E-mail service is a pure best-effort service and has not any QoS requirement; however some amount of bandwidth is to be provisioned in order to avoid network congestion.

The following table summarizes the service characteristics.

Service	**E-mail**
Typology	block transfer uni-directional

Block size	11670 bytes
Packet size	816 bytes
QoS requirements	No requirement (the message is assumed to be delivered within 1 hour)

Table 2-10: Services requirements – E-mail

The construction of the traffic matrix for this service starts from the assumption of a generic amount of messages received daily by each POP. These assumptions are reported in a table in the [WP3_T2] document.

2.3.2.3 Customer use assumptions.

As the set of services delivered through the network include a sort of video on demand service, a number of video server farms is supposed being active and connected with the four main sites: Milan, Rome, Bologna and Naples. It is supposed that a certain amount of the contents stored and available on a server is mirrored and available also on the other servers. So a user usually downloads its preferred entertainment item from the nearest Video server. But it is also assumed that each video server farm located on one of the principal site has its own specific and not mirrored stuff. So everywhere the user is located, he necessarily must get from a given PoP when it would like to access to some particular programs.

IP telephony (ToIP-Telephony over IP) is managed through a couple of call servers located in Rome and Milan. Each principal backbone site (Milan, Rome, Bologna and Naples) has a Vocal gateway for OUT-NET voice traffic (the traffic exchanged between the backbone network and the other voice operators). Call servers handle signalling messages only, including the signalling dialogue with other operators (both traditional TDM/SS#7 and IP-centric operators). Packet streams of IN-NET voice traffic are directly exchanged among the users connected to the network while packet streams of OUT-NET voice traffic are terminated on voice gateways.

The Web traffic is exchanged between all the backbone sites, especially the four principal ones, but a significant component is supposed exchanged with the Big Internet (downloaded at most) through international links. The same scheme is applicable for E-mail traffic.

2.3.2.4 IP traffic flows estimations

See Appendix LD1

2.3.3 Scenarios and case studies.

2.3.3.1 Scenario 1: IP over SDH over WDM

Architectural aspects

Three network layer are present in Scenario 1.

IP is present with its proper functionalities.

In both the case studies concerning the scenario 1 presented below the SDH networking capabilities are implemented through ADMs and the network structure is a “two level” interconnected rings. High reliable “double homing” interconnection between rings is used for joining the peripheral ring (South and North ring) to the core ring.

Depending on the specific case study and within each of them WDM is present in Scenario 1 in different portion of the network in terms of:

point-to-poit systems (WDM Line Terminal-LT)

ring of OADMs

set of OXCs connected together by a meshed topology

Resilience aspects

As IP level as concern standard recovery mechanisms run according specific routing protocol employed (OSPF, IS-IS, BGP). MPLS is a possible option to improve resilience performances. It makes also possible traffic engineering capabilities at the client layer (layer 3).

As architecture for the SDH layer is interconnected rings (and equipment are ADMs) the SDH layer can rely on its proper protection mechanisms.

WDM layer adopt ring protection on the portion implemented with ADM rings and protection and/or restoration in case of meshed OXCs.

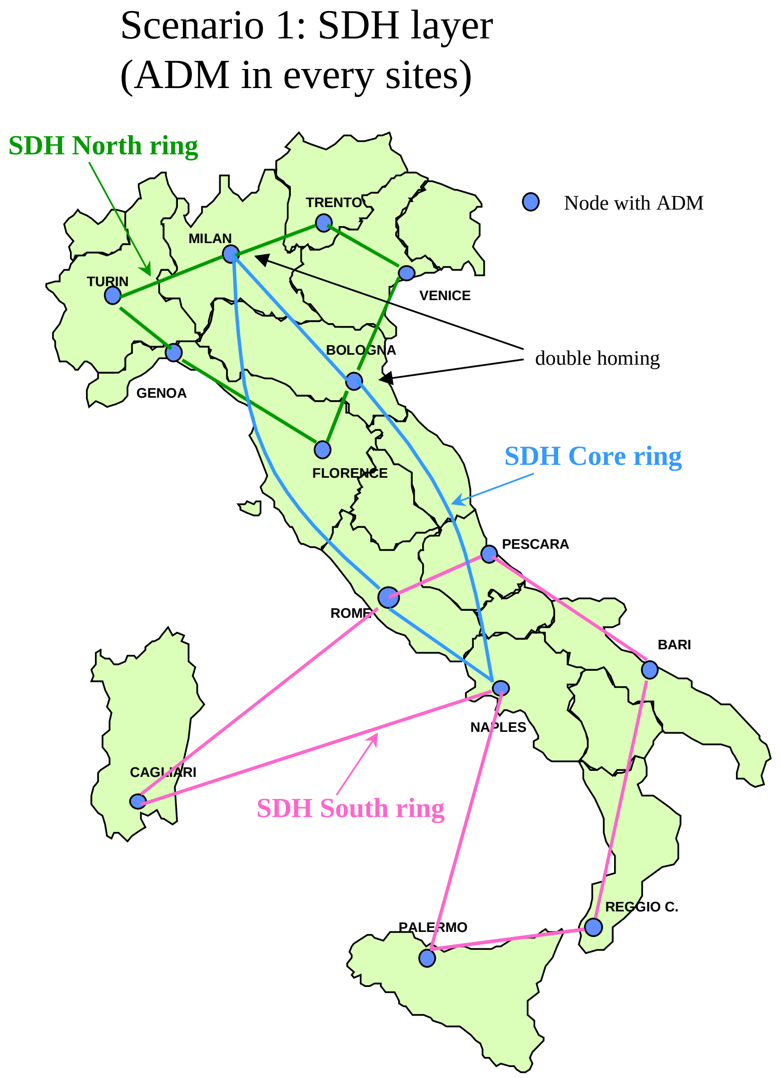


Figure 2-15 [long haul context, scenario 1, SDH network] : the SDH layer for Scenario 1

2.3.3.1.1 Case studies

Two case studies have been defined for scenario 1. Both case studies have the same SDH network structure. The structure is depicted in Figure 2-15 [long haul context, scenario 1, SDH network].

Case study 1

Case study 1 of Scenario 1 present at OTN layer the structure depicted in Figure 2-16 [long haul context, scenario 1, case study1 OTN network]. The network is structured on two levels and the configuration of the rings is the same as the one defined for the SDH layer. On peripheral rings WDM LT are present while in the core ring ADM allows optical networking.

Scenario 1/Case study 1: OTN layer

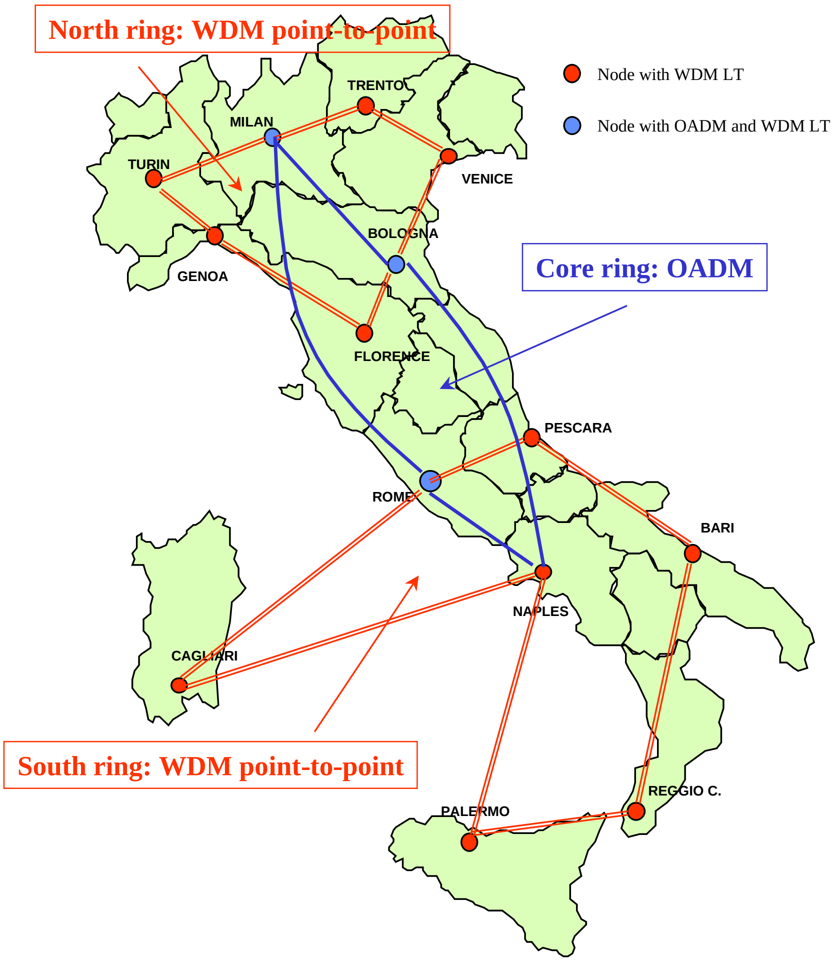


Figure 2-16: [long haul context, scenario 1, case study 1 OTN network]: the OTN layer for Case study 1 of Scenario 1

Case study 2

Case study 2 of Scenario 1 present at OTN layer the structure depicted in Figure 2-17 [long haul context, scenario 1, case study 2 OTN network]. The optical transport network is structured on two levels: two peripheral rings similar to the one defined for the SDH layer (North and South ring) and a full mesh interconnecting the four nodes belonging to the core. Sites that belong only to Peripheral rings hosts OADM while core sites that take part of both peripheral rings and central mesh have ADMs as well as OXCs.

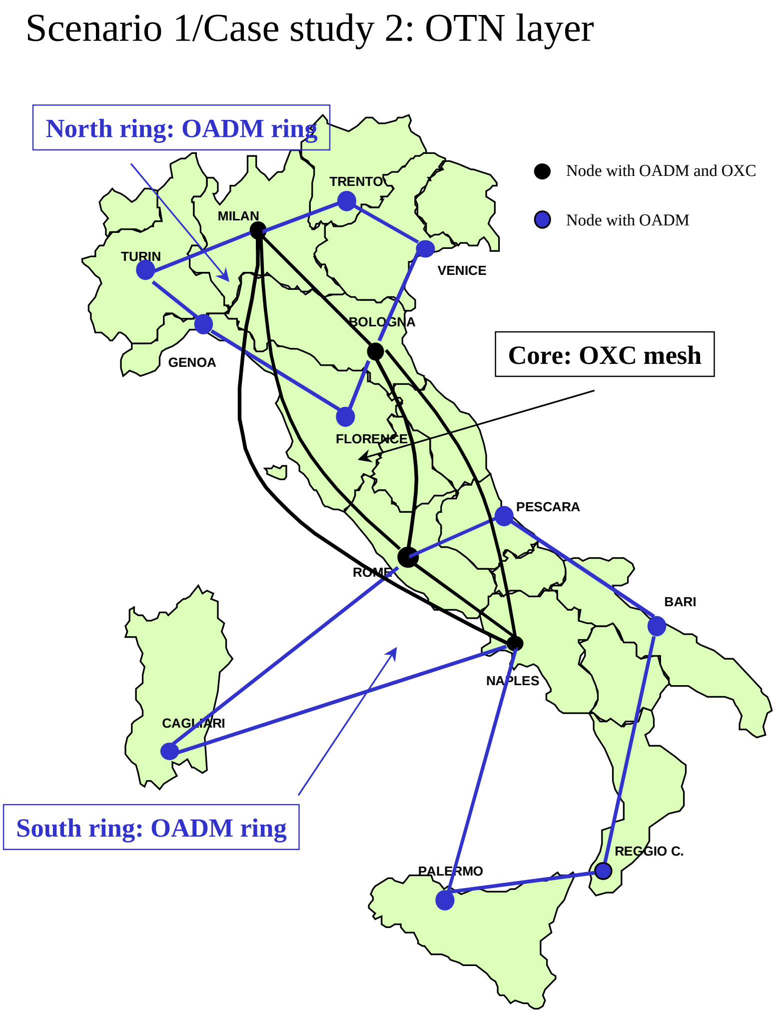


Figure 2-17 [long haul context, Scenario 1, case study 2 OTN network]: the OTN layer for Case study 2 of Scenario 1

2.3.3.2 Scenario 2: IP over WDM

Architectural aspects

Scenario 2 IP is directly mapped on OTN without an intermediate SDH layer and use the full capabilities in switching wavelength (i. e. optical switches or OXC).

POS only for framing (not SDH networking as SDH stratum is not present) purpose is the most suitable candidate for the mapping of the IP layer on OTN: Each STMx (x=64, for instance) flow interconnecting a couple of links could directly mapped through digital wrapper in a wavelength and transported across the OTN.

Resilience aspects

As in the previous scenario IP level can rely on classical (and slow) layer 3 recovery mechanisms. In addition MPLS (LS at electrical level) is still a possible option to improve resilience performances and to make possible traffic engineering capabilities at the client layer.

Traditional protection and/or restoration techniques is possible in case of meshed OXC as this architecture is the one we are considering in Scenario 2. MPλS is another opportunity to handle the traffic flows in the network. It makes possible resilience strategies similar to that defined in electrical LS and it allows an separate transportation of traffic flow in the two directions between a couple of nodes and this potentially implies a more efficient use of the physical resources.

An important difference between O-MPLS (thus MPλS) and E-MPLS is that O-MPLS uses dedicated protection while E-MPLS uses shared protection

2.3.3.2.1 Case studies

Case study 1

Case study 1 of Scenario 2 present at OTN layer the structure depicted in Figure 2-18 [long haul context, Scenario 2, case study 1 OTN network]. The network is "flat" and all the sites have optical switches (compact optical switches or full OXCs, with the possibility to introduce MPλS capabilities). The topology of the network interconnections between optical switches derive directly from the fiber deployement (i. e. the legacy network).

Figure 2-18: [long haul context, Scenario 2, Case study 1, OTN network]: the OTN layer for Case study 1 of Scenario 2

3 Overview on available planning and simulation tools

This section collects information about planning and simulation tools available to the project team. Information was collected by means of charts, which the partners filled in with details concerning the tools at their disposal.

As regards the planning tools, all the participants contributed to the identification of software programs that can cover planning issues about the IP/MPLS, SDH and WDM technologies/layers.

The information provided on the characteristics/ functionalities of the planning tools (IMEC, SIRTI and CSELT) is quite detailed. It must however be stressed that the planning tools are able to handle one network layer at a time; so far we have been unable to identify any multi-layer tools. It follows that when we have to use the tools in order to plan / dimension a case study network we will have to use the tools separately, one by one, from the higher to the lower layer and not simultaneously in an integrated way, as it would be possible with a multi-layer tool.

In addition, when we use the tools it is a very hard task –or an impossible task- to take issues like multi-layer resilience strategies into consideration. This aspect should be taken into account in the other tasks of the WP3.

A couple of partners (UPC and IMEC) contributed with the description of simulators that cover IP network layer and DPT technology (SRP-fa Protocol). Although these simulators cannot directly support a network planning process they can be used to derive dimensioning criteria for network elements or –alternatively- to evaluate the performance of a roughly designed network.

The following Figure 3-1 shows the relationships between the tools described in this document and the protocol stack assumed as a reference in the LION project.

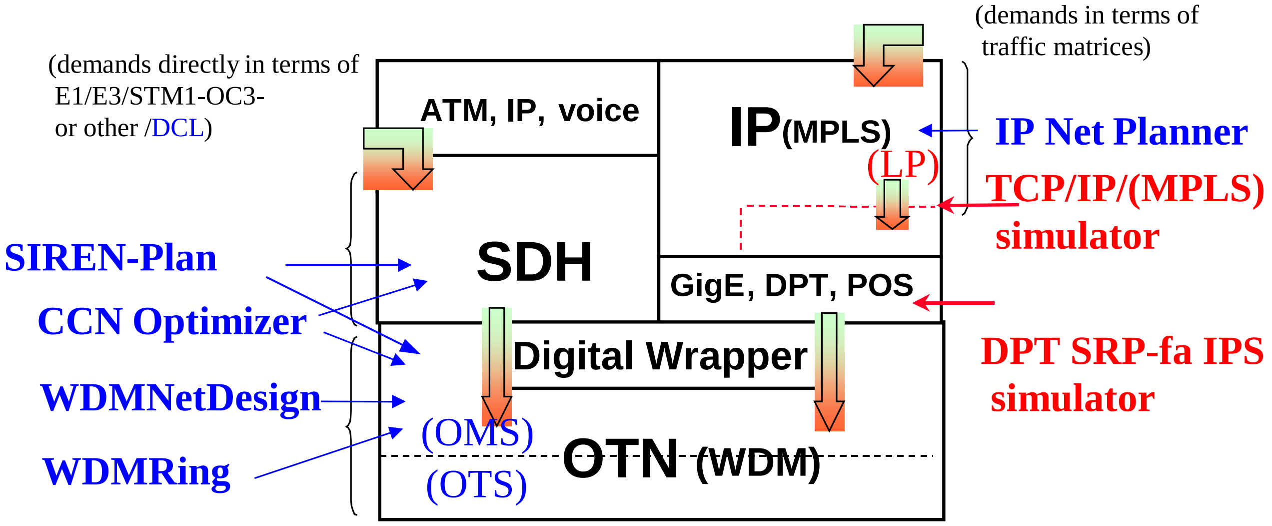


Figure 3-1: The protocol stack and the available planning and simulation tools

This collection of contributions also includes a strategic planning tool called OPTIMUM (proposed by AGH). This tool is not a planning tool like the tools that we mentioned above, which are tools based on dimensioning and optimization criteria and whose purpose is the technical design of the network.

OPTIMUM is a tool that enables its users to evaluate economic features such as investments, revenues, life cycle costs, cash balance and so on connected with the construction and running of the network in a given period.

Even though the tool achieves a rough dimensioning of the network it doesn't perform a detailed project of the network and in particular it doesn't take into account factors like architectural details, resilience or grade of service. In addition, the tool carries out evaluation on the access portion of the network while transport on the backbone is disregarded.

This is the reason why OPTIMUM doesn't seem to be workable at present within our project, but in the future it could be used to carry out case studies focused on economic evaluation of network solutions.

In addition some partners declared that new computer programs or upgrades of existing tools (both for network planning and simulation) is under development or planned for the near future. For example NTUA is thinking about the development of a network simulator for evaluating network performances in terms of robustness/recovery against failures. IMEC is refining its computer programs for planning and dimensioning robust MPLS/MPλS networks. UPC is completing its DPT simulator (to add the IPS part). CSELT is also thinking about the introduction of resilience strategies in IP planner. So we shouldn't consider the work connected to collect information about planning and simulation tool finished and all the partner are encouraged to circulate information about new functionalities of existing tools or new computer programs when they will be reach a stable version and they could be employed in WP3 activities.

3.1 Planning tools

Available planning tools cover the following network layers:

IP

SDH (only rings)

OTN (both meshes and rings)

Other layers, and in particular layer 2 or 2/3 implemented in Router-Switches like DPT or MPLS are not covered by any planning tool declared available within the consortium.
So, when the WP3 participants will decide about which scenarios have to be analyzed through numerical techno-economic case studies, the ways to perform the case studies have to be discussed. In particular it will be necessary to decide about the need to develop some custom "informal tools" (through spreadsheets for example) or develop/adapt new functionalities on existing tools to cover the planning and dimensioning issues for layer 2 or 2/3 (OSI).

3.1.1 IP layer

The tool available for optimising and dimensioning the IP layer is IP-planner.

The **assets** of the tool are the following.

IP Nertworks Planner allows a full topology capacity and flow assignment in an IP network. The tool allows us to derive an optimal minimum cost IP network topology when the packet traffic matrix, the mean network delay requirement and the cost parameters of transport services (which are modeled as "generic" transportation service) are given.

The tool assumes the OSPF algorithm as a principle to route the traffic flows on the network. As a secondary output of the algorithm the weight of the links in the OSPF topology is provided by the tool.

The principal **weaknesses** of the tool are the following:

no possibility to differentiate the traffic into classes of services (for instance, Diffserv offer a kind of CoS inIP networks). This happens because IP Net planner implements a model for which all the packets are routed, queued and forwarded with the same policy rule.

no possibilty to make a robust project: the optimal network structure doesn't take into account any diversity criterion to face with link or node failures. So it is not possible to carry out a project taking into account resilience requirements.

no possibility to take into account special kinds of traffic management (MPLS) or level 2 transportation (DPT)

no possibility to take into account equipment costs: only transportation costs are modeled

only dimensioning starting from a green-field context

So, the tool is good to perform a dimensioning of the resources requested by IP level only when the protection relies on the lower layers of the network.

3.1.2 MPLS/DPT/GbEthernet/POS

Up to now there aren't any tools available for planning/dimensioning DPT or GbEthernet network functionalities while there are some computer programs (not planning tools but prototypes) for planning and dimensioning network that use MPLS/MPλS techniques available in IMEC.

In fact , these functionalities should be modeled and handled, for planning/dimensioning/simulating purposes, in a proper way when they are present in the IP over OTN layer stack.

For instance, if MPLS is the technique used to make traffic engineering on the network, a proper tool for planning and dimensioning the network should take into account the mechanism for routing and managing the traffic flows typical of MPLS technology and, for example, the presence of given resilience strategies to protect the Label Paths. This is what it is implemented in the research programs under refinement in IMEC.

GbEthernet should be employed in two options: only framing or full switching.

In the former case IP flows are framed into GbEthernet frame and use only point-to-point connection between GbE interface cards installed on the routers. In this case no specific tool is required and the implications on the project involve only the overhead of GbEthernet framing and the cost.

In the latter case a full layer 2 infrastructure, that uses layer 2 switches, is used to interconnect the network.

POS could require a point-to-point SDH flows that can either use or not an SDH infrastructure as a in-between layer between IP and OTN. Also in this case an infrastructure (SDH) can be present or not depending on the scenario considered.

3.1.3 SDH layer

SIREN-Plan

A tool for planning and dimensioning SDH infrastructure called SIREN-Plan is currently produced by SIRTI.

The principal **asset** of the tool is that SIREN-Plan produces a very detailed project of a transmission SDH network. In fact it is a tool oriented to Operators (it is not a research tool). In particular the tool gives as outputs the configurations of each piece of equipment and the details of the routing of the single flows. SIREN-Plan allows accurate cost comparisons among different dimensioning scenarios.

A WDM infrastructure under SDH is also modelled as point-to-point systems in order to economically compare alternative projects in which new fibres are supposed to be deployed or WDM system is introduced in order to multiply the transportation capacity of existing fibres.

In addition functionality for grooming lower order flows is offered. A number of protection strategy, associated to single flows, is also allowed and routing strategies can be chosen from a set by the user.

The SIREN-Plan is not a tool that optimises the network topology, infact the structure of each ring, the points of the interconnections between rings and other architectural details have to be assigned from the user.

The SIREN-Plan is a dimensioning tool that produces economic evaluation of the networks very accurated and probably too accurate in a context like WP3 of LION, in which techno-economic evaluation should be done on general case study, and not on detailed project of a real network.

CCN Optimiser

CCN Otimiser is a computer program for ATM, SDH and WDM network optimisation available in CSELT. It is not focused on a particular technology and it is a designed to optimise the topology and sizing the link groups of a generic cross connected meshed network (Network which is supposed to use Deterministic Multiplexing).

Only two network layers are considered by the program: a generic client layer which relies on a generic server layer.

CCN Optimiser requires a definition of the cross connecting nodes, the definition of the demands for permanent connections (circuits of the client layer, each one characterised by source, destination, bandwidth, directionality, maximum hops permitted along its path), the cost of transport services offered by the server layer.

On the basis of these inputs, CCN Optimiser provides

the optimal topology of the network (set of topology edges)

the number of links required on each edge

the optimal path for each circuit

the minimum cost of the network

The principal **weakness** of the algorithm implemented in CCN optimiser is the fact that the optimisation process doesn't take into account any resilience strategy; so the resources allocated by the algorithm are enough only for routing the whole traffic over the network without any chance of recovery in case of failure.

3.1.4 OTN

A complete set of planning tools for planning and dimensioning OTN is provided by IMEC.

With WDM_NetDesign and WDMRing (see APENDIXES D and E) both meshed and ring OTN networks can be optimised and dimensioned.

WDMNet Design

WDMNet Design is a planning tool that allows to perform the planning and dimensioning of a multy-layer network:a digital client layer (DCL), an optical channel layer (OCh), and a Physical layer (OMS and OTS).

At DCL demands are expressed as a list of STM1/OC3 to be transported (demands are also entered at DCL in Mbit/s). At OCh layer demands are expressed in number of optical channel (2.5 or 10 Gbit/s) or also in raw bandwidth (Gbit/s).

Physical topology is assigned and the dimensioning algorithm can work either with or without an optimization algorithm that tries to minimize (reduce) the network installation cost by changing some OCh routes that imply an inefficient use of the network. The tool outputs the topology, the routing of the demands (both working and protection) and costs.

Assets:

many kinds of protection and routing strategies are available

detailed model for equipment

for both green field and existent networks (during optimization step, already existent facilities and demands are not changed)

accurate model of cost components

Weaknesses:

no optimization strategy in mapping DCL level on OCh level (DCL traffic routing require that OChs has already been set up)

no assurance that diverse routes for protected DCL demands are physically disjoint.

WDMRing

WDM Ring is a planning tool that allows to perform the planning and dimensioning of a two layer network: a client layer (OCh) and a server layer (OMS and OTS). Demands are expressed as a list of optical channel transported over the network. The physical topology in terms of the meshed structure of the fiber/cable mesh is assigned. The tool selects the optimal rings to route the Optical Channel demands. Channels are supposed to carry STM-16 SDH flows.

Assets:

full optimization tool for ring OTN (on the basis of both the physical topology and the Och demands WDM Ring build up the structure of the network in terms of configuration and dimensioning of the rings following an optimization criterion that minimizes the overall cost of the network)

many kinds of protection and routing strategies are available

for both green field and existent networks

cost model: taking into account fiber and equipment costs, the cost of some summarized network components are evaluated (single specific ring cost, cost for routing a specific wavelength on a specific ring, cost for transiting a wavelength between two rings). This can be very useful in techno-economic evaluations and comparisons.

Weaknesses:

the matrix of optical channels to be transported must be symmetric and channels are suppose carrying STM-16 flows

wavelength conversion is allowed only when a channel transiting between two rings

3.2 Simulation environments and simulation models

Available simulation models deal with two aspects:

IP based network, in particular available models allows to analyze the behavior and the performance of TCP and OSPF protocols;

DPT evaluation, and in particular simulator for SRP-fa and IPS protocols/algorithms;

The two models rely on two general purpose simulation environments OPNET and NS respectively. A detailed description of the main characteristics of NS and OPNET is given in the first part of appendixes F and G respectively of the [WP3_M1] document.

3.2.1 IP based network simulator

The IP-based networks simulation models developed with the support of NS and available in IMEC concern the following two aspects of IP networks:

The study of the influence of recovery time on TCP flows

The analysis of the time it takes OSPF to recover from link failure.

In general models developed with the support of NS, as they can employ a fairly detailed traffic model, could be used to validate numbers used as parameters for more high-level simulations or planning algorithms. Such parameters values (throughput for instance) may be used as input for capacity planning algorithms.

In order to consider the use in planning context the first model could be used in order to find out whether fast protection is really necessary in networks carrying TCP/IP traffic, while the second for evaluating link recovery times when OSPF is running on a IP-based network.

3.2.2 DPT simulator

The DPT simulator owned by UPC was mainly developed for evaluating the performance of the SRP fairness algorithm (SRP-fa).

Basically, the SRP-fa controls the access to the shared media ensuring fairness, bounding latency and avoiding privileged nodes or conditions while undertaking to prevent congestion.

The current version of DPT simulator allows to verify some DPT features such as bandwidth efficiency, fairness among the different nodes of the ring, support for priority traffic, etc.

For network planning purposes simulation results that can be obtained with the SRP-fa algorithm simulation model could be useful for supporting the following activities:

evaluation of the maximum number of nodes of a ring when the traffic generated by a node is known. In fact, if we assume that each node forming part of a DPT ring connected through a given type of transmission system offers a certain amount of traffic, the higher is the number of nodes that constitute a ring the less is the traffic that could be offered by a node. This is true when a certain level of service is imposed.

evaluation of the maximum traffic that could be generated by each router that forms part of a DPT ring when the number of nodes of the ring is fixed, the transmission interconnecting system is assigned and the traffic is supposed (for instance, but not necessarily) equally directed to the other routers of the ring.

a-posteriori evaluation of the performance of a given DPT network (traffic, number of nodes, transmission systems are supposed assigned) in order to validate a network structure obtained without any other design supports or with low-accurate planning tools. Following that approach refinements and changes of the project are then possible.

The other simulator concerning DPT technology (not yet available but under development at UPC) is designed to perform studies on the time IPS takes to recover from link and node failures, and the impact of the failures on the packet loss rate.

IPS provides the ability of SRP ring to recover from events and faults as fibre cuts or node failures. IPS is able to monitor and handles events at layers 1, 2 and 3 instead of just layer 1 events monitored and recovered by SONET/SDH protection.

This kind of simulator could be employed in a planning context too, for instance in order to evaluate in a DPT network the recovery performance and , eventually, the opportunity of an additional protection mechanism at the lower layer (SDH transmission layer using its own protection, for instance).

3.3 A tool for strategic planning

OPTIMUM is a tool that enables its users to evaluate economic features such as investments, revenues, life cycle costs, cash balance and so on connected with the construction and running of the network in a given period.

In short, the main **strength** of the tool seems to be the accurate financial analysis of the project, performed through a set of parameters like cash balance, net present value (NPV), internal rate of return and life cycle cost. The **weaknesses** are that the tool uses a very generic (it is not devoted to IP network) and not very accurate model for the network and that the portion of network considered for the investments is the access portion and not the backbone, which is the interesting aspect of our investigation.

4 Preliminary results

In Section 3 an overwiew on available tools was presented. A subset of the tools identyfied are used in this Section 4 in order to carry out the planning of some of the case studies as they were identified in Section 2.

This Section 4 contains the preliminary results obtained by the planning of particular case studies. It also describes which assumptions are made in order to set up the single-module planning procedures and which adaptations are made among adjacent layers planning modules.

4.1 Preliminary results from the Metropolitan Scenario 1/ case study 1

In this subsection results of the planning process carried out on the case study 1 of the scenario 1, belonging to the metropolitan context, are presented.

The aim of the planning experiment is to give a concrete example of network planning of an IP over transport network using the available tools as they are available at the present stage of the project. The experiment uses separate planning tools for a layer by layer planning approach . Planning strategy is de-coupled between the involved layers, being resilience and recovery issues independently defined at each layer.

Within WP3 we could consider this experiment as a starting point for further work and developments towards an integrated approach that takes into account resilience and recovery issues, that are important objectives and expected results in the mid term of WP3 activities.

The metropolitan case study 1 of scenario 1 is presented in the subsection 2.2.3.1.1.

Scenario 1 is a hypothetical IP metropolitan backbone network located in Milan, which is supposed carrying a number of representative services (Web based and classical e-mail as well as video streaming services and IP telephony). The reference architecture is IP over SDH over OTN.

Distances between network sites are relatively short while traffic matrices at IP level present great differences between their entries. So if the whole traffic matrix is considered (the total traffic matrix in terms of bandwidth exchanged between the routers) a factor of about 10000 is shown between the greatest and the lowest traffic demands. The reason is the presence in the metro network of few nodes that have a function of content server (in particular video server) and by the fact that only a restricted set of nodes retrieve from the servers the flows belonging to the greedy bandwidth services. Other routers exchange IP classical traffic and voice over IP traffic that requires not so graet amount of bandwidth.

In Section 2.2.1 a configuration of the topology at the IP level is depicted. As the IP planning tool at our disposal (IP-planner) allows us to optimise (i. e. minimize the cost of the network) without any constraint on the grade of robustness of the network, we perform the design of the IP layer without taking into account any restrictions regarding the connectivity of the network as well as any kind of resilience strategy. So the logical topology at IP level has been freely found by the planning tool.

The transport network is structured on 6 rings: 5 peripheral plus one central ring. The detail about the topology of the transmission network is given in Section 2.2.1. WDM point-to-point system are employed only in the central ring while in the peripheral ring only traditional line system is employed. Assumption on types of systems and other details on technological solutions employed for planning the transport network are presented in Section 4.1.3. For planning the transport network the topology is supposed fixed (in other words the configuration of the rings is supposed assigned and then no optimisation on the network structure is pursued) while the dimensioning of the network (type and quantities of apparatus on each sites and needs of fibers between sites) has been performed by the tool SIREN-Plan.

The planning process followed the scheme described below.

First the traffic matrices of different services as defined in scenario description are processed in order to derive a unique traffic matrix in terms of packets per seconds. The mean length and the variance of the packet length are also computed on the basis of the statistics of the single services. That unique matrix is used to dimension the IP network in terms of links necessary between routers. Outputs of the IP dimensioning are given in terms of SDH flows.

Secondly the outputs of IP planner in terms of STM1 flows are used as input for the SDH and WDM planning tool in order to perform the dimensioning of the rings of the network. Outputs are type and number of apparatus on each site of the network (both for SDH networking and WDM point-to-point systems) and the number of fibres required on each edge of the topology.

4.1.1 Metropolitan IP network planning results

IP layer planning has been performed by the dimensioning program IP-planner based on Kleynrock approach [A1] and using MG1 queuing to model the link. The IP-planner is described in section 3.1.1 .

In short the IP planner program requires as inputs.

- the traffic matrix in packets per seconds
- statistical parameters of packet length (the first two moments, mean and variance)
- the distance matrix (logical or physical) between nodes (this matrix defines also the reference starting topology)
- the set of available type of links that can be employed for interconnecting the nodes
- the cost model structure parameters (the cost of a link between a given couple of nodes depends on the distance and the type of link)
- the quality of service requirement, in terms of maximum mean end-to-end packet delay

The outputs are:

- the resulting topology (that could be less connected than the starting one) and the number of links of each type between the nodes
- traffic flow, delay and link utilization on each edge of the resulting topology
- the routing plan and the mean packet delay between each couple of nodes

In the following it is explained how the data describing the scenario 1 has been adapted to the IP planner input format.

Traffic Matrix

In order to derive the traffic matrix for dimensioning the IP layer we have proceeded as follows.

The whole traffic matrix in terms of Mbit/s has been derived as a sum of the matrices associated to the six services (web user to server and web user to user, e-mail, Telephone over IP, Video HL e LQ). Then the mean packet length at network level has been computed using the following simple weighting formula

$$\bar{l} = \frac{\sum_k \Lambda_k l_k}{\sum_k \Lambda_k} \qquad (4.1)$$

Where Λ_k is the total amount of traffic at network level of service k in packet per second and l_k is the mean packet length of service k.

The variance of packet length is evaluated taking into account that services as Video and Voice stream have a constant packet length (in other words their length is deterministic, which implies that variance of their distribution is equal to zero) while web browsing or e-mail service have non-deterministic packet length. In lack of more detailed information statistical packet length has been assumed poissonian (i. e. the mean equals standard deviation). The variance of packet length is calculated as the mean of the square packet length minus the square of the mean packet length:

$$\sigma^2 = \overline{l^2} - \bar{l}^2 = \frac{\sum_k \Lambda_k l_k^2}{\sum_k \Lambda_k} - \bar{l}^2 \qquad (4.2)$$

For services with fixed packet length (deterministic) $\overline{l^2} = \bar{l}^2$ while for other services that shows poissonian distribution $\overline{l^2} = 2 \cdot \bar{l}^2$.

The resulting value of packet length is 8402 bit (1050 bytes approximately) and the resulting variance is 25.2 10^6 bit^2.

The packet matrix has been derived dividing each element of the whole bandwidth matrix by the mean packet length.

In the table 4-1 [packet traffic] the traffic matrix in packet per second is the following one .

Table 4-1 [packet traffic]: traffic matrix in packet per second for the Metro context

	R1	R2	R3	R4	R5	R6	R7	R8	R9	R10	S1	S2	S3
R1	0.00E+00	4.50E+03	1.83E+03	1.51E+04	6.33E+03	1.43E+04	5.90E+03	1.50E+02	1.43E+04	7.00E+03	1.39E+04	0.00E+00	0.00E+00
R2	7.87E+03	0.00E+00	8.25E+02	5.09E+03	2.92E+02	3.89E+03	2.12E+03	5.00E+02	2.27E+03	1.30E+03	6.93E+03	0.00E+00	0.00E+00
R3	5.13E+03	3.30E+03	0.00E+00	4.20E+03	7.65E+03	0.00E+00	4.23E+03	5.00E+01	1.73E+03	6.33E+03	4.62E+03	8.93E+03	0.00E+00
R4	1.15E+04	4.72E+03	2.40E+03	0.00E+00	4.50E+03	1.22E+04	1.09E+04	6.66E+01	1.09E+04	1.33E+03	9.24E+03	0.00E+00	0.00E+00
R5	1.05E+04	2.77E+02	5.22E+03	5.40E+03	0.00E+00	9.18E+03	3.68E+03	1.33E+02	4.03E+02	3.27E+03	7.39E+03	0.00E+00	0.00E+00
R6	4.62E+03	2.62E+03	0.00E+00	4.93E+03	2.77E+03	0.00E+00	3.00E+03	8.33E+02	4.15E+03	3.33E+03	9.24E+03	9.52E+03	0.00E+00
R7	9.50E+03	1.45E+03	2.73E+03	1.03E+04	3.80E+03	3.60E+03	0.00E+00	1.67E+02	8.33E+02	3.33E+03	9.24E+03	0.00E+00	0.00E+00
R8	1.50E+03	5.00E+03	5.00E+02	6.66E+02	1.33E+03	8.33E+03	1.67E+03	0.00E+00	1.28E+03	0.00E+00	0.00E+00	0.00E+00	0.00E+00
R9	6.71E+03	4.19E+03	2.32E+03	7.91E+03	5.68E+02	4.79E+03	1.40E+03	1.28E+02	0.00E+00	3.85E+03	3.23E+03	7.08E+04	0.00E+00
R10	1.06E+04	1.12E+03	3.93E+03	1.45E+03	2.97E+03	3.63E+03	3.63E+03	0.00E+00	4.16E+03	0.00E+00	8.32E+03	1.61E+04	0.00E+00
S1	5.37E+04	2.87E+04	2.20E+04	3.80E+04	3.78E+04	3.54E+04	4.01E+04	0.00E+00	1.78E+04	3.41E+04	0.00E+00	0.00E+00	0.00E+00
S2	0.00E+00	0.00E+00	8.93E+05	0.00E+00	0.00E+00	1.90E+06	0.00E+00	0.00E+00	2.29E+06	1.61E+06	0.00E+00	0.00E+00	0.00E+00
S3	0.00E+00	0.00E+00	0.00E+00	0.00E+00	0.00E+00	0.00E+00	0.00E+00	0.00E+00	0.00E+00	0.00E+00	0.00E+00	0.00E+00	0.00E+00

Distance matrix

Distance matrix is necessary to evaluate the cost of a link between the nodes.

The distance matrix for the IP layer is given in terms of crossed transport rings from the source to the destination and, for the scenario 1, is reported in Table M_2-17 (sub-appendix M_2.2).

The set of available links for interconnecting the nodes are assumed to be the full set of SDH flows from STM1 to STM64. Table 4-2 [available SDH links] shows the bandwidths at SDH level, the VCs payloads (concatenated VC4 are considered for flows grater than STM1) and the bandwidth assuming a 5% POS overhead.

Table 4-2 [available SDH links]: available links for interconnecting routers and their bandwidth parameters

SDH Flow/ virtual container	*SDH bit rate [Mbit/s]*	*VC payload [Mbit/s]*	*IP payload [Mbit/s] (5 % POS overhead considered)*
STM1/VC4	155.052	149.760	142.272
STM4/VC4-4c	622.080	599.040	569.088
STM16/VC4-16c	2488.320	2396.160	2276.352
STM64/VC4-64c	9953.280	9584.640	9105.408

As the logical distance between nodes ranges between 1 to 5 (only integer value is considered) we have assumed as cost structure for the available links the one presented in Table 4-3 [cost structure]. This cost structure satisfy the necessary conditions required by the algorithm implemented in the IP-planner. In fact the algorithm require a concave cost structure respect the bandwidth of the available discrete link set. Table 4-3 is derived taking into account a saving factor of 12.5% (due to economy of scale) in the passage from a level to the next one of the SDH hierarchy (for example on the same logical distance one STM4 costs as).

Table 4-3 [cost structure]: cost of a single SDH link for the set of discrete distances

SDH flow/VC container	*Logical distance between network sites*				
	1	*2*	*3*	*4*	*5*
STM1/VC4	1.00	2.00	3.00	4.00	5.00
STM4/VC4-c4	3.75	7.50	11.30	15.00	18.80
STM16/VC4-16c	14.10	28.10	42.20	56.30	70.30
STM64/VC4-64c	52.70	105.00	158.00	211.00	264.00

Quality of service parameters

IP-planner models the packet traffic as generic packet traffic while in the metro scenario traffic types are very different in terms of type (streaming vs. elastic) and delay requirements (both no requirement at all to stringent requirement for audio and video streams).

For dimensioning the network we assumed as unique value for end-to-end maximum mean packet delay **1 ms** , that is a quite stringent value. Obiouvsly there isn't any assurance that the grade of service in terms of delay or jitter is satisfied for all the involved services as grade of service is defined for each service. A detailed network simulation should be made a-posteriori inorder to verify the correctness of the dimensioning reached.

Results

In Figure 4-1 [IP topology] the connectivity between routers obtained with dimenisoning program IP-planner is depicted. The Figure is a visual representation of the table 4-4 [STM requirements] in which STM requirement obtained with IP-planner are reported. In Figure 4-1 [IP topology] all the topology edges have one link of a given type except for the three edges connecting Server S2 to R6 and R9, and R8 to R9: in those cases the topology edge require multiple STM64 links. In figure 4-1[IP topology] multiple STM64 links are expressed through the numbers close to their graph representation. The resulting topology has 19 edges with single STM1 links, 8 edges with single STM4 link, one edge with one STM16 and 4 edges with multiple STM64 systems. In total the network has 32 connections between nodes in comparison with a full meshed connectivity of 78. All router are connected to the network with almost other four routers (except the S3 which only exchanges signaling traffic ignored for network dimensioning). Huge bandwidth connections are required between R3, R6, R9, R10 and S2 because the four routers exchange lot of traffic with the video server S2. R10 is not directly connected to S3 and use R9 as tandem to exchange traffic with S2.

Table 4-4 [STM requirements]: requirements in terms of STM flow between nodes

	R1	R2	R3	R4	R5	R6	R7	R8	R9	R10	S1	S2	S3
R1		STM1	STM1				STM4	STM1	STM1	STM1	STM4		
R2	STM1		STM1			STM1						STM4	
R3	STM1	STM1		STM1	STM1		STM1			STM1		STM64	
R4			STM1		STM1		STM1			STM1	STM4	STM4	
R5			STM1	STM1		STM4		STM1					
R6		STM1			STM4		STM4	STM1				2 STM64	
R7	STM4		STM1	STM1		STM4		STM1					
R8	STM1				STM1	STM1	STM1		STM1	STM1			
R9	STM1							STM1		2 STM64		4 STM64	
R10	STM1		STM1	STM1				STM1	2 STM64		STM4		
S1	STM4			STM4						STM4		STM16	STM1
S2		STM4	STM64	STM4		2 STM64			4 STM64		STM16		STM1
S3											STM1	STM1	

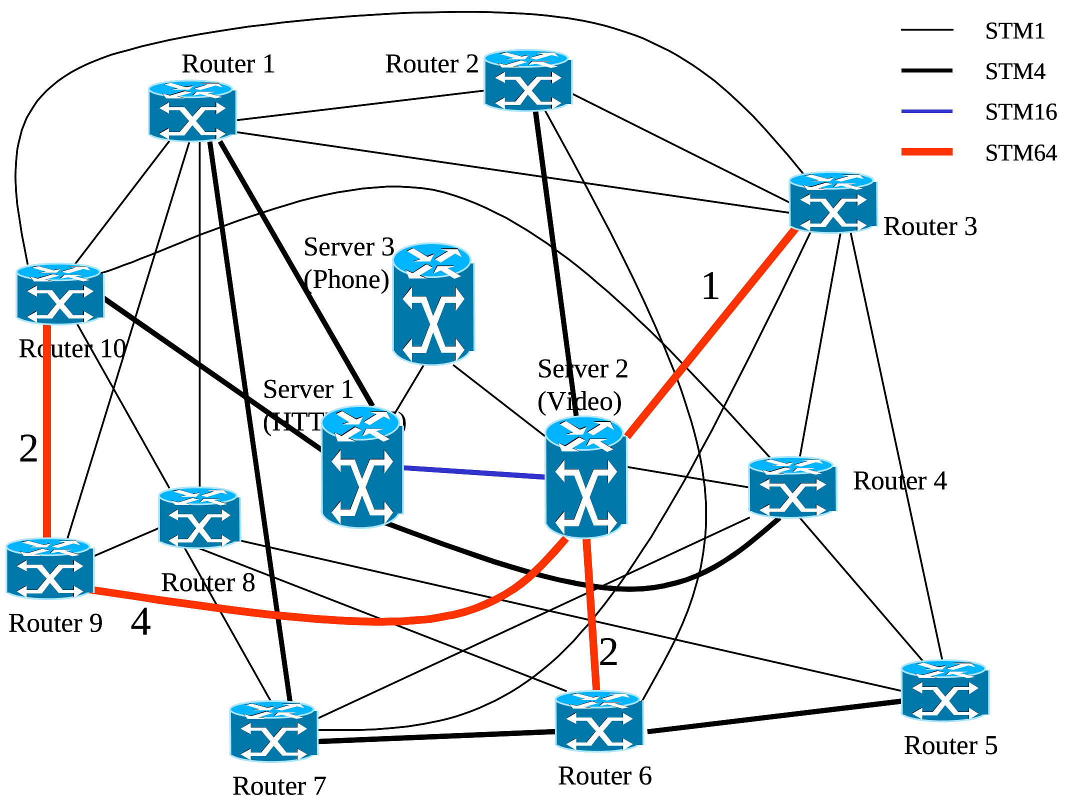


Figure 4-1: [IP topology]: Network planned links by IP-planner of the Metro network (Numbers next to STM64 links (bulk red lines) means the number of parallel links on the topology edge)

For other results regarding the Metropolitan IP network planning, see Appendix M_3.1 .

4.1.2 Adaptation between IP-planner outputs and SIREN-Plan inputs

SIREN-Plan, the SDH planning tool used to perform the planning of the SDH layer, requires as input a matrix of STM1 flows. As the requirements in terms of flows of IP-planner, the tool employed for IP layer planning, could range between STM1 to STM64, an adaptation between outputs of IP- planner and input of SIREN-Plan is required.

In order to perform such an adaptation, the matrix of generic STM requirements (see the Table 4-4 [STM requirements] reported in section 4.1.1), is converted in terms of equivalent STM1 flows and this matrix is used for planning and dimensioning the SDH layer.

Table 4-5 [STM equivalent requirements]

	R1	R2	R3	R4	R5	R6	R7	R8	R9	R10	S1	S2	S3
R1	0	1	1	0	0	0	4	1	1	1	4	0	0
R2	1	0	1	0	0	1	0	0	0	0	0	4	0
R3	1	1	0	1	1	0	1	0	0	1	0	64	0
R4	0	0	1	0	1	0	1	0	0	1	4	4	0
R5	0	0	1	1	0	4	0	1	0	0	0	0	0
R6	0	1	0	0	4	0	4	1	0	0	0	128	0
R7	4	0	1	1	0	4	0	1	0	0	0	0	0
R8	1	0	0	0	1	1	1	0	1	1	0	0	0
R9	1	0	0	0	0	0	0	1	0	128	0	256	0
R10	1	0	1	1	0	0	0	1	128	0	4	0	0
S1	4	0	0	4	0	0	0	0	0	4	0	16	1
S2	0	4	64	4	0	128	0	0	256	0	16	0	1
S3	0	0	0	0	0	0	0	0	0	0	1	1	0

4.1.3 Metropolitan SDH and WDM network planning results

In this subsection the results of SDH and WDM layers on case study 1 scenario 1 are presented. As the network scenario doesn't involve a full optical networking and the WDM systems are used with the aim of saving fibres on the topology edges, the results of both the components, SDH and WDM are presented together.

First some details on protection and characteristics of equipment employed are discussed, and then the result of network dimensioning is reported and explained.

Protection

The flows protection used inside the case study is: 1+1 Drop&Continue.

This type of protection assures the highest-level protection for a SDH rings network; infact this protection mechanism allows to recover multiple failures: even one link or node failure per each crossed ring.

When a dual-node path is present the protection is opened at the start-end of flows and is closed at the end-end. In each interconnection node the equipments forward flow demand towards the next ring (drop) and, at the same time, towards the second interconnection node.

When a single-node interconnection exists the 1+1 Drop&Continue protection is closed on the first ring crossed by the flows and the protection is re-opened on the following ring crossed by the flows.

Equipment

Concerning SDH networking, two types of SDH equipments are considered in the case study.
The main characteristics of two equipment are briefly described below:

Insert and extract tributary flows onto STM-16 systems
Partially access to VC-4 in transit on line
Presence of HO a LO matrixes to manage HO and LO flows respectively
Presence of PDH tributary ports at 2 and 34 Mbit/s so that we can access to the line capacity without external multiplier.

In the table 4-6 [ADM for SDH networking 1] the more important characteristics of the equipments used during the dimension of the case study are presented.
In the table 4-7 [ADM for SDH networking 2] the equipment configuration type used during the dimensioning are presented.

Table 4-6 [ADM for SDH networking 1]

	ADM 16/1, ADM 16/1c
Line interface Type/bit rate	Optical 2,5 Gbit/s
Matrix	LO and HO
Tributary ports	2, 34, 140 Mbit/s STM-1, STM-4

Table 4-7 [ADM for SDH networking 2]

	Tributary units				
	2 Mbit/s	34 Mbit/s	140 Mbit/s	STM-1	STM-4
ADM 16/1c	504	24	16	16	4
ADM 16/1	2016	96	32	32	4

The general criterias used during dimensioning are:

Use of ADM 16/1 for central WDM ring (RING-4) because of its higher number of managed protected flow.

Use of smaller equipments (ADM 16/1c) for SDH-only rings, as shown in table 4-8 [SDH/WDM systems on rings].

Table 4-8 [SDH/WDM systems on rings]

Ring	SDH system	SDH equipment	WDM equipment
RING 1	STM 16	COMPACT ADM 16	--
RING 2	STM 16	COMPACT ADM 16	--
RING 3	STM 16	COMPACT ADM 16	--
RING 4	STM 16	CLASSIC ADM 16	WDM 16, WDM 4
RING 5	STM 16	COMPACT ADM 16	--
RING 6	STM 16	COMPACT ADM 16	--

Planning results

In Figure 4-2 [SDH planning result] the principal results are depicted, in terms of SDH and WDM systems. In each ring are shown the number of SDH systems necessary to carry out the SDH STM1 flow demands reported in table 4-5 [STM equivalent requirements]. In the central ring WDM technology is also used.

For detailed results regarding the Metropolitan SDH and WDM network planning, see Appendix M_3.2

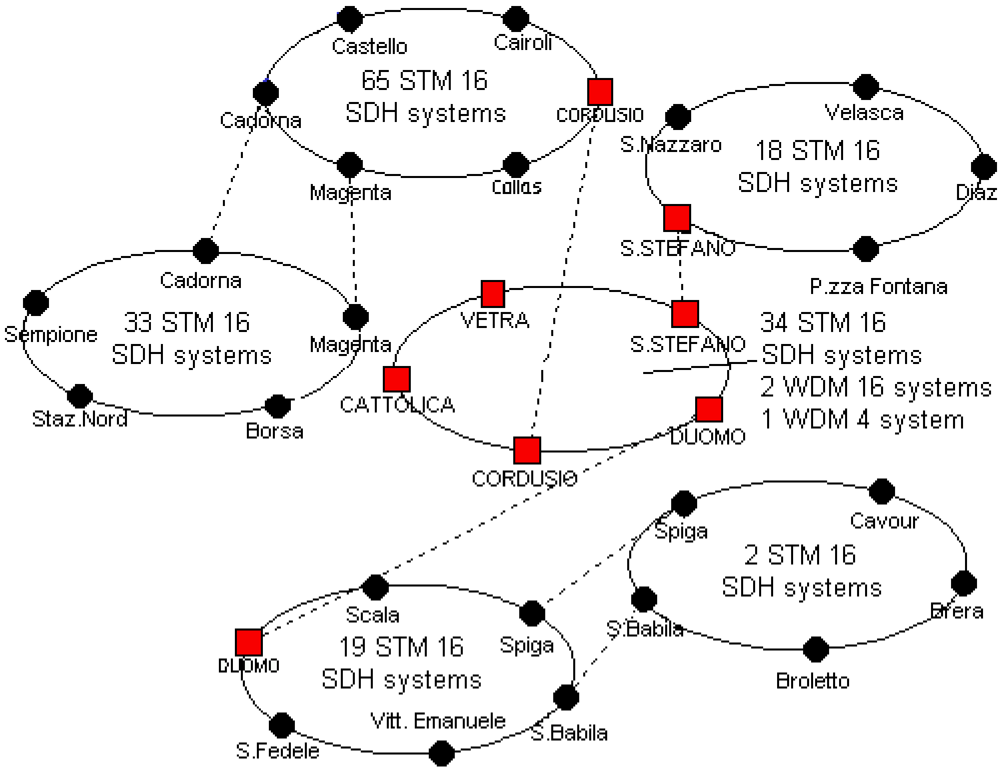


Figure 4-2: SDH planning results

4.2 Preliminary results from the Metropolitan Scenario 3/ case study 1

The purpose of the scenario 3 (IP over DPT/SRP) is to propose a data optimized solution with respect to the IP over SDH over WDM scenario due to the limitations of SDH when carrying IP traffic (see Section 2.2.3). The IP over DPT scenario pretends the elimination of the SDH equipment thus obtaining the following benefits according to Cisco:

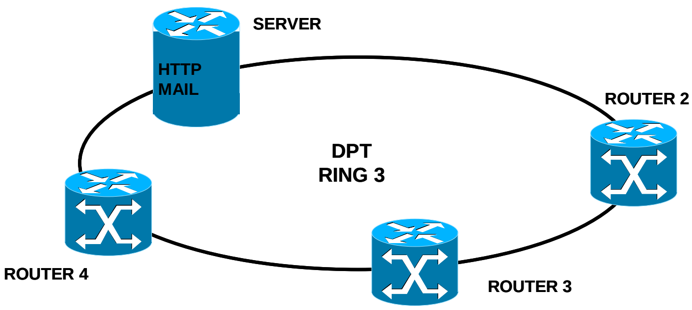
- Cost reduction by eliminating the high cost of SDH multiplexing equipment (ADMs).
- To exploit the price/performance offered by data networking equipment permitting a more efficient bandwidth usage.
- To overcome the limitations that TDM/circuit-based architectures imposed on data communications allowing direct, any-to-any, connectivity among all ring devices without circuit provisioning.

4.2.1 Planning methodology

In this section we have used the DPT/SRP simulator available at the UPC (see Section 3.2.2) for planning purposes. According to this, we have done a-posteriori evaluation of the performance of a given DPT network (in which traffic, number of nodes and DPT rate are fixed). As a result we have came out with the percentage of service that can be offered within the scenario 3 . Since the DPT simulator only treats individual rings we have simplified the scenario 3 planning each ring individually. The methodology used in order to validate the services supported by each DPT ring is the following:

- To fix all the parameters (traffic load, load distribution, number of nodes, DPT interface rate, etc.).
- To assign the low and high priority traffic quotas according to the services studied.
- To examine, after simulation, the performance results obtained which will determine whether the services offered can be supported and the percentage of penetration of every service.

For the preliminary results of the scenario 3, the following planning example has been chosen: the DPT ring 3 which is composed of 3 routers (ROUTER 2, ROUTER 3 and ROUTER 4) and one server (HTTP/MAIL SERVER) (see Figure 4-3). The figure also shows the services, with their QoS requirements, to be supported by this ring in particular.



Services Offered	*QoS Requirements*
Mail	None
Http	Loosely limited delay
Phone	Delay, jitter
Low quality video	Packet delay (50 ms), Jitter (25 ms)

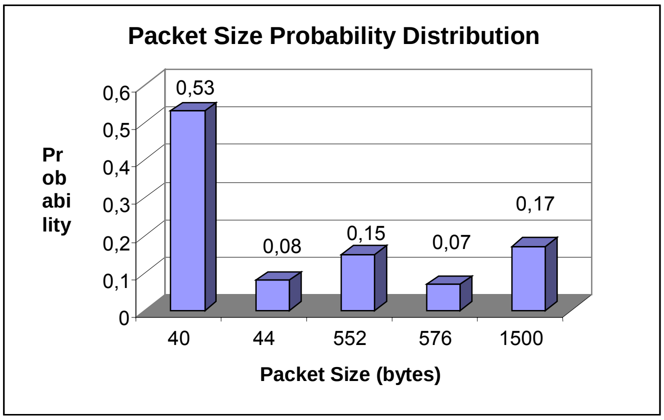
Figure 4-3: DPT Ring from scenario 3

DPT interfaces are expected to run at speeds ranging from OC-3c/STM-1c (155 Mbps) to OC-192c/STM-64c (10 Gbps). According to the traffic and service requirements specified in [WP3-T2] low quality video service cannot be supported at OC-3c and OC-12c rates without the use of WDM equipment. As this case study poses a scenario in which the external rings do not use WDM equipment, our objective is to check the QoS requirements of all services offered and, in the case of the low quality video service, to determine its penetration (i.e. how many inhabitants could make use of the video service).

4.2.2 Simulation environment

The following list shows the parameters used in the simulations carried out. In addition to the traffic load and load distribution calculated in the [WP3-T2] document, these parameters have been:

- DPT Rates: OC-12 (622Mbps), OC-48 (2,5Gbps), OC-192 (10Gbps)
- Packet size distribution[1]



"SDL Data Link Specification", Lucent Technologies – White Paper

Figure 4-4: SDL Data Link Specification

- Data: Mean packet size of 402 bytes (3216 bits)
- Voice: Mean packet size of 44 bytes (352 bits)
- Video: Mean packet size of 512 bytes (4096 bits)

- Packet arrival distribution: Poisson with a mean packet arrival of λ. Values used for the mean packet arrival are listed in the next Table 4-9. This parameter (λ) depends on the traffic load offered by each node in accordance with the type of service.

		Traffic Offered (Mbps)	Mean Packet Arrival (sec/packet)
SERVER	*Data*	1262,767	2,65E-06
	Voice	167,216	2,87E-06
	Video	7500	5,63E-07
ROUTER 2	*Data*	261,23	1,28E-05
	Voice	-	-
	Video	-	-
ROUTER 3	*Data*	312,945	1,07E-05
	Voice	-	-
	Video	75	5,63E-05
ROUTER 4	*Data*	344,91	9,70E-06
	Voice	224	2,14E-06
	Video	-	-

Example: 3344 bits / (1262,767 Mbps) = 2.65E-06 sec/packet

Table 4-9: Metro Scenario 3/ Case study 1 – Mean packet arrival

[1] The packet size distribution corresponds to IP packets which are the payload of the SRP packets.

4.2.3 Results obtained

The first situation taken into account has been without considering the video service. According to the methodology exposed above, once the traffic load and distribution has been fixed the next step has been to assign the high priority to the phone service and the low priority to the rest of the services (data services such as mail, web and http based).

The following Table 4-10 shows the results obtained. It is worth to note that in all rings the phone service cannot be guaranteed using OC-12 interfaces.

		Network Throughput (Gbps)	ETE Delay High Priority	Variance High Priority	Std. Dvtion High Prio.	ETE Delay Low Priority	Variance Low Priority	Std. Dvtion Low Prio.
RING 1	OC-12							
	OC-48	3,132	826,960E-9	1,712E-12	1,309E-6	3,274E-6	14,522E-12	3,811E-6
	OC-192	3,157	104,330E-9	32,607E-15	180,574E-9	535,580E-9	502,20E-15	708,661E-9
RING 2	OC-12	-	-	-	-	-	-	-
	OC-48	2,857	1,860E-6	111,00E-15	333,167E-9	2,896E-6	225,00E-15	474,342E-9
	OC-192	2,862	188,410E-9	109,68E-15	331,180E-9	476,200E-9	410,00E-15	640,312E-9
RING 3	OC-12	-	-	-	-	-	-	-
	OC-48	2,694	1,436E-6	200,0E-12	14,142E-6	90,880E-6	125,6E-9	354,401E-6
	OC-192	2,694	489,1E-9	400,0E-12	20,000E-6	35,260E-6	123,9E-9	351,994E-6

Table 4-10: Metro Scenario 3/ Case study 1 – Results obtained without the Video service

Next, in case of considering the video service, the high priority has been assigned to the phone and video services whereas the low priority still corresponds to the rest of the services.

The following Table 4-11 shows the results got using OC-48 and OC-192 DPT interfaces. In this case, the objective was to find the maxim percentage of inhabitants whose services (data, video and voice) could be guaranteed.

RING 1		Network Throughput (Gbps)	ETE Delay High Priority	Variance High Priority	Std. Dvtion High Prio.	ETE Delay Low Priority	Variance Low Priority	Std. Dvtion Low Prio.
OC-48	0.5%	4,487	2,391E-6	12,020E-12	3,467E-6	5,885E-6	61,700E-12	7,855E-6
	1%.	5,843	5,144E-6	39,640E-12	6,296E-6	56,205E-6	29,080E-9	170,529E-6
OC-192	4%	13,860	1,527E-6	2,568E-12	1,602E-6	1,432E-06	6,713E-12	2,591E-6
	5%	16,480	2,271E-6	5,234E-12	2,288E-6	2,580E-06	37,39E-12	6,115E-6

RING 2		Network Throughput (Gbps)	ETE Delay High Priority	Variance High Priority	Std. Dvtion High Prio.	ETE Delay Low Priority	Variance Low Priority	Std. Dvtion Low Prio.
OC-48	0.2%	3,168	2,930E-6	1,790E-12	1,338E-6	3,820E-6	8,320E-12	2,884E-6
	0.5%	3,675	4,890E-6	2,820E-12	1,679E-6	8,350E-6	10,100E-12	3,178E-6
OC-192	4%	9,291	2,203E-6	1,197E-12	1,094E-6	2,460E-6	9,330E-12	3,055E-6

	5%	10,895	3,730E-6	4,730E-12	2,175E-6	13,500E-6	1,080E-9	32,863E-6

RING 3		Network Throughput (Gbps)	ETE Delay High Priority	Variance High Priority	Std. Dvtion High Prio.	ETE Delay Low Priority	Variance Low Priority	Std. Dvtion Low Prio.
OC-48	3%	4,150	14,095E-6	600,0E-12	24,495E-6	185,0E-6	101,6E-9	318,748E-6
	4%	4,700	16,491E-6	600,0E-12	24,495E-6	-	-	-
OC-192	10%	7,650	18,140E-6	6,75E-12	2,598E-6	154,8E-6	10,4E-9	101,980E-6
	15%	10,215	18,775E-6	500,0E-12	22,361E-6	-	-	-

Table 4-11: Metro Scenario 3/ Case study 1 – Results obtained with the Video service

The best case is found in the ring 3 where can be concluded that:

- at OC-48 the limit for using the video service is the 3% of inhabitants since considering the 4% of residents the low priority traffic (mail, web and http-based services) cannot be served.
- at OC-192 we find the same situation. In this case a percentage of 10% of inhabitants can use the video service whereas, considering the 15% of inhabitants, the performance of the low priority services is severely affected.

The table also shows the limit for using the video service in the rest of the rings.

4.3 Preliminary results from the Long Distance Scenario 2 / Case Study 1

4.3.1 Study description and assumptions

In this subsection results of the planning process carried out on the Scenario 2 (IP over WDM) / Case Study1of the Long Distance Context are presented. The goal of this exercise is to design a reliable **IP-over-WDM** network.

The design is based on a **top-down approach** (see Figure 4-5). **First** of all, the **total IP traffic matrix** is computed. **Secondly** the **IP network** is dimensioned, resulting in the number of wavelength paths to be established by the optical network. **Thirdly**, the **optical network** is dimensioned. Both layers are dimensioned independent of each other. The remainder of this section will clarify each step in more detail.

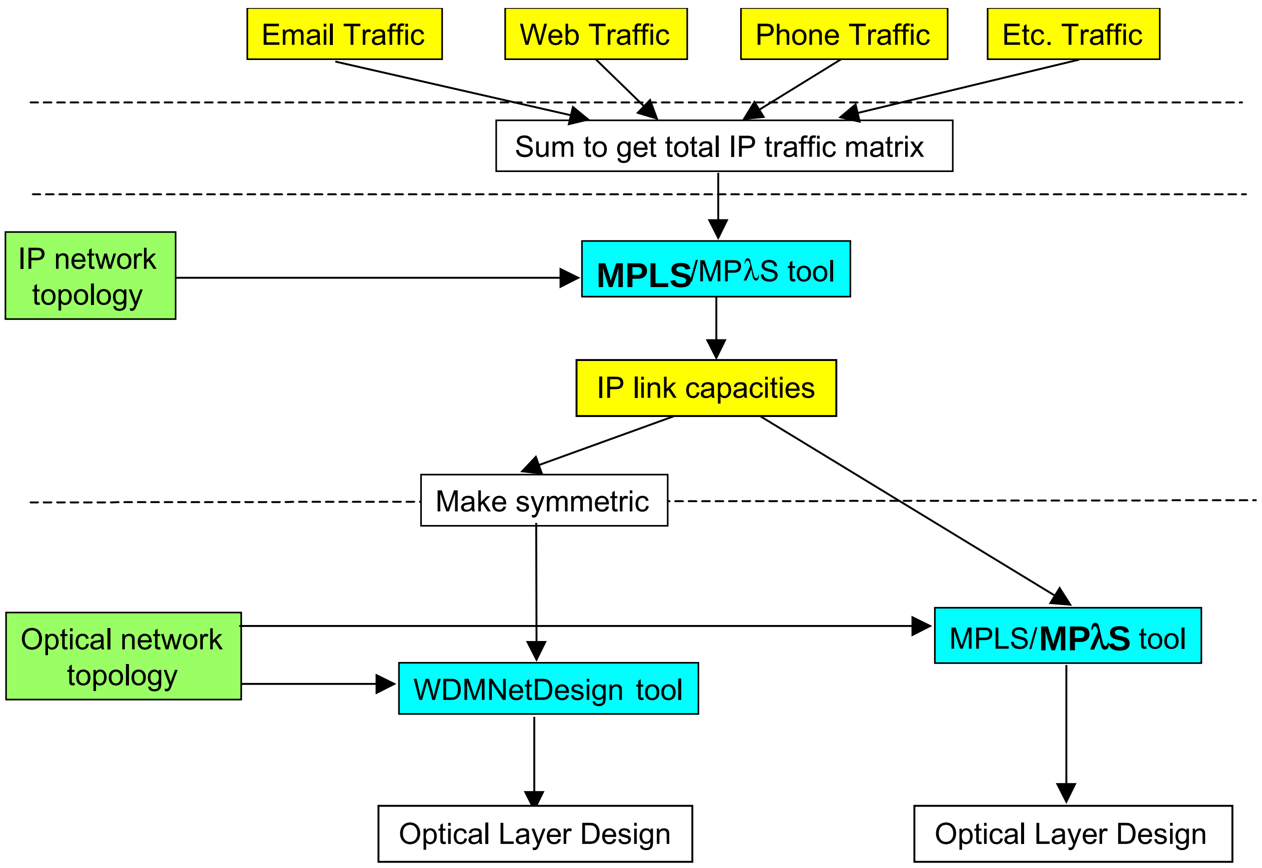


Figure 4-5: the top-down planning approach for an IP-over-WDM network

The [WP3_T2] document contains several traffic matrices: one for each defined service. These traffic matrices already take into account the necessary overhead and represent average values (specified in Mbps). The total IP traffic matrix is obtained by simply summing up all individual demands for the same node pair. Note also that IP typically results in asymmetric traffic (and thus asymmetric traffic matrices).

This total IP traffic matrix is fed into the IP dimensioning process in order to obtain the required capacity (in terms of Mbps) for each logical IP link. The traffic is routed along a (single) shortest path: the hop-count was assumed as metric. The routing is thus not optimized. Also a single unidirectional flow is routed at each time, resulting in the possibility that both directions between the same end-points are routed along another path. In a second phase, IP router failures are also taken into account[2]. For this purpose, a dimensioning (in a similar way) for MPLS Local Protection was considered. Each router is protected by a backup LSP, pre-established[3] between the IP routers adjacent to the router being protected (the dimensioning of the spare capacity is obtained by simulating each failure and verifying if enough capacity is already provided). This is thus clearly a dimensioning process in the sense that the logical topology is given by [WP3_T2] as input, and that the routing is not optimized at all.

The last step is to design the optical network. Therefore, the line capacities (in Mbps) have to be translated to an (integer) number of wavelengths in the optical domain: 2.5 Gbps wavelengths were considered (thus, dividing the line capacities by 2500 Mbps). Note that this traffic matrix is still asymmetric. The optical domain was chosen to provide the (first-line) reliability: single line and node failures were assumed to be realistic for the optical network (since it is server layer and thus no complex secondary failures have to be considered). We have chosen to design the optical domain both as a reliable MPλS network and as a reliable "classical" operator managed network.

MPλS network: the same tool is used as for the dimensioning of the IP layer and thus similar remarks exist. The routing is not optimized: a single, unidirectional (working, alternative or backup) path is routed at each time independently, based on a shortest path algorithm considering fiber length as routing metric[4]. An important difference between O-MPLS (thus MPλS) and E-MPLS is that O-MPLS uses dedicated protection while E-MPLS uses shared protection[5]. For Rerouting and FTCR (see [ONM]) it is still needed to simulate one failure after the other and verify if enough capacity is already foreseen[6].

"Classical" operator managed optical network: this case differs (from a planning point of view) mainly in two aspects (due to the properties of WDMNetDesign).

First of all, bi-directional symmetric demands are routed. This implies that the traffic matrix has to be made symmetrical: the maximum capacity of both directions is chosen as the new value for both directions. A second implication is that both flows between the same end-points (in opposite direction) are not allowed anymore to use different paths.

Secondly, the dimensioning starts from a shortest path routing (based on the fiber length) and continues with an optimization, which minimizes the number of line-systems in the network. The MPλS dimensioning is straightforward in the sense that it routes everything along a shortest path and counts the number of required wavelengths on each link. WDMNetDesign takes into account a cost per line system (e.g., line-systems of 32 wavelengths were assumed). More precisely, the tool will try to remove inefficiently used line-systems by rerouting the traffic through line-systems which have enough unused capacity available.

Of course, a third difference is a result of the technology: other recovery schemes are needed here than in the MPλS case. This makes it very attractive to compare the results for MPλS recovery and classical recovery with each other. Link and Path Restoration and 1+1 Path Protection were

---

[2] No (logical) line failures were considered in the IP network, since it was assumed that the supporting lightpaths are restored in the optical layer.

[3] But only occupying resources when the protected segment is failing, leading to shared protection.

[4] One exception exists to this rule. We included for completeness also a shortest cycle algorithm, finding always two physically disjoint routes (in case of Path Protection or Local Loop-back) on a node bi-connected network.

[5] [ONM] proposes some improvements for the protection in MPλS networks, making dedicated protection an upper bound for the cost.

[6] The downstream part of the rerouted LSPs is assumed to be torn-down.

considered as recovery techniques for this "classical" optical networking case (the routing of the alternative/backup paths is also considered in the above explained optimization process).

The network cost is in both cases modeled as the number of wavelengths on the various links multiplied with the link length. Both cases also assume that the OXCs are able to perform wavelength conversion.

4.3.2 Summary of the results

This section presents the IP traffic matrix and the resulting optical layer design for the long-distance network of [WP3_T2]. In section 4.3.2.1 the obtained network design is able to cope with single line or node failures in the optical layer. In section 4.3.2.2, the network can also recover from IP router failures, by using an extra protection mechanism in the IP layer.

4.3.2.1 Design of a reliable optical network

Table 4-12 presents the IP demand matrix[7] between the nodes of the IP topology from [WP3_T2] (Row = from, Column = to) that was used as input to the design of the optical network.

	Milan1	Milan2	Rome1	Rome2	Bologna	Naples	Turin	Genoa	Trento	Venice	Florence	Pescara	Cagliari	Palermo	Bari	ReggioC
Milan1	0	0	1444	1444	3068	2475	2065	2066	617	1629	1660	372	742	993	742	491
Milan2	0	0	1444	1444	3068	2475	2065	2066	617	1629	1660	372	742	993	742	491
Rome1	1552	1552	0	0	1703	3865	1144	1144	340	899	925	585	1162	1552	1162	772
Rome2	1552	1552	0	0	1703	3865	1144	1144	340	899	925	585	1162	1552	1162	772
Bologna	2355	2355	711	711	0	1047	941	942	281	746	765	158	314	420	314	207
Naples	1511	1511	883	883	878	0	594	594	175	459	484	300	593	795	598	394
Turin	705	705	561	561	410	531	0	276	81	210	223	80	160	213	159	105
Genoa	706	706	561	561	411	531	276	0	81	210	224	80	160	214	159	105
Trento	151	151	119	119	87	110	58	58	0	45	48	17	33	44	33	22
Venice	312	312	249	249	181	225	118	119	36	0	99	34	68	91	68	44
Florence	687	687	551	551	408	526	269	269	80	209	0	80	158	211	158	104
Pescara	147	147	124	124	84	116	57	57	17	44	47	0	33	45	34	22
Cagliari	292	292	241	241	166	224	114	114	33	86	94	33	0	90	66	44
Palermo	430	430	354	354	246	333	168	168	49	128	138	50	99	0	98	67
Bari	291	291	241	241	166	227	113	113	33	86	94	34	66	89	0	44
ReggioC	153	153	127	127	86	118	59	59	17	44	49	17	34	48	35	0

Table 4-12: Original input: IP demand matrix (Mbit/s)

Next, we routed the IP demand using the MPLS part of the MPLS/MPλS tool (shortest path routing, no recovery mechanisms was used) in order to obtain the demand between the nodes of the optical

[77] The matrix was obtained by summing up the different traffic contributions and rounding them towards the nearest integer Mbit/s demand value.

server layer[8]. As explained before, we divided this demand by 2500 (Mbit/s) to get the number of needed wavelength channels between these nodes.

The results of the construction of the server layer demand matrix are shown in Appendix MPLS_3: Intermediate results for the long-distance scenario 2, more specific in Table MPLS_3-1.

Some additional figures are presented in Table 4-13: in total 168938 Mbit/s traffic has to be transported by the optical network. (Note: intra-Milan and intra-Rome traffic is *excluded* from this figure.) The average (over all nodes that exchange IP traffic) and maximum IP traffic between two optical nodes are also mentioned.

Total traffic that has to be transported	168938 Mbit/s
Avg traffic between two nodes	3249 Mbit/s
Max traffic between two nodes	13010 Mbit/s
Avg. filling of the λ channels	60.4%
Max filling of the λ channels	94.2%

Table 4-13: Summarized figures for IP dimensioning (demand for server layer)

4.3.2.1.1 Results for MPλS

Table 4-14 presents the results of the dimensioning for the different recovery techniques. For an explanation about these techniques, see Appendix MPLS_2: Short Description of MPLS recovery schemes. The shortest cycle based recovery mechanisms (SC local-loopback and SC path protection) (see footnote 4) are not included because they are equivalent to the shortest path techniques for this specific network scenario. Figure 4-6 focuses on the total number of needed 2.5 Gbit/s lamdbas and Figure 4-7 highlights the total cost (# lambdas x fibrelength). The wavelengths (lambdas) are unidirectional. It's important to mention that we have *dedicated protection* for local protection, local loop-back and path protection. On the other hand, *FTCR* and *rerouting* are shared mechanisms: it is assumed that the working part of the failing MPλS path (LSP) is torn down first and then a new route is set up along the unused capacity.

	No Protection	Local Protection	FTCR	Rerouting	Local Loop-back	Path Protection
Total # used λ channels	119	381	287	286	344	319
Avg # used λ channels on a link	2.05	6.57	4.95	4.93	5.93	5.50
Max # used λ channels on a link	11	22	16	16	22	22
Total # unidirectional line-	44	48	48	48	49	48

[8] One difficulty came up: the Milan routers (Milan1 and Milan2) in the IP layer are connected to a single optical node in Milan in the server layer (for the server layer topology, see [WP3_T2]). Therefore, we

assumed that IP traffic from different routers has to be merged into different wavelengths. Furthermore, the intra-node traffic in Milan was not considered as long-distance traffic. The same applies to Rome.

systems						
Total cost	35953	98921	77510	77542	89092	83222

Table 4-14: Dimensioning (working + spare) of the different recovery mechanisms in the server layer (MPλS),

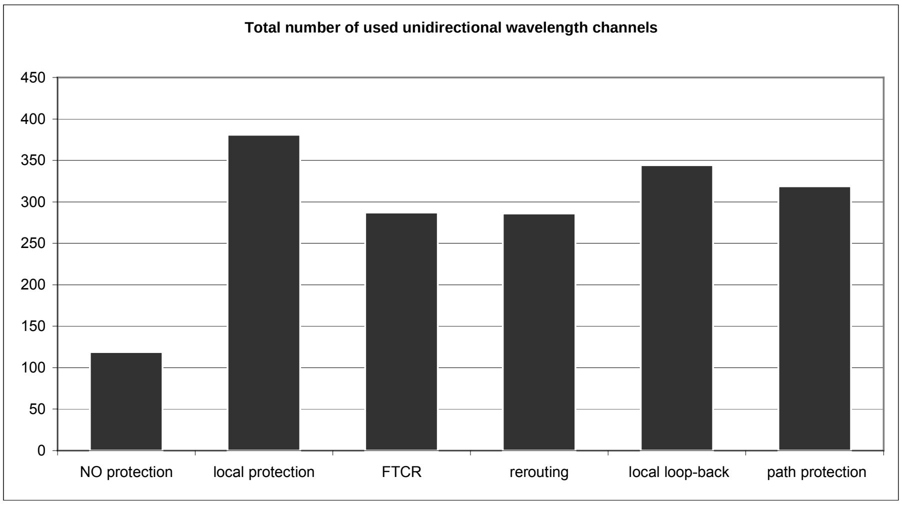


Figure 4-6: Comparison of the different recovery mechanisms in the server layer (MPλS): used wavelength channels

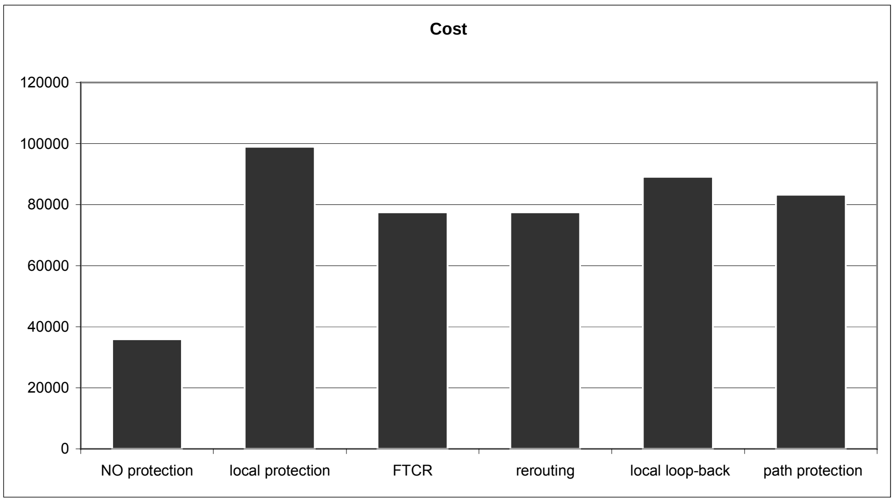


Figure 4-7: Comparison of the different recovery mechanisms in the server layer (MPλS): cost

Discussion of the results (see also [ONM]):

when using recovery mechanisms in the server layer the cost multiplies here by about 3

local protection is the most expensive solution, but not tremendously: this is probably due to the fact of a relatively high average nodal degree of 4 (see [ONM])

due to the fact that we have dedicated protection (see [ONM]): local loop-back is more expensive than path protection

FTCR and rerouting are the cheapest techniques (they are not relying on pre-established paths), it is remarkable that FTCR is somewhat cheaper than rerouting

4.3.2.1.2 Results for "classical" optical networking

The network is dimensioned for 1+1 path protection and both link and path restoration. Line-systems with 32 wavelengths are assumed on each fiber and each wavelength channel transports an STM-16 (2.5 Gbit/s) signal. The dimensioning is based on a shortest path heuristic, which includes an extra optimization step (see Section 4.3.1). To facilitate the comparison between the various back-up mechanisms, the unprotected results are also shown. This will also help to compare the MPλS solution with "classical" optical networking. The results for the dimensioning are shown on Figure 4-8 and a summary is given in Table 4-15.

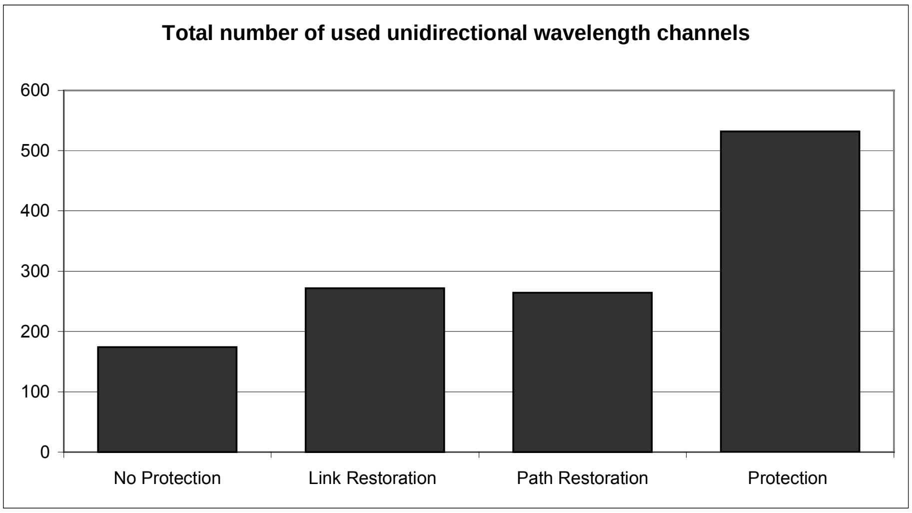


Figure 4-8: Comparison of the different recovery mechanisms in the server layer (OTN): used wavelength channels

When comparing the various back-up mechanisms, the conclusion can be drawn that both link and path restoration need around 1.5 times as much capacity compared to the unprotected case. As could be expected, path restoration gives slightly better results than link restoration. Protection needs even more capacity: more than 3.1 times as much as in the unprotected case.

With all back-up schemes, not every optical link is used. Figure 4-9 shows the distribution of the usage of the links.

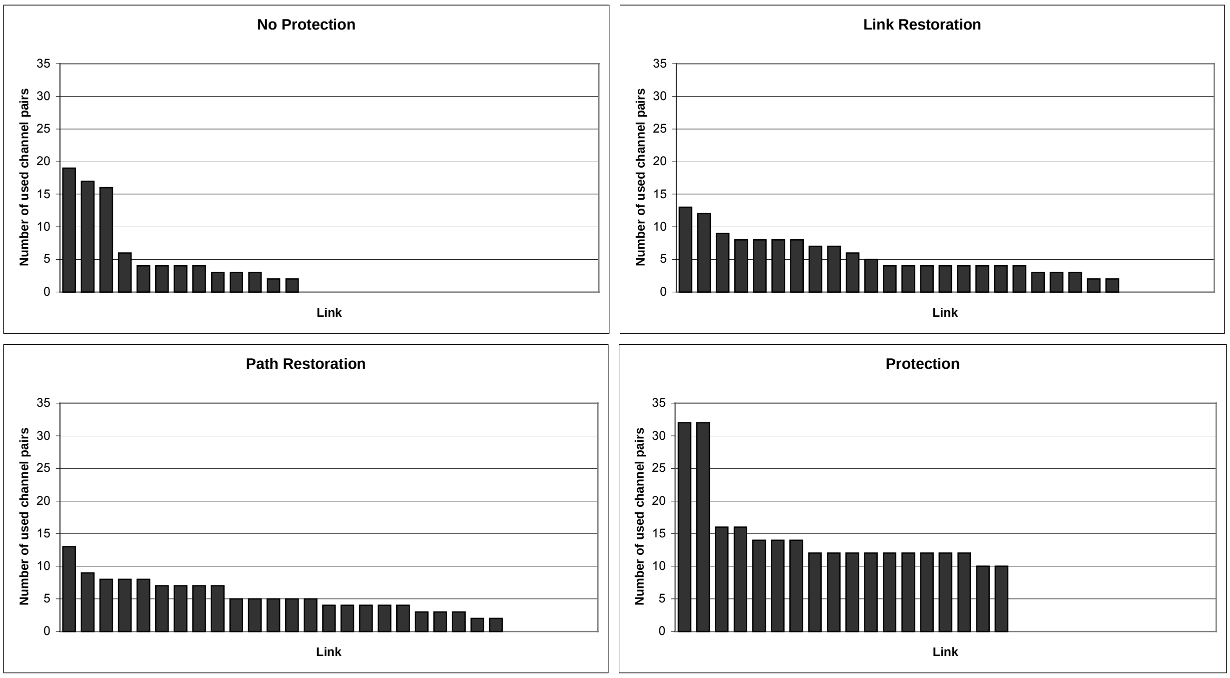


Figure 4-9: Distribution of link usage for the various back-up mechanisms

If we look into the design in more detail, we see that the second link between Milan and Rome is one of the links that is never used. There is always enough spare capacity in the network to find a back-up path along links on which there is already capacity installed, making it unnecessary to install any capacity on this second link between Rome and Milan.

The results are summarized in Table 4-15. The wavelength channels are considered to be unidirectional. Cost is here assumed to be the number of used (unidirectional) wavelength channels on a link multiplied with the length of the link.

	No Protection	Link Restoration	Path Restoration	Protection
Total # used λ channels	174	272	264	532
Avg # used λ channels on a link	3.00	4.69	4.55	9.17
Max # used λ channels on a link	19	13	13	32
Total cost	51058	89710	83938	153172

Table 4-15: Dimensioning (working + spare) of the different recovery mechanisms in the server layer (OTN)

For the unprotected case, the filling of the wavelength channels can be calculated. The average filling is 72.09% and the most filled channel has a usage of 91.89%. This means that this network design can handle a traffic variation of 8.11%. This is also the deviation between peak and average traffic that the network will be able to cope with.

4.3.2.1.3 Comparison

It would be very interesting to compare the results obtained with “classical” optical networking with those resulting from the MPλS study. The only meaningful comparisons are 1) between working, unprotected traffic in MPλS and no protection in “classical” optical networking and 2) between path protection in MPλS and path protection in “classical” optical networking.

Figure 4-10 shows the difference in number of used wavelength channels. Here the “classical” optical network solution (OTN) performs worse than MPλS.

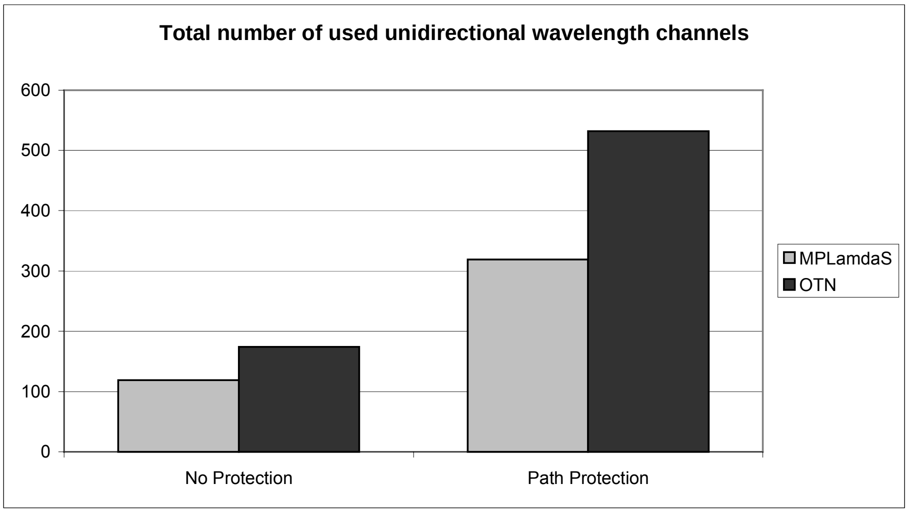


Figure 4-10: Comparison between MPλS and “classical” optical networking: used wavelength channels

This result is partially caused by the difference in routing methodology used by the MPλS tool and the “classical” networking tool: the MPλS tool routes unidirectional connections while the optical networking tool routes bi-directional symmetric connections.

Figure 4-11 shows the comparison in number of used line-systems of 32 wavelengths. The “classical” optical networking solution is here better than the one obtained with MPλS. This result was anticipated, as the WDMNetDesign tool minimizes the number of line-systems when designing the network, while the MPλS tool simply routes all traffic along the shortest path.

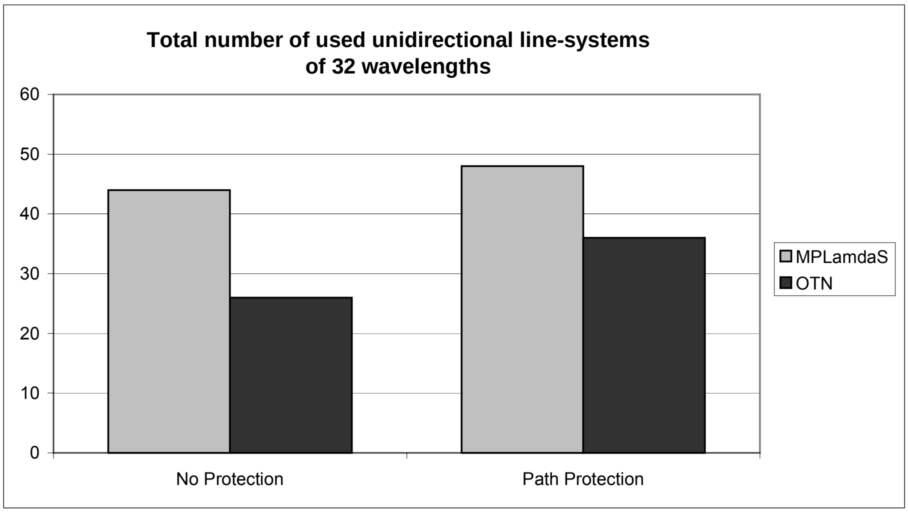


Figure 4-11: Comparison between MPλS and "classical" optical networking: used line-systems

A last issue for comparison between both the MPλS and the optical networking solution is the network cost. Cost is still assumed to be the number of used wavelength channels multiplied with their length. As can be seen on Figure 4-12, "classical" optical networking gives a worse result than the MPλS case.

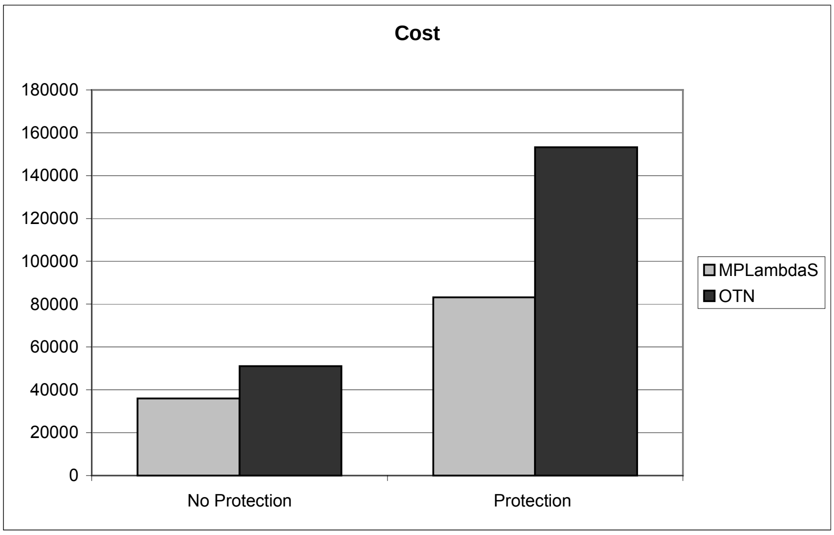


Figure 4-12: Comparison between MPλS and "classical" optical networking: cost

This result could also be expected, as the MPλS tool routes all traffic along the shortest path, while the "classical" optical networking tool (WDMNetDesign) minimizes the number of line-systems used in the network. As a result some connections are routed along a path that is longer than the shortest path, but makes better use of the available capacity in the network

4.3.2.2 Increased reliability: importance of IP router failures

Again we used Table 4-16 as the starting point. And again we routed the IP demand using the MPLS part of the MPLS/MPλS tool. This time we included local protection against node failures in the routing. The reason is that IP node failures can't be covered by lower layer protection schemes. For an explanation of the used recovery mechanisms, see Appendix MPLS_2: Short Description of MPLS recovery schemes. Using the same methodology as discussed in section 4.3.2.1, we obtained the demand between the nodes of the optical server layer. The results are shown in Appendix MPLS_3: Intermediate results for the long-distance scenario 2, more specific in Table MPLS_3-2.

The total traffic has increased by a factor of 1.71. This is also true for the average traffic between two nodes. This factor is less than 2 and that is explained by the fact that the capacity for IP node failure protection can be shared.

Total traffic that has to be transported	289483 Mbit/s
Avg traffic between two nodes	5567 Mbit/s
Max traffic between two nodes	17462 Mbit/s
Avg filling of λ channels	75.9%
Max filling of λ channels	99.9%

Table 4-16: Summarized figures for IP with recovery (demand for server layer)

4.3.2.2.1 Results for MPλS

Completely similar to the case without recovery in the IP layer (see section 4.3.2.1.1), the results are now presented for the case of recovery in the IP layer (see Table 4-17, Figure 4-13 and Figure 4-14). In the figures, the corresponding results for the case without IP recovery are also shown.

	No Protection	Local Protection	FTCR	Rerouting	Local Loop-back	Path Protection
Total # used λ channels	167	527	406	401	480	457
Avg # used λ channels on a link	2.88	9.09	7.00	6.91	8.28	7.88
Max # used λ channels on a link	13	27	20	20	27	27
Total # unidirectional line-systems	44	48	48	48	49	48
Total cost	50752	135711	108822	108037	123876	118908

Table 4-17: Dimensioning (working + spare) of the different recovery mechanisms in the server layer (MPλS), in case of IP with recovery

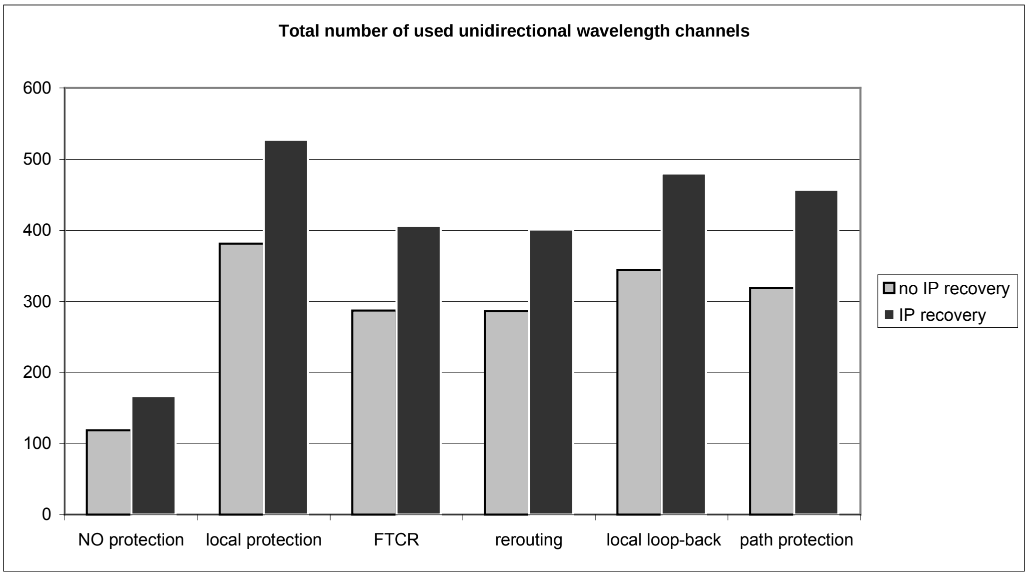


Figure 4-13: Comparison of IP with and without recovery for the different recovery mechanisms in the server layer (MPλS): used wavelength channels

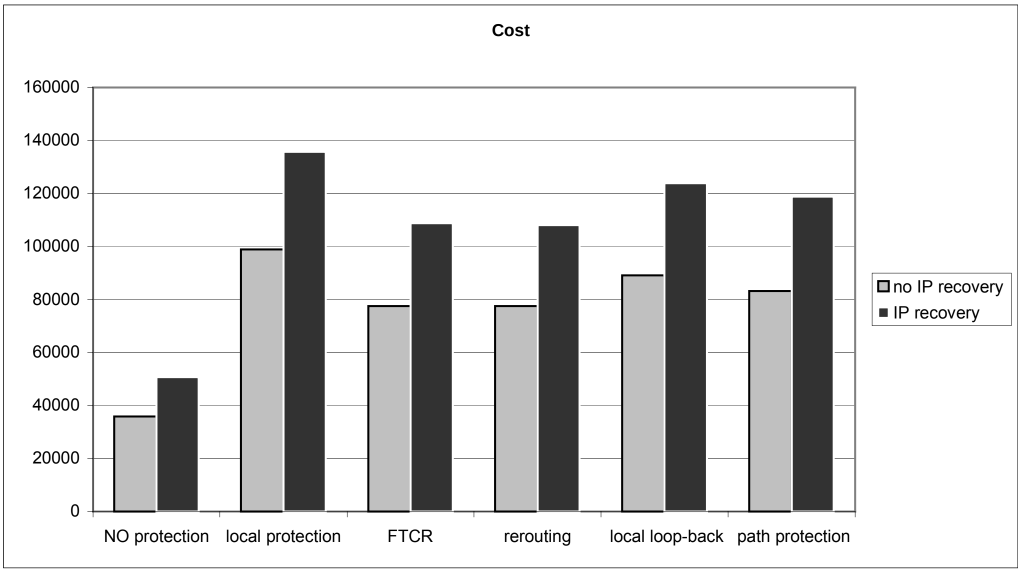


Figure 4-14: Comparison of IP with and without recovery for the different recovery mechanisms in the server layer (MPλS): cost

When compared to the case without IP recovery, the number of needed wavelengths and the total cost figures are less than doubled. See Table 4-18 and for a visual representation of the results see Figure 4-15. The increase factor is even less than the one for IP traffic (1.71, see explanation for Table 4-16). As a consequence, the filling of the wavelengths has increased.

Increase factor	No Protection	Local Protection	FTCR	Rerouting	Local Loop-back	Path Protection
…in total # lambdas	1.41	1.37	1.40	1.39	1.39	1.43

…in total cost	1.40	1.38	1.41	1.40	1.40	1.43

Table 4-18: Comparison of IP with and without recovery for the different recovery mechanisms in the server layer (MPλS): increase factors

A remarkable fact to notice in Figure 4-15 is that the most expensive recovery technique (local protection), suffers the least from the increase in traffic demand (- increase in demand due to recovery in the IP layer). This result is not yet explained.

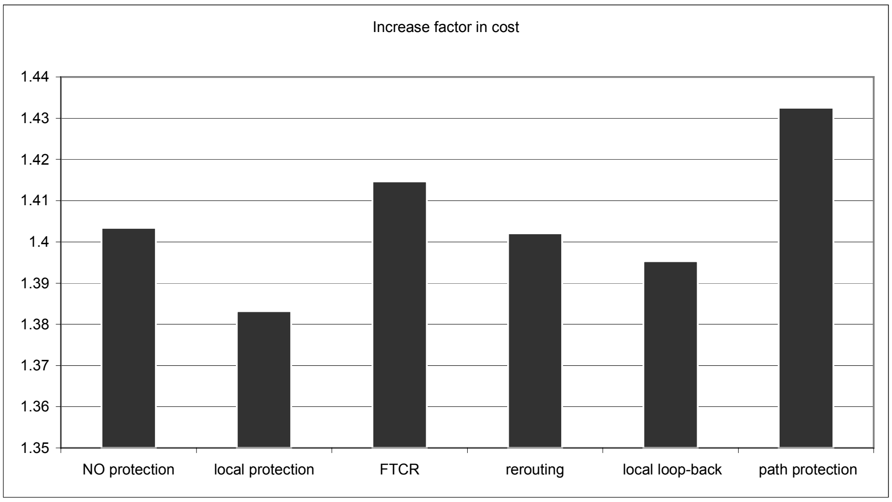


Figure 4-15: Comparison of IP with and without recovery for the different recovery mechanisms in the server layer (MPλS): increase factor in cost

4.3.2.2.2 Results for "classical" optical networking

Figure 4-16 shows the difference in capacity between the design with local protection of the nodes the IP layer and the one without such a protection mechanism (see section 4.3.2.1.2). As expected, more capacity is needed when protection is used in the IP layer, but this design has the advantage that router failures can be dealt with.

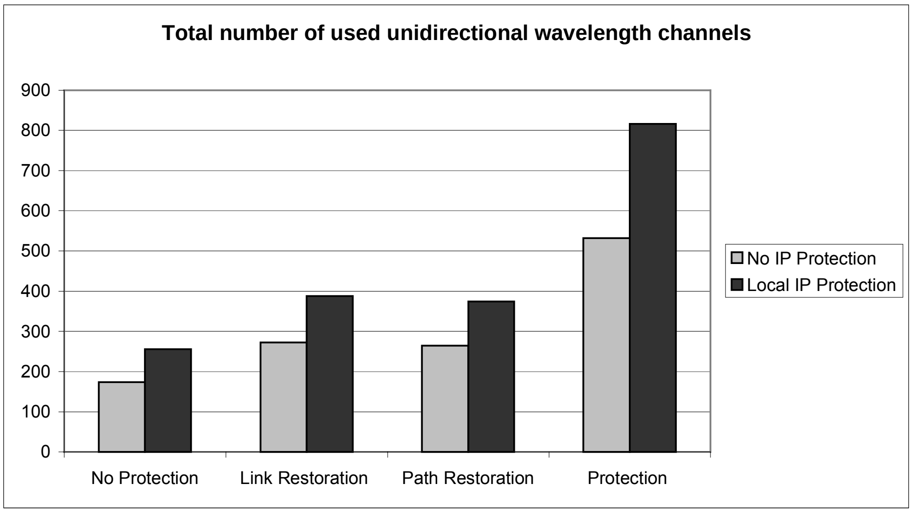


Figure 4-16: Comparison of IP with and without recovery for the different recovery mechanisms in the server layer (OTN): used wavelength channels

In order to make a better comparison, the costs of both designs were calculated. Again, cost is assumed to be the number of used wavelength channels on a link multiplied with the length of the link.

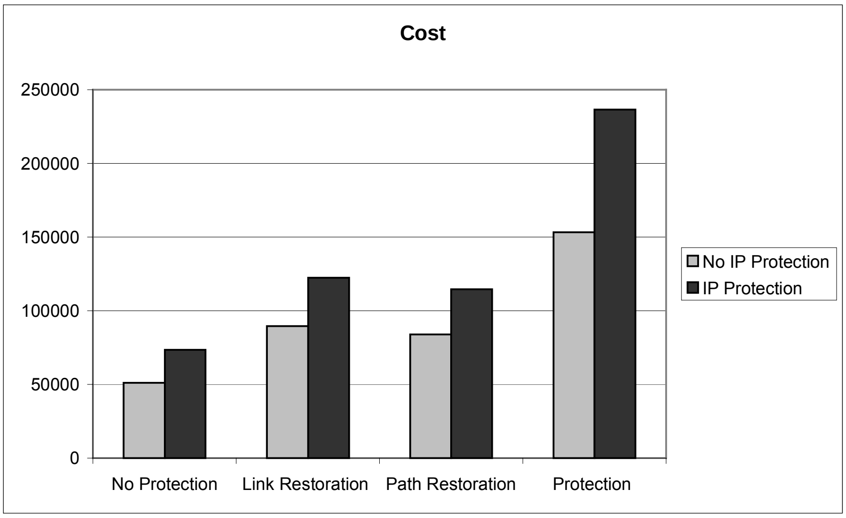


Figure 4-17: Comparison of IP with and without recovery for the different recovery mechanisms in the server layer (OTN): cost

On average, the cost of the design has increased with a factor 1.43 due to the use of local protection in the IP layer. The exact increase factor for the cost is shown in Figure 4-18 for the different back-up schemes.

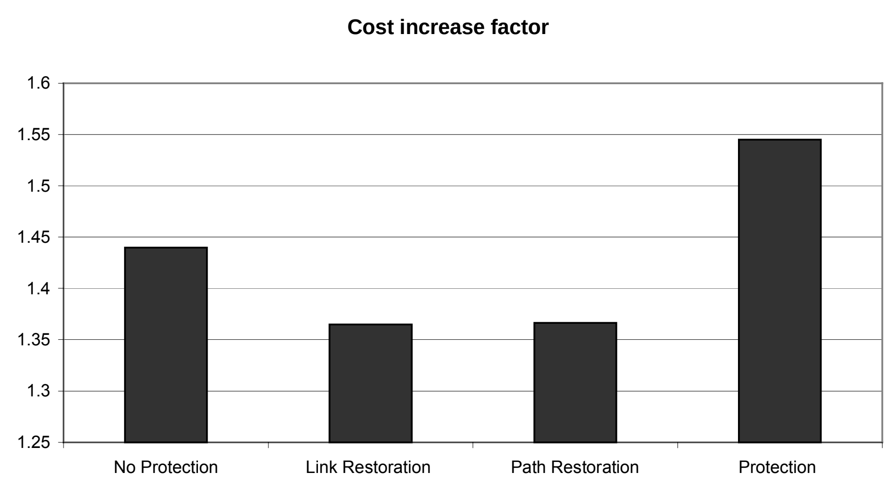


Figure 4-18 Comparison of IP with and without recovery for the different recovery mechanisms in the server layer (OTN): cost increase factor

When comparing the total number of bi-directional line-systems that needs to be installed in the network, only when protection is used in the optical layer there is a difference of 1 line-system between the options with and without local protection in the IP layer. For all other cases the same number of line-systems is obtained.

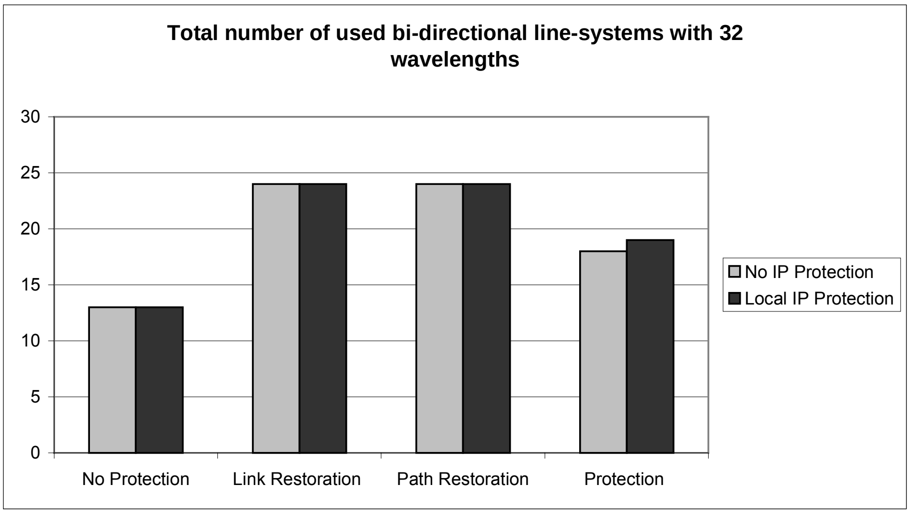


Figure 4-19: Comparison of IP with and without recovery for the different recovery mechanisms in the server layer (OTN): used line-systems

We can again compare the filling for the case no protection is used in the optical layer. On average, the channels are better used, compared with the previous design (see Section 4.3.2.1.2. The average filling rate is now 84.18%. The maximum filling rate over all channels is 95.90%. As a consequence, this network design can cope with less traffic variation (or peak-to-average variation).

4.3.2.2.3 Comparison

The remarks concerning the differences between MPλS and “classical” optical networking on the number of used wavelength channels and the number of used line-systems as in section 4.3.2.1.2 remain valid:

MPλS performs better in total number of used wavelength channels.

“Classical” optical networking performs better in number of used line-systems than MPλS, due to the characteristics of the respective design tools, although the results differ not as much as in section 4.3.2.1.2, especially when path protection is used.

MPλS is the cheaper solution, when cost is calculated as the number of channels on a link multiplied with the length of the respective link. This is again a result of the used design tools, as explained in section 4.3.2.1.3

5 Main indications and guidelines

In this Section some first indications and general guidelines are given, referring to the specific cases as they were planned.

5.1 Indications from the design of the case studies

In section 2 a criteria based on a classification structured on three levels has been proposed in order to identify real world case studies. From the higher to the lower level the classification implyes the following classification items: *Context, Scenario and Case study*. Two contexts, a metro network and a national backone, are introduced. For each context a number of scenarios/ case studies have been defined taking also into account a migration perspective from a multilayer network structure (with SDH as a in-beetween layer) towards a more integrated solutions (IP directly on WDM).

It was not simple to think of and to produce with significant and complete characterizations of such new networks. One main reason was that it is still hard to collect concrete topological and traffic distribution models and references. Then, rather than drawing up complex and articulate configurations, our policy was trying to identify at first simple and preliminary case studies. In this selection phase, the policy was trying to follow, for the scenarios as well as for the single case studies, the most probable evolutionary and migratory trace. These basic modules could then be reproduced or combined, with proper modifications, up to constitute a larger or an entire network.

5.2 Issues raised by performing the planning studies

Section 2 already provided a lot of detailed information for the different case studies. Nevertheless, by performing the network planning studies, being described in section 4, we have shown that there is still a gap in this large bunch of detailed information.

First of all, section 4.1.1 and 4.2.3 make different assumptions and calculations on packet inter-arrival time and size distributions. After being agreed, the necessary information should be included in the case study definitions. Also we should look in the literature for and perhaps develop the appropriate mathematical models to compute for example equivalent bandwidths.

Secondly, several services have been defined. However, no clear information is available on the importance of each service compared to other services. For example, the section 4.2.3 (“obtained results”) has assumed that both video and phone service are assigned the high priority (and thus it is expected that both their traffic will be dropped equally in the case of capacity shortage during a failure).

Thirdly, there is no agreement yet on the equipment models and corresponding cost structures. For example, section 4.1.3 assumed compact ADMs for the SDH ring networks.

The studies in section 4 also raised some concrete issues concerning a practical planning approach:

As mentioned already, some mathematical models are needed to compute for example equivalent bandwidths. But another issue regarding the traffic, is the asymmetric nature of IP traffic. If a tool requires symmetric traffic, then the traffic should be made symmetric: the question is of course, if this has to be done directly on the IP traffic matrix or when calculating the demand for the transmission network (this was the case in section 4.3). And if asymmetric is routed in a layer, then both directions have to be routed independently or along the same path.

How to design the logical network(s)? Is it actually a good idea to consider a predefined logical topology (as was assumed in section 4.1 and 4.3). If yes, then does the cost for each unit of capacity per link have to be estimated/calculated, based on the server layer (as was done in section 4.1) or can the IP network consider minimal hop routing (as in section 4.3)?

Finally, section 4.3.2.2 illustrated that considering router failures can have a significant impact on the overall network cost. Thus, the following question is raised: which failure scenarios have to be taken into account and in which layer is each failure scenario resolved? This consideration has to be made, even if a truly integrated multilayer planning approach is practically infeasible.

Not only section 4.1 and 4.3 raised some concrete issues regarding a practical planning methodology. Section 4.2 presented a rather unconventional planning methodology, based on simulations. We should carefully think about the applicability of such methodology: section 4.2 showed that such methodology could be rather promising (in some cases).

5.3 Indications from the Metropolitan Scenario1/Case study 1 planning

We can get these first indications:

- As resulting from the planning reports, we can observe that traffic demands and consequent infrastructure needs are not uniformly distributed along the transport network: some nodes communicate more than others, they need a higher bandwidth, and consequently a major number of SDH and WDM systems. Then, a topology pre-planning would be opportune. It would be very useful to perform an optimisation for the transport network topology in terms of link capacities, structure of each ring, points of interconnections between rings and other architectural details, that at moment must be assigned from the user.
- The flows protection for the transport network, inside this case study, is 1+1 Drop&Continue. This type of protection assures the highest-level protection for a SDH rings network, allowing to recover multiple failures. On the other hand, an equivalent grade of resilience cannot be guaranteed by the IP network planning. Indeed, the optimal IP network structure doesn’t take into account any diversity criterion to face with link or node failures. Then, at moment, it is not possible to carry out a project taking into account resilience requirements that are reasonably balanced among client and transport layers.

5.4 Indications from the Metropolitan Scenario3/Case study 1 planning

Simulations done over the scenario 3 shown that the current available DPT equipment, which works at 622 Mbps and cannot support WDM, cannot cope with the requirements established in Section 2.2 for a MAN context.

We have carried out simulations for 622 Mbps (OC-12) and the higher bit rates that Cisco will put in place in the near future: 2.5 Gbps (OC-48) and 10 Gbps (OC-192).

As a result:

1. at 622 Mbps neither the phone nor the video service can be guaranteed.
2. at 2.5 and 10 Gbps all services can be supported, but there is a limitation in the percentage of inhabitants that can be served.

5.5 Indications from the Long Distance Scenario2/Case Study1 planning

In conclusion we can say that for the MPλS case, the various recovery mechanisms perform as expected. The shared mechanisms need less wavelength channels (lambdas) and are cheaper than the protection schemes. However, the number of needed 32-wavelength line-systems is not very different over the different schemes. Using node protection in the IP layer increases the cost by a factor of about 1.4. This has however no influence on the number of 32-wavelength line-systems that are needed in the network.

For the “classical” optical networking solution, path restoration gives the best results, although the difference with link restoration is quite small (both in number of used wavelength channels as in cost). Also in this case the cost due to protection in the IP layer is 1.45 times higher compared to the case where the IP routers are not protected.

“Classical” optical networking uses less 32-wavelength line-systems compared to the MPλS solution, but MPλS performs better when comparing the number of used wavelength channels (lambdas) and the cost. It is important to note that these results are partially caused by the different goals of the respective design tools. As mentioned before, WDMNetDesign routes bi-directional symmetrical connections and optimizes the number of used line-systems, while the MPLS/MPλS tool routes unidirectional connections and uses a shortest path algorithm, without optimization.

A better comparison between both solutions would be possible with a “classical” optical network design tool that is able to take unidirectional and asymmetrical traffic as input.

6 APPENDICES

Appendix M_1: Interconnection nodes

In the following figure it is described the structure of an Interconnection node, in which we can find both ADM and WDM equipment.

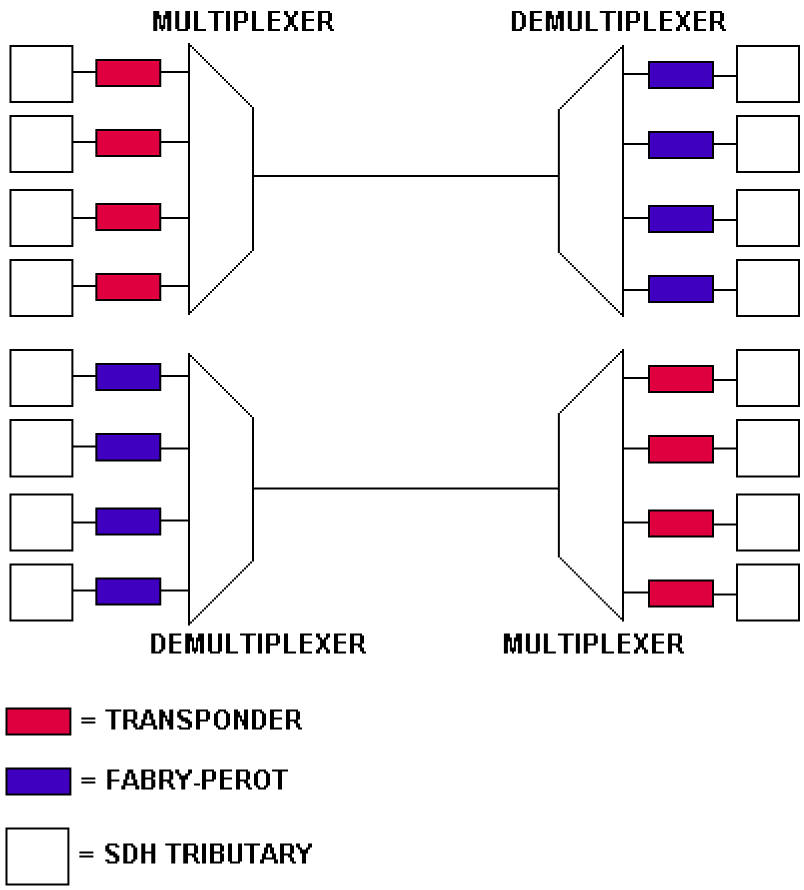


Figure M_1-1: Interconnection node structure with a WDM 4 point-to-point technology

WDM 4 technology allows the operator to multiplex 4 SDH systems on the same fiber. In these kinds of node it is necessary to put some others components, like some Transponders, one for each wavelength to multiply, and some Fabry-Perot filters, one for each wavelength to demultiply.

Appendix M_2: Traffic Matrixes and logical distances in the Metropolitan Context

M_2.1 Traffic matrices

Estimating the **web browsing** traffic flows is simpler than the other services flows, because, in the described network, the http dedicated server is only one and the flows are not mediated by other nodes. So we can suppose that every flow is directed from the http server to the router connected to the interested part and vice versa. In the following tables the web browsing flows per part are listed.

Source	Destination	IP flows (bit/s)	Total Flow (Mbit/s)
Server 1	Router1	105000*3950	414.75
Server 1	Router2	52500*3950	207.375
Server 1	Router3	35000*3950	138.25
Server 1	Router4	70000*3950	276.5
Server 1	Router5	56000*3950	221.2
Server 1	Router6	42000*3950	165.9
Server 1	Router6	28000*3950	110.6
Server 1	Router7	70000*3950	276.5
Server 1	Router9	24500*3950	96.775
Server 1	Router10	63000*3950	248.85
			2156.7

Table M_2-1: Web browsing service supplying flows per origin and destination

Source	Destination	IP flows (bit/s)	Total Flow (Mbit/s)
Router1	Server 1	105000*395	41.475
Router2	Server 1	52500*395	20.735
Router3	Server 1	35000*395	13.825
Router4	Server 1	70000*395	27.65
Router5	Server 1	56000*395	22.12
Router6	Server 1	42000*395	16.59
Router6	Server 1	28000*395	11.06
Router7	Server 1	70000*395	27.65
Router9	Server 1	24500*395	9.6775
Router10	Server 1	63000*395	24.885

			215.945

Table M_2-2: Web browsing service request flows per origin and destination

Estimating the http based service flows is more complex, because there are some relations between every routers. Two important considerations must be done:

The service penetration is 70%

Flow numbers between two router is controlled by the **percentage** parameter, that means how many people of the interested part (70% of the total part) request services to the destination router

In the following table are shown the flows related with the **service request** traffic

Origin	**Destination**	**Percentage**	**Flows number**	**Flows (bit/sec)**	**Flows (Mbit/s)**
Router 1 interested part : 105000					
Router1	Router2	15%	15750	15750*400	6.3
Router1	Router3	10%	10500	10500*400	4.2
Router1	Router4	5%	5250	5250*400	2.1
Router1	Router5	20%	21000	21000*400	8.4
Router1	Router6	2%	2100	2100*400	0.84
Router1	Router7	18%	18900	18900*400	7.56
Router1	Router8	3%	3150	3150*400	1.26
Router1	Router9	7%	7350	7350*400	2.94
Router1	Router10	20%	21000	21000*400	8.4
Router 2 interested part: 52500					
Router2	Router1	15%	7875	7875*400	3.15
Router2	Router3	13%	6825	6825*400	2.73
Router2	Router4	17%	8925	8925*400	3.57
Router2	Router5	1%	525	525*400	0.21
Router2	Router6	9%	4725	4725*400	1.89
Router2	Router7	5%	2625	2625*400	1.05
Router2	Router8	20%	10500	10500*400	4.2
Router2	Router9	16%	8400	8400*400	3.36
Router2	Router10	4%	2100	2100*400	0.84
Router 3 interested part: 35000					
Router3	Router1	8%	2800	2800*400	1.12
Router3	Router2	3%	1050	1050*400	0.42

Router3	Router4	12%	4200	4200*400	1.68
Router3	Router5	27%	9450	9450*400	3.78
Router3	Router6	--	--	--	--
Router3	Router7	14%	4900	4900*400	1.96
Router3	Router8	3%	1050	1050*400	0.42
Router3	Router9	13%	4550	4550*400	1.82
Router3	Router10	20%	7000	7000*400	2.8
Router 4 interested part: 70000					
Router4	Router1	5%	3500	3500*400	1.4
Router4	Router2	17%	9800	9800*400	3.92
Router4	Router3	12%	8400	8400*400	3.36
Router4	Router5	15%	10500	10500*400	4.2
Router4	Router6	3%	2100	2100*400	0.84
Router4	Router7	28%	19600	19600*400	7.84
Router4	Router8	2%	1400	1400*400	0.56
Router4	Router9	14%	9800	9800*400	3.92
Router4	Router10	4%	2800	2800*400	1.12
Router 5 interested part: 56000					
Router5	Router1	20%	11200	11200*400	4.48
Router5	Router2	1%	560	560*400	0.224
Router5	Router3	27%	15120	15120*400	6.048
Router5	Router4	15%	8400	8400*400	3.36
Router5	Router6	7%	3920	3920*400	1.568
Router5	Router7	13%	7280	7280*400	2.912
Router5	Router8	5%	2800	2800*400	1.12
Router5	Router9	2%	1120	1120*400	0.448
Router5	Router10	10%	5600	5600*400	2.24
Router 6 interested part: 70000					
Router6	Router1	3%	2100	2100*400	0.84
Router6	Router2	11%	7700	7700*400	3.08
Router6	Router3	--	--	--	--
Router6	Router4	9%	6300	6300*400	2.52
Router6	Router5	27%	18900	18900*400	7.56
Router6	Router7	10%	7000	7000*400	2.8
Router6	Router8	25%	17500	17500*400	7
Router6	Router9	5%	3500	3500*400	1.4
Router6	Router10	10%	7000	7000*400	2.8
Router 7 interested part 70000					
Router7	Router1	15%	10500	10500*400	4.2

Router7	Router2	6%	4200	4200*400	1.68
Router7	Router3	12%	8400	8400*400	3.36
Router7	Router4	30%	21000	21000*400	8.4
Router7	Router5	10%	7000	7000*400	2.8
Router7	Router6	8%	5600	5600*400	2.24
Router7	Router8	5%	3500	3500*400	1.4
Router7	Router9	4%	2800	2800*400	1.12
Router7	Router10	10%	7000	7000*400	2.8
Router 8 interested part : 0					
Router8	Router1	--	--	--	--
Router8	Router2	--	--	--	--
Router8	Router3	--	--	--	--
Router8	Router4	--	--	--	--
Router8	Router5	--	--	--	--
Router8	Router6	--	--	--	--
Router8	Router7	--	--	--	--
Router8	Router9	--	--	--	--
Router8	Router10	--	--	--	--
Router 9 interested part : 24500					
Router9	Router1	3%	735	735*400	0.294
Router9	Router2	16%	3920	3920*400	1.568
Router9	Router3	13%	3185	3185*400	1.274
Router9	Router4	14%	3430	3430*400	1.372
Router9	Router5	3%	735	735*400	0.294
Router9	Router6	4%	980	980*400	0.392
Router9	Router7	6%	1470	1470*400	0.588
Router9	Router8	11%	2695	2695*400	1.078
Router9	Router10	30%	7350	7350*400	2.94
Router 10 interested part: 63000					
Router10	Router1	20%	12600	12600*400	5.04
Router10	Router2	4%	2520	2520*400	1.008
Router10	Router3	20%	12600	12600*400	5.04
Router10	Router4	4%	2520	2520*400	1.008
Router10	Router5	10%	6300	6300*400	2.52
Router10	Router6	10%	6300	6300*400	2.52
Router10	Router7	10%	6300	6300*400	2.52
Router10	Router8	--	--	--	--
Router10	Router9	22%	13860	13860*400	5.544

Table M_2-3: http based service supplying flows per origin and destination

In the following table are shown the flows related with the **service supplying** traffic This kind of flows is strictly connected to the service request flows.

Origin	Destination	Flows number	Flows (bit/sec)	Flows (Mbit/s)
Router1	Router2	7875	7875*4000	31.5
Router1	Router3	2800	2800*4000	11.2
Router1	Router4	3500	3500*4000	14
Router1	Router5	11200	11200*4000	44.8
Router1	Router6	2100	2100*4000	8.4
Router1	Router7	10500	10500*4000	42
Router1	Router8	--	--	--
Router1	Router9	735	735*4000	2.94
Router1	Router10	12600	12600*4000	50.4
Router2	Router1	15750	15750*4000	63
Router2	Router3	1050	1050*4000	4.2
Router2	Router4	9800	9800*4000	39.2
Router2	Router5	560	560*4000	2.24
Router2	Router6	7700	7700*4000	30.8
Router2	Router7	4200	4200*4000	16.8
Router2	Router8	--	--	--
Router2	Router9	3920	3920*4000	15.68
Router2	Router10	2520	2520*4000	10.08
Router3	Router1	10500	10500*4000	42
Router3	Router2	6825	6825*4000	27.3
Router3	Router4	8400	8400*4000	33.6
Router3	Router5	15120	15120*4000	60.48
Router3	Router6	--	--	--
Router3	Router7	8400	8400*4000	33.6
Router3	Router8	--	--	--
Router3	Router9	3185	3185*4000	12.74
Router3	Router10	12600	12600*4000	50.4
Router4	Router1	5250	5250*4000	21
Router4	Router2	8925	8925*4000	35.7
Router4	Router3	4200	4200*4000	16.8

Router4	Router5	8400	8400*4000	33.6
Router4	Router6	6300	6300*4000	25.2
Router4	Router7	21000	21000*4000	84
Router4	Router8	--	--	--
Router4	Router9	3430	3430*4000	13.72
Router4	Router10	2520	2520*4000	10.08
Router5	Router1	21000	21000*4000	84
Router5	Router2	525	525*4000	2.1
Router5	Router3	9450	9450*4000	37.8
Router5	Router4	10500	10500*4000	42
Router5	Router6	18900	18900*4000	75.6
Router5	Router7	7000	7000*4000	28
Router5	Router8	--	--	--
Router5	Router9	735	735*4000	2.94
Router5	Router10	6300	6300*4000	25.2
Router6	Router1	2100	2100*4000	8.4
Router6	Router2	4725	4725*4000	18.9
Router6	Router3	--	--	--
Router6	Router4	2100	2100*4000	8.4
Router6	Router5	3920	3920*4000	15.68
Router6	Router7	5600	5600*4000	22.4
Router6	Router8	--	--	--
Router6	Router9	980	980*4000	3.92
Router6	Router10	6300	6300*4000	25.2
Router7	Router1	18900	18900*4000	75.6
Router7	Router2	2625	2625*4000	10.5
Router7	Router3	4900	4900*4000	19.6
Router7	Router4	19600	19600*4000	78.4
Router7	Router5	7280	7280*4000	29.12
Router7	Router6	7000	7000*4000	28
Router7	Router8	--	--	--
Router7	Router9	1470	1470*4000	5.88
Router7	Router10	6300	6300*4000	25.2
Router8	Router1	3150	3150*4000	12.6
Router8	Router2	10500	10500*4000	42

Router8	Router3	1050	1050*4000	4.2
Router8	Router4	1400	1400*4000	5.6
Router8	Router5	2800	2800*4000	11.2
Router8	Router6	17500	17500*4000	70
Router8	Router7	3500	3500*4000	14
Router8	Router9	2695	2695*4000	10.78
Router8	Router10	--	--	--
Router9	Router1	7350	7350*4000	29.4
Router9	Router2	8400	8400*4000	33.6
Router9	Router3	4550	4550*4000	18.2
Router9	Router4	9800	9800*4000	39.2
Router9	Router5	1120	1120*4000	4.48
Router9	Router6	3500	3500*4000	14
Router9	Router7	2800	2800*4000	11.2
Router9	Router8	--	--	--
Router9	Router10	7350	7350*4000	29.4
Router10	Router1	21000	21000*4000	84
Router10	Router2	2100	2100*4000	8.4
Router10	Router3	7000	7000*4000	28
Router10	Router4	2800	2800*4000	11.2
Router10	Router5	5600	5600*4000	22.4
Router10	Router6	7000	7000*4000	28
Router10	Router7	7000	7000*4000	28
Router10	Router8	--	--	--
Router10	Router9	7350	7350*4000	29.4

Table M_2-4: http based service request flows per origin and destination

For the **e-mail service** traffic flows estimation, it is necessary to assign a source and a destination to each flow. In the next table the e-mail traffic flows are described, with their origin, destination, the server in which they transit, and the percentage of users.

Origin	Destination	Transit	Percentage	Flows number	Flows (bit/sec)	Flows (Mbit/s)

ROUTER 1 SERVES PART 1 AND PART 2 (150000 INHABITANTS) **100% OF INHABITANTS USE MAIL SERVICE**						
Router1	Router2	Server1	15%	22500	22500 * 500	11.25
Router1	Router3	Server1	10%	15000	15000*500	7.5
Router1	Router4	Server1	5%	7500	7500*500	3.75
Router1	Router5	Server1	20%	30000	30000*500	15
Router1	Router6	Server1	2%	3000	3000*500	1.5
Router1	Router7	Server1	18%	27000	27000*500	13.5
Router1	Router8	Server1	--	--	--	--
Router1	Router9	Server1	10%	15000	15000*500	7.5
Router1	Router10	Server1	20%	30000	30000*500	15
ROUTER 2 SERVES PART 3 (75000 INHABITANTS)						
Router2	Router1	Server1	15%	11250	11250*500	5.62
Router2	Router3	Server1	13%	9750	9750*500	4.875
Router2	Router4	Server1	17%	12750	12750*500	6.375
Router2	Router5	Server1	1%	750	750*500	0.375
Router2	Router6	Server1	9%	6750	6750*500	3.375
Router2	Router7	Server1	25%	18750	18750*500	9.375
Router2	Router8	Server1	--	--	--	--
Router2	Router9	Server1	16%	12000	12000*500	6
Router2	Router10	Server1	4%	3000	3000*500	1.5
ROUTER 3 SERVES PART 4 (50000 INHABITANTS)						
Router3	Router1	Server1	8%	4000	4000*500	2
Router3	Router2	Server1	3%	1500	1500*500	0.75
Router3	Router4	Server1	12%	6000	6000*500	3
Router3	Router5	Server1	27%	13500	13500*500	6.75
Router3	Router6	Server1	--	--	--	--
Router3	Router7	Server1	17%	8500	8500*500	4.25
Router3	Router8	Server1	--	--	--	--
Router3	Router9	Server1	13%	6500	6500*500	3.25
Router3	Router10	Server1	20%	10000	10000*500	5
ROUTER 4 SERVES PART 5 (100000 INHABITANTS)						
Router4	Router1	Server1	5%	5000	5000*500	2.5
Router4	Router2	Server1	17%	17000	17000*500	8.5
Router4	Router3	Server1	12%	12000	12000*500	6
Router4	Router5	Server1	15%	15000	15000*500	7.5

Router4	Router6	Server1	3%	3000	3000*500	1.5
Router4	Router7	Server1	28%	28000	28000*500	14
Router4	Router8	Server1	--	--	--	--
Router4	Router9	Server1	16%	16000	16000*500	8
Router4	Router10	Server1	4%	4000	4000*500	2
ROUTER 5 SERVES PART6 (80000 INHABITANTS)						
Router5	Router1	Server1	20%	16000	16000*500	8
Router5	Router2	Server1	1%	800	800*500	0.4
Router5	Router3	Server1	27%	21600	21600*500	10.8
Router5	Router4	Server1	15%	12000	12000*500	6
Router5	Router6	Server1	7%	5600	5600*186	2.8
Router5	Router7	Server1	18%	14400	14400*500	7.2
Router5	Router8	Server1	--	--	--	--
Router5	Router9	Server1	2%	1600	1600*500	0.8
Router5	Router10	Server1	10%	8000	8000*500	4
ROUTER 6 SERVES PART 7,8 (100000 INHABITANTS)						
Router6	Router1	Server1	3%	3000	3000*500	1.5
Router6	Router2	Server1	11%	11000	11000*500	5.5
Router6	Router3	Server1	--	--	--	--
Router6	Router4	Server1	9%	9000	9000*500	4.5
Router6	Router5	Server1	27%	27000	27000*500	13.5
Router6	Router7	Server1	10%	100000	10000*500	5
Router6	Router8	Server1	--%	--	--	--
Router6	Router9	Server1	30%	30000	30000*500	15
Router6	Router10	Server1	10%	10000	10000*500	5
ROUTER 7 SERVES PART 9 (100000 INHABITANTS)						
Router7	Router1	Server1	15%	15000	15000*500	7.5
Router7	Router2	Server1	6%	6000	6000*500	3
Router7	Router3	Server1	12%	12000	12000*500	6
Router7	Router4	Server1	30%	30000	30000*500	15
Router7	Router5	Server1	10%	10000	10000*500	5
Router7	Router6	Server1	13%	13000	13000*500	6.5
Router7	Router8	Server1	--	--	--	--
Router7	Router9	Server1	4%	40000	4000*500	2
Router7	Router10	Server1	10%	100000	10000*500	5

Router8	Router1	Server1	--	--	--	--
Router8	Router2	Server1	--	--	--	--
Router8	Router3	Server1	--	--	--	--
Router8	Router4	Server1	--	--	--	--
Router8	Router5	Server1	--	--	--	--
Router8	Router6	Server1	--	--	--	--
Router8	Router7	Server1	--	--	--	--
Router8	Router9	Server1	--	--	--	--
Router8	Router10	Server1	--	--	--	--
ROUTER 9 SERVES PART 10 (35000 INHABITANTS)						
Router9	Router1	Server1	3%	1050	1050*500	0.525
Router9	Router2	Server1	16%	5600	5600*500	2.8
Router9	Router3	Server1	13%	4550	4550*500	2.275
Router9	Router4	Server1	14%	4900	4900*500	2.45
Router9	Router5	Server1	3%	1050	1050*500	0.525
Router9	Router6	Server1	4%	1400	1400*500	0.7
Router9	Router7	Server1	17%	5950	5950*500	2.975
Router9	Router8	Server1	--	--	--	--
Router9	Router10	Server1	30%	10500	10500*500	5.25
ROUTER 10 SERVES PART 11 (90000 INHABITANTS)						
Router10	Router1	Server1	20%	18000	18000*500	9
Router10	Router2	Server1	4%	3600	3600*500	1.8
Router10	Router3	Server1	20%	18000	18000*500	9
Router10	Router4	Server1	4%	3600	3600*500	1.8
Router10	Router5	Server1	10%	9000	9000*500	4.5
Router10	Router6	Server1	10%	9000	9000*500	4.5
Router10	Router7	Server1	10%	9000	9000*500	4.5
Router10	Router8	Server1	--	--	--	--
Router10	Router9	Server1	22%	19800	19800*500	9.9

Legenda:

Origin: origin router

Destination: destination router

Transit: transit service (because it is a server mediated service)

Percentage: percentage of the interested people that use the service from the considered origin to the considered destination.

Flows number: number of flows. It is calculated as: number of (inhabitants * percentage of interested people to this service * percentage of people that use this service from that origin to that destination)

Flows: this field represent the bit rate in bit per second

Table M_2-5: E-mail flows

In the following table are shown the flows related with the **phone traffic.** This kind of service has a penetration of 10%.

Origin	Destination	Percentage	Flows number	Flows (bit/sec)	Flows (Mbit/s)
ROUTER 1 : Interested people 15000					
Router1	Router2				
Router1	Router3				
Router1	Router4	33%	4950	4950*22400	110.88
Router1	Router5				
Router1	Router6	33%	4950	4950*22400	110.88
Router1	Router7				
Router1	Router8				
Router1	Router9	34%	5100	5100*22400	114.24
Router1	Router10				
ROUTER 4 : Interested part 10000					
Router4	Router1	33%	3300	3300*22400	73.92
Router4	Router2				
Router4	Router3				
Router4	Router5				
Router4	Router6	34%	3400	3400*22400	76.16
Router4	Router7				
Router4	Router8				
Router4	Router9	33%	3300	3300*22400	73.92
Router4	Router10				
ROUTER 6 : Interested part 4000					
Router6	Router1	33%	1320	1320*22400	29.568
Router6	Router2				
Router6	Router3				
Router6	Router4	34%	1360	1360*22400	30.464
Router6	Router5				
Router6	Router7				
Router6	Router8				
Router6	Router9	33%	1320	1320*22400	29.568

Router6	Router10				
ROUTER 9 SERVES PART 10 (3500 INHABITANTS) **Because the 10% of inhabitants use phone service**					
Router9	Router1	34%	1190	1190*22400	26.656
Router9	Router2				
Router9	Router3				
Router9	Router4	33%	1155	1155*22400	25.872
Router9	Router5				
Router9	Router6	33%	1155	1155*22400	25.872
Router9	Router7				
Router9	Router8				
Router9	Router10				

Legenda:

See table M_2-5

Table M_2-6: Telephony flows

For **Video on demand** (low quality) service the following two tables can be applied; the first represents the flows related with the downstream traffic, and the second one with the upstream traffic.

Source	Destination	Total Flow (number)	Total Flow (Mbit/s)
Server 2	Router1		
Server 2	Router2	--	
Server 2	Router3	7500	7500
Server 2	Router4	--	
Server 2	Router5	--	
Server 2	Router6	--	
Server 2	Router7	--	
Server 2	Router8	--	
Server 2	Router9	5250	5250
Server 2	Router10	13500	1350

Table M_2-7: VoD (low quality) downstream flows

Source	Destination	Total Flow (number)	Total Flow (Mbit/s)
Router1	Server2	--	--
Router2	Server 2	--	--

Router3	Server 2	7500	75
Router4	Server 2	--	--
Router5	Server 2	--	--
Router6	Server 2	--	--
Router7	Server 2	--	--
Router8	Server 2	--	--
Router9	Server 2	5250	52.5
Router10	Server 2	13500	135

Table M_2-8: VoD (low quality) upstream flows

For **Video on demand** (high quality) service the following two tables can be applied; the first represents the flows related with the downstream traffic, and the second one with the upstream traffic.

Source	Destination	Total Flow (number)	Total Flow (Mbit/s)
Server 2	Router1		--
Server 2	Router2		--
Server 2	Router3		--
Server 2	Router4		--
Server 2	Router5		--
Server 2	Router6	4000	16000
Server 2	Router7		--
Server 2	Router8		--
Server 2	Router9	3500	14000
Server 2	Router10		--

Table M_2-9: VoD (high quality) downstream flows

Source	Destination	Total Flow (number)	Total Flow (Mbit/s)
Router1	Server 2		--
Router2	Server 2		--
Router3	Server 2		--
Router4	Server 2		--
Router5	Server 2		--
Router6	Server 2	4000	80
Router7	Server 2		--
Router8	Server 2		--
Router9	Server 2	3500	70
Router10	Server 2		--

Table M_2-10: VoD (high quality) upstream flows

Taking into account the preceding traffic estimations, the total traffic flows matrices can be build:

In the following matrices routers in abscissa represent the traffic origin and the routers in ordinate represent the destinations.

	R1	R2	R3	R4	R5	R6	R7	R8	R9	R10	S1	S2	S3
R1	0	0	0	0	0	0	0	0	0	0	414.75		
R2	0	0	0	0	0	0	0	0	0	0	207.35	0	0
R3	0	0	0	0	0	0	0	0	0	0	138.25	0	0
R4	0	0	0	0	0	0	0	0	0	0	276.5	0	0
R5	0	0	0	0	0	0	0	0	0	0	221.2	0	0
R6	0	0	0	0	0	0	0	0	0	0	276.5	0	0
R7	0	0	0	0	0	0	0	0	0	0	276.5	0	0
R8	0	0	0	0	0	0	0	0	0	0	--	0	0
R9	0	0	0	0	0	0	0	0	0	0	96.775	0	0
R10	0	0	0	0	0	0	0	0	0	0	248.85	0	0
S1	41.475	20.735	13.825	27.65	22.12	27.65	27.65	--	9.6775	24.885	0	0	0
S2	0	0	0	0	0	0	0	0	0	0	0	0	0
S3	0	0	0	0	0	0	0	0	0	0	0	0	0

Table M_2-11: Web browsing traffic flows

	R1	R2	R3	R4	R5	R6	R7	R8	R9	R10	S1	S2	S3
R1	0	66.15	43.12	22.4	88.48	9.24	79.8	12.6	29.694	89.04	0	0	0
R2	37.8	--	27.72	39.62	2.324	21.98	12.18	42	35.168	9.408	0	0	0
R3	15.4	6.93	--	20.16	43.848	--	22.96	4.2	19.474	33.04	0	0	0
R4	16.1	42.77	35.28	--	45.36	10.92	86.8	5.6	40.572	12.208	0	0	0
R5	53.2	2.45	64.26	37.8	--	23.24	31.92	11.2	4.774	24.92	0	0	0
R6	9.24	32.69	--	26.04	77.168	--	30.24	70	14.392	30.52	0	0	0
R7	49.56	17.85	35.56	91.84	30.912	25.2	--	14	11.788	30.52	0	0	0
R8	1.26	4.2	0.42	0.56	1.12	7	1.4	--	1.078	--	0	0	0

	R1	R2	R3	R4	R5	R6	R7	R8	R9	R10	S1	S2	S3
R9	5.88	19.04	14.56	17.64	3.388	5.32	7	10.78	--	34.944	0	0	0
R10	58.8	10.92	53.2	11.2	27.44	28	28	--	32.34	--	0	0	0
S1	0	0	0	0	0	0	0	0	0	0	--	0	0
S2	0	0	0	0	0	0	0	0	0	0	0	--	0
S3	0	0	0	0	0	0	0	0	0	0	0	0	--

Table M_2-12: Http based traffic flows

	R1	R2	R3	R4	R5	R6	R7	R8	R9	R10	S1	S2	S3
R1	0	0	0	0	0	0	0	0	0	0	36.645	0	0
R2	0	0	0	0	0	0	0	0	0	0	34	0	0
R3	0	0	0	0	0	0	0	0	0	0	46.45	0	0
R4	0	0	0	0	0	0	0	0	0	0	42.875	0	0
R5	0	0	0	0	0	0	0	0	0	0	96.025	0	0
R6	0	0	0	0	0	0	0	0	0	0	20.875	0	0
R7	0	0	0	0	0	0	0	0	0	0	60.8	0	0
R8	0	0	0	0	0	0	0	0	0	0	--	0	0
R9	0	0	0	0	0	0	0	0	0	0	52.45	0	0
R10	0	0	0	0	0	0	0	0	0	0	37.5	0	0
S1	75	37.495	25	50	40	50	50	0	17.5	45	0	0	0
S2	0	0	0	0	0	0	0	0	0	0	0	0	0
S3	0	0	0	0	0	0	0	0	0	0	0	0	0

Table M_2-13: E-mail traffic flows

	R1	R2	R3	R4	R5	R6	R7	R8	R9	R10	S1	S2	S3
R1	0	0	0	73.92	0	29.568	0	0	26.656	0	0	0	0
R2	0	0	0	0	0	0	0	0	0	0	0	0	0
R3	0	0	0	0	0	0	0	0	0	0	0	0	0

	R1	R2	R3	R4	R5	R6	R7	R8	R9	R10	S1	S2	S3
R4	110.88	0	0	0	0	30.464	0	0	25.872	0	0	0	0
R5	0	0	0	0	0	0	0	0	0	0	0	0	0
R6	110.88	0	0	76.16	0		0	0	25.872	0	0	0	0
R7	0	0	0	0	0	0	0	0	0	0	0	0	0
R8	0	0	0	0	0	0	0	0	0	0	0	0	0
R9	114.24	0	0	73.92	0	29.568	0	0	0	0	0	0	0
R10	0	0	0	0	0	0	0	0	0	0	0	0	0
S1	0	0	0	0	0	0	0	0	0	0	0	0	0
S2	0	0	0	0	0	0	0	0	0	0	0	0	0
S3	0	0	0	0	0	0	0	0	0	0	0	0	0

Table M_2-14: Phone traffic flows

	R1	R2	R3	R4	R5	R6	R7	R8	R9	R10	S1	S2	S3
R1	0	0	0	0	0	0	0	0	0	0	0	0	0
R2	0	0	0	0	0	0	0	0	0	0	0	0	0
R3	0	0	0	0	0	0	0	0	0	0	0	7500	0
R4	0	0	0	0	0	0	0	0	0	0	0	0	0
R5	0	0	0	0	0	0	0	0	0	0	0	0	0
R6	0	0	0	0	0	0	0	0	0	0	0	0	0
R7	0	0	0	0	0	0	0	0	0	0	0	0	0
R8	0	0	0	0	0	0	0	0	0	0	0	0	0
R9	0	0	0	0	0	0	0	0	0	0	0	5250	0
R10	0	0	0	0	0	0	0	0	0	0	0	13500	0
S1	0	0	0	0	0	0	0	0	0	0	0	0	0
S2	0	0	75	0	0	0	0	0	52.5	135	0	0	0
S3	0	0	0	0	0	0	0	0	0	0	0	0	0

Table M_2-15: Video on demand low quality traffic flows

	R1	R2	R3	R4	R5	R6	R7	R8	R9	R10	S1	S2	S3
R1	0	0	0	0	0	0	0	0	0	0	0	0	0
R2	0	0	0	0	0	0	0	0	0	0	0	0	0
R3	0	0	0	0	0	0	0	0	0	0	0	0	0
R4	0	0	0	0	0	0	0	0		0	0	0	0
R5	0	0	0	0	0	0	0	0	0	0	0	0	0
R6	0	0	0	0	0	0	0	0	0	0	0	16000	0
R7	0	0	0	0	0	0	0	0	0	0	0	0	0
R8	0	0	0	0	0	0	0	0	0	0	0	0	0
R9	0	0	0	0	0	0	0	0	0	0	0	14000	0
R10	0	0	0	0	0	0	0	0	0	0	0	0	0
S1	0	0	0	0	0	0	0	0	0	0	0	0	0
S2	0	0	0	0	0	80	0	0	70	0	0	0	0
S3	0	0	0	0	0	0	0	0	0	0	0	0	0

Table M_2-16: Video on demand high quality traffic flows

M_2.2 Logical distances/costs matrices

The table below reports an estimation of the costs of the IP level connections. The weight is given by the number of rings to be run along the underlying transport network, as configured for the Metropolitan scenario 1.

	R1	R2	R3	R4	R5	R6	R7	R8	R9	R10	S1	S2	S3
R1	--	3	3	3	4	3	3	2	2	2	2	2	2
R2	3	--	1	1	4	3	3	4	4	4	2	2	2
R3	3	1	--	1	4	3	3	4	4	4	2	2	2
R4	3	1	1	--	4	3	3	4	4	4	2	2	2
R5	4	4	4	4	--	2	2	5	5	5	3	3	3
R6	3	3	3	3	2	--	1	4	4	4	2	2	2
R7	3	3	3	3	2	1	--	4	4	4	2	2	2
R8	2	4	4	4	5	4	4	--	1	1	3	3	3
R9	2	4	4	4	5	4	4	1	--	1	3	3	3
R10	2	4	4	4	5	4	4	1	1	--	3	3	3
S1	2	2	2	2	3	2	2	3	3	3	--	1	1
S2	2	2	2	2	3	2	2	3	3	3	1	--	1
S3	2	2	2	2	3	2	2	3	3	3	1	1	--

Table M_2-17: logical distance/cost matrix for metro scenario1

The table below reports an estimation of the costs of the IP level connections. The weight is given by the number of rings to be run along the underlying transport network, as configured for the Metropolitan scenario 2.

	R1	R2	R3	R4	R5	R6	R7	R8	R9	R10	S1	S2	S3
R1	--	3	3	3	3	3	3	1	1	1	2	2	2
R2	3	--	1	1	3	3	3	3	3	3	2	2	2
R3	3	1	--	1	3	3	3	3	3	3	2	2	2
R4	3	1	1	--	3	3	3	3	3	3	2	2	2
R5	3	3	3	3	--	1	1	3	3	3	2	2	2
R6	3	3	3	3	1	--	1	3	3	3	2	2	2
R7	3	3	3	3	1	1	--	3	3	3	2	2	2

	R1	R2	R3	R4	R5	R6	R7	R8	R9	R10	S1	S2	S3
R8	1	3	3	3	3	3	3	--	1	1	2	2	2
R9	1	3	3	3	3	3	3	1	--	1	2	2	2
R10	1	3	3	3	3	3	3	1	1	--	2	2	2
S1	2	2	2	2	2	2	2	2	2	2	--	1	1
S2	2	2	2	2	2	2	2	2	2	2	1	--	1
S3	2	2	2	2	2	2	2	2	2	2	1	1	--

Table M_2-18: logical distance/cost matrix for metro scenario 2

Appendix M_3: Metropolitan Scenario1 /case study 1

M_3.1 Other results from the Metropolitan IP network planning

Delays

Table M_3-1 [delays] shows the mean packet delays in [ms] on each planned edge of the topology. About end-to-end packet delays the best relation has less than 1 microsecond (0.26 μs from R2 to S2) while the worst case is 0.678 ms for packets from R2 to R10.

Table M_3-1 [delays]: packet delay in [ms] on the topology edges

	R1	R2	R3	R4	R5	R6	R7	R8	R9	R10	S1	S2	S3
R1		0,1108	0,0640				0,0235	0,0608	0,4032	0,1223	0,0223		
R2	0,0986		0,0808			0,0831						0,0166	
R3	0,0767	0,0955		0,1082	0,0924		0,0726			0,0832		0,0009	
R4			0,0884		0,0738								
R5			0,0771	0,0780									
R6		0,0773			0,0468		0,1882	0,0613				0,0005	
R7	0,0222		0,0669	0,1219		0,0282		0,0596					
R8	0,0843				0,0729	0,0982	0,0636		0,0639	0,0714			
R9	0,0962							0,0596		0,2150		0,0259	
R10	0,2733		0,0713	0,0649				0,0680	0,0623		0,2741		
S1	0,2741			0,0512						0,0249		0,0088	na
S2		0,0249	0,0044	0,0171		0,2707			0,2398		0,0041		na
S3											na	na	

In most of the cases values of packet delays are very low (GoS is 1 ms) because the link utilization (the ratio between the carried traffic and the payload of the link) are generally low. Table M_3-2 [utilization] reports the utilization of the links (or set of links) in both the directions. The mean value of utilization is generally rather low, and this is for two reasons: firstly the traffic requirements are not symmetrical while SDH circuits used to interconnect the routers are symmetrical, secondly the bandwidth granularity in SDH is rather poor. The **mean utilization of transmission network resources is 39.7 %.** The planned network shows high value of link utilization (next to 100%) between video server S2 and R3, R6 and R9 routers, due to high load of video stream downloading, and very low values in the opposite direction (few percents) because in upload direction the low traffic requirements can’t load the huge symmetrical pipes.

Table M_3-2 [utilization]: link utilization on the topology edges

	R1	R2	R3	R4	R5	R6	R7	R8	R9	R10	S1	S2	S3
R1		56,2%	10,8%				46,6%	3,8%	89,5%	61,1%	42,8%		
R2	49,5%		35,0%			37,3%						15,5%	
R3	30,4%	47,5%		55,0%	45,3%		25,0%			37,5%			
R4			42,1%		26,6%		64,5%			8,3%			
R5			30,9%	32,0%		46,4%		20,1%					
R6		25,7%			76,1%		94,5%	4,9%				2,4%	
R7	42,5%		16,2%	60,9%		57,2%		1,0%					

R8	38,5%				25,4%	49,2%	9,9%		10,5%	23,3%			
R9	48,0%							1,1%		99,8%		2,9%	
R10	84,2%		23,3%	12,5%				18,0%	1,5%		12,3%		
S1	96,3%			78,4%						50,4%		67,0%	
S2		50,2%	84,7%	19,0%		99,9%			99,9%		15,0%		
S3													

Routing

The routing plan derives directly by the weight assigned to each edge by the program. The weights assigned by the program to each edge is shown in table M_3-3 [edge weights for routing plan].

According to a shortest path algorithm that applies the weighting factors reported in table M_3-3 [edge weights for routing plan] the route of any traffic flow requires at most 3 links (2 intermediate node). In particular for the relevant traffic flows (not null) we have 50 one link paths, 40 two links paths and 12 three link paths.

Table M_3-3 [edge weights for routing plan]: value of edge weights to be used for a shortest path algorithm in IP metro network

	R1	R2	R3	R4	R5	R6	R7	R8	R9	R10	S1	S2	S3
R1		21,5	21,7				19,7	14,5	14,4	14,4	13,0		
R2	21,5		7,3			21,6						13,1	
R3	21,7	7,3		6,6	28,7		21,8			28,8		11,3	
R4			6,6		28,8		21,5			28,6	12,2	14,4	
R5			28,7	28,8		13,0		36,0					
R6		21,6			13,0		6,5	28,7				11,3	
R7	19,7		21,8	21,5		6,5		29,3					
R8	14,5				36,0	28,7	29,3		7,6	7,4			
R9	14,4							7,6		5,7		17,0	
R10	14,4		28,8	28,6				7,4	5,7		19,6		
S1	13,0			12,2						19,6		6,1	1,0
S2		13,1	11,3	14,4		11,3			17,0		6,1		1,0
S3											1,0	1,0	

Switching equipment

Traffic load and interface card requirements of IP nodes are reported in Table M_3-4 [figures about routers].

The table reports for each node the amount of switched packets in million packet per second, the total throughput which include the terminating traffic plus the transit traffic, the percentage of transit traffic and the number of interface cards required on each site.

Nodes R1, R2, R4, R5, R7 have requirements in terms of throughput and interfaces compatible with today commercial available routers (throughput is less than 2 Gbit/s and few interface cards not fast than STM4 is required).

Nodes R3, R6, R9 and R10 as well as S2 and S3, switch a large amount of bandwidth and require many high bandwidth interfaces (up to 60 Gbit/s and up to 7 STM64 interface cards). In practical implementation we could be think those sites, at least the greatest among them (S2), as cluster of Giga-Switch-Routers that could be locally interconnected via GbitEthernet LAN.

About the transit traffic switched by the routers the network seems to switch the traffic towards the destination quite efficiently (i.e. without much effort of Layer 3 switching on intermediate nodes). Only the R8 shows a consistent percentage of transit traffic (40%). In fact R8 works as a tandem for video streaming traffic coming from S2 and directed to R10. Other nodes have not very high or low percentages of transit traffic.

Table M_3-4 [figures about routers]

Router	*Throughput [Million Packet/s]*	*Total Throughput [Gbit/s]*	*Percentage of Transit Traffic*	*STM1 interface cards*	*STM4 interface cards*	*STM16 interface cards*	*STM64 interface cards*
R1	0,22	1,85	7%	5	2	0	0
R2	0,09	0,73	0%	3	1	0	0
R3	0,99	8,32	1%	6	0	0	1
R4	0,18	1,47	8%	4	2	0	0
R5	0,13	1,07	11%	3	1	0	0
R6	2,17	18,20	6%	2	2	0	2
R7	0,16	1,32	23%	3	2	0	0
R8	0,03	0,24	22%	6	0	0	0
R9	4,09	34,37	40%	2	0	0	6
R10	1,73	14,53	0%	4	1	0	2
S1	0,41	3,41	7%	1	3	1	0
S2	7,09	59,55	4%	1	2	1	7
S3	0,00	0,00	-	2	0	0	0

M_3.2 Other results from the metropolitan SDH and WDM network planning

The Table M_3-5 [summary of planned SDH systems on rings] shows the SDH systems planned on the rings of the metro network planned by SIREN-Plan.

As RING-4 relies on WDM point-to-point systems, its Km fibres requirement, together with WDM system needs, are reported in Table M_3-6 [summary of planned WDM system on RING-4].

Table M_3-5 [summary of planned SDH systems on rings]

Ring	Number of STM16 systems	fiber requirement [Km]	Percentage of occupation	

RING-1	33	944.922	About 50%	
RING-2	65	1697.54	About 50%	
RING-3	18	424.872	About 50%	
RING-4	34	(Relies on WDM point-to-point systems)		
RING-5	19	549.538	About 50%	
RING-6	2	54.932	50%	

Table M_3-6 [summary of planned WDM system on RING-4]

Ring	Number of WDM4 systems	Number of WDM16 systems	fiber requirement [Km]	Percentage of occupation of WDM systems
RING-4	1	2	127.998	Near 100%

Node Equipment consistencies

For each node SDH equipments requirements are reported in tables M_3-7 and M_3-8 [list of planned SDH equipments part a and b]. Type of device and details concerning each piece of equipments are shown site by site. The type of WDM devices and the detail in terms of components (like Transponder and Fabry-Perot filters) for the ring 4 are also reported in the Table M_3-9 [list of planned WDM equipments]

Table M_3-7 [list of planned SDH equipments part a]

Name	Equipment	Number of Equipment	Ring	STM1 Port
Borsa	ADM 16/1 C	1	RING-1	5
CATTOLICA	ADM 16/1	1	RING-4	4
CATTOLICA	ADM 16/1	15	RING-4	16
CATTOLICA	ADM 16/1 C	1	RING-4	12
CORDUSIO	DXC 1024	1	Interconnection	522
CORDUSIO	ADM 16/1	16	RING-4	16
CORDUSIO	ADM 16/1	1	RING-4	4
CORDUSIO	ADM 16/1	1	RING-4	1
CORDUSIO	ADM 16/1 C	32	RING-2	8
CORDUSIO	ADM 16/1 C	1	RING-2	5
Cadorna	ADM 16/1 C	32	RING-1	8
Cadorna	ADM 16/1 C	1	RING-1	5
Cadorna	ADM 16/1 C	32	RING-2	8
Cadorna	ADM 16/1 C	1	RING-2	5
Castello	ADM 16/1 C	65	RING-2	8
DUOMO	DXC 512	1	Interconnection	266
DUOMO	ADM 16/1	25	RING-4	16
DUOMO	ADM 16/1	1	RING-4	4
DUOMO	ADM 16/1	1	RING-4	1
DUOMO	ADM 16/1 C	18	RING-5	8
DUOMO	ADM 16/1 C	1	RING-5	5

Table M_3-8 [list of planned SDH equipments part b]

Name	Equipment	Number of Equipment	Ring	STM1 Port
Diaz	ADM 16/1 C	8	RING-3	8
Magenta	ADM 16/1 C	32	RING-1	8
Magenta	ADM 16/1 C	1	RING-1	5
Magenta	ADM 16/1 C	32	RING-2	8
Magenta	ADM 16/1 C	1	RING-2	5
P.zza Fontana	ADM 16/1 C	8	RING-3	8
S.Babila	ADM 16/1 C	1	RING-5	4
S.Babila	ADM 16/1 C	16	RING-5	8
S.Babila	ADM 16/1 C	2	RING-6	8
S.Fedele	ADM 16/1 C	3	RING-5	8
S.Fedele	ADM 16/1 C	1	RING-5	1
S.STEFANO	DXC 512	1	Interconnection	288
S.STEFANO	ADM 16/1 C	18	RING-3	8
S.STEFANO	ADM 16/1	7	RING-4	16
S.STEFANO	ADM 16/1	2	RING-4	4
S.STEFANO	ADM 16/1	2	RING-4	12
Sempione	ADM 16/1 C	16	RING-1	8
Staz.Nord	ADM 16/1 C	16	RING-1	8
Staz.Nord	ADM 16/1 C	1	RING-1	2
Velasca	ADM 16/1 C	2	RING-3	8

Table M_3-9 [list of planned WDM equipment]

Name	Equipment	Number of Equipment	Transponders	Fabry-Perot Filters
CATTOLICA	WDM 16	4	64	64
CATTOLICA	WDM 4	2	4	4
CORDUSIO	WDM 16	4	64	64
CORDUSIO	WDM 4	2	4	4
DUOMO	WDM 16	4	64	64
DUOMO	WDM 4	2	4	4
S.STEFANO	WDM 16	4	64	64
S.STEFANO	WDM 4	2	4	4
VETRA	WDM 16	4	64	64
VETRA	WDM 4	2	4	4

In Figure M_3-1 [WDM connection] a WDM connection between two nodes (Cattolica and Cordusio) is depicted inside the ring 4. In this example 34 SDH systems are multiplied in 3 WDM point-to-point systems (6 fibres are needed). The fibre gain is 62 fibres.

In the following picture is depicted the schema used:

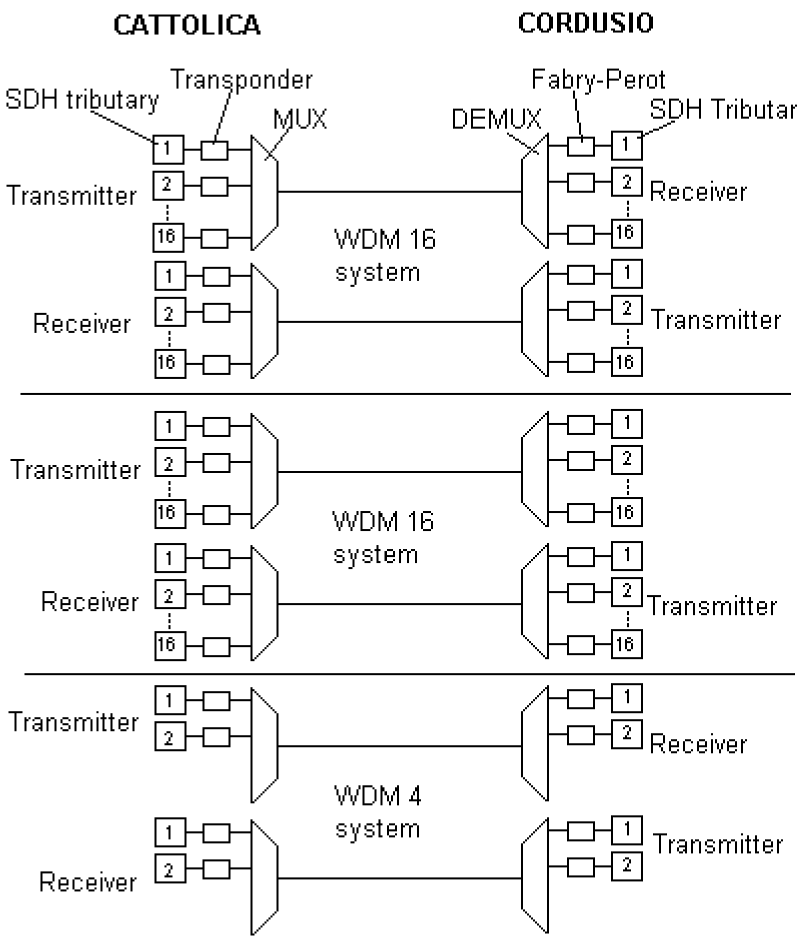


Figure M_3-1: WDM connection between two nodes

In order to complete the presentation of the data planned by SIREN-Plan, in the following table is presented, for every origin-destination the type of carrier planned:

Origin	Destination	type of carrier
Borsa	CATTOLICA	--
Borsa	Magenta	100 III window optical fibres
Borsa	Staz. Nord	100 III window optical fibres
Brera	Broletto	20 III window optical fibres

Brera	Cavour	20 III window optical fibres
Broletto	S. Babila	20 III window optical fibres
Broletto	Scala	--
CATTOLICA	CORDUSIO	20 III window optical fibres
CATTOLICA	VETRA	20 III window optical fibres
CORDUSIO	Cairoli	400 III window optical fibres
CORDUSIO	Callas	400 III window optical fibres
CORDUSIO	DUOMO	20 III window optical fibres
Cadorna	Castello	400 III window optical fibres
Cadorna	Magenta	400 III window optical fibres
Cadorna	Sempione	100 III window optical fibres
Cairoli	Callas	--
Cairoli	Castello	400 III window optical fibres
Callas	Magenta	400 III window optical fibres
Cavour	Spiga	20 III window optical fibres
DUOMO	S.Fedele	50 III window optical fibres
DUOMO	S.STEFANO	20 III window optical fibres
DUOMO	Scala	50 III window optical fibres
Diaz	P.zza Fontana	50 III window optical fibres
Diaz	Velasca	50 III window optical fibres
P.zza Fontana	S.STEFANO	50 III window optical fibres
S.Babila	Spiga	60 III window optical fibres
S.Babila	Vitt.Emanuele	50 III window optical fibres
S.Fedele	Scala	--
S.Fedele	Vitt. Emanuele	50 III window optical fibres
S.Nazzaro	S.STEFANO	50 III window optical fibres
S.Nazzaro	Velasca	50 III window optical fibres
S.STEFANO	VETRA	20 III window optical fibres
Scala	Spiga	50 III window optical fibres
Sempione	Staz.Nord	100 III window optical fibres

Appendix LD_1: Traffic matrixes in the Long Distance Context

Traffic matrices for Web traffic

The following tables are the traffic matrix in Mbit/s for the WEB browsing service.

	Milan	Rome	Bologna	Naples	Turin	Genoa	Trento	Venice	Firenze	Pescara	Cagliari	Palermo	Bari	Reggio C.
Milan + Intl	5000.0	2400.0	2400.0	3200.0	1600.0	1600.0	480.0	1280.0	1280.0	480.0	960.0	1280.0	960.0	640.0
Rome + Intl	2000.0	4000.0	2100.0	2800.0	1400.0	1400.0	420.0	1120.0	1120.0	420.0	840.0	1120.0	840.0	560.0
Bologna	1500.0	1200.0	450.0	600.0	300.0	300.0	90.0	240.0	240.0	90.0	180.0	240.0	180.0	120.0
Naples	1750.0	1400.0	525.0	700.0	350.0	350.0	105.0	280.0	280.0	105.0	210.0	280.0	210.0	140.0
Turin	1250.0	1000.0	375.0	500.0	250.0	250.0	75.0	200.0	200.0	75.0	150.0	200.0	150.0	100.0
Genoa	1250.0	1000.0	375.0	500.0	250.0	250.0	75.0	200.0	200.0	75.0	150.0	200.0	150.0	100.0
Trento	250.0	200.0	75.0	100.0	50.0	50.0	15.0	40.0	40.0	15.0	30.0	40.0	30.0	20.0
Venice	500.0	400.0	150.0	200.0	100.0	100.0	30.0	80.0	80.0	30.0	60.0	80.0	60.0	40.0
Firenze	1250.0	1000.0	375.0	500.0	250.0	250.0	75.0	200.0	200.0	75.0	150.0	200.0	150.0	100.0
Pescara	250.0	200.0	75.0	100.0	50.0	50.0	15.0	40.0	40.0	15.0	30.0	40.0	30.0	20.0
Cagliari	500.0	400.0	150.0	200.0	100.0	100.0	30.0	80.0	80.0	30.0	60.0	80.0	60.0	40.0
Palermo	750.0	600.0	225.0	300.0	150.0	150.0	45.0	120.0	120.0	45.0	90.0	120.0	90.0	60.0
Bari	500.0	400.0	150.0	200.0	100.0	100.0	30.0	80.0	80.0	30.0	60.0	80.0	60.0	40.0
Reggio C.	250.0	200.0	75.0	100.0	50.0	50.0	15.0	40.0	40.0	15.0	30.0	40.0	30.0	20.0

Table LD_1-1: Web browsing download traffic matrix [Mbit/s]

	Milan	Rome	Bologna	Naples	Turin	Genoa	Trento	Venice	Firenze	Pescara	Cagliari	Palermo	Bari	Reggio C.
Milan + Intl	420.0	168.0	126.0	147.0	105.0	105.0	21.0	42.0	105.0	21.0	42.0	63.0	42.0	21.0
Rome + Intl	201.6	336.0	100.8	117.6	84.0	84.0	16.8	33.6	84.0	16.8	33.6	50.4	33.6	16.8
Bologna	201.6	176.4	37.8	44.1	31.5	31.5	6.3	12.6	31.5	6.3	12.6	18.9	12.6	6.3
Naples	268.8	235.2	50.4	58.8	42.0	42.0	8.4	16.8	42.0	8.4	16.8	25.2	16.8	8.4
Turin	134.4	117.6	25.2	29.4	21.0	21.0	4.2	8.4	21.0	4.2	8.4	12.6	8.4	4.2
Genoa	134.4	117.6	25.2	29.4	21.0	21.0	4.2	8.4	21.0	4.2	8.4	12.6	8.4	4.2
Trento	40.3	35.3	7.6	8.8	6.3	6.3	1.3	2.5	6.3	1.3	2.5	3.8	2.5	1.3
Venice	107.5	94.1	20.2	23.5	16.8	16.8	3.4	6.7	16.8	3.4	6.7	10.1	6.7	3.4
Firenze	107.5	94.1	20.2	23.5	16.8	16.8	3.4	6.7	16.8	3.4	6.7	10.1	6.7	3.4
Pescara	40.3	35.3	7.6	8.8	6.3	6.3	1.3	2.5	6.3	1.3	2.5	3.8	2.5	1.3
Cagliari	80.6	70.6	15.1	17.6	12.6	12.6	2.5	5.0	12.6	2.5	5.0	7.6	5.0	2.5
Palermo	107.5	94.1	20.2	23.5	16.8	16.8	3.4	6.7	16.8	3.4	6.7	10.1	6.7	3.4
Bari	80.6	70.6	15.1	17.6	12.6	12.6	2.5	5.0	12.6	2.5	5.0	7.6	5.0	2.5

Reggio C.	53.8	47.0	10.1	11.8	8.4	8.4	1.7	3.4	8.4	1.7	3.4	5.0	3.4	1.7

Table LD_1-2: Web browsing upload traffic matrix [Mbit/s]

	Milan	Rome	Bologna	Naples	Turin	Genoa	Trento	Venice	Firenze	Pescara	Cagliari	Palermo	Bari	Reggio C.
Milan	0.0	2568.0	2526.0	3347.0	1705.0	1705.0	501.0	1322.0	1385.0	501.0	1002.0	1343.0	1002.0	661.0
Rome	2201.6	0.0	2200.8	2917.6	1484.0	1484.0	436.8	1153.6	1204.0	436.8	873.6	1170.4	873.6	576.8
Bologna	1701.6	1376.4	0.0	644.1	331.5	331.5	96.3	252.6	271.5	96.3	192.6	258.9	192.6	126.3
Naples	2018.8	1635.2	575.4	0.0	392.0	392.0	113.4	296.8	322.0	113.4	226.8	305.2	226.8	148.4
Turin	1384.4	1117.6	400.2	529.4	0.0	271.0	79.2	208.4	221.0	79.2	158.4	212.6	158.4	104.2
Genoa	1384.4	1117.6	400.2	529.4	271.0	0.0	79.2	208.4	221.0	79.2	158.4	212.6	158.4	104.2
Trento	290.3	235.3	82.6	108.8	56.3	56.3	0.0	42.5	46.3	16.3	32.5	43.8	32.5	21.3
Venice	607.5	494.1	170.2	223.5	116.8	116.8	33.4	0.0	96.8	33.4	66.7	90.1	66.7	43.4
Firenze	1357.5	1094.1	395.2	523.5	266.8	266.8	78.4	206.7	0.0	78.4	156.7	210.1	156.7	103.4
Pescara	290.3	235.3	82.6	108.8	56.3	56.3	16.3	42.5	46.3	0.0	32.5	43.8	32.5	21.3
Cagliari	580.6	470.6	165.1	217.6	112.6	112.6	32.5	85.0	92.6	32.5	0.0	87.6	65.0	42.5
Palermo	857.5	694.1	245.2	323.5	166.8	166.8	48.4	126.7	136.8	48.4	96.7	0.0	96.7	63.4
Bari	580.6	470.6	165.1	217.6	112.6	112.6	32.5	85.0	92.6	32.5	65.0	87.6	0.0	42.5
Reggio C.	303.8	247.0	85.1	111.8	58.4	58.4	16.7	43.4	48.4	16.7	33.4	45.0	33.4	0.0

Table LD_1-3: Web browsing total traffic matrix [Mbit/s]

International links (total traffic in Mbit/s)		
	upstream	downstream
Milan	420.0	5000.0
Rome	336.0	4000.0

Table LD_1-4: Web browsing total international traffic [Mbit/s]

Traffic matrices for Voice over IP telephony

OUT-NET telephony traffic matrix In Erlang. The traffic exchanged from the customers attached to the fourteen sites of the backbone and the other telephone networks through the Voice gateways (GW) located in Milan, Rome, Bologna and Naples.

	Milan/GW	Rome/GW	Bologna/GW	Naples/GW	Turin	Genoa	Trento	Venice	Firenze	Pescara	Cagliari	Palermo	Bari	Reggio C.
Milan/GW	0.0	0.0	0.0	0.0	600.0	600.0	180.0	480.0	480.0	0.0	0.0	0.0	0.0	0.0
Rome/GW	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	180.0	360.0	480.0	360.0	240.0
Bologna/GW	0.0	0.0	0.0	0.0	400.0	400.0	120.0	480.0	320.0	0.0	0.0	0.0	0.0	0.0

Naples/GW	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	120.0	240.0	320.0	360.0	160.0
Turin	600.0	0.0	400.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Genoa	600.0	0.0	400.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Trento	180.0	0.0	120.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Venice	480.0	0.0	320.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Firenze	480.0	0.0	320.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Pescara	0.0	180.0	0.0	120.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Cagliari	0.0	360.0	0.0	240.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Palermo	0.0	480.0	0.0	320.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Bari	0.0	360.0	0.0	240.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Reggio C.	0.0	240.0	0.0	160.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0

Table LD_1-5: OUT-NET telephony traffic matrix In Erlang

IN-NET telephony traffic matrix in Erlang. The traffic between the fourteen sites of the network. It colllects the IP telephone native traffic that is originating and terminating on the IP network.

	Milan	**Rome**	**Bologna**	**Naples**	Turin	Genoa	Trento	Venice	Firenze	Pescara	Cagliari	Palermo	Bari	Reggio C.
Milan	0.0	325.9	498.9	185.2	818.8	870.3	510.0	384.6	373.7	165.8	145.3	116.8	122.7	94.8
Rome	325.9	0.0	314.8	623.3	179.5	225.3	167.6	223.4	372.5	521.5	232.2	231.0	244.7	175.6
Bologna	498.9	314.8	0.0	132.6	134.7	190.9	148.6	272.9	400.1	83.9	66.1	60.4	63.6	41.8
Naples	185.2	623.3	132.6	0.0	84.9	97.0	73.3	102.3	130.1	260.0	128.2	203.3	261.2	163.1
Turin	818.8	179.5	134.7	84.9	0.0	290.0	85.3	90.6	98.5	42.0	59.0	46.7	41.0	30.9
Genoa	870.3	225.3	190.9	97.0	290.0	0.0	86.0	103.6	141.7	45.9	61.8	49.3	43.3	31.5
Trento	510.0	167.6	148.6	73.3	85.3	86.0	0.0	163.1	67.3	23.7	32.1	31.4	29.9	18.3
Venice	384.6	223.4	272.9	102.3	90.6	103.6	163.1	0.0	125.1	53.2	45.0	44.6	48.9	29.9
Firenze	373.7	372.5	400.1	130.1	98.5	141.7	67.3	125.1	0.0	63.6	59.3	53.6	51.4	33.2
Pescara	165.8	521.5	83.9	260.0	42.0	45.9	23.7	53.2	63.6	0.0	45.5	58.8	82.0	36.0
Cagliari	145.3	232.2	66.1	128.2	59.0	61.8	32.1	45.0	59.3	45.5	0.0	109.7	51.8	54.6
Palermo	116.8	231.0	60.4	203.3	46.7	49.3	31.4	44.6	53.6	58.8	109.7	0.0	87.0	174.1
Bari	122.7	244.7	63.6	261.2	41.0	43.3	29.9	48.9	51.4	82.0	51.8	87.0	0.0	81.1
Reggio C.	94.8	175.6	41.8	163.1	30.9	31.5	18.3	29.9	33.2	36.0	54.6	174.1	81.1	0.0

Table LD_1-6: IN-NET telephony traffic matrix In Erlang

Total Traffic matrix is in [Erlang]

	Milan	**Rome**	**Bologna**	**Naples**	Turin	Genoa	Trento	Venice	Firenze	Pescara	Cagliari	Palermo	Bari	Reggio C.
Milan	0.0	325.9	498.9	185.2	1418.8	1470.3	690.0	864.6	853.7	165.8	145.3	116.8	122.7	94.8
Rome	325.9	0.0	314.8	623.3	179.5	225.3	167.6	223.4	372.5	701.5	592.2	711.0	604.7	415.6

Bologna	498.9	314.8	0.0	132.6	534.7	590.9	268.6	752.9	720.1	83.9	66.1	60.4	63.6	41.8
Naples	185.2	623.3	132.6	0.0	84.9	97.0	73.3	102.3	130.1	380.0	368.2	523.3	621.2	323.1
Turin	1418.8	179.5	534.7	84.9	0.0	290.0	85.3	90.6	98.5	42.0	59.0	46.7	41.0	30.9
Genoa	1470.3	225.3	590.9	97.0	290.0	0.0	86.0	103.6	141.7	45.9	61.8	49.3	43.3	31.5
Trento	690.0	167.6	268.6	73.3	85.3	86.0	0.0	163.1	67.3	23.7	32.1	31.4	29.9	18.3
Venice	864.6	223.4	592.9	102.3	90.6	103.6	163.1	0.0	125.1	53.2	45.0	44.6	48.9	29.9
Firenze	853.7	372.5	720.1	130.1	98.5	141.7	67.3	125.1	0.0	63.6	59.3	53.6	51.4	33.2
Pescara	165.8	701.5	83.9	380.0	42.0	45.9	23.7	53.2	63.6	0.0	45.5	58.8	82.0	36.0
Cagliari	145.3	592.2	66.1	368.2	59.0	61.8	32.1	45.0	59.3	45.5	0.0	109.7	51.8	54.6
Palermo	116.8	711.0	60.4	523.3	46.7	49.3	31.4	44.6	53.6	58.8	109.7	0.0	87.0	174.1
Bari	122.7	604.7	63.6	501.2	41.0	43.3	29.9	48.9	51.4	82.0	51.8	87.0	0.0	81.1
Reggio C.	94.8	415.6	41.8	323.1	30.9	31.5	18.3	29.9	33.2	36.0	54.6	174.1	81.1	0.0

Table LD_1-7: Total telephony traffic matrix In Erlang

Total Traffic matrix is in [Mbit/s]

	Milan	**Rome**	**Bologna**	**Naples**	Turin	Genoa	Trento	Venice	Firenze	Pescara	Cagliari	Palermo	Bari	Reggio C.
Milan	0.0	5.9	9.0	3.3	25.5	26.5	12.4	15.6	15.4	3.0	2.6	2.1	2.2	1.7
Rome	5.9	0.0	5.7	11.2	3.2	4.1	3.0	4.0	6.7	12.6	10.7	12.8	10.9	7.5
Bologna	9.0	5.7	0.0	2.4	9.6	10.6	4.8	13.6	13.0	1.5	1.2	1.1	1.1	0.8
Naples	3.3	11.2	2.4	0.0	1.5	1.7	1.3	1.8	2.3	6.8	6.6	9.4	11.2	5.8
Turin	25.5	3.2	9.6	1.5	0.0	5.2	1.5	1.6	1.8	0.8	1.1	0.8	0.7	0.6
Genoa	26.5	4.1	10.6	1.7	5.2	0.0	1.5	1.9	2.6	0.8	1.1	0.9	0.8	0.6
Trento	12.4	3.0	4.8	1.3	1.5	1.5	0.0	2.9	1.2	0.4	0.6	0.6	0.5	0.3
Venice	15.6	4.0	10.7	1.8	1.6	1.9	2.9	0.0	2.3	1.0	0.8	0.8	0.9	0.5
Firenze	15.4	6.7	13.0	2.3	1.8	2.6	1.2	2.3	0.0	1.1	1.1	1.0	0.9	0.6
Pescara	3.0	12.6	1.5	6.8	0.8	0.8	0.4	1.0	1.1	0.0	0.8	1.1	1.5	0.6
Cagliari	2.6	10.7	1.2	6.6	1.1	1.1	0.6	0.8	1.1	0.8	0.0	2.0	0.9	1.0
Palermo	2.1	12.8	1.1	9.4	0.8	0.9	0.6	0.8	1.0	1.1	2.0	0.0	1.6	3.1
Bari	2.2	10.9	1.1	9.0	0.7	0.8	0.5	0.9	0.9	1.5	0.9	1.6	0.0	1.5
Reggio C.	1.7	7.5	0.8	5.8	0.6	0.6	0.3	0.5	0.6	0.6	1.0	3.1	1.5	0.0

Table LD_1-8: Total telephony traffic matrix In Mbit/s

Traffic matrix for VOD service

This section includes the traffic matrix of the VOD demand service. The matrix is between the four sites that host the video server farms from which the content could be delivered and the 14 backbone sites.

Traffic matrix for Video on demand service

	Milan/GW	Rome/GW	Bologna/GW	Naples/GW	Turin	Genoa	Trento	Venice	Florence	Pescara	Cagliari	Palermo	Bari	Reggio C.
Milan/GW	0.0	3200.0	3600.0	1600.0	2400.0	2400.0	720.0	1920.0	1920.0	240.0	480.0	640.0	480.0	320.0
Rome/GW	4000.0	0.0	1200.0	4800.0	800.0	800.0	240.0	640.0	640.0	720.0	1440.0	1920.0	1440.0	960.0
Bologna/GW	3000.0	40.0	0.0	400.0	600.0	600.0	180.0	480.0	480.0	60.0	120.0	160.0	120.0	80.0
Naples/GW	1000.0	120.0	300.0	0.0	200.0	200.0	60.0	160.0	160.0	180.0	360.0	480.0	360.0	240.0

Table LD_1-9: Traffic matrix for VoD service In Mbit/s

Traffic matrix for E-mail

Matrix for E-mail service in message/day

	Milan	**Rome**	**Bologna**	**Naples**	Turin	Genoa	Trento	Venice	Firenze	Pescara	Cagliari	Palermo	Bari	Reggio C.
Milan	1350000	1080000	405000	540000	270000	270000	81000	216000	216000	81000	162000	216000	162000	108000
Rome	1150000	920000	345000	460000	230000	230000	69000	184000	184000	69000	138000	184000	138000	92000
Bologna	350000	280000	105000	140000	70000	70000	21000	56000	56000	21000	42000	56000	42000	28000
Naples	400000	320000	120000	160000	80000	80000	24000	64000	64000	24000	48000	64000	48000	32000
Turin	300000	240000	90000	120000	60000	60000	18000	48000	48000	18000	36000	48000	36000	24000
Genoa	300000	240000	90000	120000	60000	60000	18000	48000	48000	18000	36000	48000	36000	24000
Trento	75000	60000	22500	30000	15000	15000	4500	12000	12000	4500	9000	12000	9000	6000
Venice	125000	100000	37500	50000	25000	25000	7500	20000	20000	7500	15000	20000	15000	10000
Firenze	300000	240000	90000	120000	60000	60000	18000	48000	48000	18000	36000	48000	36000	24000
Pescara	75000	60000	22500	30000	15000	15000	4500	12000	12000	4500	9000	12000	9000	6000
Cagliari	150000	120000	45000	60000	30000	30000	9000	24000	24000	9000	18000	24000	18000	12000
Palermo	200000	160000	60000	80000	40000	40000	12000	32000	32000	12000	24000	32000	24000	16000
Bari	150000	120000	45000	60000	30000	30000	9000	24000	24000	9000	18000	24000	18000	12000
Reggio C.	75000	60000	22500	30000	15000	15000	4500	12000	12000	4500	9000	12000	9000	6000

Table LD_1-10: Traffic matrix for E-mail service In Message/day

Matrix for E-mail service in Mbit/s

	Milan	**Rome**	**Bologna**	**Naples**	**Turin**	**Genoa**	**Trento**	**Venice**	**Firenze**	**Pescara**	**Cagliari**	**Palermo**	**Bari**	**Reggio C.**
Milan + Intl.	1.46	1.17	0.44	0.58	0.29	0.29	0.09	0.23	0.23	0.09	0.18	0.23	0.18	0.12
Rome +	1.24	0.99	0.37	0.50	0.25	0.25	0.07	0.20	0.20	0.07	0.15	0.20	0.15	0.10

Intl.														
Bologna	0.38	0.30	0.11	0.15	0.08	0.08	0.02	0.06	0.06	0.02	0.05	0.06	0.05	0.03
Naples	0.43	0.35	0.13	0.17	0.09	0.09	0.03	0.07	0.07	0.03	0.05	0.07	0.05	0.03
Turin	0.32	0.26	0.10	0.13	0.06	0.06	0.02	0.05	0.05	0.02	0.04	0.05	0.04	0.03
Genoa	0.32	0.26	0.10	0.13	0.06	0.06	0.02	0.05	0.05	0.02	0.04	0.05	0.04	0.03
Trento	0.08	0.06	0.02	0.03	0.02	0.02	0.00	0.01	0.01	0.00	0.01	0.01	0.01	0.01
Venice	0.14	0.11	0.04	0.05	0.03	0.03	0.01	0.02	0.02	0.01	0.02	0.02	0.02	0.01
Firenze	0.32	0.26	0.10	0.13	0.06	0.06	0.02	0.05	0.05	0.02	0.04	0.05	0.04	0.03
Pescara	0.08	0.06	0.02	0.03	0.02	0.02	0.00	0.01	0.01	0.00	0.01	0.01	0.01	0.01
Cagliari	0.16	0.13	0.05	0.06	0.03	0.03	0.01	0.03	0.03	0.01	0.02	0.03	0.02	0.01
Palermo	0.22	0.17	0.06	0.09	0.04	0.04	0.01	0.03	0.03	0.01	0.03	0.03	0.03	0.02
Bari	0.16	0.13	0.05	0.06	0.03	0.03	0.01	0.03	0.03	0.01	0.02	0.03	0.02	0.01
Reggio C.	0.08	0.06	0.02	0.03	0.02	0.02	0.00	0.01	0.01	0.00	0.01	0.01	0.01	0.01

Table LD_1-11: Traffic matrix for E-mail service In Mbit/s

Appendix LD_2 - air distance matrix in the Long Distance Context

	Milan	Rome	Bologna	Naples	Turin	Genoa	Trento	Venice	Firenze	Pescara	Cagliari	Palermo	Bari	Reggio C.
Milan	0	476	202	654	121	110	167	243	246	517	685	882	783	972
Rome	476	0	305	186	525	404	479	396	234	155	407	425	372	497
Bologna	202	305	0	468	298	194	176	126	82	318	612	728	582	793
Naples	654	186	468	0	710	589	633	534	408	180	473	315	219	327
Turin	121	525	298	710	0	122	288	361	316	595	658	905	862	1016
Genoa	110	404	194	589	122	0	248	285	197	475	576	793	742	897
Trento	167	479	176	633	288	248	0	115	257	468	775	904	718	960
Venice	243	396	126	534	361	285	115	0	203	362	735	819	605	860
Firenze	246	234	82	408	316	197	257	203	0	279	531	653	546	729
Pescara	517	155	318	180	595	475	468	362	279	0	557	491	267	500
Cagliari	685	407	612	473	658	576	775	735	531	557	0	389	689	582
Palermo	882	425	728	315	905	793	904	819	653	491	389	0	450	203
Bari	783	372	582	219	862	742	718	605	546	267	689	450	0	349
Reggio C.	972	497	793	327	1016	897	960	860	729	500	582	203	349	0

Table LD_2-1: Air distances between nodes in Km in the Long Distance Context

Appendix MPLS_1: Multilayer planning in MPLS networks

The purpose of this Appendix MPLS_1 is to describe some aspects dealing with multilayer planning in MPLS networks. This is the planning of an electrical MPLS network allowing label stacking or an MPλS network (covering both electrical and optical layer).

The appendix is structured as follows. The next section describes the typical grooming problem, to be solved when planning an MPLS network. Further sections then transforms this grooming problem to the label stacking within electrical MPLS (resulting in multiple sub-layers) and MPλS dealing with electrical MPLS over optical MPLS.

Problem situation: grooming

The following questions have to be answered:
Between which nodes does a tunnel (i.e., a big LSP) need to be provided?
Which LSPs have to be multiplexed/groomed into a particular tunnel → routing of original (small) LSPs?
What is the routing of the tunnels?

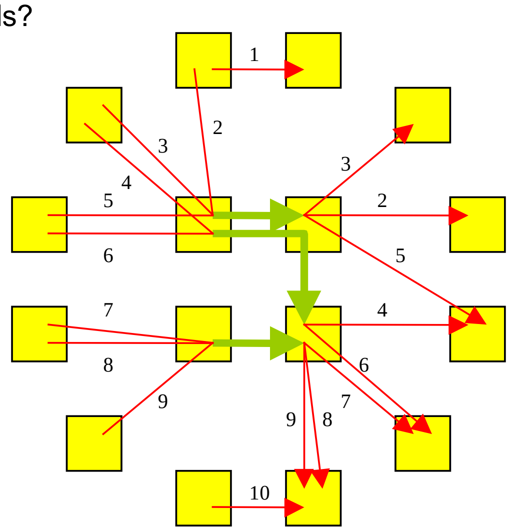


Figure MPLS_1-1: small example.

Figure MPLS_1-1 shows an example. The red (fine) arrows represent the LSPs to be transported by the network (LSP-IDs are also indicated). The green (thick) arrows represent the tunnels. One of the questions to be answered is: "what is the core network (i.e., the nodes between which tunnels are setup)?" The answer to this question, for this small example, is the four central nodes. The next step could be to identify the pairs of core nodes, between which there are enough LSPs to be groomed into a single (big) LSP/tunnel. Then one can proceed by routing the green (big) tunnels. Note that it is not necessary to multiplex/groom all LSPs through a big tunnel (e.g., LSP 1 and 10). It can also be appropriate to modify the routing of a few LSPs: e.g., it could be better to route LSP 5 through the single hop tunnel, because LSP 6, which is already routed through the double hop tunnel, is a very large one.

Note that this grooming of original (small) LSPs into big tunnels result in a multilayer network. This means also that the planning of the survivability has to come up with a multilayer resilience strategy. When choosing for recovery in multiple layers, it becomes interesting to examine how the common pool concept can be adopted in such an MPLS context.

Pure Electrical MPLS

The tunnels, described above, are easily achieved via label stacking (<shim header big tunnel><shim header original LSP><IP packet>). Due to the fact that only the shim header of the big tunnel has to be processed, a single entry per tunnel is sufficient in the label translation tables and thus an important reduction of these tables obtained.

Since electrical MPLS is packet-switched, the tradeoffs are not as clear as in regular grooming problems for circuit switched networks. However, even if there is no capacity trade-off, there are some important driving forces:

The size of the label translation tables should be kept reasonable.

Recovery of a single tunnel is much more beneficial than restoring each individual LSP independently.

Providing big tunnels in the core network will also reduce the management complexity and cost.

However, at the opposite site, there are also some arguments against grooming LPSs into bigger tunnels:

The routing of the original LSPs can change (i.e., become longer) due to the grooming (i.e., back-hauling), which will potentially result in an increase of the required resources.

The number of levels should also be kept reasonable. Not only because a large label stack will probably be nonsense, but also because each additional label induces additional overhead.

MPλS: electrical over optical MPLS

The MPλS grooming is very similar to the pure electrical MPLS problem: the lightpath represents here the big tunnel and the wavelength corresponds to the stacked label. However, there are some major differences between both problems:

There are only two labels: an electrical (original small LSP) and an optical (big tunnel).

The bandwidth (used or unused) of an optical LSP is fixed and the label space on each link is (very) small.

A tunnel transiting a node without being terminated leads to the net cost saving of an O/E and an E/O-interface. This is in clear contrast with the pure electrical case, where there is no need for an interface card performing the label-pop operation to terminate a big tunnel.

Incoming optical LSPs cannot be merged into a single output LSP. This merging problem thus emphasizes the limited label space problem.

Due to the fixed bandwidth and the merge incapability, protection (which means here pre-established backup LSPs) results in dedicated protection. However, this is the worst case: improvements of this worst case will be discussed in the PNET paper.

We can thus say that the MPλS case has to deal with a hard grooming problem and the pure electrical MPLS case with a soft grooming problem, in the sense that the tradeoffs (cost or capacity) in the MPλS case are much clearer than in the pure electrical case.

Appendix MPLS_2: Short Description of MPLS recovery schemes

MPLS recovery mechanisms

Introduction

The dynamic routing protocols in IP networks provide inherently some restoration capability. Each router is able to build up an overview of the current topology (in the form of the link-state database). If a failure occurs, then adjacent routers will detect this failure and they will not advertise anymore the affected link(s), resulting in the disappearance of the affected link(s) from the link-state database in each router. The final result is that each router will update his routing table with respect to this change. Experience has shown that this process is rather slow. Therefore, some faster techniques for MPLS recovery have been proposed in the IETF [1], [2], [3], [4], profiting from the path-oriented nature of MPLS. An overview is given in the following subsections.

Local Protection

MPLS protection is based on a pre-established disjoint backup LSP [3], [1], [6], [5], [PNC]. This backup LSP spans a single link or a single node in the case of local protection. The node where the backup LSP originates is called the Protection Switch LSR (PSL), because the LSR has to choose on which (working or backup) LSP to forward the packets. The LSR terminating the backup LSP is called a Protection Merge LSR (PML), since it simply merges both working and backup LSPs into the downstream part of the LSP.

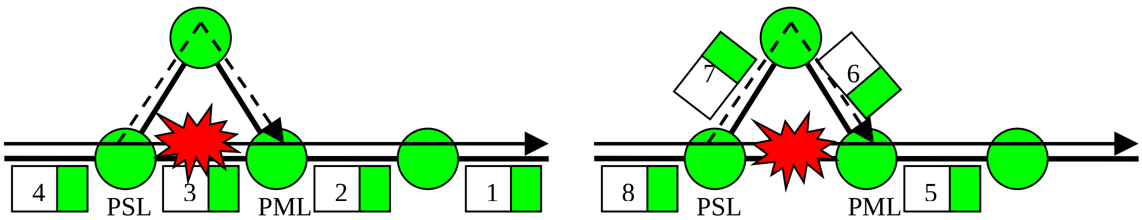


Figure MPLS_2-2: shows Local Protection at the time that a failure occurs (left side) and immediately after the protection switching (right side). Packet 3 gets lost because it was transmitted on the failing link at the time that the failure occurred and packet 4 because it arrived in the PSL before the protection switch.

An example of link protection is shown in Figure MPLS_2-2. The left side shows that the protected links fails at the moment that the third packet is being sent on this link (and thus this packet will get lost). As long as the PSL is not triggered, it keeps forwarding packets along the primary LSP (e.g., packet 4 is also lost, as illustrated by the right side of the figure, because packet 5 is the first packet forwarded along the backup LSP). Important to note is that the backup LSP does not occupy any resources as long as there is no failure, making it possible to share resources with other backup LSPs protecting other equipment.

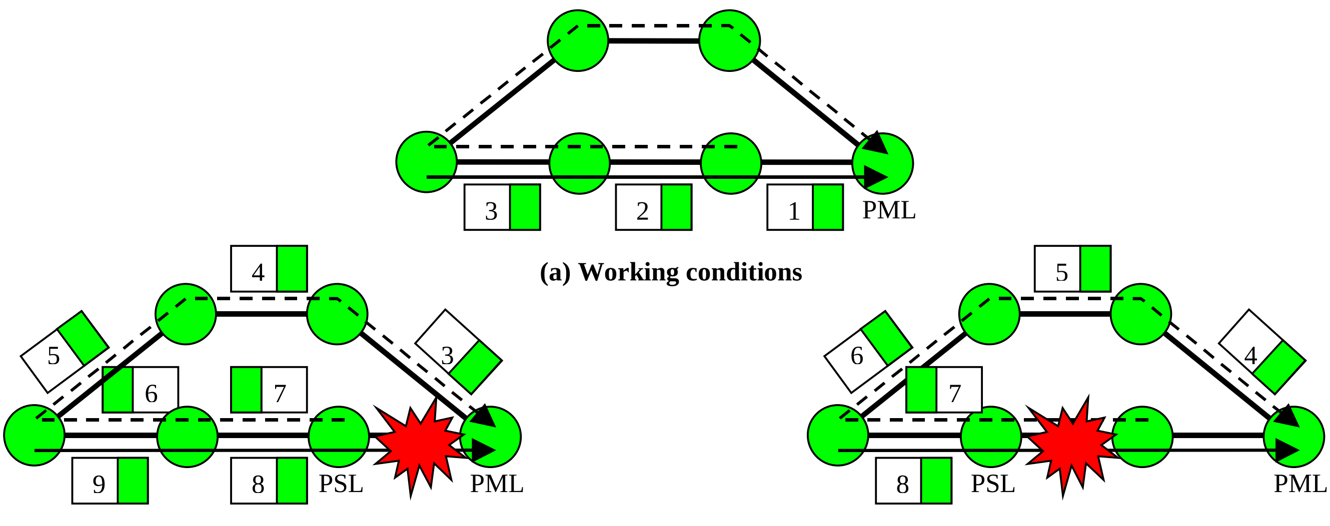
If N LSPs transit the protected link, then also N backup LSPs have to be provided (protection switching is performed at LSP level). This implies that each LSR, transited by the backup LSPs, has to provide for each (thus N in the case that all backup LSPs are routed similarly) backup LSP an entry in the Label Information Base. Therefore it could be worth to aggregate all these backup LSPs into a single LSP tunnel, by applying label stacking, in order to make all the individual backup LSPs invisible for the intermediate routers (their LIB only needs a single entry for the aggregate LSP tunnel).

Path protection

End-to-end protection [3], [4], [PNC] can be provided in a similar way as local protection: setting up a pre-established disjoint backup LSP, spanning the working LSP from ingress to egress. A drawback of path protection is that more packets will get lost (compared to local protection). First of all the PSL (being the ingress node in this case) has to be notified of the failure before it can perform the protection switch. Secondly, at the time of the protection switch many packets are already traveling along the working path upstream from the failure: all these packets will simply disappear after a while in a “black hole” (the failure). The advantage of path protection is that its global nature allows a better spreading of its impact (e.g., spare resource requirements) all over the network and that only a single backup LSP is required per working LSP (no distinct backup LSP for each potential failure along the working path, as with Local Protection).

Local Loop-back

The previous sub-sections on Local Protection and Path Protection have shown that both techniques have their advantages and disadvantages. Local Loop-back (also called “Fast-Reroute” or “Alternative Path”) [1], [5], [PNC] which combines some advantages of Local Protection (i.e., smallest amount of lost packets due to the local protection switch) and Path Protection (i.e., end-to-end character and single backup LSP). The idea is to setup a pre-established path, which contains two concatenated parts. The first part is routed from the last but one LSR on the working path, back to the source (ingress) node in the opposite direction of the working LSP. The backup LSP continues via a physically disjoint route from the source to the destination LSR. The destination LSR will always function as PML. The LSR performing the protection switching (thus the PSL) is not known in advance: the LSR immediately upstream from the failure will loop-back the traffic from the working LSP via the backup LSP back to the source and then via the disjoint route to the destination. Figure MPLS_2-2 shows an example. The top figure shows the situation at the time that a failure occurs. The two bottom figures show each a different failure scenario, assuming that the packet on the failing link is lost and that a single packet arrives before the protection switch (packets 1 and 2 and packets 2 and 3 are lost respectively).



(a) Working conditions

(b) Failure scenario I

(c) Failure scenario II

Figure MPLS_2-2: shows Local Loop-back, during working conditions (a) and after protection switching for two different failure scenarios (b) and (c). The packet being transmitted on the failing link at the moment of the failure and another packet arriving in the PSL before the protection switch are lost.

Rerouting

Although we mentioned in the introduction of this Appendix MPLS_2 that the inherent IP restoration may be rather slow compared to MPLS protection, it is possible to update the routing of the LSPs automatically, according to changes in the IP routing tables [2], [5], [PNC], [6]. This is thus an MPLS-equivalent of the path restoration concept. The advantage of this technique is that it can provide a better failure coverage, since the MPLS protection schemes, described above, can fail when a double failure affects the working and backup LSP simultaneously. The drawback is of course the low restoration speed, but this may be less critical than the reachability for some applications.

Fast Topology-driven Constrained-based Rerouting (FTCR)

Fast Topology-driven Constraint-based Rerouting [5], [PNC] is a scheme developed in our department. The idea relies on the fact that an LSR consists of a Link-State Database and that the LSR immediately upstream from the failure detects the failure. From the moment that it detects the failure, it can remove the link from the Link-State Database in order to get an updated view of the topology (other routers have still an outdated overview of the topology) and calculate a new route for the downstream part for each LSP. Once the new route is known, the downstream part of the LSP could be torn down and set up again along the new route. Explicit routing (thus CR-LDP signaling) has to be used, since other LSRs still have an outdated overview of the network. Of course, the Link-State Advertisement (LSA) flooding process is initiated in parallel and thus after a while the routing tables will be updated accordingly to the failure: this will not affect the already rerouted LSP, due to the explicit routing.

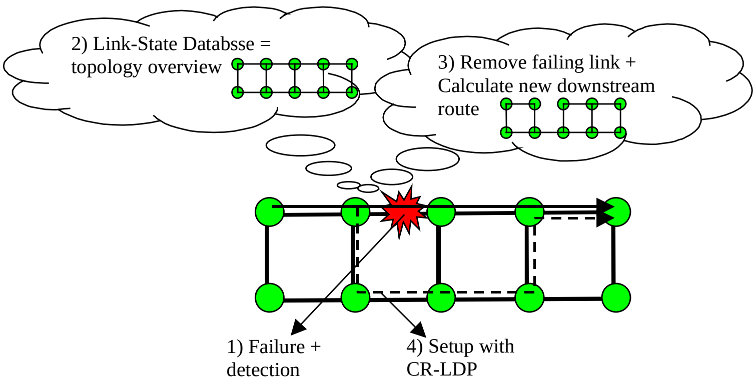


Figure MPLS_2-3: shows the different recovery actions/phases in FTCR

A problem is that this technique can only take into account the failure(s), which can be directly detected by the LSR taking recovery actions. Thus, an LSR detecting failure I, almost at the same time that another failure (failure II) was detected, is not yet aware of failure II and thus cannot take into account this failure, in the computation of an alternative route which does not contain failure I.

Appendix MPLS_3: Intermediate results for the long-distance scenario 2

The following table gives the unidirectional demand in 2.5 Gbit/s λ channels (also called lambdas) between the optical nodes (Rows = from, Columns = to) as mentioned in Section 4.3.2.1.

	Milan	Rome	Bologna	Naples	Turin	Genoa	Trento	Venice	Florence	Pescara	Cagliari	Palermo	Bari	ReggioC
Milan	0	6	4	5	3	3	1	3	3	0	0	0	0	0
Rome	7	0	5	4	0	0	0	0	0	1	2	3	2	2
Bologna	2	3	0	1	1	1	1	1	1	0	0	0	0	0
Naples	4	2	1	0	0	0	0	0	0	1	1	1	1	1
Turin	2	0	1	0	0	0	0	0	0	0	0	0	0	0
Genoa	2	0	1	0	0	0	0	0	0	0	0	0	0	0
Trento	1	0	1	0	0	0	0	0	0	0	0	0	0	0
Venice	1	0	1	0	0	0	0	0	0	0	0	0	0	0
Florence	2	0	1	0	0	0	0	0	0	0	0	0	0	0
Pescara	0	1	0	1	0	0	0	0	0	0	0	0	0	0
Cagliari	0	1	0	1	0	0	0	0	0	0	0	0	0	0
Palermo	0	1	0	1	0	0	0	0	0	0	0	0	0	0
Bari	0	1	0	1	0	0	0	0	0	0	0	0	0	0
ReggioC	0	1	0	1	0	0	0	0	0	0	0	0	0	0

Table MPLS_3-1: Results of IP dimensioning (without recovery) = demand for server layer (2.5 Gbits lambdas)

Again, a table that is completely analoguous to the previous one, but now for the case of recovery in the IP layer (client layer).

	Milan	Rome	Bologna	Naples	Turin	Genoa	Trento	Venice	Florence	Pescara	Cagliari	Palermo	Bari	ReggioC
Milan	0	8	8	7	4	4	2	3	3	0	0	0	0	0
Rome	8	0	8	6	0	0	0	0	0	1	2	3	2	2
Bologna	5	6	0	2	3	3	1	3	3	0	0	0	0	0
Naples	5	2	2	0	0	0	0	0	0	1	2	3	2	2
Turin	2	0	2	0	0	0	0	0	0	0	0	0	0	0
Genoa	2	0	2	0	0	0	0	0	0	0	0	0	0	0
Trento	1	0	1	0	0	0	0	0	0	0	0	0	0	0
Venice	1	0	1	0	0	0	0	0	0	0	0	0	0	0
Florence	2	0	2	0	0	0	0	0	0	0	0	0	0	0
Pescara	0	1	0	1	0	0	0	0	0	0	0	0	0	0
Cagliari	0	1	0	1	0	0	0	0	0	0	0	0	0	0
Palermo	0	2	0	2	0	0	0	0	0	0	0	0	0	0
Bari	0	1	0	1	0	0	0	0	0	0	0	0	0	0
ReggioC	0	1	0	1	0	0	0	0	0	0	0	0	0	0

Table MPLS_3-2: Results of IP dimensioning (with recovery) = demand for server layer (2.5 Gbit/s lambdas)