Interactive Realtime Multimedia Applications on Service Oriented Infrastructures

ICT FP7-214777

WP 7 Intelligent Networking

D7.5.1 ISONI Proof of Concept with limited functionality

IRMOS_WP7_D7_5_1_PU_ALUD_v1_0

Scheduled Delivery: 30.11.2009
Actual Delivery: 21.12.2009
Version 1.0

Project co-funded by the European Commission within the 7th Framework Programme		
Dissemination Level		
PU	Public	X
PP	Restricted to other programme participants (including the Commission)	
RE	Restricted to a group specified by the consortium (including the Commission)	

CO	**Confidential, only for members of the consortium (including the Commission)**	

Responsible Partner: Alcatel-Lucent Deutschland AG (ALUD)

Revision history:

Date	Editor	Status	Version	Changes
18.09.2009	Manuel Stein	Draft	0.1	Initial Draft
01.12.2009	Manuel Stein	Draft	0.2	Integrated input from partners, added component and sequence diagrams, phases and feature descriptions, innovations 1-4
07.12.2009	Manuel Stein	Final Draft for QA	0.3	fixed inconsistencies
18.12.2009	Manuel Stein	Release Candidate	0.4	Addressed internal review comments
21.12.2009	Karsten Oberle	Final	1.0	Final version for submission to the EC, implementing recommendations from QA process

Authors
Manuel Stein, Thomas Voith, Karsten Oberle (ALUD), Eduardo Oliveros (TID), Roland Kübert (USTUTT), Ralf Einhorn (DTO).

Internal Reviewers
Uwe Brähler (DFT), Dimosthenis Kyriazis (NTUA); Consolidating Reviewer: Alessandro Mazzetti (GILABS)

Acknowledgements
The research leading to these results has received funding from the EC Seventh Framework Programme FP7/2007-2011 under grant agreement n° 214777

More information

The most recent version of this document and all other public deliverables of IRMOS can be found at http://www.irmosproject.eu

Glossary of Acronyms

Acronym	Definition
API	Application programming interface
ASC	Application Service Component
CPU	Central Processing Unit
DM	Deployment Manager
DRS	Document Review Sheet
EC	European Commission
EEDL	Execution Environment Description Language
FWS	IRMOS Framework Services
IDM	Inter-Domain Manager
iGW	Interworking Gateway
IP	Internet Protocol
IRMOS	Interactive Realtime Multimedia Applications on Service Oriented Infrastructures
ISONI	Intelligent Service-Oriented Network Infrastructure
IXB	ISONI eXchange Box
IXB_{PH} / IXB_N	IXB Physical Host / IXB Node
NTP	Network Time Protocol
OWD	One-Way-Delay
PM_N / PM_D	Path Manager Node / Path Manager Domain
PO	Project Officer
QoS	Quality of Service
RM_N / RM_D	Resource Manager Node / Resource Manager Domain
SLA	Service Level Agreement
SNMP4J	Simple Network Control Protocol for Java
T-SLA	Technical Service Level Agreement
VMU	Virtual Machine Unit
VSN	Virtual Service Network
VSND	VSN Description
WP	Work Package
XML	eXtended Markup Language
XML-RPC	XML Remote Procedure Calls

Table of Contents

List of Figures

List of Tables

1. Executive Summary

The deliverable at hand is the result of the preliminary integration of all Intelligent Networking (WP7) contributions to the IRMOS Overall architecture [1]. The preliminary integration was performed after the individual solutions for connectivity, traffic management, flow control and path supervision had been finalized in the individual reports on “ISONI Addressing Scheme” [4], “Initial version of Path Manager: Architecture” [5], “Initial version of Flow Control: Architecture” [6] and “Initial version of Path supervision: Architecture” [7].

As an important aspect of the integration is to evaluate the quality of the results, the Intelligent Networking contribution to the research community was validated by reflecting upon the innovations of the Intelligent Networking solutions and their realization within the feature and component developments of the prototype (cf. chapter 3 “Innovations”). For the sake of brevity, the contributions to fulfil the IRMOS platform requirements have been revisited and are referred to as far as they impose challenges on the innovative approach.

Further, the Intelligent Networking activities have been structured according to the IRMOS application lifecycle described in D4.2.1 [3]. Since each step in the lifecycle of an IRMOS application prescribes expected IRMOS platform activities to be carried out, the tasks performed by Intelligent Networking component development contributions in fulfilment of ISONI activities were identified for each phase and put in relation to the IRMOS Framework Services activities. The “Phases” chapter has been created in alignment with the IRMOS Framework Services (WP5) and the Execution Environment (WP6), that have developed separate mechanisms and activities performed during the lifecycle of an IRMOS application.

Lastly, the Intelligent Networking prototypical developments of each task were integrated into a common software architecture description. The resulting UML component, activity and sequence diagrams that are depicted in this deliverable are a refinement of the ISONI management functional building blocks (cf. [1] chapter 5.3.2.2) that were specified in collaboration with the Execution Environment (WP6) to build a consistent ISONI for the deployment of interactive real-time applications. The component specification shall serve as specification for the IRMOS Integration and Evaluation (WP8).

The specification also accompanies a feature description (cf. chapter 5.1) that was created in accordance with IRMOS Integration and Evaluation (WP8) to identify and describe the Intelligent Networking contributions to ISONI features. Conclusively, a tabular overview was created to track the relations between innovations, IRMOS features, ISONI features and Intelligent Networking components.

Note, that the prototype at hand is yet an ISONI Proof of Concept with limited functionality, since the developments of the remaining advancements in traffic management, flow control and path supervision rely on the preliminary integration in

order to investigate on and develop the remaining features, such as SLA renegotiation, network support for a seamless change of the used infrastructure during live migration, detection of path degradation, SLA violations, counter-measurements, etc.

2. Introduction

This document accompanies the first set of prototypical software developments within WP7 on "Intelligent Networking" with yet a limited feature set for networking within the overall Intelligent Service-Oriented Network Infrastructure (ISONI) of the IRMOS platform.

In the proceedings of summarizing the prototypical developments in Intelligent Networking, the document starts with a short description of the innovations that have motivated the developments of Intelligent Networking features and architecture aspects. Chapter 3 "Innovations" subdivides into descriptions for each innovation along with the concepts and prototypical components that are involved in the realization of the innovative solution.

Next in the document, chapter 4 "Phases" outlines the ISONI Intelligent Networking tasks stepwise in the IRMOS application lifecycle [3]. The steps are described in the scope of Intelligent Networking, i.e., each step lists the prototype components involved in the IRMOS platform and further describes the component's task in the fulfilment of the IRMOS application life-cycle.

Finally, chapter 5 "Components" describes the architecture, features and interfaces of the prototype software developed in the Intelligent Networking framework. The chapter starts with an outline of the ISONI component architecture that highlights the Intelligent Network developments for ISONI. In order to integrate network features as a subsystem to the overall IRMOS platform integration, subchapter 5.1 "Features" summarizes the component mechanisms into feature topics, whereby each feature topic shows the contribution of the Intelligent Networking components to the ISONI features. The subsequent chapter 5.2 displays the interworking of the components by showing the detailed sequence diagrams for each functional interface of the software architecture.

For simplicity, three tables have been attached in the Annex of this document that summarize the relationships between Intelligent Networking innovations, the IRMOS platform features and ISONI features that are carried out by or in support of the components described in this deliverable.

It is recommended that the reader of this prototype description is also familiar with the concepts of addressing (D7.1.1 [4]), management (D7.2.1 [5]), flow control (D7.3.1 [6]), path supervision (D7.4.1 [7]) and their individual contributions to the overall component design. It is important to regard the content of this deliverable complementary to other IRMOS prototype descriptions, as outlined in the IRMOS Overall Architecture [1] specification.

2.1. Objectives

This document delivers the ISONI Proof of Concept with limited functionality from the IRMOS Intelligent Networking work package (WP7). The report summarizes and integrates the prototypical developments of Intelligent Networking, namely addressing, management, flow control and path supervision and contains all components, interfaces and algorithms developed in the deliverables D7.1.1 [4], D7.2.1 [5], D7.3.1 [6] and D7.4.1 [7].

The key concepts of Intelligent Networking as described per task are summarized and referenced in the innovation descriptions. The target of the summary is to show that the individual concepts are completely reflected in their implementation counterpart as was intended by the individual task. By outlining the relations between the concepts and the prototypical feature implementation, this document provides a comparison between the conceptual approaches and the prototypical implementation.

The individual developments have been implemented under different aspects each, so the target of the preliminary integration is to show that the individual approaches taken and the components implemented collectively fulfil the functionality of the Intelligent Networking in the IRMOS prototype. Further, the developments are described in their relation to the IRMOS application life-cycle to show the contribution of Intelligent Networking to the IRMOS project.

The interaction with other work packages' components has been documented as interface sequence diagrams along with the internal interactions (chapter 5.2) to support the integration with other work packages' components (WP6: Execution Environment, WP5: Framework Services). Please note, that the API specifications of the components are confidential mostly and given that the current document is of "Public" dissemination level, sequence diagrams were placed instead of interface specifications in chapter 5.2.

3. Innovations

This chapter briefly summarizes the innovations of IRMOS Intelligent Networking that have motivated certain aspects of the networking prototypical component developments. The innovation subchapters are organized according to the tasks of ISONI Intelligent Networking. The following abbreviations are used for requirements as listed in the "IRMOS Overall Architecture", please refer to D3.1.2 [1] for a detailed description of these requirements and their interdependencies:

<VS-x>: Video and Audio Streaming/Multi-videoconference functionality
<DM-x>: Data Management
<NET-x>: Network
<SLA-x>: Service Level Agreement
<EE-x>: Execution Environment
<SEC-x>: Security and Users profiles

3.1. Virtual Service Network

3.1.1. Isolation

Concurrent deployment of independent, customer-specific application service networks in IRMOS demands for mutual network address space isolation to prevent crosstalk. In fact, all three IRMOS application scenarios identified **application service isolation** a crucial requirement of the IRMOS platform to not allow any communication but the desired connections for the reasons of secure data exchange <DM-3>, separation from other services running over the same infrastructure <EE-10>. Further, virtualized private connectivity is required across networks <NET-16>, i.e. both across the existing transport networks but also across the virtual network address spaces spanned on the ISONI <NET-13>. A unified deployment model requires a level of network virtualization that sufficiently abstracts from heterogeneous transport technologies in use, such as Multi-Protocol Label Switching, Synchronous Optical Network or Asynchronous Transfer Mode adaption on Digital Subscriber-Lines, leased lines or Virtual Private Networks. Transparent break-out points that open pathways from the isolated virtual service network into pre-existing network address spaces are provided to hook up the application to external endpoints, such as consumers or non-virtualized components, so that **ASCs have external communication if required**, e.g. to connect multiple users <NET-2> and to visualize generated multimedia content remotely <VS-1>.

The innovative ISONI addressing scheme developed in [4] provides an independent, isolated interconnection model to organize application endpoints in isolated address namespaces that are virtualized to provide a flexible component positioning in the network infrastructure. The network heterogeneity difficulties in developing a unified interconnection model have been tackled by terminating the virtual environment at the IP layer and by choosing IP-layer virtualization on the various transport technology adaption stacks below. The solution acknowledges the existing approaches for Layer 2 virtualization techniques, which accumulate endpoints in virtual Layer 2 networks which do not provide the same degree of freedom in IP sub-network connection isolation. Moreover, the virtual service network approach taken suggests explicit annotation of the required connectivity (Virtual Links) to ensure a strong isolation among application service components that can not be found in virtualization solutions that introduce an independent protocol layer for labelling network namespaces, such as VLAN. Further details can be found in [4].

The innovative addressing scheme to isolate service-specific overlay networks and to avoid crosstalk is employed at the network resource virtualization level by the **ISONI eXchange Box (IXB)** component in the prototype. The complementary network connection modelling approach is reflected in the Execution Environment Description Language (EEDL) (cf. VSN Concept [1] ch. 5.3.2.1) as exemplified in D7.1.1 [4]. In the lifecycle of an IRMOS application, the feature of isolated VSN network connectivity applies to the “Use / Execution” phase (see Figure 1).

3.1.2. Network support for live migration

The ISONI Execution Environment is a dynamic context <EE-9> in which proactive migration is used to achieve an **enhanced reliability of application service** in the IRMOS platform. With the help of a mechanism that allows **ASC (VMU) relocation during application runtime**, the ISONI can use the live migration technology to offload a computational node and to consolidate physical hosts to have the resource usage balanced and minimized <EE-11>. For a **seamless change of used infrastructure resources** the ISONI Intelligent Networking has targeted to support the component relocation processes by network migration of virtual network connections. Current network virtualization approaches support a relocation of connections during the migration of a virtual machine with minimal link down time, but an autonomous relocation decision of services by ISONI must not breach the T-SLA terms of a deployment to ensure a seamless service perception for the consumer. The live migration mechanism in the Execution Environment requires a flexible network virtualization that supports seamless handover of the VSN connectivity – also across computational sites (Nodes).

The events of a switchover or VMU migration require coordination and have been found to perform seamless best with a managed infrastructure reconfiguration [4], so the layered addressing scheme and the network elements (IXB) were designed to support a transactional reconfiguration of the virtual link routing. The findings in support of live migration strongly affected the design of the Path Management hierarchy and the selection of the network virtualization layer. Further details can be found in the description of the ISONI Addressing Scheme [4] and the initial version of the Path Manager Architecture [5]. The network support for inter-node live migration is executed by the **Path Manager Node (PM_N)** and **IXB** components whereby the Path Manager Node is triggered by Node resource management which decides upon the event of a live migration. After the preparation transaction has been performed by the management components. The IXB is the component that is advised to forward and encapsulate traffic according to the reconfiguration. By terminating the relocation negotiation at the node-level, the innovative network support for live migration can achieve a coordinated switchover of Virtual Links that is aligned with the virtual machine migration process and network capacity management.

The relocation of an ASC (VMU) can happen after initial resources for an IRMOS application have been allocated in the "Use / Reservation" phase until the termination of the VSN in the "Use / Cleanup" phase. While the VMU has not been started, the relocation can be performed by the management components only thanks to the technology abstraction at node-level and late binding of network configurations. In case of an already started VMU, the negotiation of the relocation among node-level management components needs to include a decision whether the relocation can be performed without interrupting the application service, i.e. without breaching the low-level performance guarantees committed by the T-SLA.

Note: This feature will be integrated in the Final ISONI Prototype D7.5.2 [10].

3.2. Hierarchical infrastructure [path] management

3.2.1. QoS-enabled network resource discovery and instantiation

Several objectives of the IRMOS platform require a flexible network resource management that can discover free resources for a denoted time period and instantiate virtual service networks at the desired quality when required in the dynamic context of application deployments <EE-9>. For the **automated negotiation and establishment of an SLA** on network quality terms, a set of real-time parameters on network resource QoS have been identified and formalized in the VSND specification to create **low-level VSN descriptions** and are used throughout the Path Management components in an ontological resource model. But the negotiation capability further requires the ability to run an automated discovery and allocation process that finds and reserves the required resources to fulfil the negotiated terms and conditions. Besides, an **immediate VSN service instantiation** is provided as well as a **VSN service instantiation according to time plan** to automatically **instantiate the application inside IRMOS**. In case of negotiation failure, the ISONI should further support **pre-emptive termination of confirmed T-SLA** to allow SLA cancellations. These tasks for discovery and deployment around the automation of SLA negotiation for Virtual Service Networks have been equipped with a novelty approach to consider QoS constraints in resource selection and instantiation as well as to be scalable in large infrastructures for real-time deployments <EE-1>.

The new infrastructure supports the requirements to a scalable advance reservation of network QoS, by developing the network resource discovery and instantiation processes for an innovative 2-layered hierarchical network resource management that separates the resource discovery from the actual allocation. In the first stage of the discovery process, the lightweight domain-level proposes a set of nodes for the deployment while in the second stage the node-level management allocates particular Physical Hosts for interconnection <NET-1>. The reporting of available capacities runs concurrently to the VSN-individual reservation processes. Further details on the so called Path Availability Check and Path Reservation can be found in [5].

The prototypical implementation of the 2-layered QoS-enabled network resource discovery and instantiation is realized in the components **Path Manager Domain (PM_D)** and **Path Manager Node (PM_N).** During the lifecycle of an IRMOS application, the PM_D is active during the "Use / Discovery, SLA negotiation" phase. The Path Manager Node remains longer in the lifecycle, since it maintains the node-local network reservations of an IRMOS application from the reservation ("Use / Reservation" phase) to the termination of the application ("Use / Clean-up"). Details of the discovery and allocation process can be found in [5].

3.2.2. Automated SLA negotiation

Approaches to automated service level agreement negotiation have mostly come from the agent domain, for example from agent communication studies of the Foundation for Intelligent Physical Agents or as been investigated intensively by the BREIN project[1]. This even led to the development of a special negotiation protocol for agents, the Contract Net Interaction Protocol Specification[2]. The autonomy of agents makes them not fit for the demands in IRMOS, since individual decision autonomy is undesired in a managed domain. However, a varying degree of automation is wanted, since service providers do not want to maintain total manual control over recurrent negotiation processes for the sake of exploring new approaches for new services and to focus on high-profile decision regarding high-priority customers. Approaches to use third-party brokers for negotiation have been acknowledged, but the expansion of the negotiation chain has been found inapplicable to IRMOS, where the IRMOS platform exceeds the tasks of a simple broker when mediating between Clients, Application Providers and Infrastructure Providers, so that SLA negotiation is automated for the related parties of recurrent application deployments only – between Clients and Application Providers and between IRMOS Providers and ISONI Providers. Following the European Commission's directive 1999/93/EC[3], electronic signature laws have been already implemented in 18 of the European Union's 27 member states. Electronic contracts can now be, supposing correct surrounding conditions, legally binding, leading to an increased importance of desired outcomes when performing automated negotiation.

The Intelligent Networking developments for automated SLA negotiation focus on the T-SLA negotiation between IRMOS Providers and ISONI Providers and concluded the necessity to contain both, a higher ("contextual") level regarding the overall contract and a lower ("resource") level to facilitate an **automated negotiation and establishment of an SLA**. The contextual level mostly deals with non-functional properties (price, support, etc.) whereas the resource level contains the functional requirements in form of a **low-level VSN description** (cf. chapter 3.2.1). Obviously, no contract should be established if the resource level requirements cannot be fulfilled, i.e. the ISONI internal discovery and reservation is a pre-requisite to a successful contract establishment. However, high-level criteria may prevent the formation of a contract or

[1] http://www.eu-brein.com/
[2] http://www.fipa.org/specs/fipa00029/
[3]http://eurlex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&numdoc=31999L0093&model=guichett&lg=en

even prevent the providers from setting up automated negotiation. More details on the composition of a T-SLA can be found in [5], that allows an **immediate VSN service instantiation** as well as **VSN service instantiation according to a time plan**.

It has been found in IRMOS that there is a strong demand for **SLA renegotiation**, i.e. that the performance requirements can be altered when runtime conditions change, e.g. due to changing usage of the interactive applications. Since the performance guarantees are part of a contractual agreement, renegotiation of the T-SLA is inevitable. A **pre-emptive termination of a confirmed T-SLA** and **T-SLA renegotiation** will be covered in the report on the Final Version of Path Manager Architecture [8] and thence integrated into the final prototype D7.5.2 [10].

The prototypical implementation of the T-SLA negotiation is provided in the ISONI SLA Manager. The negotiation counterpart at the IRMOS provider is the IRMOS T-SLA Manager, which is part of the IRMOS Framework Services.

3.3. Flow Control

3.3.1. Temporal network traffic isolation

As described in chapter 3.1.1, ISONI provides the creation of co-existing service overlays on a single network infrastructure isolating the services avoiding crosstalk. The key feature is extended by sustaining the given networking QoS guarantees of co-existing service overlays expressed during the execution. ISONI Intelligent Networking as part of IRMOS platform has to ensure an **application execution keeping QoS guarantees** by enforcing flow control mechanisms for the deployed virtual service network in ISONI from edge-to-edge <NET-6/NET-15> as committed for networking.

The infrastructure therefore has been advanced to control the individual flows of deployed services, which leads to traffic (flow) isolation in respect to sustaining QoS conditions. The most important function reaching traffic isolation for QoS is to police (limit) the service-related flows in respect to agreed QoS in the T-SLA (described in D7.3.1 [6]) in order to **ensure confirmed real-time during execution phase** of the application.

The QoS can only be sustained if the network resources are not overloaded. Sustaining QoS <NET-17> for network traffic of services can only be met, if the network resources are managed as described with the Hierarchical infrastructure [path] management (see ch 3.2).

The IRMOS project was started to create a real-time enabled platform for running application services. The outcome of the flow control process is reliability for tasks, which must rely on a certain network throughput or which are sensitive to delay or jitter.

The prototypical implementation of flow control is realised on host-level. It consists of network flow policers limiting the network traffic on the Virtual Links of deployed service, and network packet scheduler implementing prioritized network multiplexing. The IXB_{PH} realises the policer and scheduler whereas the IXB_N realises the re-scheduling of inter-node encapsulated application service traffic.

3.3.2. QoS classification for resource usage optimization

ISONI internally structures the transport network resources for optimization of transport resources. Therefore ISONI correlates the available transport network resources with classified network classes namely ISONI QoS classes representing an adequate scheduling and forwarding behaviour strategy followed within this ISONI Domain. The ISONI QoS classes represent the abstract behaviour that persists across ISONI Node borders, which is very important for providing seamless migration of running ASCs across the infrastructure. It is necessary for **ASC (VMU) relocations during application runtime** from one location to another, that the same QoS conditions can be provided on the new paths used by the Virtual Links. The **enhanced reliability for application service** can be achieved only, when Virtual Link relocation is possible regardless of the varieties of transport network technologies used. Since it would be impossible to cover the QoS low-level parameters individually (cf. [6] chapter 4.1.1.), the ISONI QoS classification avoids the burden dealing with the QoS low-level parameter individually and enables to have enough space for later concurrent deployments independent from location. This allows targeting dedicated network paths depending on QoS requirements e.g. routing best effort traffic a cheaper way like Internet in opposite to using leased lines for delay and jitter sensitive traffic. This possibility of differentiating the traffic based on QoS metrics allows ISONI to optimize the usage of available transport network resources. Details are described in D7.3.1 [6].

The prototypical implementation is realized on node level in the **Path Manager Node (PM_N)**, dealing with transport network adaptation and abstraction using the ISONI QoS classes. PM_N reports the availability to the domain level namely the **Path Manager Domain (PM_D)**, which needs the information for electing adequate network resources namely ISONI network paths during reservation process. Through the prototype development it is feasible to demonstrate the path routes in respect to different ISONI QoS classes.

3.4. Path supervision

The Path supervision covers two aspects of ISONI, namely the network monitoring of deployed executed Virtual Service Networks (VSN) <NET-4> and the network infrastructure health supervision, detecting outages and degradation of available transport resources. The first aspect deals with measurements of the individual virtual links to provide **customer monitoring of the running application**. A challenge herein is to allow individual measurement of the Virtual Links with minimum intrusive influence to the Virtual Links allowing for the scalability of the infrastructure. The second aspect deals with the detection of link outage and degradation, and the possible effect on SLA management, counter measures to take to minimise the negative impact of failures and enforce the SLA or, if this is not possible, the detection and reporting of SLA violations, which requires a permanent **infrastructure health supervision**.

To minimise the impact on the network different measurement techniques are used: for inter-node measurement an active measurement method has been selected, the information collected from the different links is aggregated and correlated with the Virtual Links that share the same network path. For intra-node measurement passive techniques are used, see [7] for more detail.

The flow of monitoring information (described in D7.4.1 [7]) is sent to the Path Manager Node and then to the Deployment Manager, which is in charge of collecting all the information for the different Nodes and correlating it to the individual Virtual Links. The inter-node measurements are performed continuously, independent of any VSN deployments. The measurement data are collected continuously to the Deployment Manager who **provides the low-level infrastructure monitoring reports** to the FWS Monitoring Service, depending on the SLA specification for each specific VSN.

At the Path Manager Node, the health status of the path measurements is continuously checked against the network infrastructure configuration and reported along with availability reporting to the domain-level in order to establish permanent **transport network supervision**.

In summary, the path supervision mechanisms have consolidated network measurement techniques for the infrastructure elements and deployed VSNs under a common monitoring architecture that feeds both ISONI and IRMOS Framework Services to supervise and react to the overall IRMOS platform environment status.

One important requirement of the implementation is the time synchronization among the nodes, to correctly measure OWD and delay variation. For the proof of concept NTP has been used.

4. Phases

IRMOS has identified three crucial lifecycle phases of interactive multimedia applications (see D4.2.1 [3]), i.e. the "Application Component Development" phase for the individual modules that make up an application, the "Application Service Design" phase for the composition and design of network service components and client components and finally, the "Use" phase for the concretion and deployment of an IRMOS application onto an ISONI. The ISONI is not involved in the development and design phases of the application, since the infrastructure is targeted to be unspecific about application details whenever possible. The ISONI is only involved in the "Use" phase of an IRMOS application. The following figure shows the steps of the IRMOS "Use" phase from "Application Concretion" in the upper left to "Cleanup" in the lower right. The figure indicates the involvements of the Client, Framework Services and ISONI in the application lifecycle. Please note that the indications made for ISONI also belong to the complementary components of the ISONI Execution Environment.

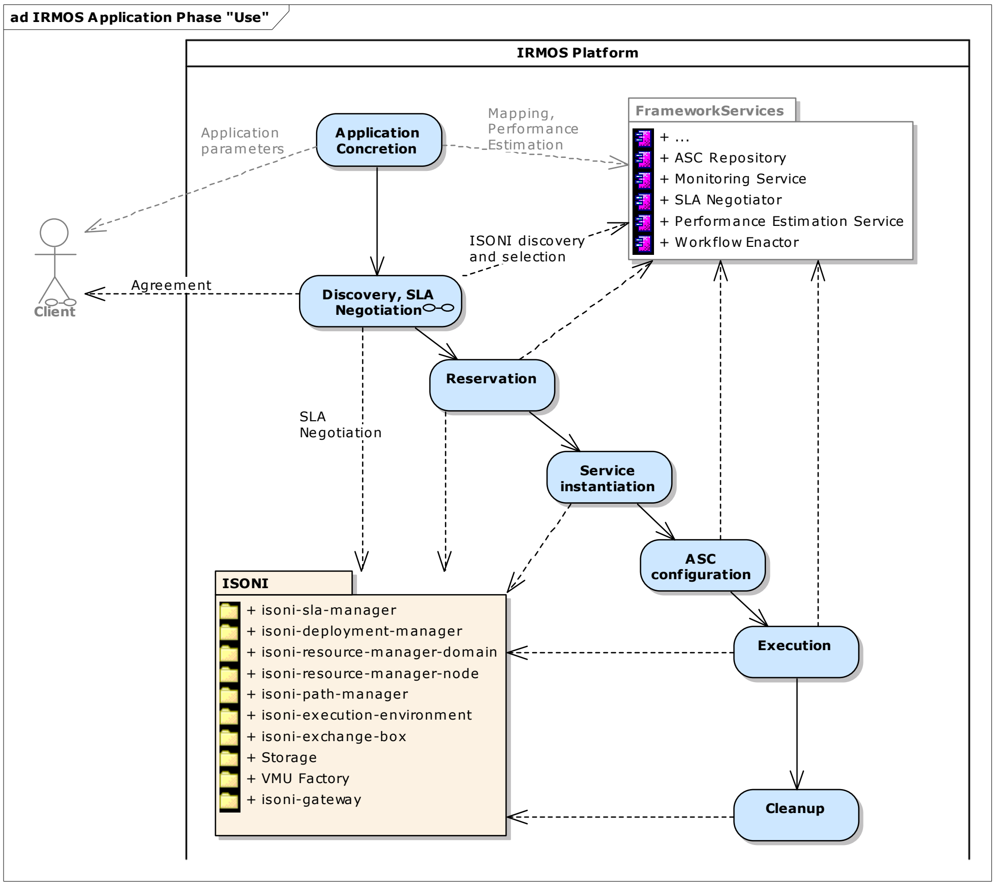

Figure 1 IRMOS Application Phase "Use"

The following chapters display how Intelligent Networking components directly or indirectly contribute to the activities in each step of the IRMOS application lifecycle.

4.1. Application Concretion

ISONI is first involved in the IRMOS application lifecycle when the IRMOS Framework Services concretize the application and derive a deployable infrastructure requirement model that is formalized in EEDL. The Virtual Service Network Description (VSND) needs to declare the components and interconnections for the deployment time, so the ISONI Addressing Scheme model of Virtual Links with attached configuration and real-time constraints has been incorporated in the EEDL for a coherent description of the technical requirements.

For the Framework Services to know about the possible directives in a VSND, the specification of the EEDL shall serve. However, the directives implemented by ISONI providers might differ from the potential set of low-level technical requirements, e.g. cloud infrastructure providers without the capability to enforce jitter and delay network guarantees and without the possibility of virtual machine real-time scheduling (e.g. Amazon EC2[4]) can choose for each QoS parameter individually whether or not to include it in the capability advertisement. This also applies to non-functional requirements expressed in the VSND, such as supported operating systems, CPU instruction sets, etc. As a consequence, the infrastructure provider would not be considered for deployments of applications that rely on having these requirements guaranteed, so the ISONI provider is asked to register with the IRMOS Framework Services and to advertise its individual set of supported EEDL directives.

The networking parameters available to the Application Concretion have been indicated in the example models in D7.1.1 [4] and the QoS model described in D7.3.1 [6]. The ISONI Intelligent Networking prototype component involved in the ISONI capabilities advertisement for application concretion is the **ISONI Info System**. The component performs the "Capability Advertisement" process, i.e. an interface that is planned to be specified in D3.1.3 [2]. It will be used to upload the ISONI prototype capabilities through the ISONI Gateway to the IRMOS Framework Services Advertisement Service.

Note: The ISONI process "Capability Advertisement" is regarded a part of the IRMOS application phase "Application Concretion" since the discovery and VSND creation are the first application lifecycle steps that depend upon the ISONI capabilities

4.2. Discovery, SLA Negotiation

Having derived the low-level requirements of the particular deployment in the VSND, the IRMOS Provider further iterates through ISONI capability advertisements to find the best provider(s) for the VSN deployment. For this reason, each ISONI provider has deposited the set of supported EEDL directives along with maximum/minimum availabilities in its advertisement at the IRMOS Framework Services. During the discovery process, an ISONI provider might drop from list of potential suppliers if the application profile imposes QoS requirements that cannot be fulfilled by the provider's infrastructure (e.g. too tight delay constraints or exceeding bandwidth allocations). too

[4] http://aws.amazon.com/ec2/

tight delay constraints or exceeding bandwidth allocations on the provider's infrastructure. Eventually, the IRMOS T-SLA Manager triggers the favoured ISONI provider with an "Invitation To Treat" to negotiate the deployment.

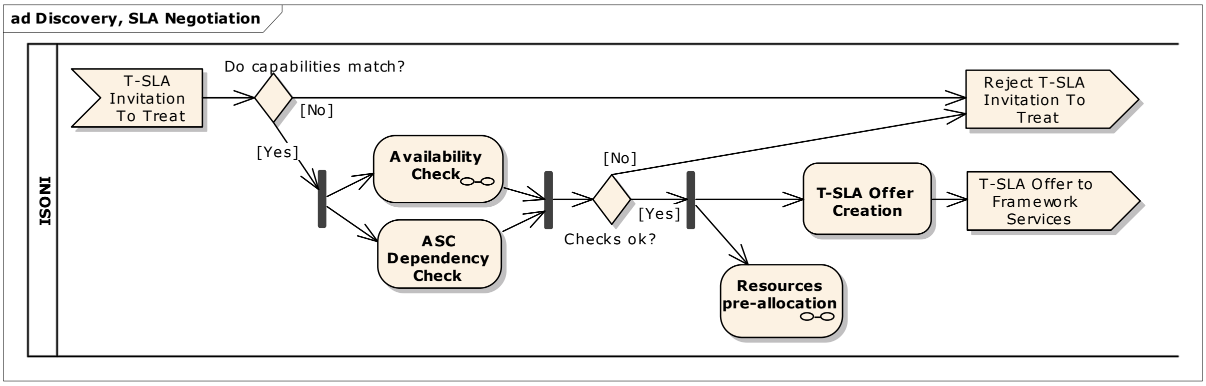

Figure 2 Prototype activities for "Use / Discovery, SLA Negotiation"

Figure 2 shows the ISONI activities for step "Discovery, SLA Negotiation". The ISONI SLA Manager checks the denoted capabilities first before the Deployment Manager starts the Availability Check on domain-level resource functions and the software dependency check for dependent software modules in the ISONI Repository by the VMU Factory. If the parallel checks successfully return, the resources are pre-allocated at the node-level controllers, i.e. Path Manager Node, Resource Manager Node and the node's Storage Manager have scheduled a resource reservation according to the times, capacities and QoS requirements of the VSND. If any of the parallel checks does not succeed (e.g., missing software dependencies or a sudden resource shortage due to competing reservation queries), the Deployment Manager would release any pre-reservations made and eventually return a negative response to the ISONI SLA Manager which in turn rejects the T-SLA "Invitation To Treat". In the positive case, the SLA Manager receives the deployment configuration to extract endpoint references and to assemble a T-SLA Offer that is eventually proposed to the IRMOS T-SLA Manager (including expiration terms and endpoint-references for service invocation). For ISONI, the step concludes successful if the ISONI SLA Manager provides a T-SLA Offer about the pre-allocated resources to the Framework Services. At the IRMOS platform, the Framework Services would check the proposed terms and conditions (e.g. contract expiry and binary upload expiry). The step "Discovery, SLA Negotiation" finishes when the Framework Services present the favoured offer through the IRMOS portal and ask for the Client's final agreement on the selected contract.

The ISONI Intelligent Networking prototypical components' participation in this step is as follows:

- The **ISONI SLA Manager** is the mediating component between the IRMOS T-SLA Manager and the rest of ISONI (e.g. Deployment Manager, VMU Factory, etc.).
- The **Path Manager Domain** performs the validation of the required inter-node connections in each deployment proposal made by the Resource Manager Domain during the "Availability Check". Eventually, the **Path Manager Node** is involved in this step by selecting and allocating the inter-node connections during the activity of "Resource Pre-allocation".

- The **ISONI Gateway** secures the "Invitation To Treat" and T-SLA Offer exchanges between the Framework Services and ISONI.

4.3. Reservation

The step starts with the Client's decision on a proposed offer for the IRMOS Application Deployment. If the Client accepts the deployment, Framework Services would countersign the T-SLA Offer to reach an agreement with ISONI. At ISONI, the SLA Manager already awaits a response of the IRMOS T-SLA Manager that accepts or rejects the T-SLA Offer within the contract expiration time. The VMU Factory would already await the ASC binaries to create the VMUs.

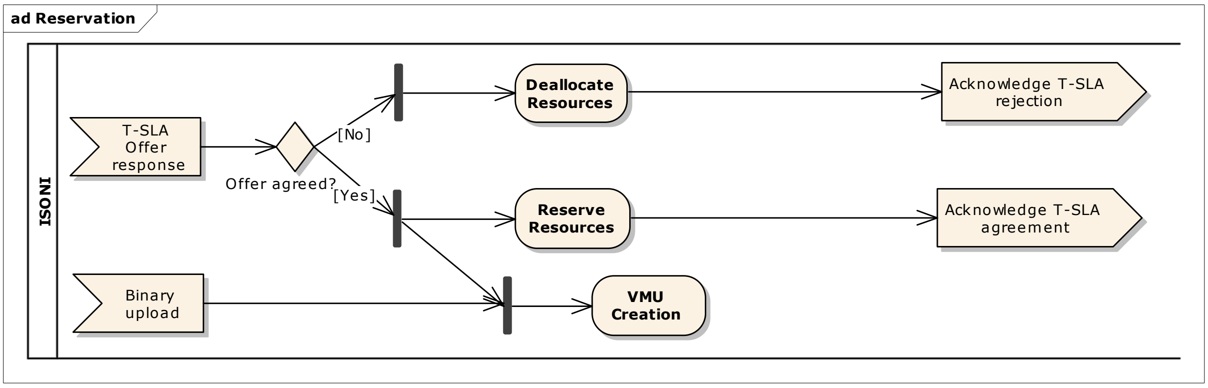

Figure 3 ISONI activities "Use / Reservation"

Figure 3 shows the activities of ISONI upon the response. Upon a rejection of the T-SLA Offer, all pre-allocated resources are de-allocated at all node-level controllers and freed for further selection. Upon an agreement on the T-SLA Offer, the ISONI would reserve the resources identified in the pre-allocation. Upon the retrieval of binaries within the upload expiration, the VMU creation process starts to tailor the VMUs with ASC software and have them stored in the ISONI Repository. For ISONI, the step completes either by acknowledging the T-SLA Offer rejection of the T-SLA Manager FWS or by tailoring the VMUs of an agreed VSN deployment. As a result of an agreed T-SLA, all infrastructure reservations have been made for the deployment time period, the VMU snapshots are available at the Repository Manager for deployment and the "Service instantiation" step is scheduled to run autonomously.

The components from ISONI Intelligent Networking involved in this step are:

- The **ISONI SLA Manager** completes the SLA negotiation protocol sequence towards the IRMOS T-SLA Manager.
- The **Path Manager Node** instances that host part of the Virtual Links in the VSND will either complete or rollback the reservation transaction. A successful completion might trigger an altered network resource availability report from the PM_N to the PM_D. Note, that binary upload and the VMU creation is coupled with SLA Negotiation but out of scope of Intelligent Networking.
- The **ISONI Gateway** secures the finalization of the SLA Negotiation protocol sequence

4.4. Service instantiation

Prior to the IRMOS application's deployment time period, the ISONI has to start-up the Execution Environment and to configure the VSN overlay at the involved IXBs. The ISONI autonomously sets up the virtual machines and network configuration according to the VSND. The step concludes successful when the Deployment Manager indicates to the Framework Services that the VSN has started and starts collecting monitoring data from the node-level controllers RM_N and PM_N.

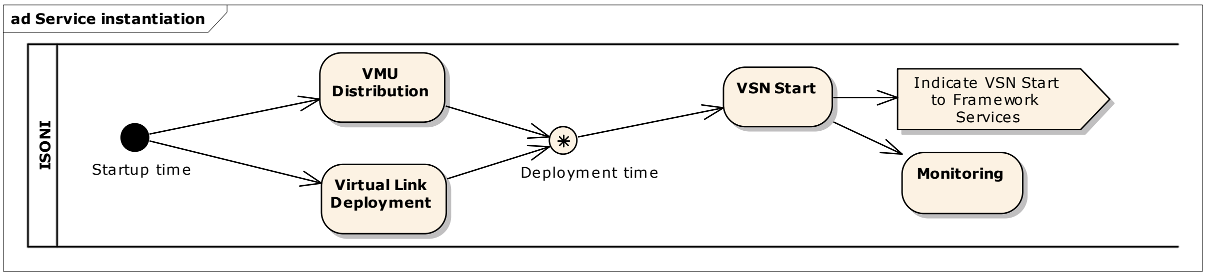

Figure 4 ISONI activities "Use / Service Instantiation"

The step of service instantiation happens at ISONI completely autonomously, i.e. triggered by the reservation schedule timing, the VMU images are downloaded to the Physical Hosts (VMU Distribution) and Virtual Links are deployed on the network infrastructure, both intra- and inter-node. At the scheduled deployment time, the Execution Environment start-up and Intelligent Networking setup processes should have finished, so that the VSN can be officially announced started and monitoring can start collecting values (see step "Execution / Monitoring").

As of Intelligent Networking, this phase is preoccupied by the PM_N and the IXB:

- The **Path Manager Node** awaits the assignment of VMUs to Physical Hosts by the RM_N. As soon as the PM_N receives the Physical Host selection, it creates the virtual link configurations of the involved IXBs and deploys the Virtual Link configuration.
- The **ISONI eXchange Box** receives configurations of Virtual Links by the PM_N. An IXB_N would activate the Virtual Link configurations immediately. An IXB_{PH} serves a VMU endpoint and hence has to await the start-up of the VM. As soon as the configuration is active, monitoring values are collected for the Virtual Links (if not yet enabled).

4.5. ASC configuration

The ASC configuration is solely performed by the Framework Services at the IRMOS platform. This step starts with the notification of the Framework Services by the Deployment Manager about the instantiation of the VSN. In turn, the Workflow Enactor Service will connect to the VSN and orchestrate the application execution in the VMUs on ISONI.

4.6. Execution / Monitoring

The step Execution of the IRMOS application "Use" phase is considered part of the VSN deployment time, i.e. it starts after the "ASC Configuration" and lasts until the VSN is shutdown in the "Cleanup" step, so the actions performed in the Execution step have the IRMOS application up and running within the deployed VSN, i.e. the ASCs are up and running in VMUs and communicate across Virtual Links.

The ISONI task during the Execution is to collect monitor reports about the deployment's utilization of the reserved resources, which are used by the IRMOS platform services to display customer Monitoring of running application, to enhance the reliability for application service in ISONI and the estimation of infrastructure low-level parameters based on application high-level parameters. ISONI would internally detect outages from the monitoring reports, so the enhanced reliability results from the ISONI's ability to induce counter measures when the T-SLA commitments are jeopardized. Eventually, a detected outage might affect the state of the T-SLA.

The scope of the ISONI monitoring reports is not only a single ASC, but an entire VMU or an entire Virtual Link of a deployment, although some components of the FWS (Workflow Enactor, Monitoring and ASC Wrapper) are executed along with the ASC inside the VMU and a Virtual Link usually spans multiple networking hops in a distributed deployment on ISONI. As of the FWS deployed alongside the ASCs, it is in fact hidden to the ISONI Execution Environment which software is actively running inside the VMU, so potential overhead produced by the FWS components inside a VSN is considered by the FWS when formulating the resource requirements in the VSND as part of the T-SLA. During execution, monitoring information is sent periodically from the Deployment Manager sub-part "Monitoring" to the IRMOS Monitoring FWS through the ISONI Gateway (as specified by the T-SLA, for instance every second) using XML format. The periodicity should be carefully decided to not squander infrastructure resources and to not jeopardize the real-time guarantees of the deployments while providing enough information to perform use cases of monitoring. See [7] for more details on ISONI VSN monitoring

The FWS will receive those monitoring reports from ISONI, but also establish application monitoring and the ASCs executing inside ISONI. The information will be used for A-SLA management and cross-checked to determine root causes in case of an A-SLA violation. Further, the information is used to improve the mapping process performed by the Benchmarking Service and Performance Estimations Service. In addition, customer monitoring of the running application is created from the collected monitoring reports.

Within ISONI Intelligent Networking, transport monitoring reports are used at the node-level to measure the degradation of transport resources in order to provide more accurate availability reports based on infrastructure health supervision. Further in ISONI, it is planned for the Final ISONI Prototype [10] to have the Deployment Manager reporting transgressions of the negotiated real-time parameter ranges to an additional component part of the ISONI SLA Manager, named "Violation Analyzer", that would check the impact of such occurrences against the terms and conditions of the T-SLA.

The following ISONI Intelligent Networking components are involved in the Execution/Monitoring

- The **ISONI eXchange Boxes (IXBs)** creates Virtual Link reports for the PM_N about the utilization of a virtual connection for the time of a Virtual Link deployment
- **IXB-Nodes (IXB_N)** create Path monitor reports for the PM_N about the QoS state of their served Path-IDs during the complete lifetime of the Path-ID
- At the **Path Manager Node (PM_N)**, the Path monitor reports are projected onto the active sub-VSN deployments and combined with the Virtual Link deployment reports. The result is a partial VSN deployment report of the parts deployed on the ISONI Node. Further, it is planned to consider measurable path degradation in availability reports
- The **Deployment Manager / Monitoring** module collects the partial reports from all involved PM_N's, correlates a VSN deployment report and delivers it to the IRMOS Monitoring Service for further use by the IRMOS Provider.
- The **SLA Manager / Violation Analyzer** module is a planned sub-component to the ISONI SLA Manager that remains informed about monitored transgressions of resource guarantees. It compares duration and frequency of such occurrences against allowable limit transgressions of the contracted T-SLA.

4.7. Cleanup

After the IRMOS application's execution, the final step of the "Use" phase is reached: "Cleanup". The step starts with the scheduled end time of the VSN deployment, i.e. by expiry of the T-SLA or expiry of the VSN reservation time. Besides, an expiry can be induced by pre-emptive cancellation of a T-SLA through the FWS. With this step, the deployment-specific obligations between the IRMOS Provider and the ISONI Provider are removed. The step concludes successful for the IRMOS platform when all run-time monitoring data have been analyzed and incorporated in the benchmarking and performance estimation.

During this step, ISONI has to remove the VSN-specific configurations and processes (VMU, network configuration), reservations (computational, storage, network) and the VSN-individual Deployment Manager. Upon time-out, the VSN simply expires at all levels which triggers a cleanup procedure. In case of a pre-emptive termination of the T-SLA, the cleanup procedure would be triggered by a cleanup control message throughout the infrastructure.

Note that the details of the Cleanup procedure in ISONI have not yet been specified but are planned as part of the final ISONI prototype D7.5.2 [10].

As of Intelligent Networking, the components for control and reservation of a VSN are mostly involved, i.e.:

- The **Path Manager Node** instances that host part of the Virtual Links in the VSND will remove the deployment information (mapping, etc.) from the reservation schedule (which might trigger availability reporting in case of pre-emptive T-SLA termination)

- The **ISONI eXchange Boxes** will close the Virtual Links by revoking the configuration from the network transport interfaces in the infrastructure
- The **ISONI SLA Manager** will archive the contract and stop analyzing outages for violations of the expired T-SLA

5. Components

The ISONI development has been split into ISONI Execution Environment and the ISONI Intelligent Networking (D7.5.x). Figure 5 highlights the components/modules developed within Intelligent Networking for the ISONI prototype. The Intelligent Networking contributes to ISONI with the following component s:

- ISONI Gateway
- SLA Manager
- Path Manager Node
- Path Manager Domain
- ISONI eXchange Box
- Deployment Manager - the "Monitoring" sub-component.

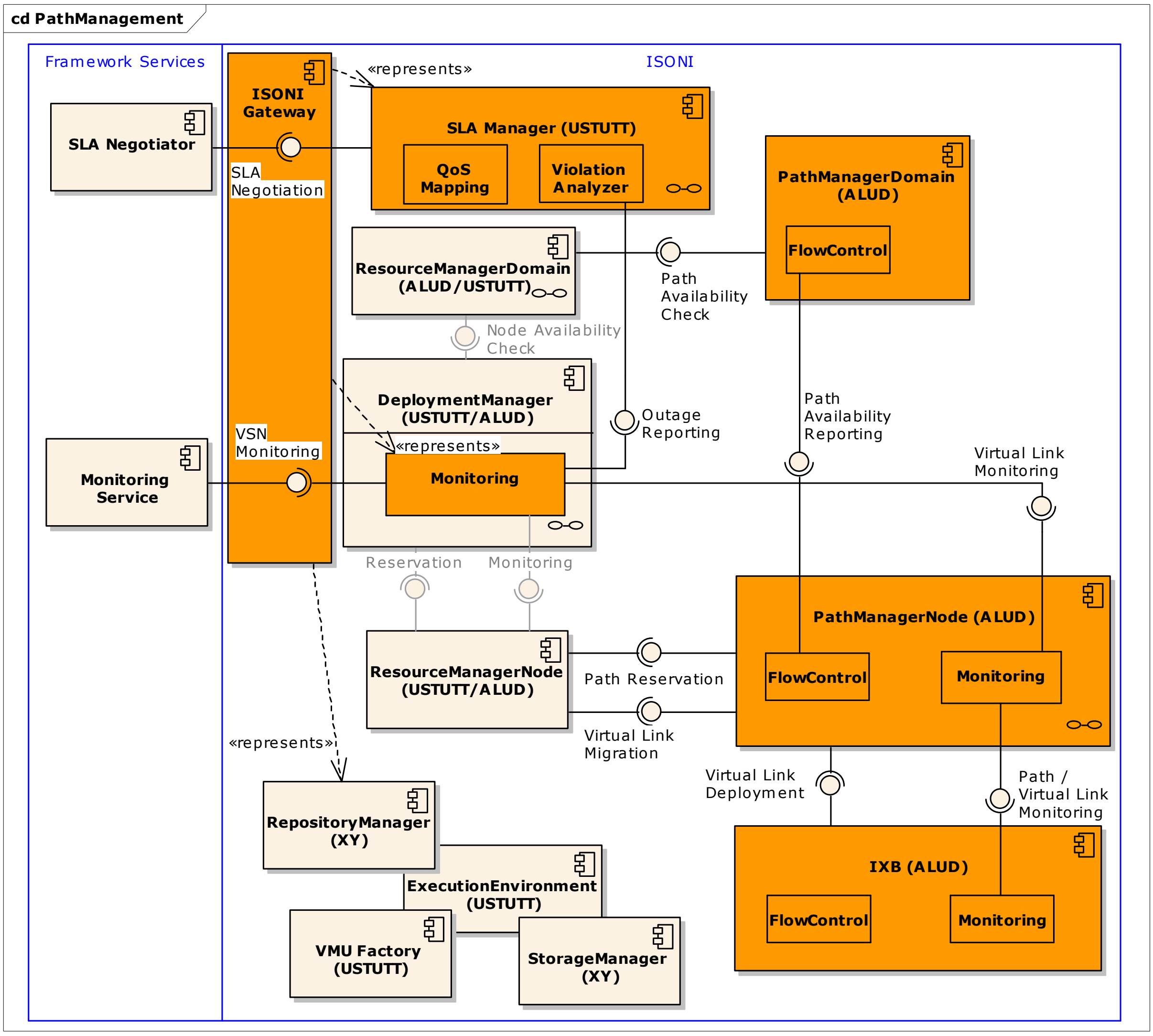

Figure 5 Intelligent Networking Component Diagram

The developments for Flow Control, Path supervision and Automated SLA negotiation are highlighted in the figure as parts of the components, i.e. "Violation Analyzer", "Flow

Control", "QoS Mapping", "Monitoring" to indicate the individual contributions to the architecture. The diagram also shows all interfaces of the ISONI Intelligent Networking management architecture. More details about the interface sequence diagrams can be found in chapter 5.2 "Interfaces" lists all component parts developed within this WP with their accommodating deliverables.

Component	Deliverable
ISONI Gateway	D7.2.1
SLA Manager	D7.2.x
SLA Manager / QoS Mapping	D7.3.x
SLA Manager / Violation Analyzer	D7.2.2
Path Manager Domain	D7.2.x
Path Manager Domain / Flow Control	D7.3.x
Deployment Manager / Monitoring	D7.4.x
Path Manager Node	D7.2.x
Path Manager Node / Flow Control	D7.3.x
Path Manager Node / Monitoring	D7.4.x
ISONI eXchange Box (IXB)	D7.1.x
IXB / Flow Control	D7.3.x
IXB / Monitoring	D7.4.x

Table 1 Component / Deliverable mapping

When comparing the component developments with the individual concept descriptions for connectivity [4], traffic management [5], flow control [6] and path supervision [7], the components for ISONI inter-domain traffic management and flow control, namely the "Inter-Domain Manager" (IDM) and "interworking Gateway" (iGW) remain conceptual parts of the ISONI for which no prototypical implementation is foreseen (cf. D7.2.1 chapter 4.3 [4]).

5.1. Features

This chapter describes the ISONI features provided by or with the help of the prototypical implementation of the Intelligent Networking components "ISONI Gateway", "SLA Manager", "Path Manager Node", "Path Manager Domain" and "ISONI eXchange Box". Note that each component, each interface and design decision in Intelligent Networking individually contributes to the features of an integrated ISONI. The following list of ISONI features are realized by or in support of the Intelligent Networking components:

- providing public IP address and external access
- isolated VSN network connectivity
- ISONI enforce authentication and authorization for FS interactions
- low-level VSN description
- providing ISONI capabilities information
- non-binding T-SLA negotiation
- VSN service instantiation according time plan

- immediate VSN service instantiation
- binding T-SLA negotiation
- reservation of dedicated network resources
- T-SLA renegotiation
- pre-emptive termination of confirmed T-SLA
- reservation of dedicated networking resources
- isolated VSN network connectivity
- ensuring confirmed real-time during execution phase
- low-level monitoring performance data during VSN execution
- transport network supervision
- ASC (VMU) relocation during application runtime

The following subchapters summarize the Intelligent Networking contributions to ISONI features in feature topics for VSN connectivity, SLA negotiation, etc.

5.1.1. VSN Connectivity

The most obvious feature carried out by Intelligent Networking is the connectivity of deployed VSNs running on top of the infrastructure. As discussed in D7.1.1 [4], an ISONI Domain is considered a confederation of geographically distributed ISONI Nodes that are interconnected via owned and rented transport network resources. The ISONI Path Management has been aligned to the node and domain-level structure to gradually derive the deployment of Virtual Links onto the transport infrastructure in collaboration with the Resource Management, that maps data to storage resources and service components onto computational resources.

The Path Manager Domain selects transport paths for the Virtual Links that require connectivity to external transport networks and that run between ISONI Nodes upon a request by the RM_D through the Path Availability Check interface. During this assignment, the Path Manager Domain decides on the location of the VSN's transitions to external networks, also known as Point-of-Presence, for **providing public IP address and external access**.
After the domain-level mapping of the VSN to the infrastructure, a node-level mapping is carried out by the Path Manager Node upon request by the RM_N through the Path Reservation interface. The two-phase commit reservation transaction maps Virtual Links to the node-internal infrastructure by selecting and configuring the interface hops of the required connections. Upon deployment, the Virtual Link configurations are activated by the IXBs upon request by the Path Manager Node via the Virtual Link Deployment interface.

The abovementioned Virtual Link configurations for each interface hop in the infrastructure are designed in accordance with the ISONI Addressing scheme to completely isolate all Virtual Links from each other to enforce **isolated VSN network connectivity**.

5.1.2. Security

The **ISONI Gateway** has been put in place to let **ISONI enforce authentication and authorization for FS interactions**. Three components communicate through the ISONI Gateway with IRMOS Framework Services. The *ISONI Info System* uses the ISONI Gateway to securely advertise the ISONI's VSN ontology at the IRMOS Providers' (i.e. the specification of allowed directives and quality limits in the particular ISONI Domain). The *ISONI SLA Manager* is registered with the ISONI Gateway to become the denoted service instance for T-SLA Negotiation. Henceforward, the protocol for T-SLA negotiation between the IRMOS T-SLA Manager and the ISONI SLA Manager is secured by the ISONI Gateway. Analogously, each *Deployment Manager instance* of a VSN deployment registers its endpoint with the ISONI Gateway to deliver the ISONI low-level monitoring reports to the IRMOS Monitoring FWS.

5.1.3. Formalized requirements and capabilities

The automation of several processes in IRMOS did not only shape the protocol developments for transactional handshakes between components, but also required a formalized model to represent resource requirements and infrastructure descriptions in a globally unique way to automate the data exchange at the interfaces during discovery, allocation, reservation, execution monitoring, etc. A T-SLA in particular is negotiated based on a **low-level VSN description (VSND)**. The VSND is an ontological annotation of the application deployment model with particular resource requirements for each deployment location and connection. Since with Web Ontology Language (OWL), the semantics of a document (VSND) can be specified in the ontology (VSN Ontology), the EEDL specification is of increased interest to the interface implementation between an IRMOS Provider and an ISONI Provider. While the EEDL is a kind of global specification that is valid to all ISONIs, a particular ISONI Provider can choose a subset of the global semantics and introduce additional restrictions (e.g. no QoS on public links) on its individual ISONI capabilities. By **providing ISONI capabilities information** to the IRMOS Provider, the IRMOS Framework Services can use the ISONI capabilities to discover an appropriate ISONI for a particular deployment.

The EEDL is used throughout Intelligent Networking components, i.e. the SLA Manager matches a requested VSND against the ISONI Domain capabilities specified in a VSN ontology. The PM_D manages its ISONI Nodes and ISONI Path-IDs in a resource ontology document that provides the interconnection of Nodes (see D7.3.1 [6], Correlation Matrix). At the PM_N, the Path-ID resources document is used to setup availability reporting about the QoS class and capacity schedule of a Path-ID.

5.1.4. Automated SLA Negotiation

One of the most obvious IRMOS features refers to the automation of the SLA negotiation process between the IRMOS Provider and the ISONI Provider in the IRMOS application phase "Use" under the steps "Discovery, SLA Negotiation" and "Reservation". The T-SLA Negotiation separates the T-SLA Offer creation and the final agreement on a T-SLA Offer.

The interface "SLA negotiation" and the component "SLA Manager" perform the automated SLA negotiation. See chapter 5.2.1 for more details on the T-SLA negotiation.

The T-SLA Offer creation for an "Invitation To Treat" is a **non-binding T-SLA negotiation**. The offer creation includes an ontology check of the requested VSND to check if the EEDL constraints on resources can be treated. Upon creation of the T-SLA Offer, the list of pre-allocated resources at the node-level controllers is maintained to retain the validity of the contractual offer until agreement. The T-SLA Offer contains expiry times as ISONI terms and conditions for pre-allocation and an expiry date for the provisioning of external software binaries. The T-SLA Offer further lists endpoint references that denote the monitoring and access interfaces to the VSN at execution time. Typically, the "Invitation To Treat" would contain a preserved time period for the execution of the IRMOS application to reserve a **VSN service instantiation according time plan**. However, if no starting point of the deployment period is given, the agreement on the T-SLA offer will trigger **immediate VSN service instantiation**.

The agreement on a T-SLA Offer turns the pre-allocation into a **binding T-SLA negotiation** with a fixed **reservation of dedicated network resources**.

Note, that the features **T-SLA renegotiation** and **pre-emptive termination of confirmed T-SLA** will be implemented and integrated in the final prototype - planned for PM30 [10].

5.1.5. Flow Control

The real-time network communication of IRMOS applications is ensured with the mechanisms of Intelligent Networking Flow Control that are algorithmic extensions to the components in the negotiation, selection, deployment and instantiation chain, i.e. SLA Manager, PM_D, PM_N, IXB. Flow Control subsumes the mechanisms of temporal network isolation and QoS classification for resource usage optimization in Intelligent Networking.

The SLA Manager, Path Manager Domain and Path Manager Node share a Virtual Link annotation mechanism to realize the **reservation of dedicated networking resources**. Hereby, the SLA Manager characterizes each Virtual Link with a QoS class, i.e. a virtual tag that classifies the bandwidth, delay and/or jitter constraints. This annotation is performed during the acceptance test of the T-SLA "Invitation To Treat", where the SLA Manager reasons EEDL directives of the VSND into network QoS classes. The classification is used again during the "Path Availability Check", when the Path Manager Domain chooses a transport path that suffices the denoted QoS class of the virtual link. Hereby, the Path Manager Domain chooses a concatenation of Node's external interfaces (Path-IDs) to realize the inter-node transmission of Virtual Links. Eventually, the Path Manager Node uses the annotation again to make reservations under the right QoS class for the predetermined Path-ID and when it assigns dedicated capacities to each link.

Further, the Path Manager Node and Path Manager Domain collaborate in an availability reporting that is enabled to report multiple QoS class capacities of a single path resource

(Path-ID). The Path Manager Node maintains its external path resources (Path-ID) by keeping track of the network path reservations for virtual link deployments on behalf of the Deployment Manager. Each reservation affects the availability schedules of a Path-ID's QoS classes. By the use of classifications, the Path Manager Domain can make informed decisions whether a path is capable to support the deployment of a virtual link. Together with the Path abstraction, that hides network technology details of the Node, the innovative QoS class concept allows the "Path Availability Check" to be performed light-weight and in parallel to the software dependency check.

At runtime, the IXBs in charge control a Virtual Link's share of the network resources by applying network interface admission policies to the temporally isolated Virtual Link traffic in order to provide an **isolated VSN network connectivity** that is not only isolated in terms of preventing cross talk but also isolated in a way that it prevents a Virtual Link from affecting the delay and latency constraints of a concurrent deployment, thus **ensuring confirmed real-time during execution phase**. Further details about the temporal isolation mechanisms can be found in the initial version of the Flow Control architecture [6].

5.1.6. Network Monitoring

Monitoring in IRMOS covers both, the application behaviour and the infrastructure resource provisioning. While application monitoring data, such as state changes or functional progress is monitored and consumed independently from ISONI, the infrastructure utilization by a VSN as well as the infrastructure health is measured within ISONI.

ISONI continuously provides **low-level infrastructure monitoring reports** containing the performance measurements during VSN execution. Intelligent networking contributes to the feature by performing inter-node measurements. Therefore, IXB components at each node are equipped with a sub-component "Monitoring" to perform the OWD and jitter measurements and to measure Virtual Link bandwidth usage. The components collect the information for a specific period of time and report the monitoring data to the Path Manager Node.

Secondly, Intelligent Networking contributes to the feature by providing the sub-component "Monitoring" of the Deployment Manager that correlates execution, storage and networking reports and delivers those reports to the IRMOS Monitoring FWS. It is further planned to support the ISONI SLA Manager sub-component "Violation Analyzer" by reporting occurrences of short-term transgressions of the negotiated performance guarantees.

In addition, the network measurements are checked against the scheduled resource availability to detect resource degradation for continuous **transport network supervision** at the node-level of the ISONI**.**

5.1.7. SLA Violation

The ISONI SLA Manager features autonomous evaluation of outage indications under the negotiated T-SLA to recognize a possible violation of the negotiated VSN performance guarantees.

In Intelligent Networking, the detection and treatment of an SLA violation would be performed by the SLA Manager. Therefore, ISONI Monitoring has preserved outage indications to the ISONI SLA Management to feed the process.

Note that this feature topic is planned for the Final ISONI Prototype [10] and will be specified in the planned deliverable D7.2.2 [8].

5.1.8. Virtual Link Migration

In support for live migration, the ISONI Intelligent Networking components are planned to support a prepared network link reconfiguration with an instant switchover between the old and new configuration. Virtual Link relocation is required for **ASC (VMU) relocation during application runtime** where parts of a VSN can be migrated across the infrastructure to provide an enhanced reliability for application service.

In Intelligent Networking, an exchange of a running network configuration is performed by and in alignment with the hierarchical path management components Path Manager Domain, Path Manager Node and ISONI eXchange Box (IXB). The Virtual Link Migration interfaces required to prepare and trigger an instant switchover are

Note, that migration is a feature planned for the Final ISONI Prototype [10]. Possible interface extensions to the Path Manager Node will be described in the final version of the Path Manager Architecture [8], the integration of the Virtual Link Migration feature into Intelligent Networking will be described in the final version of this document [10].

5.2. Interfaces

This chapter illustrates the interworking of Intelligent Networking components together with the interfacing components to illustrate the feature topics described in the previous chapter but also to give a detailed view on the interfaces shown in the component diagram (Figure 5).

5.2.1. SLA Negotiation

As specified in D7.2.1 [5], the T-SLA negotiation protocol is a 4-step sequence between the IRMOS T-SLA Manager Framework Service and the ISONI SLA Manager to negotiate a T-SLA covering the terms and conditions, endpoint references, and the VSN description, i.e. the VMUs, interconnections, requirements, timing, software specification, etc.

In the negotiation diagram depicted in Figure 6, the T-SLA Manager FWS inquires about the deployment of a VSN with an "Invitation To Treat" containing the T-SLA requirements. Upon inquiry, the SLA Manager internally employs a VSN-individual Deployment Manager and triggers a resource pre-allocation which includes an inquiry about the VMU creation, an availability check about possible resource locations and a pre-reservation of the Node resources. Consecutively, the interaction with the ISONI Deployment Manager can return with three different error messages as indicated in the sequence diagram, i.e. due to missing software dependencies for VMU creation, due to sudden resource shortage caused by competing reservation queries or due to an allocation failure that occurred at the node-level during pre-reservation. If the Deployment Manager returns successful, the SLA Manager retrieves the endpoint references of the planned resources and the projected VMU tailoring time to create a T-SLA Offer.

The T-SLA Manager FWS can reject the T-SLA Offer or respond with a co-signed T-SLA to arrange the agreement. In case of explicit rejection or by expiry of the T-SLA Offer, the SLA Manager advises the VSN Deployment Manager to free all pre-allocated resources and to shutdown. In case of an agreement, the SLA Manager advises the Deployment Manager to fix the node-level allocation of resources and to schedule the VMU tailoring.

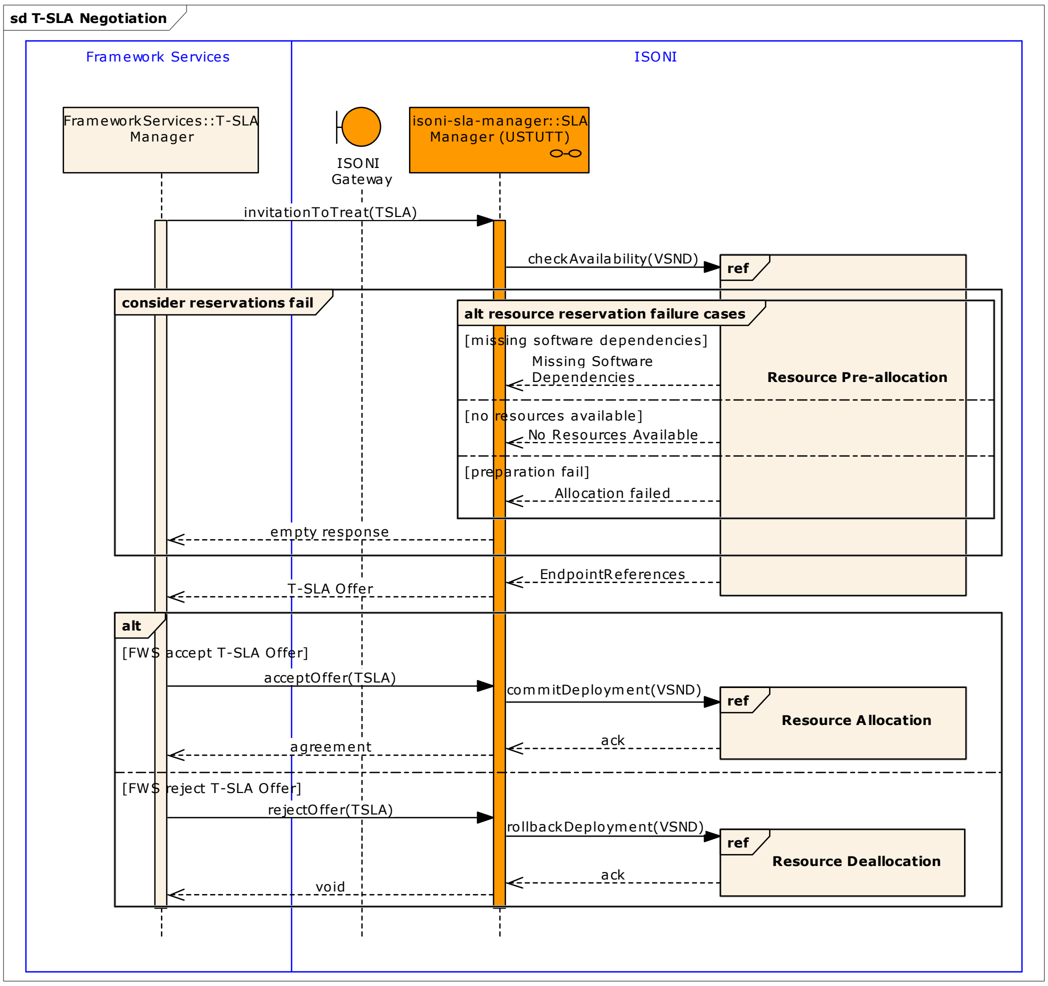

Figure 6 SLA Negotiation

5.2.2. Path Availability Reporting

Concurrently in ISONI Path Management, the PM_N delivers availability reports about the free capacities per QoS class on the Node's transitions to other Nodes or into other networks. An introduction to the Path Management's network resource model can be found in the initial version of the Path Manager Architecture [5]. A detailed description of the QoS class concept and the reported values can be found in the initial version of the Flow Control Architecture [6].

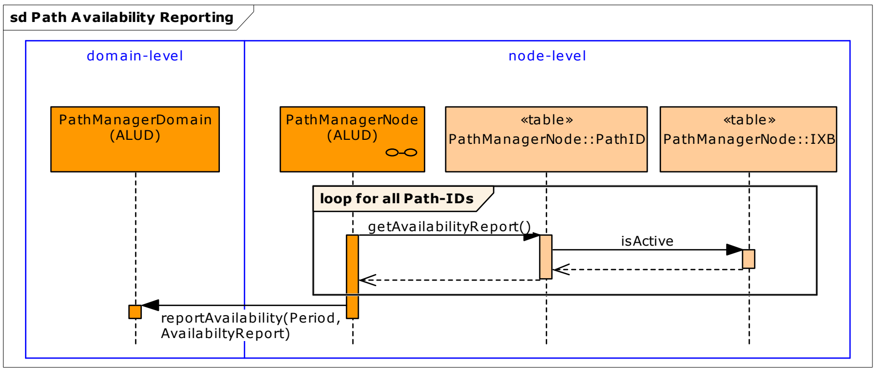

Figure 7 Path Availability Reporting

5.2.3. Path Availability Check

During the T-SLA Offer creation of the SLA negotiation, the Deployment Manager starts an availability check by requesting a coarse grained resource mapping of the VSN onto ISONI Nodes. The resource mapping process is an iteration that revisits the Path Availability Check with the Path Manager Domain, i.e. when the RM_D has found a viable Node Set, it lets the PM_D select the path mapping of Virtual Links onto Path-IDs. The Path Availability Check starts by loading the node mapping ontology model (with references, such as the EEDL spec and the VSND). For each Virtual Link that interconnects the VSN to an external network (e.g. Internet), the PM_D selects a Path-ID as transition (Point of Presence). Further the PM_D loops through all Virtual Links that run across two or more Nodes to select a Path-ID for the inter-node transmission of these links. Eventually, the PM_D responds with a path mapping that complements and validates the node selection of the RM_D.

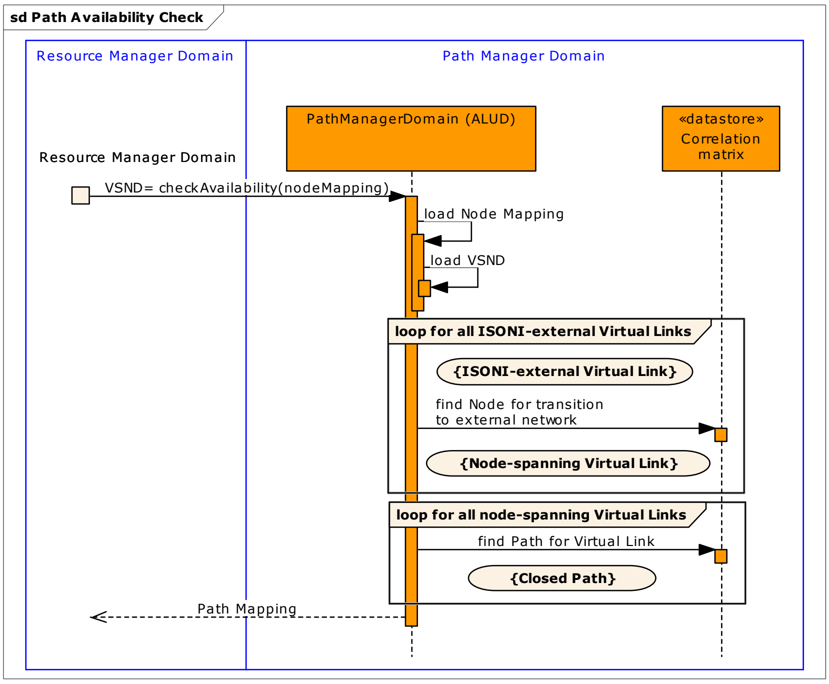

Figure 8 Path Availability Check

5.2.4. Path Reservation

Further during the T-SLA Offer creation of the SLA Negotiation, the Deployment Manager would pre-allocate the node-level resources denoted in the validated VSN resource mapping of the domain-level availability check. The 2-phase commit transaction has been applied to realize the pre-reservation. The transaction is run from the DM to the RM_N and is chained with the Path Reservation transaction to make the node-level network resource pre-allocations.

Upon request for a new deployment, the PM_N parses the Virtual Links that have a Path-ID assigned to retrieve the IXB interface configuration. If the requirements fit the capacities, the PM_N maintains deployment information for each sub-VSN that is deployed onto its path resources. The deployment contains the interface and virtualization configurations along with the Virtual Link specification (addresses, timing etc.). When finished, the transaction is responded with a virtual link configuration of the node-external path resources (for correlation at the DM).

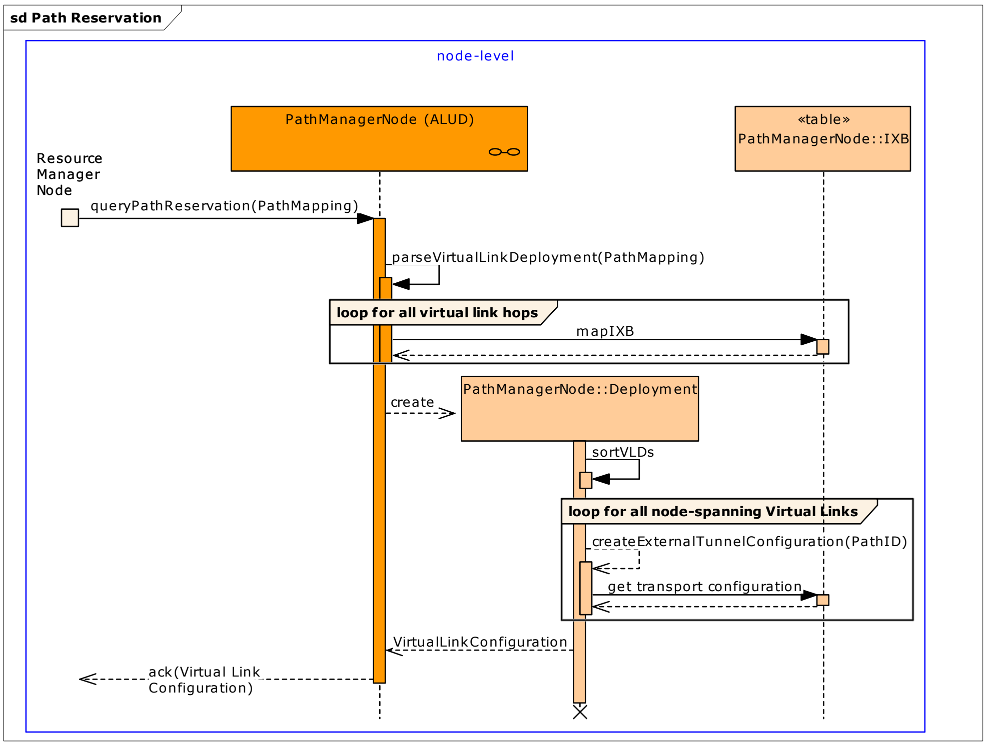

Figure 9 Query Path Reservation

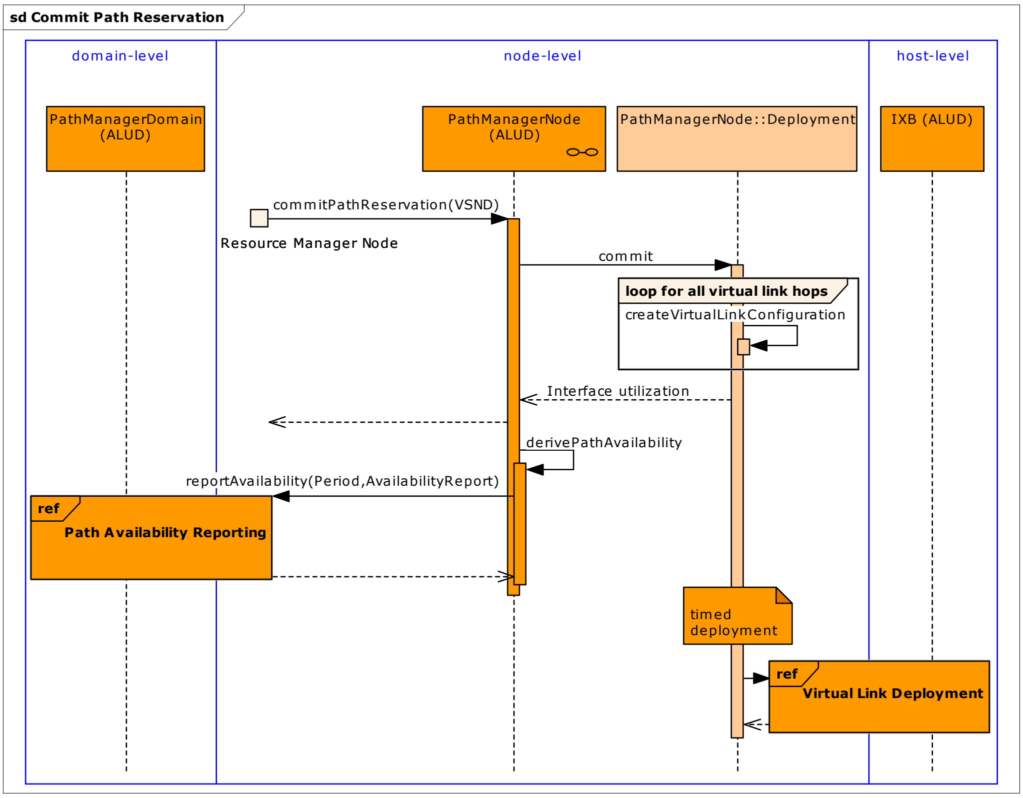

Figure 10 Commit Path Reservation

When the T-SLA Offer has been accepted in time and the agreement is arranged, the DM will fix the node-level resource reservations with the RM_N. When the RM_N has selected the host-level resources for deployment, it completes the Path Reservation transaction and delivers the correlated network path information (of node-spanning Virtual Links) along with the host-level resource selections for the sub-VSN deployment. A completed reservation at the node-level might affect the availability schedule of the PM_N's path resources and trigger an updated path availability report to the PM_D. Each reservation will trigger Virtual Link Deployment autonomously upon the scheduled deployment time.

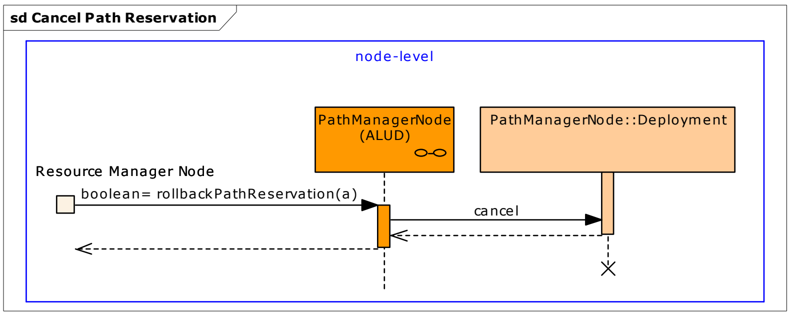

Figure 11 Rollback Path Reservation

During resource de-allocation, e.g. due to a rejected T-SLA Offer or a cancelled T-SLA, the DM frees the node-level resources by cancelling the reservation. A cancellation at the RM_N leads to a cancellation at the PM_N.

5.2.5. Virtual Link Migration

The demonstration of Virtual Link Migration is not part of the ISONI Proof of Concept with limited functionality. Path reconfiguration will be specified in the final version of the Path Manager Architecture [8], integrated and described in the Final ISONI Prototype [10], the successor of this deliverable.

5.2.6. Virtual Link Deployment

Upon deployment start time, the reservation in the PM_N will trigger the setup of virtual links at the host-level by advising each IXB to employ the provided Virtual Link configuration per used interface. During the deployment time, i.e. during transmission of data on Virtual Links, the IXB exchanges Virtual Link Monitoring data with the PM_N. At the scheduled deployment end time (or exceptional request), the Virtual Link configuration is removed from the interfaces of the employed IXBs.

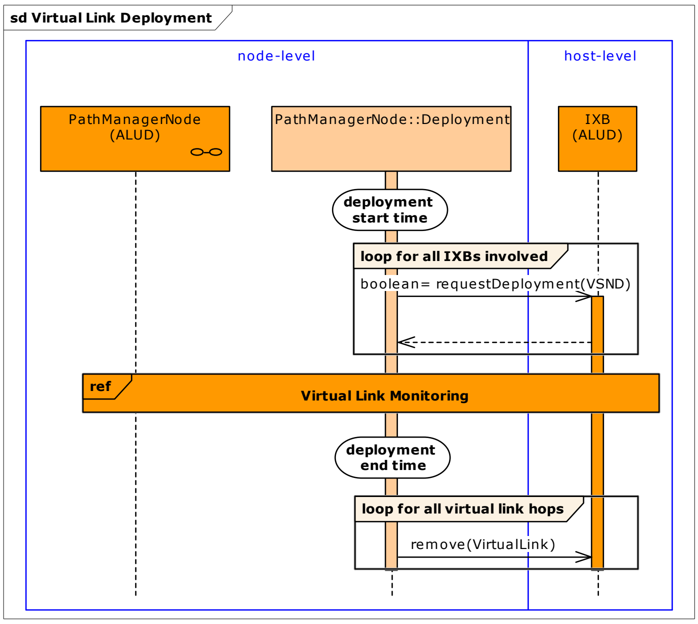

Figure 12 Virtual Link Deployment

5.2.7. Path / Virtual Link Monitoring

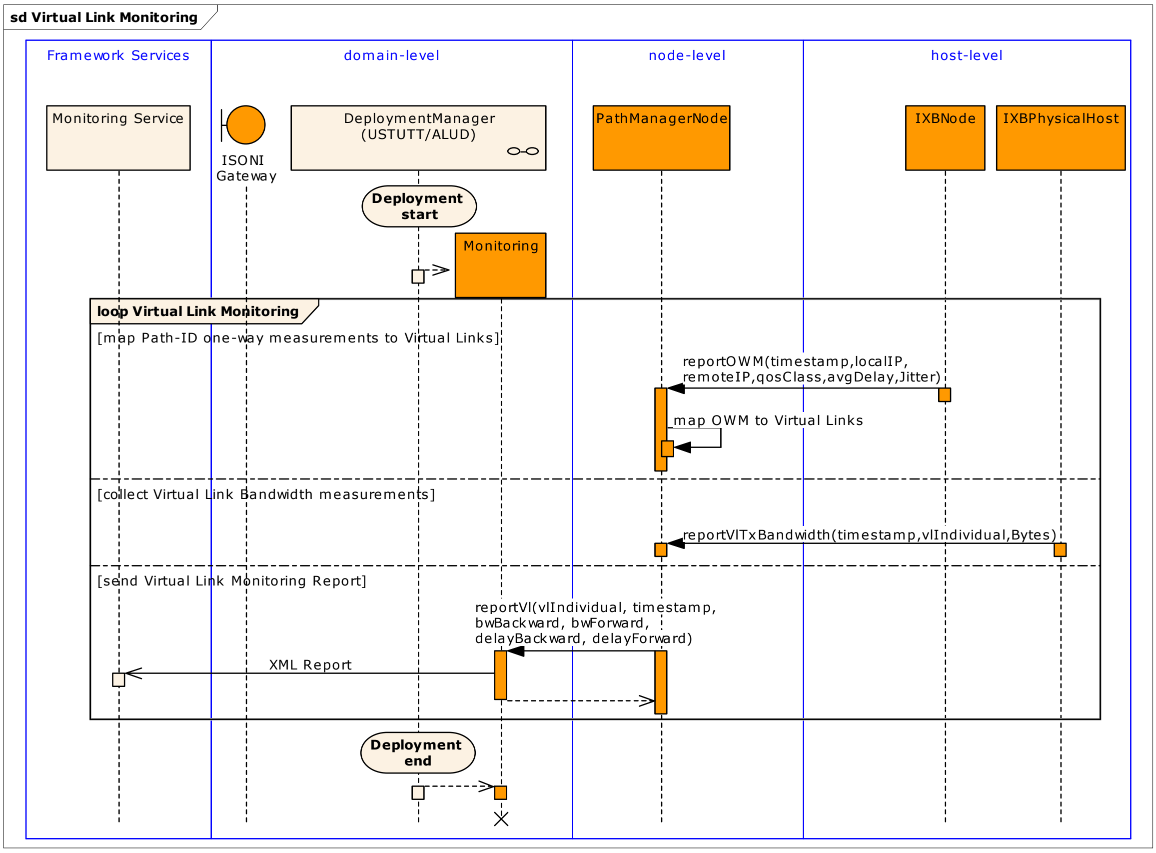

Figure 13 Virtual Link Monitoring

- **Inter-node measurement components and Path Manager**: the interface is implemented using XML-RPC. The inter-node measurements components report on predefine periods the set of values for OWD and jitter on the links running to the Path Manager.

- **Path Manager Node**: the PM_N projects path measurements onto virtual links and correlates virtual link bandwidth information to deliver Virtual Link monitoring reports to the Deployment Manager component's Monitoring part for the sub-VSN per reported time period
- **Deployment Manager / Monitoring**: Virtual Link monitoring reports are collected from each sub-VSN and correlated with monitoring reports of utilized computational and storage resources to a full VSN monitoring report that is delivered to the IRMOS Framework Services Monitoring component via the ISONI Gateway

5.2.8. Outage Reporting

The demonstration of Outage reporting is not part of the ISONI Proof of Concept with limited functionality (current deliverable). However, outage reporting in support of the Violation Analyzer will be specified in the final version of the Path supervision architecture [9] and integrated into the final ISONI Prototype [10], the successor of this deliverable.

6. References

[1] IRMOS Project D3.1.2 IRMOS Overall Architecture, NTUA and other partners, February 2009

[2] IRMOS Project D3.1.3 Updated version of IRMOS Overall Architecture, NTUA and other partners, January 2010

[3] IRMOS Project D4.2.1 Interface Definition to the IRMOS SOI, GILABS and other partners, June 2009

[4] IRMOS Project D7.1.1 ISONI addressing schemes, USTUTT and other partners, November 2008

[5] IRMOS Project D7.2.1 Initial version of Path Manager Architecture, ALUD and other partners, May 2009

[6] IRMOS Project D7.3.1 Initial version of Flow Control Architecture, ALUD and other partners, August 2009

[7] IRMOS Project D7.4.1 Initial version of Path supervision Architecture, ALUD and other partners, November 2009

[8] IRMOS Project D7.2.2 Final version of Path Manager Architecture, ALUD and other partners, planned May 2010

[9] IRMOS Project D7.4.2 Final Version of Path supervision Architecture, ALUD and other partners, planned May 2010

[10] IRMOS Project D7.5.2 Final ISONI Prototype, ALUD and other partners, planned August 2010

Annex A. Innovations, features and components

A.1. IRMOS features by Intelligent Networking innovations

Intelligent Networking Innovations / IRMOS features containing Intelligent Networking innovations	Isolation (ch 3.1.1)	Network support for live migration (ch 3.1.2)	QoS-enabled network resource discovery and instantiation. (ch. 3.2.1)	Automated SLA negotiation (ch. 3.2.2)	Temporal network traffic isolation (ch. 3.3.1)	QoS classification for resource usage optimization (ch. 3.3.2)	Path supervision (ch. 3.4)
Automated negotiation and establishment of an SLA			X	X			
SLA renegotiation				X			
IRMOS resource reservation for the application execution				X			
Instantiation of the application inside IRMOS			X				
Application execution keeping QoS guarantees					X		
Enhanced reliability for application service		X				X	
Application service isolation	X						
ASCs have external communication if required	X						
Customer monitoring of running application							X
Seamless change of used infrastructure resources		X					
Infrastructure health supervision							X

Table 2 IRMOS features vs. Intelligent Networking innovations

A.2. ISONI features / IRMOS features

IRMOS features supported by ISONI Intelligent Networking features / ISONI features supported by Intelligent Networking developments	Automated negotiation and establishment of an SLA	SLA renegotiation	Discovery of ISONI Providers capabilities	IRMOS resource reservation for the application execution	Instantiation of the application inside IRMOS	Application execution keeping QoS guarantees	Enhanced reliability for application service	Application service isolation	ASCs have external communication if required	Customer monitoring of running application	Seamless change of used infrastructure resources	The developer can execute benchmarking applications	Infrastructure health supervision	General IRMOS platform authentication and authorization
Transport network supervision													X	
Providing public IP address and external access									X					
ISONI enforces authentication and authorization for FS interactions														X
Low-level VSN description	X													
Non-Binding T-SLA negotiation			X											
Binding T-SLA negotiation				X										
T-SLA renegotiation		X												
Reservation of dedicated networking resources				X										
Immediate VSN service instantiation	X				X									
VSN service instantiation according time plan	X				X									
Isolated VSN network connectivity								X						
Ensuring confirmed real-time during execution phase						X								
Providing low-level infrastructure monitoring reports										X		X		
ASC (VMU) relocation during application runtime							X				X			
Pre-emptive termination of confirmed T-SLA	X													

Table 3 ISONI features vs. IRMOS features

A.3. ISONI features / Intelligent Networking component parts

ISONI features supported by Intelligent Networking components \ Intelligent Networking components involved in carrying out the ISONI feature	ISONI gateway	SLA Manager (base)	SLA Manager / QoS Mapping	SLA Manager / Violation Analyzer	Path Manager Domain (base)	Path Manager Domain / Flow Control	Deployment Manager / Monitoring	Path Manager Node (base)	Path Manager Node / Flow Control	Path Manager Node / Monitoring	IXB (base)	IXB / Flow Control	IXB / Monitoring
Transport network supervision										X			X
Providing public IP address and external access					X			X			X		
ISONI enforces authentication and authorization for FS interactions	X												
Low-level VSN description		X	X	X	X			X			X		
Non-Binding T-SLA negotiation	X	X			X	X							
Binding T-SLA negotiation	X	X			X			X	X				
T-SLA renegotiation[5]	X[5]	X[5]			X[5]	X[5]		X[5]	X[5]				
Reservation of dedicated networking resources		X			X	X		X	X				
Immediate VSN service instantiation								X			X		
VSN service instantiation according time plan								X			X		
Isolated VSN network connectivity											X	X	
Ensuring confirmed real-time during execution phase			X	X								X	
Providing low-level infrastructure monitoring reports	X						X			X			X
ASC (VMU) relocation during application runtime					X[5]			X[5]		X[5]	X[5]		
Pre-emptive termination of confirmed T-SLA	X	X						X			X		

Table 4 ISONI features vs. Intelligent Networking components

[5] feature is scheduled for D7.5.2 Final ISONI prototype