Maßnahmen zur Sicherung von E2E-QoS bei Verketteten Diensten

Dissertation

an der

Fakultät für Mathematik, Informatik und Statistik
der
Ludwig-Maximilians-Universität München

vorgelegt von

Mark Yampolskiy

Tag der Einreichung: 27.10.2009
Tag der mündlichen Prüfung: 18.12.2009

1. Berichterstatter: Professor Dr. Heinz-Gerd Hegering, Ludwig-Maximilians-Universität München

2. Berichterstatter: Professor Dr. Johann Schlichter, Technische Universität München

Maßnahmen zur Sicherung von E2E-QoS bei Verketteten Diensten

Dissertation

an der

Fakultät für Mathematik, Informatik und Statistik
der
Ludwig-Maximilians-Universität München

vorgelegt von

Mark Yampolskiy

Tag der Einreichung: 27.10.2009
Tag der mündlichen Prüfung: 18.12.2009

1. Berichterstatter: Professor Dr. Heinz-Gerd Hegering, Ludwig-Maximilians-Universität München

2. Berichterstatter: Professor Dr. Johann Schlichter, Technische Universität München

Für meine Großeltern,

Sara und Alexander Zekhtser

Danksagung

Diese Arbeit ist im Rahmen meiner vom DFN-Verein geförderten Tätigkeit als wissenschaftlicher Mitarbeiter am Leibniz-Rechenzentrum der Bayerischen Akademie der Wissenschaften (LRZ) sowie als Mitglied des von Prof. Dr. Heinz-Gerd Hegering geleiteten Munich Network Management Teams entstanden.

Eine Arbeit, bei der man in vielerlei Hinsicht über sich selbst hinauswachsen soll, ist kaum allein zu bewältigen. Deswegen möchte ich mich ganz herzlich bei den Leuten bedanken, die mich während der Bewältigung dieser Herausforderung begleitet und oft auch durch die schwierigen Abschnitte geleitet haben.

Mein erster und besonderer Dank gilt meinem Doktorvater Prof. Dr. Heinz-Gerd Hegering, der mir durch die Aufnahme in das MNM-Team die Durchführung dieser Arbeit erst ermöglicht hat. Während der ganzen Bearbeitungszeit hat Herr Prof. Dr. Heinz-Gerd Hegering fürsorglich meine Fortschritte beobachtet und dabei geschickt meine Aufmerksamkeit auf die wichtigen Aspekte und meine Bemühungen in die richtige Richtung gelenkt, wodurch er entscheidend zum Gelingen dieser Arbeit beigetragen hat. Herzlich möchte ich mich auch bei Herrn Prof. Dr. Johann Schlichter für die Bereitschaft bedanken, die Entstehung der Arbeit als Zweitgutachter zu begleiten.

Bei meinen Kollegen aus dem MNM-Team möchte ich mich für die seltene Mischung aus sehr angenehmer persönlicher Atmosphäre und erbarmungsloser fachlicher Kritik bedanken. Insbesondere möchte ich mich bei meinen "Diss-Paten" Wolfgang Hommel, Michael Schiffers und Vitalian Danciu bedanken, die während der Entstehung dieser Arbeit sich die Zeit genommen haben, über die erarbeiteten Lösungsansätze und die aufgedeckten Probleme zu diskutieren und mir dabei sehr hilfreiche Ideen und Hinweise zur Herangehensweise gegeben haben. Aus meinem Projekt- und Arbeitsumfeld möchte ich mich vor allem bei Matthias Hamm bedanken, mit dem wir ständig und über alles Mögliche diskutiert haben, wodurch meine Argumentationsfähigkeit sich deutlich verbessert hat. Für die Hilfe bei der Fehlerkorrektur und bei der Konsistenzprüfung der entstandenen Arbeit möchte ich mich ganz herzlich bei Matthias Hamm und David Schmitz bedanken.

Während die wissenschaftliche Qualität der Arbeit überwiegend von der fachlichen Kompetenz und den didaktischen Fähigkeiten des Autors abhängt, hängt der Verlauf deren Entstehung auch von persönlichen Eigenschaften und Einflüssen ab. Aus diesem Grund möchte ich mich auch bei den Leuten bedanken, zu denen ich im Laufe der Jahre aufgeblickt habe, die mich begeistert, überrascht und nicht allzu selten aus der Bahn der gewöhnten Denkweise geworfen haben, wodurch sie meine persönliche Entwicklung auf unterschiedliche Art und Weise beeinflusst haben.

In erster Linie möchte ich mich bei meinen Großeltern, Sara und Alexander Zekhtser, sowie bei meiner Mutter, Bronislava Yampolskaya, ganz herzlich bedanken, die meine Welt- und Wertevorstellung insbesondere in jungen Jahren sehr stark geprägt

haben. Weiterhin möchte ich mich auch bei Natalia Komarova (Alias *Margo*), Efim Starostin (Alias *Star*), Svetlana Barskaya (Alias *Lisunbars*), *Sifu* Sergej Korpiun, Angelina Pak (Alias *Angelika*), Matthias Zahl und Irina Raevskaya (Alias *Kassandra*) bedanken. An dieser Stelle möchte ich mich noch einmal bei meinem Doktorvater Prof. Dr. Heinz-Gerd Hegering bedanken, der in den letzten Jahren nicht nur meine fachliche, sondern auch persönliche Entwicklung auf sehr vielfältige Art und Weise beeinflusst hat.

Allen Genannten fühle ich mich zutiefst verbunden und kann an dieser Stelle nur noch eines sagen – Danke!

München, im Oktober 2009

Abstract

Most of the international and national network connection services are realized as a concatenation of partial services provided by different *Service Providers* (SPs). Users of such connections face the overall *End-to-End* (E2E) *Quality of Service* (QoS). Currently, in order to ensure E2E-QoS, hierarchical organizational relationships between involved SPs have to be established. In order to maintain independence between service providers, the *best-effort* strategy is used. In order to foster novel international research projects and customer-faced business services, a sudden demand for the technical solutions was developed. This allowed guaranteed E2E-QoS of network connections without having to introduce hierarchical organizational forms. This thesis introduces *Concatenated Services* as defined by combination of outlined specific technical and organizational characteristics.

In order to derive requirements for the new solution, interests of involved actors in most advanced existing connection services and research projects have been analyzed. The further study of state of the art solutions in relevant research areas provide various "building blocks" and lessons learned that are considered when solving the specified challenge.

The developed solution consists of three parts: a novel SLM-aware Routing Architecture, a communication protocol, and reference processes for Service Level Management of Concatenated Services.

The SLM-aware Routing Architecture provides the core of the developed solution. During the routing process in the developed solution, not only the path of the connection but also the QoS-requirements and management functionality of all involved connection parts are defined. Assignment of actors to necessary roles and communication channels between all involved management components during provisioning phase enables the *Service Level Management* (SLM) of the established Concatenated Service instance during its operation.

The definition of a new appropriate communication protocol provides the glue for service provider collaboration. This protocol covers the signaling and the information exchange during the whole service instance life cycle from ordering till decommissioning. Specification of base processes associated with every allowed signal provides the way to unambiguous behavior definition.

The definition of reference processes for Service Level Management of Concatenated Services rounds up the developed solution. In order to ensure the customizability and easy adaptation to the additional service specific requirements, all SLM-processes are defined on the top of the communication protocol and associated base processes.

The exact operation of the elaborated solution is illustrated by one detailed example. The quality of the solution is evaluated based on the experience made by the

application of the developed concepts in several research projects and by the discussion of specified requirements. A short outline of further development of the presented solution and relevant research questions conclude the presented PhD Thesis.

Zusammenfassung

Die meisten internationalen und oft auch nationalen Netzverbindungen sind als horizontal gekoppelte Teildienste realisiert, die von mehreren Service Providern (SPs) erbracht werden. Die Ende-zu-Ende (E2E) Dienstgüte (engl. *Quality of Service*, QoS) setzt sich aus der Güte der involvierten Teildienste zusammen. In Bezug auf die E2E-QoS haben sich zwischen den SPs zwei Herangehensweisen etabliert: für die garantierte E2E-Dienstgüte werden üblicherweise hierarchische Organisationsbeziehungen aufgebaut, bei einer Gleichberechtigung der beteiligten Provider (was bei Internet- und Telefonverbindungen häufig der Fall ist) hat sich die sog. *Best-Effort*-Strategie durchgesetzt. Durch die Anforderungen der modernen internationalen Forschungsprojekte und der neuartigen kundenorientierten Dienste ist nun der Bedarf entstanden, die E2E-QoS bei Netzverbindungen auch dann zu garantieren, wenn der Aufbau hierarchischer Organisationsbeziehungen aus diversen Gründen nicht möglich ist. Die Dienstklasse, die die angesprochenen technischen und organisatorischen Eigenschaften in sich vereint, wird in dieser Arbeit als Verkettete Dienste (engl.: *Concatenated Services*) referenziert.

Um die Anforderungen für die zu entwickelnde Lösung zu bestimmen, werden in dieser Arbeit die Interessen unterschiedlicher Akteure in verschiedenen Verbindungsdiensten analysiert. Eine darauffolgende Untersuchung von existierenden Lösungen in relevanten Forschungsbereichen liefert eine Reihe von möglichen Lösungsbausteinen und lehrreichen Erfahrungen, die bei der Konzeption der eigentlichen Lösung berücksichtigt werden.

Die entwickelte Lösung besteht aus drei Teilen. Der Kern der Lösung ist durch die SLM-aware Routing-Architektur gegeben. In der entwickelten Lösung werden während des Routings nicht nur der Pfadverlauf, sondern auch die QoS-Anforderungen und die benötigte Managementfunktionalität aller involvierten Teildienste bestimmt. Durch die Bestimmung der Akteure, die die benötigten Rollen übernehmen sollen, sowie der Kommunikationswege zwischen Managementkomponenten wird die Durchführung von *Service-Level-Management* (SLM) in allen Lebenszyklusphasen ermöglicht.

Die Integrationsrolle zwischen den SPs wird von dem Kommunikationsprotokoll übernommen. Das Protokoll ist sowohl für die Signalisierung als auch für den Informationsaustausch während des kompletten Dienstinstanz-Lebenszyklus zuständig. Die mit den erlaubten Signalen assoziierten Basisprozesse erlauben eine unmissverständliche und intuitive Definition des erwarteten Verhaltens.

Die Definition von Referenzprozessen für Service Level Management bei Verketteten Diensten rundet die entwickelte Lösung ab. Die SLM-Prozesse bauen ausschließlich auf dem zuvor definierten Kommunikationsprotokoll auf, wodurch eine leichte Anpassbarkeit dieser Prozesse an zusätzliche Anforderungen gewährleistet wird.

Die Funktionsweise der entwickelten Lösung wird an einem detaillierten Beispiel illustriert. Die Güte der Lösung wird anhand der Erfahrungen mit der Integration der Lösungsteile in verschiedenen Forschungsprojekten sowie anhand der aufgestellten Anforderungen bewertet. Ein kurzer Ausblick auf die Weiterentwicklungsmöglichkeiten und auf verwandte Forschungsfragestellungen schließt diese Arbeit ab.

Inhaltsverzeichnis

Teil I.

Motivation, Szenarien und Anforderungsanalyse

1 Einleitung

1.1. Status Quo

Die ständig fortschreitende weltweite Vernetzung insbesondere von Telekommunikations- und Datennetzen erfordert oft die Kooperation von mehreren Betreiberorganisationen. Diese Kooperation, die auf sowohl auf technischer wie auf organisatorischer Ebene abläuft, umfasst sowohl vertikale als auch horizontale Kopplungen. Unter einer *vertikalen Kopplung* wird ein geschichteter Dienstaufbau verstanden, bei dem Dienste auf der Dienstfunktionalität unterliegender Schichten aufbauen. Ein Beispiel für eine vertikale Kopplung ist z.B. ein Webhosting-Dienst, der auf einen IP-Dienst angewiesen ist. Beide Dienste werden üblicherweise von unterschiedlichen Service Providern erbracht. Unter *horizontaler Kopplung* wird dagegen eine Diensterbringung verstanden, die durch Zusammenarbeit von räumlich getrennten Diensten auf derselben Schicht erbracht wird [HAN99]. Dienste, die durch vertikale bzw. horizontale Kopplung zu Stande kommen, werden in der Literatur entsprechend als *Diensthierarchie* (engl.: *Vertical Supply Chain*) bzw. *Dienstkette* (engl.: *Horizontal Supply Chain*) referenziert [DR02]. Beide Formen des Dienstaufbaus sind in Abbildung 1.1 dargestellt.

vertikale Kopplung

horizontale Kopplung

Diensthierarchie

Dienstkette

Während vertikale Kopplung und Diensthierarchien sehr gut untersucht und verstanden sind [HAN99, Lan01, Ner01], zeigt sich, dass die bereits existierenden Ansätze horizontaler Kopplung den Anforderungen aktueller internationaler Projekte an den Dienstaufbau und die Dienstgüte (*Quality of Service*, QoS) von Dienstketten nicht immer genügen.

QoS

Bislang haben sich für eine horizontale Kopplung auf derselben technischen Netzebene zum einen die (im Internet als *Peering* bekannte) Kopplung zwischen zwei gleichberechtigten Partnern und zum anderen der Aufbau von hierarchischen Customer-Provider-Strukturen als dominierende Organisationsformen durchgesetzt. Peering-ähnliche Kopplung findet starke Verbreitung in Telekommunikationsnetzen bei der Schal-

dominierende Organisationsformen bei Dienstketten

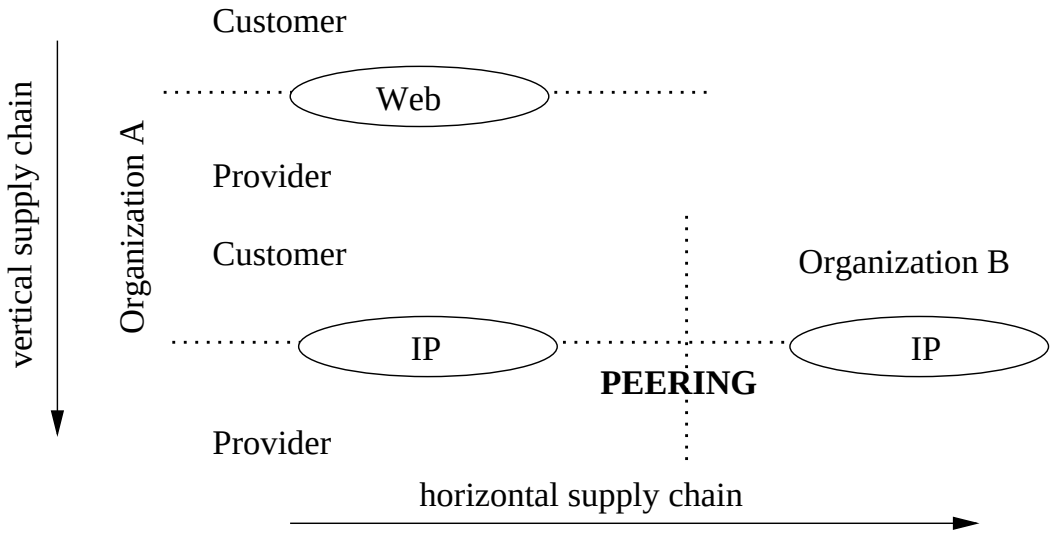


Abbildung 1.1.: Vertical and horizontal supply chain [DR02]

tung von Telefonverbindungen, im Internet bei der Kopplung von unterschiedlichen Netzen auf IP-Ebene, so wie auch bei unterschiedlichen Netzwerkprotokollen, wie z.B. bei rekursiven DNS-Anfragen. Die Bedingungen für das Peering werden in bilateralen Abkommen zwischen benachbarten Providern festgelegt.

best effort Strategie bei Peering

Die relative Einfachheit der technischen Realisierung sowie der Abrechnung trug zu der weiten Verbreitung von Peering-Verfahren bei. Allerdings weist Peering auch eine Reihe von Nachteilen auf. So werden z.B. die Qualitätsanforderungen ausschließlich in Bezug auf die Kopplung der benachbarten Netze gestellt; die Qualität und die Eigenschaften der gesamten Verbindung über mehrere Provider hinweg wird dabei jedoch nicht berücksichtigt und ausschließlich mit einer *best effort Strategie* angegangen. Folgen solcher Vorgehensweise kann man sehr deutlich am Beispiel von ISDN-Telefonverbindungen sehen, bei denen jeder der bei der Verbindung beteiligten Provider nur die Dienstmerkmale weiterleitet, die vom Provider-eigenen Netz unterstützt werden. So kann es u.U. zu reiner Sprachvermittlung ohne zusätzliche Dienstmerkmale, wie z.B. Telefonnummernanzeige des Gesprächspartners, kommen. Somit können bei Peering i.A. keine Ende-zu-Ende (*End-to-End*, E2E) QoS-Zusicherungen gewährleistet werden. Der Aufbau von E2E-Verbindungen mit einer definierten Qualität wird durch Peering nicht unterstützt, da sich die Managementfunktionalität bei diesem Verfahren ausschließlich auf die eigene Domäne beschränkt.

Für QoS-Zusicherungen haben sich zwei prinzipiell unterschiedliche Verfahren etabliert:

Overprovisioning und hierarchische Organisationsformen als etablierte Maßnahmen für QoS-Zusicherung

- Bei klassischen Peering-Diensten bemühen sich die Provider um das sog. *Overprovisioning* der eigenen Ressourcen. Das wird oft durch eine Kopplung der Dienstnutzungskosten an die Tageszeit unterstützt. So soll eine gleichmäßige Nutzung der vorhandenen Ressourcen erzielt werden.
- Falls die Dienstqualität dennoch abgesichert werden soll, so wird das häufig mit Hilfe hierarchischer Organisationsformen gelöst; dabei nimmt eine übergeordnete Organisation die Aufgabe wahr, die geforderte Dienstgüte durch eigene *Service Level Agreement* (SLA) Abkommen mit jedem der bei der Diensterbringung beteiligten Provider zu sichern und gegenüber den Kunden als alleiniger Anbieter ein eigenes SLA anzubieten. Diese Organisationsform wird auch dann verwendet, wenn ein Provider einige der für die Diensterbringung benötigten Leistungen nicht vollständig selbst erbringt, sondern bei anderen Providern (Sub-Provider) einkauft. Auch bei großen und kostspieligen Projekten, wie z.B. bei transatlantischen Verbindungen, wird normalerweise ähnlich vorgegangen und der komplette Dienst wird von einer einzigen Organisation betrieben (im Falle des Transatlantikkabels wurde ein Konsortium aus allen beteiligten Providern gebildet, wobei jeder Provider für die Instandhaltung eines Abschnittes des Kabels zuständig ist) [Tat07].

Industrie und Forschung stellen allerdings oft Anforderungen und Randbedingungen auf, die den Einsatz etablierter Verfahren verhindern.

1.2. End-to-End Links in Géant2

Die moderne Forschungslandschaft wird zunehmend durch Projekte geprägt, die nur in internationaler Kooperation bewältigt werden können und daher auch Netzverbindungen zwischen beteiligten Organisationen benötigen. Für europäische Forscher wird diese Grundvoraussetzung durch das europäische Backbone-Netz *Géant2* geschaffen. Zu den Hauptaufgaben von Géant2 gehören Entwicklung und Aufbau der Netzinfrastruktur, die die Verbindungen zwischen den nationalen Wissenschaftsnetzen (*National Research and Education Network*, NREN) realisiert. Derzeit verbindet Géant2 rund 30 europäische NRENs miteinander und bindet diese an nicht-europäische Wissenschaftsnetze wie z.B. von Nordamerika, Russland und Taiwan an [Gea09]. Als Kerndienst wird in Géant2 eine IP-Infrastruktur betrieben und ständig ausgebaut, die für die meisten Dienste ausreichend ist. Die derzeitige Topologie des Géant2 IP Backbone ist in Abbildung 1.2 dargestellt.

Géant2

NREN

Für die meisten Forschungsprojekte erfüllt dieses IP-Netz alle gestellten Anforderungen. In den letzten Jahren sind allerdings internationale Projekte entstanden, deren Anforderungen die Leistung und Ausrichtung klassischer IP-Netze übersteigen. Zwei

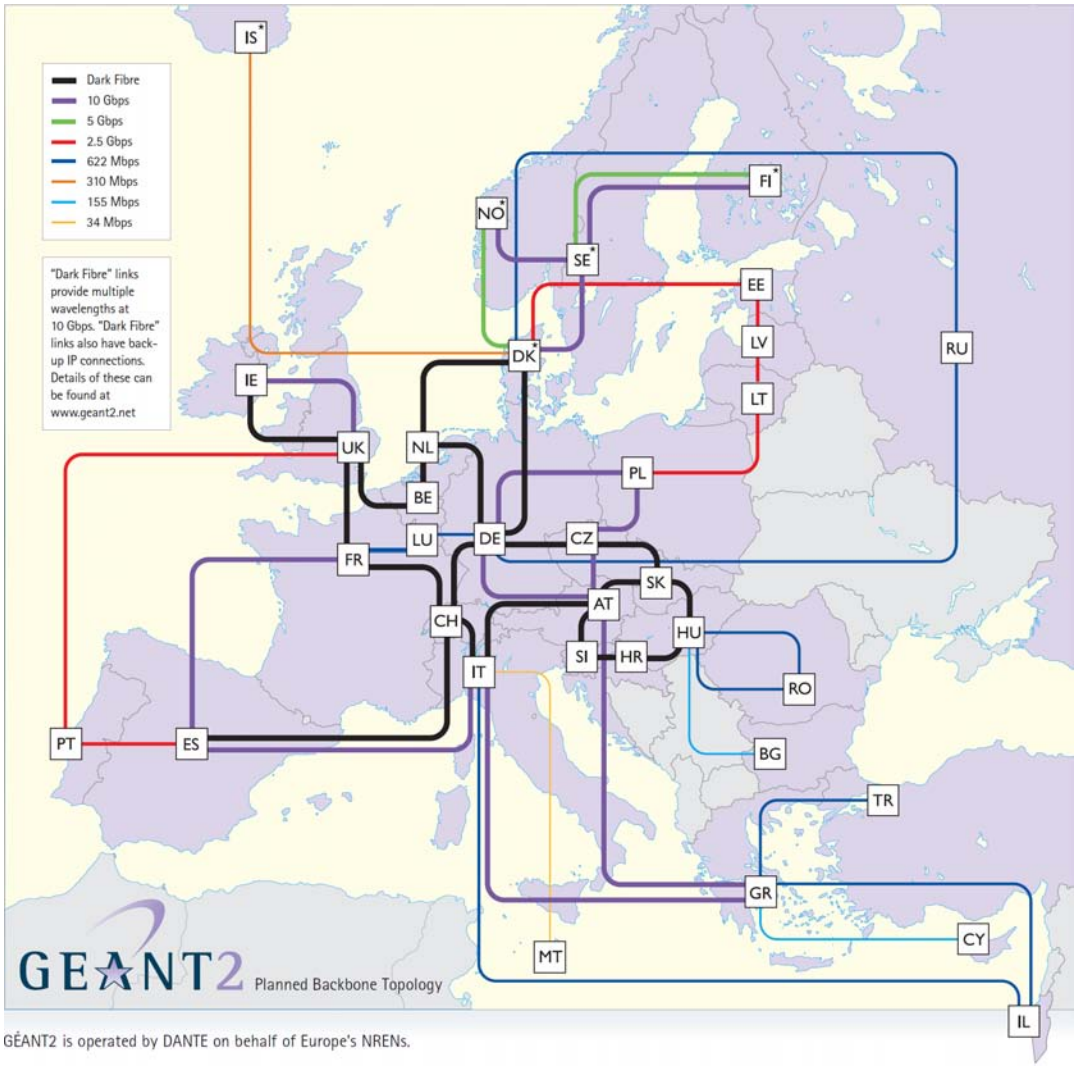


Abbildung 1.2.: Das Géant2 IP Backbone Netz, aus: [Gea09]

der prominentesten Projekte, die außerordentlich hohe Anforderungen an die Dienstgüte verwendeter Verbindungen stellen, sind LHC [LHC08a] und die europäische Grid-Initiative DEISA [DEI08a].

LHC Bei dem Large Hadron Collider (LHC) Projekt handelt es sich um einen Teilchenbeschleuniger, der zurzeit am Europäischen Kernforschungszentrum CERN bei Genf gebaut wird. Außer europäischen Ländern, USA und Kanada sind an dem Projekt u.A. auch Länder wie Russland, Japan und Israel beteiligt [LHC08b]. Die bei LHC-Experimenten erzeugten Messdaten werden auf etwa 8 PB und die bei Simulationen auf weitere 4 PB pro Jahr geschätzt [Gri08]. Allein um dieses gewaltige Datenaufkommen abspeichern und bearbeiten zu können, werden elf Höchstleistungsrechenzentren

benötigt. Die Analyse der experimentell erworbenen Daten und Simulationen wird in über 100 weiteren in der ganzen Welt verteilten Rechenzentren durchgeführt. Dafür werden permanente Netzverbindungen zwischen den Rechenzentren benötigt. Ausfälle bei diesen Verbindungen werden im LHC als sehr kritisch angesehen, da dadurch wertvolle Daten der Experimente verloren gehen können. Aus diesem Grund müssen z.B. Wartungsarbeiten, die diese Verbindungen beeinträchtigen können, mit den LHC-Verantwortlichen abgestimmt und genehmigt werden.

DEISA

Bei der Grid-Initiative DEISA (*Distributed European Infrastructure for Supercomputing Appications*) handelt es sich um ein europaweites Projekt, an dem sich elf Höchstleistungsrechnerzentren aus sieben EU-Ländern beteiligen. Ähnlich wie bei LHC werden für dieses Projekt permanente Verbindungen zwischen beteiligten Rechenzentren benötigt, die in der Lage sein müssen, mehrere Terabyte an Daten zu bewältigen. Ausfallsicherheit und Verfügbarkeit dieser Verbindungen werden nicht so kritisch wie bei LHC angesehen, da dadurch keine u.U. unwiederbringlichen Daten verloren gehen können. Dafür müssen aber strenge Anforderungen an unterschiedliche Dienstgütewerte wie z.B. Delay, Jitter und Fehlerrate einzelner Verbindungen eingehalten werden, damit die Zusammenarbeit mehrerer Rechenzentren im Rahmen eines globalen Filesystems innerhalb eines Grids möglich ist und nicht durch Synchronisationsprobleme behindert wird [NM08].

Permanentes Routing aller dieser Daten über das normale IP Backbone-Netz von Géant2 würde andere Dienste beeinträchtigen. Andererseits würden auch andere Netflows, die um dieselben physischen Ressourcen konkurrieren, den Datenverkehr von LHC und DEISA beeinflussen, wodurch erforderliche QoS-Grenzwerte nicht garantiert werden könnten.

E2E Links

Um den neuen Anforderungen gerecht zu werden, wurde in Géant2 ein neuer Dienst – End-to-End *(E2E)* Links – konzipiert.

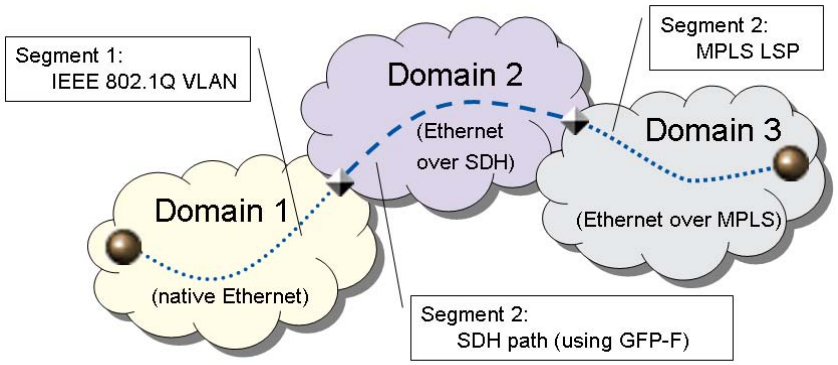


Abbildung 1.3.: Géant2 End-to-End Links mit Beispieltechnologien

E2E Links sind dedizierte optische multi-Gigabit Verbindungen

Bei *Géant2 E2E Links* handelt es sich um dedizierte optische multi-Gigabit Verbindungen zwischen zwei wissenschaftlichen Einrichtungen (im Weiteren auch Endpunkte genannt). Da bei dedizierten Verbindungen die Notwendigkeit des Routings entfällt, werden diese Verbindungen auf ISO/OSI Schicht 2 realisiert, um unnötige Kosten für die verhältnismäßig teure Router-Infrastruktur zu vermeiden [SW06]. Der für E2E Links typische Aufbau, bei dem die Endpunkte sich in unterschiedlichen Domänen befinden, ist in Abbildung 1.3 dargestellt. Dabei "zerfällt" der E2E Link in mehrere Abschnitte, die jeweils von einem anderen Netzbetreiber (Domain) zur Verfügung gestellt und betrieben werden und auch mit unterschiedlichen Netztechnologien realisiert werden können [YH07].

1.3. Verkettete Dienste

Streng genommen handelt es sich bei *Géant2 E2E Links* um Dienstketten, die durch eine horizontale Kopplung der Teildienste zustande kommen. Die Teildienste werden in diesem Fall von den Netzbetreibern aus unterschiedlichen – im Falle von E2E Links für LHC auch außereuropäischen – Ländern erbracht. Der Aufbau von hierarchischen Organisationsbeziehungen wäre daher allein aus politischen Gründen unmöglich. Somit herrscht zwischen den Providern sog. *Heterarchie* (zu Deutsch: Gleichberechtigung und Autonomie der Beteiligten) [Rei98, BK04]. Gleichzeitig wird seitens der über diese Dienstketten abgewickelten Projekte eine Reihe von i.A. unterschiedlich harten E2E Dienstgüteanforderungen an diese Verbindungen gestellt. Die Einordnung des erforderlichen Dienstes ist graphisch in Abbildung 1.4 dargestellt.

Heterarchie

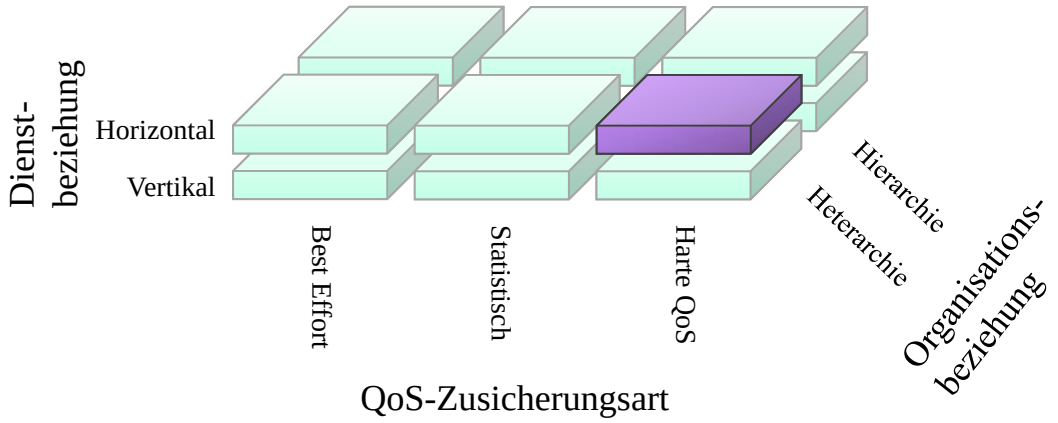


Abbildung 1.4.: Verketteter Dienst, Einordnung

Verkettete Dienste

Dienste, die alle drei Eigenschaften (Horizontale Kopplung, Heterarchie und harte E2E QoS-Zusicherung) aufweisen, werden im weiteren Verlauf dieser Arbeit als *Verkettete Dienste* (engl: *Concatenated Services*) referenziert.

Dienstgütezusicherung durch Overprovisioning gehört zu den sog. statistischen Methoden. Dabei hat sich bei den Providern von IP-Backbone Netzen eine Daumenregel eingebürgert, dass höchstens 20% der gesamt verfügbaren Bandbreite auch garantiert werden kann. Bei Nichteinhaltung dieser Regel ist die Wahrscheinlichkeit zu hoch, dass konkurrierende Nachrichtenströme einander in dem Maße beeinflussen, dass die Dienstgüte nicht garantiert werden kann. Bei den enormen Anforderungen von LHC und DEISA würde daher eine Gewährleistung von E2E QoS-Zusicherungen durch Overprovisioning die Dienstkosten in astronomische Höhen treiben.

Da der Bedarf an Verketteten Diensten enorm und dabei die Ende-zu-Ende Dienstgüteabsicherung durch die etablierten Methoden nicht gedeckt ist, ist es Ziel dieser Arbeit, einen alternativen, neuartigen Ansatz dafür zu entwickeln.

1.4. Fragestellungen und Zielsetzung

Die Hauptfrage, die sich in Bezug auf Verkettete Dienste stellt, ist: Welche Maßnahmen sind notwendig, um bei Verketteten Diensten Ende-zu-Ende Qualität garantieren zu können? Wie könnte eine generische Architektur für ein Service-Level-Management von Verketteten Diensten aussehen?

Klassische Aufgaben des Service-Level-Managements angewandt auf Verkettete Dienste stoßen auf zwei Arten von Schwierigkeiten. Zum einen müssen diese Maßnahmen von mehreren voneinander unabhängigen und vor allem gleichberechtigten Organisationen (Service-Provider-Domänen) durchgeführt werden. Zum anderen wird ein besonderer Wert auf die Abstimmung und Koordination der Maßnahmen einzelner Domänen gelegt, da durch die Dienstzusammensetzung (Verkettung der Teildienste) auch kleinste lokale Veränderungen bei einem einzelnen Glied der Kette große Auswirkungen auf die ganze Verbindung haben können.
Die daraus resultierenden Fragestellungen werden im Folgenden präsentiert. Diese Fragen werden nach den Phasen des Dienstlebenszyklus gruppiert, in denen sie auftreten.

1. Verhandlungsphase: Wer verhandelt mit dem Customer über eine neue Instanz eines Verketteten Dienstes? Wie teilt der Customer dem Verhandlungspartner mit, welche Dienstgütemerkmale bei dieser Instanz für ihn wichtig sind und welche Werte bei diesen QoS-Parametern als Ende-zu-Ende Dienstgüte eingehalten werden müssen? Wie werden die weiteren SP-Domänen in die Verhandlung miteinbezogen, um eine Realisierbarkeit dieser Anforderungen zu prüfen?

2. Verhandlungs- oder Dienstinbetriebnahmephase: Wann wird geplant, aus welchen Teildiensten eine Instanz eines Verketteten Dienstes zusammengesetzt wird sowie an welchen Übergangspunkten, mit welchen Technologien und welchen technologiespezifischen Parametern benachbarte Teildienste verbunden werden?

Wie werden SP-Domänen in den Planungsprozess miteinbezogen? Wie wird entschieden, welche Anforderungen Teildienste und ihre Verbindungen erfüllen müssen, damit die für den Verketteten Dienst erwünschte E2E-Qualität gewährleistet ist?

3. Dienstinbetriebnahmephase: Wer initiiert zu welchem Zeitpunkt die Inbetriebnahme und Konfiguration einzelner Teildienste einer Instanz eines Verketteten Dienstes?
4. Betriebsphase, Aspekte ITSM: Wie geschieht die Überwachung einzelner Instanzen eines Verketteten Dienstes, vor allem wie koordinieren dabei die beteiligten SP-Domänen ihre Mess- und Monitoringprozesse? Wie wird die Einhaltung von Zusicherungen für die Dienstinstanzen überprüft und wer übernimmt diese Aufgabe? Wer kann Incident&Problem Management Prozesse starten?
5. Betriebsphase, Aspekte CSM: Durch wen und in welchen Fällen wird ein Reporting an den Customer einer Instanz eines Verketteten Dienstes initiiert? Wer generiert Reporte für den Customer, wer stellt sie zu und was beinhalten sie? Welche Reporte werden zwischen SP-Domänen ausgetauscht, wodurch werden sie initiiert und was beinhalten sie?
6. Dienstanpassungsphase: An wen kann ein Customer veränderte Anforderungen (andere QoS-Parameter oder deren Soll-Zustände) an seine Instanz eines Verketteten Dienstes mitteilen und wie? Wie kooperieren SP-Domänen bei der Bearbeitung von Customer-Anfragen?
7. Dienstauflösungsphase: Wem teilt der Customer seinen Wunsch nach Auflösung seiner Instanz eines Verketteten Dienstes mit? Wie wird diese Information an die beteiligten SP-Domänen weitergeleitet?

Obwohl alle diese Fragen auf verschiedene Ziele ausgerichtet sind, weisen sie dennoch einige Gemeinsamkeiten auf – so liegt z.B. allen diesen Fragen der Bedarf nach der zielgerichteten koordinierten Kopplung funktionaler Komponenten einzelner beteiligter Domänen zugrunde. Weiterhin benötigt die Lösung einiger der Fragen auch die für Verkettete Dienste sinnvolle Verteilung der domänenübergreifenden Repräsentativ- bzw. Koordinationsrollen.

1.5. Vorgehensmodell

Ein grober Überblick über die Kapitelstruktur dieser Arbeit ist in Abbildung 1.5 dargestellt. Die Arbeit gliedert sich in drei Teile. In Kapitel 2 werden verschiedene Szenarios mit Verketteten Diensten analysiert. Die daraus resultierenden Anforderungen werden zunächst verwendet, um die existierenden Ansätze zu bewerten. Wegen der Notwendigkeit, eine neue Lösung zu entwickeln, werden diese Anforderungen in allen anderen Kapiteln der Arbeit berücksichtigt.

Der zweite Teil der Arbeit befasst sich mit der Entwicklung einer neuen Lösung, die den zuvor aufgestellten Anforderungen und Randbedingungen genügt. Dieser Teil beginnt mit Kapitel 3, in dem existierende Ansätze zur Thematik untersucht werden. Das Ergebnis dieses Abschnittes ist eine Analyse möglicher Lösungsbausteine und lehrreicher Erfahrungen, die bei der Entwicklung der Lösung in den weiteren drei Kapiteln einfließen. Im Kapitel 4 wird die Basis der Lösung in Form einer Routing-Architektur gelegt, die sowohl die Besonderheiten der Verketteten Dienste als auch des Service-Level-Managements bei dieser Dienstform berücksichtigt. Im Kapitel 5 wird das Kommunikationsprotokoll definiert, das für den Informations- und Anfragenaustausch zwischen den SP-Domänen notwendig ist. Die mit dem Kommunikationsprotokoll assoziierten Basisprozesse werden im darauffolgenden Kapitel 6 für die Definition der Service-Level-Management-Prozesse verwendet.

Der dritte und letzte Teil dieser Arbeit befasst sich mit der Evaluation und Bewertung der entwickelten Lösung. Im Kapitel 7 wird die entwickelte Lösung exemplarisch am Beispiel des Ordering-Prozesses detailliert durchgespielt. Im Kapitel 8 werden die Erfahrungen geschildert, die bei der Anwendung der entwickelten Konzepte und Ansätze in realen Projekten gesammelt werden konnte. Das Kapitel 9 befasst sich mit der Bewertung der entwickelten Lösung anhand der im Kapitel 2 aufgestellten Anforderungen. Die Arbeit schließt im Kapitel 10 mit einem kurzen Rückblick und der Diskussion über weiterführende Arbeiten ab.

1.6. Abgrenzung

Die wissenschaftliche Forschung im Bereich des IT-Service-Managements beschäftigt sich in den letzten Jahren verstärkt mit den Aspekten der Zusammenarbeit von IT-Providern bei der Erbringung von IT-Diensten. Diese Arbeit deckt nur eine Facette dieses breiten Forschungsfeldes ab und muss daher im Kontext mit den anderen Arbeiten sowohl innerhalb des Munich Network Management (MNM)-Teams als auch anderer akademischer und industrieller Forschungsprojekte gesehen werden. Im Folgenden werden die Gemeinsamkeiten, Unterschiede und Schnittstellen zu den Arbeiten kurz beschrieben, die in einem engeren Zusammenhang mit dieser Arbeit stehen als die übliche Literatur:

Abbildung 1.5.: Aufbau dieser Arbeit

HAMM entwickelt in seiner Dissertation [Ham09] eine Methode zur Spezifikation der IT-Service-Managementprozesse Verketteter Dienste. Die Arbeit HAMMS teilt den Untersuchungsbereich mit dieser Arbeit, beide Arbeiten sind allerdings komplementär angelegt. Während diese Arbeit sich auf Maßnahmen zur Dienstgütezusicherung fokussiert, untersucht HAMM unterschiedliche Organisationsformen, die bei Verketteten Diensten eingesetzt werden können, und definiert eine Methodik zur Definition von interorganisationalen Betriebsprozessen. Zur genauen Abgrenzung der Arbeiten siehe auch [HY08a].

MARCU [HMY08, MGL+09] untersucht in ihrer Dissertation Schnittstellen- und Architekturkonzepte für das providerübergreifende Fehlermanagement. Die Arbeit MARCUS kann ebenfalls als komplementär zu dieser Arbeit betrachtet werden, da in der vorliegenden Arbeit die *Incident&Problem Managementprozesse* nicht im Detail spezifiziert werden.

KNITTL [HK09] entwirft in ihrer Dissertation eine Architektur für eine interorganisationale föderierte Configuration Management Database (CMDB). Ebenso wie MARCU verfolgt KNITTL einen werkzeugorientierten Ansatz. Die Ergebnisse ihrer Arbeit können zur Verwaltung der Multi-Domain Managementinformationen über bereits etablierte Dienstinstanzen verwendet werden.

HOMMEL adressiert in seiner Dissertation [Hom07] Identity-Management-Konzepte in föderierten Umgebungen (FIM). Die in dieser Arbeit behandelten Fragestellungen profitieren von den Ergebnissen HOMMELS Arbeit, da bei den Betriebsprozessen für Verkettete Dienste die gegenseitige Identifikation der nicht direkt angeschlossenen und u.U. zuvor unbekannten Service Provider benötigt wird.

BOURSAS untersucht in ihrer Dissertation [Bou09] Trust- und Reputation-Management in föderierten Umgebungen. Erst durch die Verwendung ihrer Arbeit wird es möglich, Verkettete Dienste nicht nur bei geschlossenen Provider-Kooperationen zu realisieren, sondern auch auf Kooperationen auszudehnen, bei denen die kommunizierenden Service Provider i.A. keine zuvor etablierten Vertrauens- oder gar Vertragsbeziehungen haben. Die Arbeit von BOURSAS kann zur Autorisierung der erforderlichen Operationen verwendet werden.

ZIEGELMANN und KUIPERS befassen sich in ihren Dissertationen [Zie01, Kui04] mit der Problematik der Pfadsuche in Graphen unter Berücksichtigung von gleichzeitig mehreren Parametern. Diese Arbeiten sind vor allem wegen den dort entwickelten Suchalgorithmen sowie wegen des Umganges mit mehreren Dienstgüteeigenschaften als wichtige Lösungsbausteine für diese Arbeit interessant.

2

Begriffe, Szenarien und Anforderungsanalyse

Der Fokus dieses Kapitels liegt auf der Ausarbeitung der Anforderungen für die zu entwickelnde Lösung. Graphisch ist der Aufbau des Kapitels in Abbildung 2.1 dargestellt. Dabei bedeuten dicke ausgefüllte Pfeile die Leserichtung. Die dünnen gestrichelten Pfeile zeichnen die Abhängigkeiten bei der Ableitung einzelner Abschnitte.

Als erstes werden im Abschnitt 2.1 alle benötigten Begriffe eingeführt, um eine eindeutige Semantik für die Analyse zu schaffen. Sowohl deutsche als auch englische Begriffe werden eingeführt. Im Text werden beide Formen als Synonyme verwendet, um die Beschreibung aufzulockern.

Im Abschnitt 2.2 wird das Ziel dieser Arbeit auf der Grundlage der definierten Begriffe präzisiert.

Im Abschnitt 2.3 werden Szenarios beschrieben, in der sich die Problematik einer E2E QoS-Zusicherung bei Dienstketten auf unterschiedliche Art und Weise stellt. Im Anschluss an die Beschreibung werden aus unterschiedlichen Perspektiven Aspekte aufgezählt, die in den jeweiligen Szenarios für die Erfüllung der Dienstgütezusicherungen relevant sind.

Die szenarienspezifischen Aspekte werden im Abschnitt 2.4 zunächst zu einer Morphologie aller Szenarien zusammengefasst. Diese bildet wiederum eine Grundlage, um ein generisches Szenario sowie eine Reihe von Anwendungsfällen (*Use Cases*) herauszuarbeiten.

Die eigentliche Anforderungsanalyse wird im Abschnitt 2.5 durchgeführt. Die erforderliche Basis dafür liefern die zuvor aufgestellte Morphologie, das generische Szenario sowie die Use Cases.

Das Kapitel schließt mit der Bewertung existierender Ansätze zur E2E-Dienstgütezusicherung bei Dienstketten anhand der aufgestellten Anforderungen.

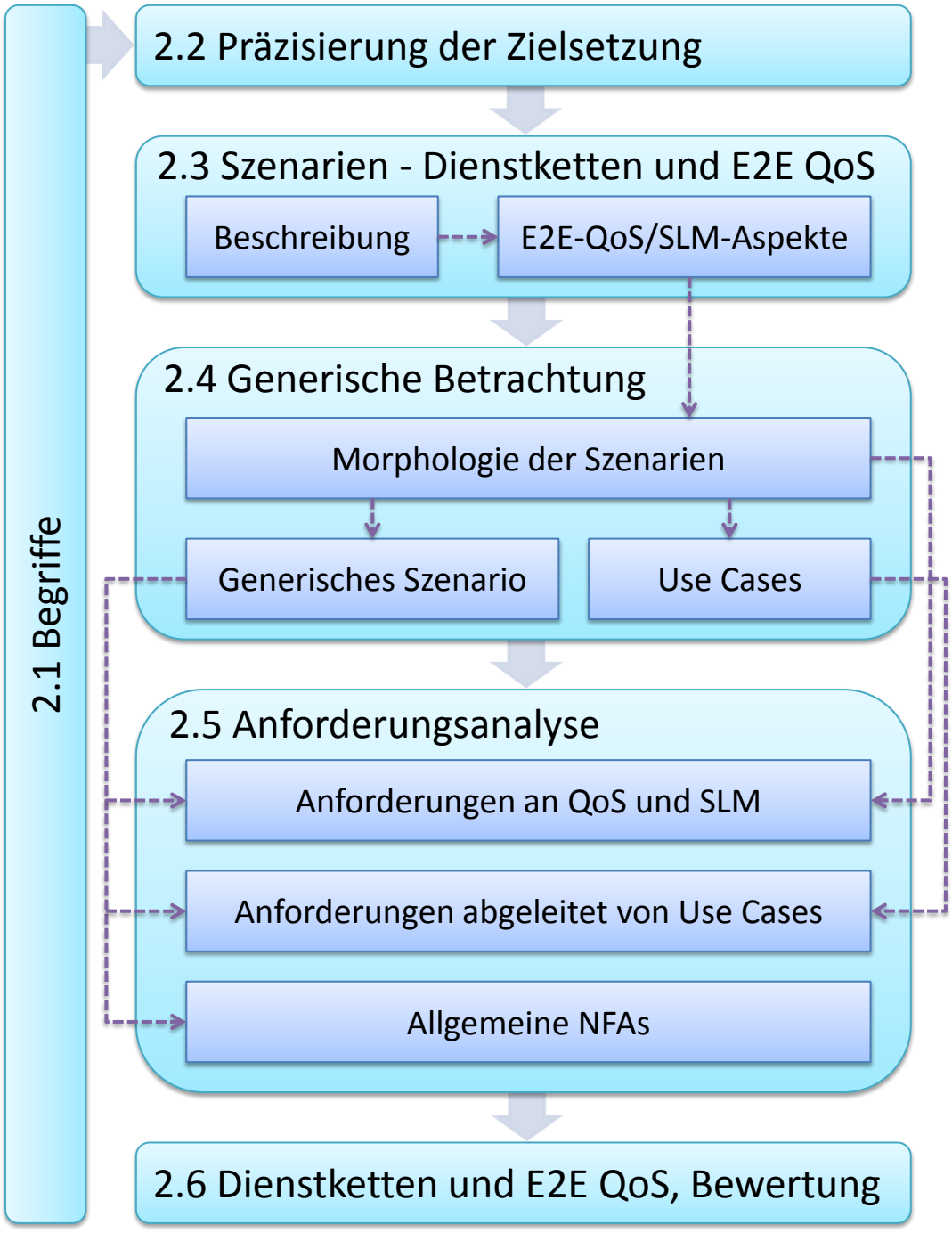


Abbildung 2.1.: Aufbau dieses Kapitels

2.1. Begriffe

Neben dem Begriff Managementarchitektur stellen der IT-Dienst selbst und seine Dienstgüte zentrale Begriffe dieser Arbeit dar.

Dienst

Unter einem *Dienst* (engl.: *Service*) wird in dieser Arbeit eine IT-Funktionalität verstanden, die von einem *Service Provider* seinem *Kunden* (engl.: *Customer*) i.a. gegen ein Entgelt zur Verfügung gestellt und von dem vereinbarten *Dienstnutzer* (engl.: *User*) genutzt wird. Der Dienst kann entweder direkt genutzt oder für die Schaffung weiterer Dienste verwendet werden.

MNM-Dienstmodell

Bereits diese informelle Definition benötigt weitere Begriffe und deren Relationen verwendet werden, die zwar intuitiv verständlich sind, dennoch explizit eingeführt werden müssen. Um einen in sich abgeschlossenen Begriffsraum zu schaffen, wird hier auf das *MNM-Dienstmodell* zurückgegriffen. Das MNM-Dienstmodell, das zuerst in [GHH+01] definiert wurde, hat sich als ein sehr gutes Hilfsmittel bewährt, um einen Dienst und seine Zusammensetzung bei *hierarchischen* Dienst- und Organisationsbeziehungen zu beschreiben (siehe Abbildung 2.2).

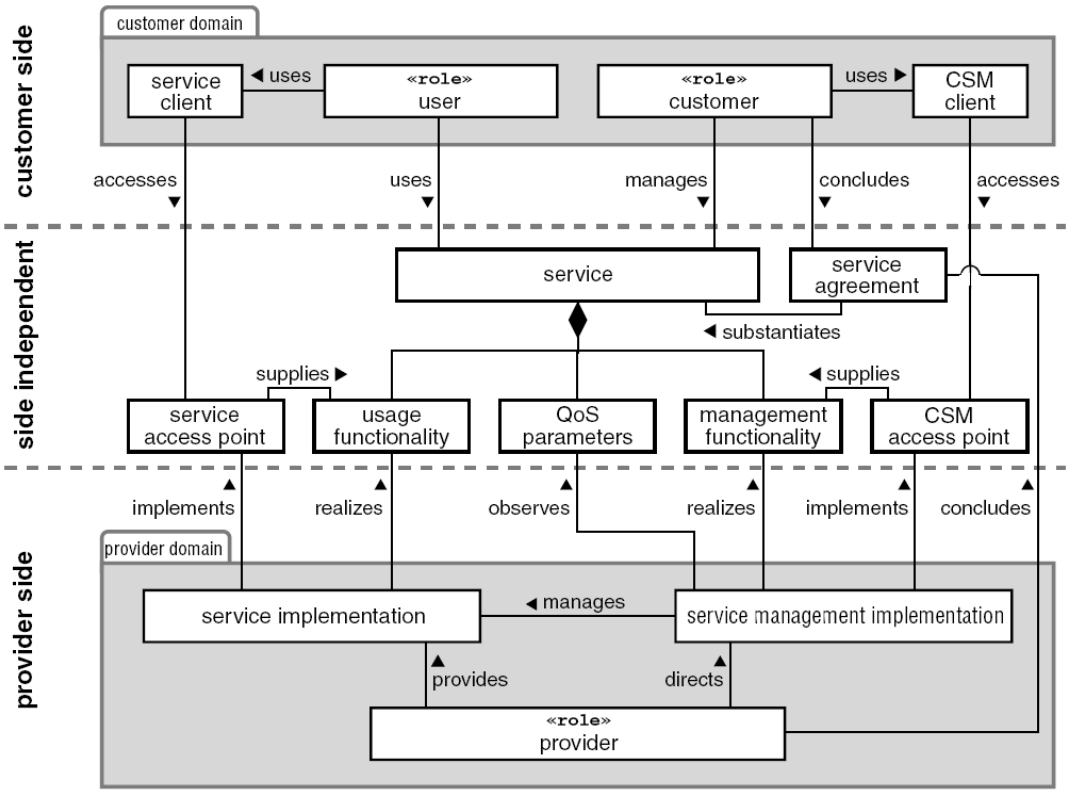


Abbildung 2.2.: MNM-Dienstmodell [GHH+01]

Das MNM-Dienstmodell definiert drei *Rollen*, die bei der Diensterbringung und -nutzung beteiligt sind: Diensterbringer, Kunde und Dienstnutzer. Diese Rollen sind durch ihre Verantwortung und Kompetenzen wie folgt abgegrenzt:

Diensterbringer Unter einem *Diensterbringer* (engl.: *Service Provider*, SP) wird eine Rolle verstanden, die einen Dienst samt seiner Nutz- und Managementfunktionalität realisiert und zur Verfügung stellt.

Kunde Als ein *Kunde* (engl.: *Customer*) wird eine Rolle verstanden, die bei einem Service Provider eine Instanz des erwünschten Dienstes bestellt. Dem Kunden wird das Recht eingeräumt, die *Managementfunktionalität* der bestellten Dienstinstanz zu nutzen.

Dienstnutzer Der Dienstnutzer (engl.: *User*) ist eine Rolle, die – laut der Vereinbarung zwischen den Provider und Customer – die eigentliche *Nutzfunktionalität* in Anspruch nehmen darf.

Alle Rollen können von unterschiedlichen Akteuren besetzt werden. Während als Service Provider üblicherweise eine Organisation auftritt, ist die Rolle User normalerweise von einer oder mehreren Personen besetzt. Als ein Kunde kann sowohl eine Organisation als auch eine Person auftreten. Ein Akteur kann auch unterschiedliche Rollen annehmen.

Der Dienst selbst wird in dem Modell als ein Tripel aus *Nutzfunktionalität*, *Managementfunktionalität* und dazugehörigen *Dienstgüteparameter* definiert.

Nutzfunktionalität Die *Nutzfunktionalität* (engl.: *usage functionality*) repräsentiert den eigentlichen Zweck des Dienstes. Sie wird von dem Dienstnutzer genutzt. Der Zugriff auf die Funktionalität findet über die sog. Service Access Point (SAP) Schnittstelle stat.

SAP

Managementfunktionalität Die *Managementfunktionalität* (engl.: *management functionality*) wird benötigt, um z.B. Dienstparameter festzulegen bzw. verändern zu können. Die Nutzung dieser Funktionalitätsart wird ausschließlich dem Kunden erlaubt. Der Zugriff auf diese Funktionalität geschieht über die sog. *Customer Service Management* (CSM) Schnittstelle; diese Schnittstelle wird auch als CSM Access Point (CSMAP) referenziert.

CSM

Dienstgüte Die *Dienstgüte* bzw. *Dienstgüteparameter* (engl.: *QoS*[1] *parameters*) legen fest, welche der unterstützten Dienstgütemerkmale welche Charakteristika aufweisen sollen. Diese können sich sowohl auf Nutz- als auch auf die Managementfunktionalität beziehen. Als ein Beispiel für die Nutzfunktionalität können hier minimale Bandbreite und maximaler Jitter einer IP-Verbindung genannt werden. Ein Beispiel für die Managementfunktionalität ist ein Recht, die QoS-Parameter im Betrieb zu ändern.

Dienstinstanz Das MNM-Dienstmodell kann als eine Art Template angesehen werden, das alle Aspekte eines Dienstes umfassen und beschreiben kann. Die Kunden und Nutzer sind jedoch an einem *instanziierten* Dienst interessiert. Der instanziierte Dienst wird in dieser Arbeit

[1] QoS steht für *Quality of Service*

als *Dienstinstanz* bezeichnet. So stellt eine konkrete Telefonverbindung zwischen zwei Gesprächspartnern eine Instanz des Typs Telefondienst dar.

Dienstgütevereinbarung

Bezogen auf eine Dienstinstanz kann zwischen dem Customer und dem Service Provider ein formaler Vertrag abgeschlossen werden, in dem alle Rechte und Pflichte beider Parteien spezifiziert werden. Dabei werden die Vereinbarungen über die zugesicherte Dienstgüte in der *Dienstgütevereinbarung* (engl.: Service Level Agreement (SLA)) festgehalten. Diese legt fest, welche Grenzwerte bei den vereinbarten Dienstgütemerkmalen eingehalten werden müssen sowie wie deren Überwachung stattfinden soll.

Service-Level-Management

Die Managementdisziplin der Definition, Vereinbarung, Aufzeichnung und Überwachung von Service Levels wird in IT-Service-Management (ITSM) als Service-Level-Management (SLM) bezeichnet. Das SLM befasst sich mit einer Reihe von Maßnahmen, die sowohl zusichern sollen, dass keine unerfüllbare Dienstgüteparameter dem Kunden in einem SLA versprochen werden, als auch mit den Maßnahmen, die dafür sorgen, dass die vereinbarten QoS-Ziele eingehalten werden. Die Maßnahmen erstrecken sich über mehrere Phasen des *Dienstlebenszyklus* und können in Abhängigkeit von der Phase auf unterschiedliches Instrumentarium zurückgreifen. So gehören die *Überwachung* (engl.: *Monitoring*) und die Berichterstattung (engl.: *Reporting*) zu den wichtigsten SLM Instrumenten in der Betriebsphase.

Monitoring
Reporting

Lebenszyklus

Je nach Fachliteratur und deren Fokus können unter dem Begriff *Dienstlebenszyklus* bzw. einfach *Lebenszyklus* (engl.: *Life Cycle*) unterschiedliche Aspekte verstanden werden. Am häufigsten werden damit die Phasen entweder eines Dienstes (im Sinne eines Templates) oder einer Dienstinstanz verstanden. Im ersten Fall, der z.B. bei NGOSS (siehe [TMF04b, TMF04a]) im Vordergrund liegt, werden die Phasen von dem Erstellen eines neuen Dienstes über ein Angebot für den Kunden und bis hin zum Abbau des Dienstangebotes behandelt. In dieser Arbeit steht die Dienstinstanz im Vordergrund und somit wird deren Lebenszyklus verwendet (siehe Abbildung 2.3).

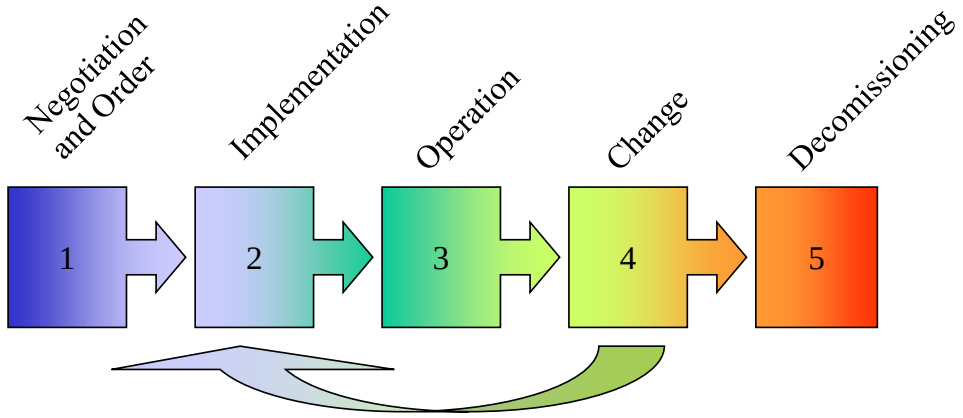


Abbildung 2.3.: Dienstlebenszyklus

Der Lebenszyklus einer Dienstinstanz beginnt mit der Verhandlung und ihrer anschließenden Bestellung. Danach werden seitens des Service Providers Maßnahmen getroffen, um die bestellte Dienstinstanz in Betrieb zu stellen. Im Betrieb kann vom Dienstnutzer die *Usage Functionality* und vom Kunden die *Management Functionalitiy* verwendet werden. Als ein Teil der Managementfunktionalität kann auch die Möglichkeit für deren Anpassung im Betrieb vorgesehen werden. Der Lebenszyklus einer Dienstinstanz endet mit ihrer Abbestellung, die den Service Provider veranlasst, die dafür verwendeten Ressourcen freizugeben.

Teildienste Die Komplexität moderner Dienste ist so hoch, dass sie oft nicht von einem einzigen Service Provider bewältigt werden kann. Daher spezialisieren sich Service Provider auf die Erbringung einfacherer Dienste, die dann zu einem kompletten Dienst zusammengesetzt werden können. Solche Teile werden in dieser Arbeit als *Teildienste* referenziert.

SP-Domäne Die Service Provider, die die Teildienste erbringen, sind i.A. unterschiedliche Organisationen. Diese Organisationen bilden somit jeweils eine organisatorische Domäne, die im Weiteren als *SP-Domänen* (engl.: *SP-Domains*) referenziert wird.

Auch wenn das MNM-Dienstmodell alle erforderlichen Aspekte eines Dienstes beschreibt, wird dabei von hierarchischen Provider- und Dienstbeziehungen ausgegangen. In Kapitel 1 wurde der Bedarf auch an solchen Diensten verdeutlicht, bei denen hierarchische Organisationsbeziehungen nicht akzeptabel sind. Obwohl manche der benötigten Begriffe bereits in dem o.g. Kapitel eingeführt wurden, werden sie hier vollständigkeitshalber erneut definiert.

Heterarchie Unter einer *Heterarchie* wird eine Organisationsform verstanden, bei der alle Beteiligten autonom und gleichberechtigt sind [Rei98, BK04]. Anders ausgedrückt, bei heterarchischen Kooperationsformen darf es keine global wirksame Rolle mit Weisungsbefugnissen geben.

Dienstkette Unter einer *Dienstkette* wird ein Dienstaufbau verstanden, bei dem Teildienste horizontal gekoppelt sind (*Horizontal Supply Chain*), siehe dazu [HAN99, DR02], wobei zwischen den Service Providern, die die Teildienste erbringen, Heterarchie herrscht. Eine Einhaltung der Dienstgüte wird bei der Dienstkette i.a. nicht gefordert.

Bemerkung: Bei einer horizontalen Kopplung der Teildienste zieht die Beeinträchtigung einzelner Teildienste – anders als bei der vertikalen Kopplung – die anderen Teildienste nicht in die Mitleidenschaft. Dafür wird hier von jedem einzelnen Teildienst die komplette Dienstinstanz, also auch in der E2E-Auswirkung, beeinflusst.

Verketteter Dienst Ein *Verketteter Dienst* (engl: *Concatenated Service*) wird in der Arbeit als eine Dienstkette definiert, für die die Einhaltung der Dienstgüteparametern gefordert wird.

Endpunkt Da es bei Dienstketten um die Verbindungen zwischen zwei Kommunikationspartner geht, verläuft eine Dienstinstanz immer zwischen zwei *Endpunkten* (engl.: *End Points*,

EPs). Unter EPs werden in der Arbeit die zwei SAPs der Kommunikationsteilnehmer verstanden, die Endnutzer der Dienstinstanz sind.

Routing

Bei Dienstketten bestehen grundsätzlich mehrere Möglichkeiten, eine Verbindung zwischen zwei Endpunkten zu realisieren. Ein Prozess, bei dem ein Weg zwischen zwei Endpunkten gesucht und idealerweise gefunden wird, wird als *Pfadfindung* (engl.: *Routing*) bezeichnet. In dieser Arbeit bezieht sich der Begriff auf das Finden eines geeigneten Pfades durch mehrere SP-Domänen.

Switching

Die *Inbetriebnahme* einer Dienstinstanz, die für den Betrieb einer Dienstinstanz notwendig ist, bezieht sich auf die Inbetriebnahme einzelner beteiligten Teildienste sowie auf ihre Zusammenschaltung. Die *Zusammenschaltung* wird in dieser Arbeit in Anlehnung an die TK-Technik auch als *Switching* referenziert.

Neben der Aufteilung und der Zusammensetzung der komplexen Dienste aus Teildiensten erfordert das Management solcher Systeme einen vielschichtigen Aufbau. Die Erfüllung von SLM-Aufgaben wird durch eine Reihe von Prozessen realisiert, die wiederum aus einer Reihe von einzelnen nacheinander ausgeführten atomaren Aktivitäten bestehen. Um dies diese Aktivitäten beschreiben zu können, wird eine Managementarchitektur-Schicht gebraucht.

Managementarchitektur

Die *Managementarchitektur* wird in OSI als bestehend aus vier Teilmodellen definiert: Informationsmodell, Organisationsmodell, Funktionsmodell und Kommunikationsmodell (siehe Abbildung 2.4).

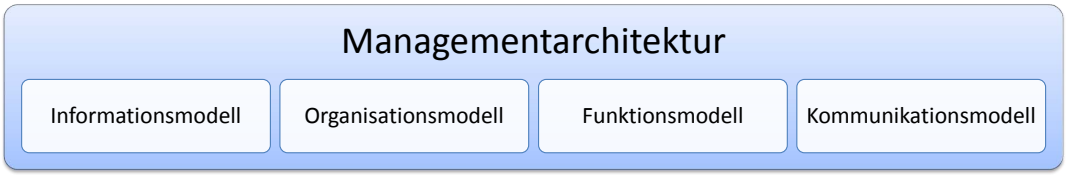


Abbildung 2.4.: Teilmodelle einer Managementarchitektur

Managed Object

Das Herzstück einer Managementarchitektur bildet das *Informationsmodell*, das die gemanagten Objekte (engl.: *Managed Objects*, MO) durch die Beschreibung ihrer Eigenschaften genau definiert. Das *Organisationsmodell* spiegelt den organisatorischen Aufbau wider. Das Modell legt fest, welche Rollen in der Architektur vorkommen und welche Akteure sie annehmen dürfen. Im *Funktionsmodell* werden funktionale Komponenten definiert und auf die in dem Organisationsmodell definierten Rollen "verteilt". Schließlich wird im *Kommunikationsmodell* definiert, auf welchen Wegen und in welcher Weise die einzelnen Rollen und funktionalen Komponenten bei der Erfüllung ihrer Aufgaben miteinander kommunizieren.

2.2. Präzisierung der Zielsetzung

Aus der Perspektive des Customers stehen immer der Dienst selbst sowie seine Qualität im Vordergrund. Weder die technische noch die organisatorische Realisierung des Dienstes spielen für den Customer eine wesentliche Rolle. Deswegen werden von ITSM Framework ITIL die Aushandlung der vom Kunden erwünschten und zugleich vom SP realisierbaren QoS-Werte sowie deren spätere Überwachung als zwei Kernaufgaben des Service-Level-Managements angesehen. Die ausgehandelten Dienstgütezusicherungen werden in der Regel in einem Service Level Agreement (SLA) festgehalten.

Im Falle von hierarchischen Organisationsbeziehungen wird das komplette Service-Level-Management eines Dienstes von einer einzigen Service-Provider-Organisation bestimmt. Diese SP-Organisation erfasst nicht nur Anforderungen des Customers und schließt mit ihm einen Vertrag ab, sondern entscheidet vor allem, aus welchen Teildiensten der gesamte Dienst zusammengesetzt wird, welche Dienstmerkmale diese Teildienste aufweisen und welche Grenzwerte bei jedem der Teildienste einzuhalten sind, damit eine Ende-zu-Ende QoS-Zusicherung gewährleistet ist. Dieser Service-Provider kann zudem entscheiden, welche der Teildienste in Eigenregie erbracht werden sollen und welche bei den anderen Providern (Subprovidern) als Dienstleistung eingekauft werden können. Weiterhin liegt es in der Hand des Dienstproviders zu entscheiden, welche Dienstgütemerkmale bei den Teildiensten wie überwacht werden müssen, sowie wem in welchen Abständen und unter welchen Bedingungen die Monitoring-Daten zur Verfügung gestellt werden müssen. Eine Absicherung der Vereinbarungen mit den Subprovidern geschieht dann in den *Underpinning Contracts*. Die Abbildung der dienstspezifischen QoS-Parameter auf die technologie- und gerätespezifischen Werte und Metriken wird durch die Fachkräfte der jeweiligen Domäne durchgeführt.

Fokus der Arbeit

Im Falle einer Heterarchie besteht dagegen die Herausforderung darin, dass ein vom Kunden erwünschter Ende-zu-Ende Dienst auf die Teildienste samt aller vorher erwähnten Festlegungen aufgeteilt wird. Das Fehlen eines zentralen Entscheidungsträgers führt zu einer Reihe von Herausforderungen. Die speziell für das Service-Level-Management Verketteter Dienste aufgeworfenen Fragen sind in Abschnitt 1.4 aufgelistet; diese wurden von der vorangegangenen umfassenderen Analyse des Problemraumes in [HY08a] abgeleitet.

In dieser Arbeit wird davon ausgegangen, dass sowohl die domäneninternen (wie z.B. Abbildung von Teildienst QoS auf die eingesetzte Infrastruktur) als auch Single-Domain (wie z.B. Annahme und Erfassung der Kundenanfrage) Aufgaben genauso wie im hierarchischen Fall ausgeübt werden können. Diese sind bereits hinreichend untersucht und ausgereift und werden daher in der Arbeit nicht genauer spezifiziert.

Sowohl im hierarchischen als auch im heterarchischen Fall weist das Service-Level-Management außer technischen noch eine Reihe von weiteren Aspekten auf, wie z.B. Dokumentation der Verträge und deren juristische Verbindlichkeit. Der Fokus dieser Arbeit liegt allerdings einzig und allein auf der Schaffung technischer Voraussetzungen für das Service-Level-Management Verketteter Dienste, weitere Aspekte werden explizit ausgeklammert.

Weiterhin wird auch bei technischen Aspekten zwischen Beziehungen nach Außen (zwischen einem Customer und seinem Service Provider) und nach Innen (zwischen allen beteiligten Service Providern und involvierten Rollen) unterschieden. Die Beziehungen nach außen bestimmen den Funktionsumfang der CSM-Schnittstelle. Diese unterscheiden sich nicht vom hierarchischen Fall. Aus diesem Grund beschäftigt sich diese Arbeit ausschließlich mit dem inneren Geflecht zwischen den Rollen, die sich bei der Diensterbringung beteiligen. Die Tiefe der Betrachtung ist durch die Kommunikationsschnittstelle zu diesen Rollen gegeben.

Ziele der Arbeit

Genauer werden die Ziele der Arbeit wie folgt definiert:

Hauptziel: Kern dieser Arbeit bildet ein Verfahren, das es den Service Providern erlaubt, die Kundenanforderungen auf die beteiligten Service Provider und auf die Service-Level-Management-relevanten Festlegungen abzubilden. Im Rahmen dieses Verfahrens wird definiert, welche Rollen dabei notwendig sind, wer von den Providern diese Rollen übernimmt und welche Aufgaben und Verantwortlichkeiten mit diesen Rollen verbunden sind.

Nebenziel: In einer Multi-Domain-Umgebung nimmt die Kommunikation zwischen den einzelnen beteiligten Service Providern eine integrierende Rolle ein. Neben der Festlegung der Kommunikationswege zwischen den Rollen wird daher ein Protokoll für den Informationsaustausch definiert, das für die Lösung SLM-spezifischer Aufgaben bei Verketteten Diensten eingesetzt werden kann. Es soll weiterhin gezeigt werden, wie das Kommunikationsprotokoll bei der Definition der SLM-Prozesse verwendet werden kann.

Nebenziel: Um eine spätere Anwendung in der Praxis zu vereinfachen, wird ein Vorschlag für die mögliche Abbildung der in dieser Arbeit entwickelten Lösung auf die Systemschicht gemacht. Vor allem soll dadurch der Informationsaustausch zwischen den beteiligten SP-Domänen verdeutlicht werden.

Der Rest dieses Kapitels beschäftigt sich mit der Aufstellung von Anforderungen an die Lösung und ist wie folgt aufgebaut. Im Kapitel 2.3 werden Szenarios beschrieben, die sich dem Problem einer E2E QoS-Zusicherung bei Dienstketten auf unterschiedliche Weise stellen. Nach einer kurzen Szenariobeschreibung wird jeweils die Relevanz des Szenarios für die Untersuchung gezeigt und es werden die im Szenario besonderen Aspekte der QoS-Zusicherung zusammengefasst. Im Kapitel 2.4 werden alle Szenarios im Überblick betrachtet. Basierend auf den Szenarioausprägungen wird ein allgemeines Szenario erarbeitet. Anschließend werden Use Cases definiert. Anforderungen an

die zu entwickelnde Lösung werden im Abschnitt 2.5 anhand des allgemeinen Szenarios und von den identifizierten Anwendungsfällen (*Use Cases*) abgeleitet. Das Kapitel schließt mit einer Bewertung der Szenarios anhand aller aufgestellten Anforderungen.

2.3. Szenarien – Dienstketten und E2E QoS

Der Kundenbedarf an Dienstketten, die über mehrere Domäne hinweg gehen müssen und bei denen E2E Dienstgüte eine wichtige Rolle spielt, zeigt sich bei einer Reihe von Projekten und Diensten. In den folgenden Unterkapiteln werden fünf Szenarien präsentiert, die sich der damit verbundenen Problematik auf unterschiedliche Art und Weise nähern.

Bei der Beschreibung aller Szenarien wird zunächst der Dienst kurz eingeführt. Unter anderem werden auch seine Zielgruppe sowie der derzeitige Reifegrad und die Verbreitung erwähnt. Danach werden alle für die Analyse relevanten Aspekte des Dienstaufbaus detailliert beschrieben und kurz bewertet. Die Reihenfolge der beschriebenen Aspekte orientiert sich sehr stark an den Phasen des Dienstlebenszyklus, in denen sie auftreten. Um unnötige Wiederholungen zu vermeiden, werden nur die Aspekte beschrieben, die zu neuen - in vorangegangenen Szenarien nicht aufgedeckten - Erkenntnissen über den möglichen Architekturaufbau bzw. die Anforderungen an den Dienst führen.

Im Anschluss an jede Szenariobeschreibung wird kurz nachgewiesen, wieso Dienstinstanzen im Szenario als eine Dienstkette betrachtet werden können. Danach wird zusammengefasst, was aus Sicht des Service-Level-Managements für die Ende-zu-Ende Dienstgütezusicherung in dem Szenario getan wurde. Diese Zusammenfassung fokussiert sich wiederum auf neue, in vorangegangenen Szenarios nicht beschriebene Aspekte und wird aus fünf Betrachtungsperspektiven durchgeführt (siehe Abbildung 2.5).

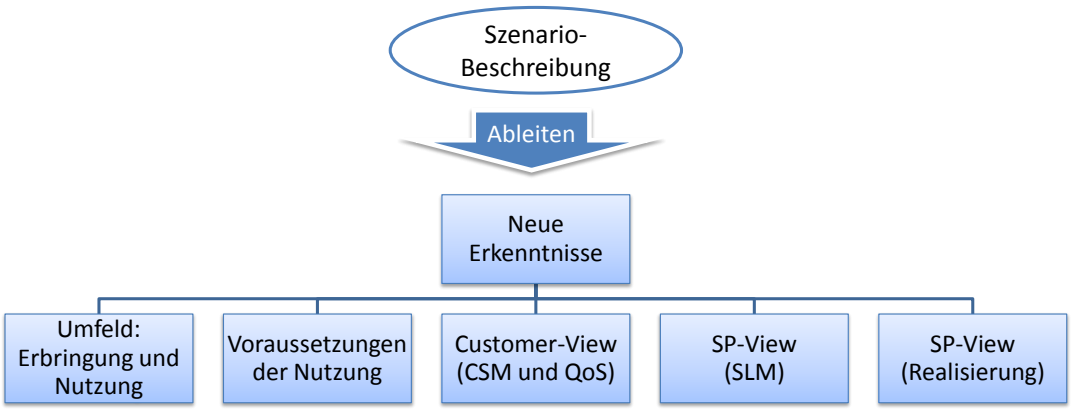
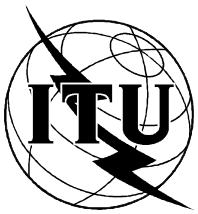


Abbildung 2.5.: Neue Aspekte im Szenario erfassen

Zunächst wird das Umfeld betrachtet, in dem der Dienst im jeweiligen Szenario angeboten wird, sowie die Dynamik seiner Nutzung durch die Kunden. Weiterhin werden Voraussetzungen zusammengefasst, die erfüllt werden müssen, um den jeweiligen Dienst überhaupt nutzen zu können. Nach diesen zwei allgemeinen Gesichtspunkten

wird das Szenario aus Kunden- und aus Providerperspektive betrachtet. Aus der Kundenperspektive sind für diese Arbeit vor allem Aspekte der CSM-Schnittstelle und QoS-Parameter von Bedeutung. Die Providerperspektive ist in der Betrachtung mit zwei Facetten vertreten. Einerseits werden Service-Level-Management-Aspekte untersucht, die für die QoS-Zusicherung relevant sind. Diese werden jedoch getrennt von den Realisierungsaspekten betrachtet, die die Zusammenfassung neuer Aspekte des Szenarios abschließen.

2.3.1. Szenario 1: Telefonnetz/PSTN



Der Telefondienst, der auch als Public Switched Telephone Network (PSTN) bekannt ist, ist das klassische Beispiel für einen Dienst, der Ende-zu-Ende Verbindungen zwischen den Dienstnutzern erlaubt. Diesem Dienst liegt eine automatische Leitungsvermittlung zugrunde, die im Falle z.B. von ISDN als Zusammenschalten von dedizierten 64 Kbit/s Kanälen realisiert ist.

2.3.1.1. Szenariobeschreibung

Der Telefondienst ist als Massendienst aufgebaut, bei dem die Anzahl von Kunden, die gleichzeitig möglichen Verbindungen und kurze Verbindungsaufbauzeiten eine entscheidende Rolle spielen. Deswegen wird großer Wert auf die durchgehende Automatisierung und Zeitverkürzung aller Prozesse gelegt, wodurch eine große Anzahl sowohl von gleichzeitigen Verbindungsanfragen als auch von gleichzeitig bestehenden Verbindungen erreicht werden kann. Dazu kommt auch eine enorme Anzahl von Telekommunikationsunternehmen, zwischen denen ein Verbindungsaufbau möglich sein muss.

Bevor der Dienst in Anspruch genommen werden kann, wird von einem Telco-SP ein Telefonanschluss installiert und eine global eindeutige Telefonnummer für den Anschluss vergeben. Der Dienstaufbau ist ausschließlich auf die Verbindung zwischen den bereits bestehenden Telefonanschlüssen beschränkt.

Um eine Verbindung aufzubauen, spezifiziert ein Anrufer die global eindeutige Nummer des Anschlusses seines Gesprächspartners. Die Telco-SPs sind darum bemüht, dass der Kunde den Dienst 24/7 in Anspruch nehmen kann. Als erwünschter Zeitpunkt und Dauer der Verbindung wird impliziert "ab sofort und bis jemand auflegt oder die Verbindung abbricht" angenommen. Es gibt nur rudimentäre Möglichkeiten, die Dienstmerkmale einer Verbindung zu beeinflussen. Zum einen gelten Parameter, die der Kunde für den Dienst beim Vertragsabschluss wählen kann, z.B. "eigene Nummer weiterleiten/verstecken", "Anklopfen". Zum anderen gibt es die Möglichkeit, manche

dieser Parameter auch durch Angabe am Telefonapparat pro Verbindung zu verändern. So festgelegte Einstellungen werden dann bei jeder Dienstanforderung übernommen.

Nachdem der Telco-SP eine Anfrage für einen Verbindungsaufbau empfängt, wird als erstes die Telefonnummer des gewünschten Gesprächspartners analysiert. Alle Telefonnummern sind i.d.R. hierarchisch (beim Festnetz bisher nach geographischen Gegebenheiten) aufgebaut. Ein strukturierter Aufbau von Telefonnummern erlaubt es, Verbindungen ohne globales Wissen über den exakten Pfadverlauf zu schalten. Anhand der angegebenen Telefonnummer kann der SP entscheiden, ob der Gesprächspartner im eigenen oder in einem anderen Telefonnetz liegt. Für die Verbindungen zum Telefonanschluss im eigenen Netz wird ein Kanal zum Zielanschluss automatisch geschaltet und das Klingeln beim Zielapparat ausgelöst. Falls das Ziel der Verbindung außerhalb des SP-Netzes liegt, entscheidet der SP anhand von zuvor festgelegten Routing-Tabellen, durch welches seiner Nachbarnetze die Verbindung aufgebaut werden soll. Es wird ein 64 Kbit/s Kanal zum Nachbarn geschaltet und es werden Verbindungsparameter zwischen beiden Netzen ausgehandelt. Obwohl Telefonnetze bereits seit sehr vielen Jahren im Einsatz sind, gibt es dennoch sehr große Unterschiede bei den unterstützten Parametern. Das Signalisierungsprotokoll SS7 [ITU93, ITU96], das von allen Ausprägungen der Telefonnetze unterstützt wird, bietet die Möglichkeit, die Schnittmenge der unterstützten Parameter beim Verbindungsaufbau zu bestimmen. Dies erlaubt es den Telco-SPs, auf die Veränderungen der Infrastruktur der Nachbarndomäne automatisch zu reagieren. Im extremen Fall müssen sich zwei Provider auf den kleinsten gemeinsamen Nenner – das sog. Quersignalisierungsprotokoll (QSIG) – einigen, das wiederum von allen Telefonnetzen unterstützt wird und ausschließlich die Schaltung von Sprachkanälen ermöglicht. Danach übernimmt der Nachbar-SP die Aufgabe für die Verbindungsaufbau für den Rest der Strecke – der nächste SP wird ausgewählt, ein Kanal bis zum nächsten SP wird geschaltet, die Kommunikationsparameter werden ausgehandelt und die Aufgabe weitergereicht. Falls an einer Stelle die Verbindung unmöglich ist, wird auf eine alternative Route ausgewichen.

Falls die Verbindung aufgebaut werden konnte, wird den Gesprächspartnern ein dedizierter 64 Kbit/s Kanal zugewiesen. Da das Routing-Verfahren auf die statisch vorkonfigurierten Tabellen beschränkt ist (Kundenwünsche und in Nachbardomänen unterstützte Parameter werden beim Routing nicht berücksichtigt), wird die Verbindung u.U. auch durch eine Domäne geleitet, die nicht alle vom Kunden erwünschten oder erwarteten Parameter unterstützt. Durch Nacheinanderschaltung von mehreren Domänen erhält die Ende-zu-Ende Verbindung die Schnittmenge der bei allen beteiligten Domänen unterstützten Parameter. Das kann zu Verwirrungen führen, z.B. in dem Fall, wenn sowohl Kundendomäne als auch Zieldomäne die Nummerweiterleitung unterstützen, aber eines der Transitnetze nicht. Das Routingverfahren ist so konzipiert, dass, falls der reguläre Pfad nicht geschaltet werden konnte (z.B. weil alle Kanäle bereits belegt sind), auf eine alternative Route ausgewichen wird. Dadurch können Effekte eintreten, dass die Nummer manchmal angezeigt und manchmal nicht angezeigt wird. Die Gründe für ein solches (von außen gesehen sporadisches) Verhalten

werden dem Nutzer vom TK-Provider nicht mitgeteilt, was wiederum zur kompletten Irritation des Dienstnutzers führen kann. Es gibt weder für den Kunden selbst noch für die TK-Provider eine Möglichkeit, die Einhaltung von erwünschten Dienstmerkmalen durchzusetzen. Das liegt daran, dass es keine Möglichkeit gibt zu signalisieren, dass nach einem Pfad gesucht werden muss, der eine Reihe von erforderlichen Dienstmerkmalen unterstützt. Es gibt keine Möglichkeit, QoS-Merkmale einzelner Abschnitte abzufragen bzw. bei der Schaltung eine gewünschte Qualität der Abschnitte zu fordern.

Falls eine Verbindung nicht aufgebaut werden konnte, erhält der Anrufer von seinem SP eine Rückmeldung über den Grund: Besetzt, Nummer nicht vergeben, etc. Manche TK-Provider bieten außerdem "Ausweichdienste" an, z.B. wird im Hintergrund versucht, eine Verbindung später aufzubauen, falls die Nummer vorher besetzt war.

Während der Verbindung wird ausschließlich die Aufrechterhaltung der Verbindung überwacht. Das wird im wesentlichen im Interesse von Service Providern gemacht, um die für die Verbindung verwendeten Ressourcen nach dem Beenden der Verbindung wieder freizugeben. Parameter wie z.B. Rauschfreiheit der E2E Verbindung werden i.a. weder überwacht noch gibt es für die Kunden eine Möglichkeit, diese Werte als erforderlich zu spezifizieren.

Falls die Verbindung abbricht, erfährt der Nutzer das zwar durch das akustische Signal, der Grund dafür (ob der Gesprächspartner aufgelegt hat oder die Verbindung zusammengebrochen ist) wird allerdings nicht mitgeteilt.

Alle Berichte, die von Telco-SPs den Kunden angeboten werden, beschränken sich i.d.R. auf Accounting und Billing. Berichte über die Qualitätsgüte einzelner Verbindungen oder generell den Dienst werden grundsätzlich nicht angeboten.

Um die Nutzung der Verbindung zu beenden reicht es, wenn einer der Gesprächspartner den Hörer auflegt. Dies wird von seinem Telco-SP erkannt und mit Hilfe von SS7 allen in der Diensterbringung beteiligten Domänen mitgeteilt. Dem anderen Gesprächspartner wird von seinem Telco-SP akustisch signalisiert, dass die Verbindung nicht mehr besteht.

2.3.1.2. E2E-QoS im Szenario

Bei der Erbringung einer Telefonverbindung können sich mehrere Telekommunikationsunternehmer (Service Provider) beteiligen. Die von den Providern erbrachten Teildienste sind horizontal verkettet. Somit liegt eine Dienstkette vor.

Die E2E-Dienstgütezusicherung ist im Szenario wie folgt vertreten.

Umfeld der Diensterbringung und -nutzung:

- Es gibt unüberschaubar viele SPs, die den Dienst anbieten
- SPs kennen i.A. nur ihre direkten Nachbarn
- SPs unterstützen i.A. unterschiedliche QoS-Parameter
- SPs können in Eigenregie (ohne Absprache mit anderen SPs) ihre Unterstützung von QoS-Parametern ändern
- Es gibt sehr viele Kunden, die den Dienst nutzen können
- Gleichzeitig mehrere Verbindungsanfragen sind möglich
- Mehrere gleichzeitig bestehende Verbindungen sind möglich

Voraussetzungen für eine Dienstinanspruchnahme:

- Ein Anschluss bei einem SP ist erforderlich
- Der Anschluss wird durch SP realisiert
- Jeder Anschluss ist mit einer global eindeutigen Anschluss-ID versehen
- Eine Verbindung ist nur zwischen bereits bestehenden Anschlüssen möglich
- Die Infrastruktur, die für die Verbindung benötigt wird, ist vorhanden und vorkonfiguriert

Kundenperspektive (CSM und QoS):

- Die Managementfunktionalität beschränkt sich auf das Bestellen und Abbestellen einer Dienstinstanz
- Verbindungsanfragen sind 24/7 möglich
- Eine Verbindungsanfrage ist automatisch eine Auftragserteilung (keine Verhandlung erforderlich)
- Customer kommuniziert dabei immer mit seinem SP
- Beginn der Verbindung: implizit "ab sofort"
- Dauer der Verbindung: bis sie explizit abbestellt wird oder abbricht
- Verbindung kann von jedem der Gesprächspartner beendet werden
- Für die Verbindung gelten Parameter aus dem Vertrag
- Manche Einstellungen können beim Telefonapparat als *default settings* verändert werden
- Feedback beschränkt sich auf die Mitteilung von Tatsachen. Genauere Aufschlüsselung der möglichen Ursachen fehlt

- Zeit bis Feedback ist sehr kurz
- QoS-Parameter beschränken sich auf qualitative Aspekte

Providerperspektive (SLM):

- Verbindungsaufbauzeiten sind extrem kurz
- Kundenwünsche werden beim Routing nicht berücksichtigt
- Es existiert ein Protokoll, das von allen SPs unterstützt und zur Aushandlung der Schnittmenge von Parametern genutzt wird
- QoS-Werte der Dienstinstanz bilden sich als Schnittmenge der in der Kette unterstützten Parameter
- Überwachung beschränkt sich auf die Aufrechterhaltung der Verbindung
- Konsumenten von Monitoring-Informationen sind die SP-Domänen, die sich an der Diensterbringung beteiligen

Providerperspektive (Dienstrealisierung):

- Bei allen SPs und für alle Aufgaben herrscht durchgehende Automatisierung
- Der Verbindungsaufbau ist ohne globales Wissen (ausschließlich anhand Tel.Nr. und Routing Tabelle) möglich
- Ein Kanal fester Bandbreite wird für eine Verbindung reserviert
- Routing und Switching geschehen in jeder SP-Domäne nacheinander, bevor die Verbindungsanfrage an die nächste SP-Domäne weitergereicht wird (keine E2E-Planung wird im Vorfeld benötigt)
- Beim Verbindungsaufbau ist das Ausweichen auf eine alternative Route möglich

2.3.2. Szenario 2: Géant2 E2E Links

Die bereits in Kapitel 1.2 erwähnten *Géant2 E2E Links* sind ein relativ neuer Dienst für Ende-zu-Ende Verbindungen mit garantierter Dienstgüte. Diesem Dienst liegen manuell geschaltete dedizierte optische Verbindungen zugrunde, die auf ISO/OSI Schicht 2 realisiert sind [Gea09, US06, CRE+07].

Die Géant2 E2E Links werden seit einigen Jahren produktiv eingesetzt. Derzeit werden Anstrengungen unternommen, diesen Dienst und die zugrunde liegenden Prozesse zu optimieren.

2.3.2.1. Szenariobeschreibung

Verglichen mit dem Telefondienst ist bei E2E Links die Anzahl der Kunden und Nutzer relativ gering. Es sind derzeit vor allem internationale Forschungsprojekte, die extrem hohe und oft auch unterschiedliche Anforderungen an die Verbindungen zwischen beteiligten wissenschaftlichen Einrichtungen stellen. Die Anzahl von Service Providern, die sich an der Erbringung dieses Dienstes beteiligen, ist auch relativ gering: es sind in etwa 30 europäische und ca. 10 außereuropäische Forschungsnetze.

Es sind keine Installationsarbeiten im Vorfeld erforderlich, bevor eine neue Verbindung bestellt werden kann. Es wird lediglich davon ausgegangen, dass Wissenschaftsorganisationen, die einen oder mehrere E2E Links bestellen wollen, in den jeweiligen NRENs bekannt sind. Eine Bestellung von E2E Links ist auch dann möglich, wenn NRENs vor Ort bzw. NRENs auf der Verbindungsstrecke keine freie Kapazitäten (Router, Switches, LWL, optische Kanäle usw.) haben. Bei Bedarf werden fehlende Komponenten nach Vertragsabschluss bestellt und installiert.

Um einen neuen E2E Link zu beantragen, entscheiden die Verantwortlichen von zwei Wissenschaftsorganisationen, die miteinander verbunden werden sollen, welche QoS-Parameter sie brauchen und welche Organisation den E2E Link beantragt. Daraufhin kontaktiert diese Organisation ihren NREN und teilt die Anforderungen an den E2E Link mit. Dieser NREN tritt dann als Verhandlungs- und Vertragspartner für den bestellten E2E Link auf. Der Bestellprozess ist auf die Öffnungszeiten des jeweiligen Ansprechpartner-NREN beschränkt.

Kunden von Géant2 E2E Links sind grundsätzlich an langfristigen permanenten Verbindungen interessiert. Sie können entweder Verbindungen mit der erwünschten Bandbreite oder auch eine Wellenlänge bestellen. Die Nutzung einer Wellenlänge hat für die Kunden den entscheidenden Vorteil, dass für einen E2E Link die volle Bandbreite verwendet wird, die sich über eine Wellenlänge übertragen lässt. Das erlaubt bei Fortschritt in der Übertragungstechnik eine Aufrüstung, um den ständig wachsenden Bedarf an Bandbreite zu decken. Andererseits gibt die Bandbreitenoption den Service Providern größeren Gestaltungsraum für die Realisierung der Verbindung. Derzeit sind für beide Optionen 1 und 10Gbps möglich, es wird aber bereits an Übertragungsgeschwindigkeiten von 40 und 100Gbps gearbeitet.

Abgesehen von der Bandbreite können Kunden projektbezogene Anforderungen an E2E Links stellen, die sich stark unterscheiden können. Zwei der prominentesten Nutzer von E2E Links sind das internationale Teilchenforschungsprojekt LHC [LHC08a] und die Grid Initiative DEISA [DEI08a]. Während für DEISA außer reiner Bandbreite noch Delay und Jitter eine wichtige Rolle spielen, sind beim LHC Projekt diese QoS-Parameter nicht relevant.

Für das LHC Projekt sind vor allem Verfügbarkeit und Zuverlässigkeit von E2E Links interessant. Außerdem müssen Wartungsarbeiten der Link Provider nicht nur wie üb-

lich im Voraus gemeldet, sondern auch mit den Verantwortlichen im LHC-Projekt abgestimmt werden. In einem Multi-Domain Umfeld stellt die Koordination von Wartungsarbeiten immer noch eine Herausforderung dar, die in Géant2 derzeit ausschließlich durch persönliche Absprachen gelöst wird. Eine weitere Herausforderung ist dadurch gegeben, dass für das LHC Projekt z.T. primäre und Backup E2E Links zwischen denselben Endpunkten installiert werden müssen.

Obwohl es für den Customer möglich ist, gleichzeitig mehrere erforderliche Dienstgüteparameter für einen E2E Link zu spezifizieren, fehlt es an der Möglichkeit, diese zu priorisieren. Durch die Priorisierung von QoS-Parametern wäre es möglich, aus mehreren alternativen Realisierungen die für den Customer am besten passende auszuwählen.

Kundenanforderungen an den Dienst werden bei der Verhandlung zunächst in einem Formular erfasst. Dieses Formular wird dann zwischen Netzverantwortlichen der NRENs zirkuliert, die die exakte Route und technische Realisierung des E2E Links manuell planen. Dabei wird das Formular mit für die Zusammenschaltung notwendigen technischen Informationen aufgefüllt. Bei der Planung entscheidet jeder NREN, wer der nächste in der Kette sein wird. Erst nachdem die interne Planung abgeschlossen ist, wird das Formular vervollständigt und an den nächsten NREN weitergereicht, der daraufhin mit seinem Teil der Planung beginnt. Da die manuelle Planung unterschiedlich lange dauern kann und da die Anzahl von Domänen, die bei Erbringung eines E2E Links involviert sind, je nach Route variieren kann, unterliegt die Dauer des gesamten Planungsprozesses großen Schwankungen und kann zwischen einigen Tagen und einigen Wochen variieren.

Nachdem die Planung abgeschlossen ist, wird dem Customer mitgeteilt, ob ein E2E Link mit den erwünschten Anforderungen realisiert werden kann und, falls ja, auch wann der E2E Link voraussichtlich in Betrieb genommen wird. Falls der Kunde dem Angebot zustimmt, wird der Inbetriebnahmeprozess gestartet.

Die Schätzung des Inbetriebnahmedatums, die dem Kunden vorgelegt wird, ist allerdings sehr ungenau. Durch das Fehlen von Multi-Domain Workflows kam es in der Vergangenheit z.T. zu Verzögerungen von mehreren Monaten. Die Schaltung von Verbindungsabschnitten geschieht größtenteils manuell und hängt zusätzlich auch von den Lieferzeiten für die fehlenden HW-Komponenten ab. Die daraus resultierende Dauer bis zur Inbetriebnahme variiert momentan von einigen Monaten bis hin zu einem Jahr. Derzeit wird intensiv an der Entwicklung von Multi-Domain-Prozessen für E2E Links gearbeitet.

Um den Zustand von E2E Links kontinuierlich zu überwachen, wurde in Géant2 ein Monitoring-Konzept entwickelt, das die Autonomie der beteiligten Domänen berücksichtigt [YH07]. Nach diesem Konzept stellt jeder NREN über eine standardisierte Schnittstelle Informationen zur Verfügung, ob der dort erbrachte Teildienst eines E2E Links ordnungsgemäß funktioniert oder nicht. Informationen der einzelnen Domänen werden von einem Monitoring-System in regelmäßigen Abständen abgefragt

und daraus ein E2E-Wert aggregiert. Das Monitoring-System wird bei einer zentralen Organisation (sog. End-to-End Coordination Unit, E2ECU) betrieben, die extra zum Zwecke der Überwachung und der Koordination von Multi-Domain Incident- und Problem-Management-Prozessen ins Leben gerufen wurde. Dabei wird kein direkter Zugriff auf die Domänen-Infrastruktur von außen benötigt, wodurch die Sicherheitsrichtlinien und die Autonomie jeder Domäne bewahrt werden. Dies erlaubt auch, alle Komponenten des Systems einfach zu halten und Technologie- und HW-spezifische Messungen in den Domänen durch die dort eingesetzten Tools zu realisieren. Ein weiterer Vorteil dieses Konzepts ist die "Autosynchronisation" von Monitoring-Informationen aller Domänen, die durch das gleichzeitige Abfragen von Ist-Zuständen durch ein Monitoring-System erreicht wird (für mehr Details siehe Abschnitt 8.1). Der größte Vorteil des Konzepts besteht aber darin, dass bei Störungen auf einem E2E Link automatisch erkannt wird, in welcher der Domänen ein Problem aufgetreten ist.

Die im Szenario umgesetzte Lösung weist allerdings eine Reihe von Defiziten auf. Es wird z.B. vorausgesetzt, dass alle Teilabschnitte eines jeden E2E Links lückenlos überwacht werden, was nicht immer möglich bzw. einfach zu erreichen ist, und dass gemeldete Zustände den tatsächlich gemessenen Werten entsprechen. Weiterhin werden kurze Ausfälle (engl.: *spikes*), die zwischen den Abfragen auftreten, vom Monitoring-System nicht erkannt. Spikes, die dagegen während der Abfrage auftreten, werden dann als Ausfälle für die Länge des Polling-Intervalls wahrgenommen. Die Problematik von unterschiedlichen Messverfahren (Traps und Polling) sowie deren Granularität wird bei der Aggregation von Ist-Zuständen der einzelnen Domänen einfach ignoriert. Zu guter Letzt kann eine Degradation der Performanz, die in einzelnen Domänen in den Toleranzgrenzen liegt und deswegen nicht als Problem erkannt wird, sich über die ganze Kette aufsummieren und zu schlechter E2E-Qualität der kundenrelevanten Parameter führen. Auf eine Ende-zu-Ende Überwachung, durch die solche Situationen erkannt werden könnten, wird bei E2E Links aus Kostengründen verzichtet.

Bei der Dienstüberwachung werden derzeit für jeden E2E Link die Gesamtverfügbarkeit und Anzahl der Ausfälle mitgeführt. Diese Informationen werden den Kunden in monatlichen Berichten zur Verfügung gestellt. Die aktuell laufenden Werte können vom Kunden über das Monitoring System abgefragt werden.

Veränderungen der Anforderungen an einen E2E Link kann der Kunde seinem NREN mitteilen. Intern wird das als Bestellung eines neuen E2E Link mit den erwünschten Parametern und als Abbestellung des alten behandelt.

Die Abbestellung eines E2E Links soll wiederum dem NREN mitgeteilt werden, das als Verhandlungs- und Vertragspartner agiert hat. Dieser NREN leitet dann die Informationen an alle bei der Diensterbringung beteiligten Domänen weiter.

2.3.2.2. E2E-QoS im Szenario

Bei der Erbringung eines E2E Links beteiligen sich mehrere NRENs, die als unabhängige Service Provider aufgefasst werden können. Die von den Providern erbrachten Teildienste sind horizontal verkettet. Somit liegt eine Dienstkette vor.

Neue Aspekte der E2E-Dienstgütezusicherung im Szenario sind:

Umfeld der Diensterbringung und -nutzung:

- Die Anzahl der bei der Diensterbringung beteiligten SPs ist recht überschaubar
- Alle SPs kennen einander
- Die Anzahl der Kunden und Nutzer des Dienstes ist relativ gering
- Die Anzahl gleichzeitig bestehender Verbindungsanfragen ist relativ gering
- Wenige gleichzeitig bestehende Verbindungen
- Alle Verbindungen sind permanent und langfristig
- Die QoS-Anforderungen können zwischen Dienstinstanzen sehr stark varieren

Voraussetzungen für eine Dienstinanspruchnahme:

- Der Customer muss lediglich bekannt sein. Ein bereits bestehender Anschluss ist für die Bestellung einer neuen Verbindung nicht erforderlich

Kundenperspektive (CSM und QoS):

- Der Bestellprozess ist auf die Öffnungszeiten des SPs beschränkt
- Die Bestellung erfolgt erst nach einer Verhandlung
- Als Verhandlungs- und Vertragspartner tritt der Anschluss-SP des Customers auf
- Es ist möglich, gleichzeitig mehrere QoS-Parameter für eine Dienstinstanz zu fordern
- QoS-Anforderungen können sich beziehen u.a. auf Verfügbarkeit, Zuverlässigkeit, quantitative QoS-Parameter (wie z.B. Bandbreite, Delay), Wartungsarbeiten usw.
- In manchen Fällen können Kunden nicht-standardisierte Anforderungen aufstellen, wie z.B. bzgl. der Dienstrealisierung
- Bei demselben SP ist es auch möglich, Veränderung der QoS-Parameter zu beantragen bzw. abzubestellen

- Die Abfrage von aktuellen Monitoringwerten ist über eine zentral gehaltene Multi-Domain Rolle (E2ECU) möglich
- Reports werden von der Multi-Domain Rolle (E2ECU) erstellt

Providerperspektive (SLM):

- Die Planung der Verbindung unterliegt großen Schwankungen. Die Gesamtzeit summiert sich über alle SP-Domänen, die sich bei der Diensterbringung beteiligen werden. Dazu kommt, dass die Planungszeit in jeder dieser Domäne unterschiedlich sein kann
- Eine Schätzung des Inbetriebnahmedatums ist sehr ungenau. Das liegt an oft schwankenden Lieferzeiten und möglichen Problemen bei der manuellen Zusammenschaltung der Abschnitte
- Das Monitoring bezieht sich auf (abstrahierte) Abschnitte innerhalb SP-Domänen (*Domain Links*) und auf die Verbindungsstücke zwischen SP-Domänen (*Interdomain Links*)
- Das Monitoring setzt voraus, dass die von Domänen gemeldete Zustände tatsächlich gemessenen Werten entsprechen
- Der Gesamtzustand des E2E Links wird von einem Monitoring-System aus den Teilinformationen errechnet
- Eine berechnete E2E-Aussage ist darauf angewiesen, dass die Überwachung lückenlos ist
- Das Monitoring verfolgt u.A. das Ziel, dass bei einer Störung die Verursacher-Domäne automatisch erkannt werden kann
- Kurze Ausfälle (spikes) werden entweder nicht erkannt (falls Information darüber zwischen den Abfragen überschrieben wird) oder falsch interpretiert (falls diese vor der Abfrage durchs Monitoring-System entdeckt wurden)
- Für das Reporting werden Gesamtverfügbarkeit und Anzahl der Ausfälle pro Dienstinstanz gemessen

Providerperspektive (Dienstrealisierung):

- Die Planung jeder Verbindungen geschieht manuell
- Die Reihenfolge der Planung erfolgt entlang einer Kette
- Die Planung läuft grundsätzlich in zwei Phasen ab. Für das Angebot wird eine vorläufige Machbarkeitsstudie durchgeführt. Die genaue Planung wird erst nach dem Vertragsabschluss erarbeitet

- Die Inbetriebnahme kann u.U. das Nachbestellen fehlender Infrastrukturkomponenten beinhalten
- Die Inbetriebnahme (vor allem die Zusammenschaltung einzelner Abschnitte) geschieht überwiegend manuell
- Das Monitoring einzelner Abschnitte wird von den Eigentümer-SPs in Eigenregie durchgeführt
- In SP-Domänen werden *trap*- und *polling*-Methoden verwendet. Die Granularität von Polling kann sich zwischen SP-Domänen unterscheiden
- Die Korrelation der Monitoringdaten aus einzelnen Domänen wird von einer Multi-Domain-Instanz (E2ECU) durchgeführt
- Die Monitoringinformationen werden von den SP-Domänen über eine standardisierte Schnittstelle abgeholt
- Die Synchronisation der Messungen einzelner Abschnitte geschieht durch das gleichzeitige Abholen der Zustandswerte

2.3.3. Szenario 3: GLIF

Das internationale Forschungsprojekt GLIF (Global Lambda Integrated Facility) hat die automatische Schaltung optischer Verbindungen über mehrere unabhängige Domänen hinweg zum Ziel [GLI08b, Mey08, GLI08a]. Im Unterschied zu Géant2 E2E Links, die auf ISO/OSI Schicht 2 realisiert werden, beschränkt sich GLIF auf die reine Lichtwellenschaltung auf ISO/OSI Schicht 1.

Das Projekt befindet sich derzeit im Entwicklungsstadium.

2.3.3.1. Szenariobeschreibung

Bevor der Dienst in Anspruch genommen werden kann, müssen sich die Customer (R&D-Organisationen) im Vorfeld selbst an die GLIF Infrastruktur einer der Domänen anschließen.

Die Bestellung einer dedizierten optischen Verbindung geschieht ähnlich wie bei Géant2, wenn auch automatisiert. Eine der Organisationen an den Endpunkten wendet sich an ihre Anschlussdomäne und teilt ihr mit, zu welchem anderen Endpunkt die Verbindung aufgebaut werden soll. Die Verantwortung dieser Domäne, die gemäß der GLIF-Terminologie die Rolle *Sourcing Organization* einnimmt, besteht darin, optische

Abschnitte (*Lightpath Sections*) der E2E Verbindung, die sich u.U. in unterschiedlichen Domänen befinden können, zu identifizieren und ihre Schaltung zu veranlassen [HGB06].

Dieses Konzept erlaubt es, dass mehrere Domänen gleichzeitig als Sourcing Organization agieren und mehrere Anfragen von unterschiedlichen Customer-Organisationen simultan bearbeiten können. Weiterhin ist es möglich, die Suchverfahren und Auswahlkriterien in jeder Sourcing Organization entsprechend eigenen Bedürfnissen zu optimieren. Andererseits benötigen Sourcing Organizations Zugriff auf Informationen über global verfügbare Ressourcen. Globale Informationssysteme, die bei geringer Anzahl der beteiligten Domänen und/oder gleichzeitigen Anfragen sehr gute Ergebnisse liefern können, führen erfahrungsgemäß bei wachsender Zahl von gleichzeitigen Anfragen zu Performance und Synchronisationsproblemen. Um den Synchronisationsaufwand möglichst gering zu halten, werden in GLIF globale Informationen zentral gespeichert, was dieses Informationssystem zu einem *Single Point of Failure* macht.

Nachdem die Planung abgeschlossen ist und eine Verbindungsmöglichkeit gefunden wurde, veranlasst die Sourcing Organization die Schaltung der benötigten Lightpath Sections. In GLIF werden dafür zwei Kommunikationsmodelle unterstützt:

- Bei sog. "*Parallel master contractor*" kontaktiert die Sourcing Organization direkt alle Domänen, die bei der Erbringung beteiligt werden müssen, mit der Anfrage fürs Schalten ihrer Lightpath Section.

- Bei sog. "*Serial master contractor*" wird die Anfrage für das Schalten einer Lightpath Section zusammen mit Informationen über alle nachfolgenden Sections nur an die nächste Domäne in der Kette geschickt. Diese Domäne schaltet ihren Teil und leitet die Anfrage weiter an die nächste Domäne in der Kette.

In beiden Fällen werden für jede beteiligte Domäne in einer *Service Level Specification* (SLS) Dienstgüteparameter für ihre Lightpath Section spezifiziert. Dadurch, dass das SLS für jede Domäne bindend ist, wird sichergestellt, dass in GLIF dem Kunden gegenüber ein domänen-übergreifendes E2E SLA angeboten werden kann.

Die Einschränkung auf eine Schicht-1-Schaltung hat folgendes Problem verursacht: Es kann sein, dass zwei Domänen in der Kette, die Schicht 2+ Technologie einsetzen, durch einen oder mehrere Abschnitte auf Schicht 1 verbunden sind. Da diese zwei Domänen nicht direkt benachbart sind und u.U. nichts über den anderen wissen, kann es dazu kommen, dass die eingesetzten Technologien nicht kompatibel sind oder eine Kombination der verwendeten Konfigurationen zu Problemen führt.

2.3.3.2. E2E-QoS im Szenario

Die Kooperationspartner bei GLIF sind unabhängige Organisationen. Sie fungieren als Service Provider, indem sie Teildienste zur Verfügung stellen, die für eine Verbindung benötigt werden. Die Teildienste sind horizontal verkettet. Somit liegt eine Dienstkette vor.

Neue Aspekte der E2E-Dienstgütezusicherung im Szenario sind:

Umfeld der Diensterbringung und -nutzung:

- Nicht nur die direkten Nachbarn, sondern auch die Technologienachbarn, die u.U. durch mehrere SP-Domänen getrennt sind, kennen einander

Voraussetzungen für eine Dienstinanspruchnahme:

- Der Anschluss an seinen SP wird von dem Customer selbst realisiert

Providerperspektive (SLM):

- Die bei der Diensterbringung beteiligten SPs sichern die Qualität ihrer Teildienste in einem SLA zu

Providerperspektive (Dienstrealisierung):

- Die Planung eines kompletten E2E-Pfades durch alle SP-Domäne wird von der Anschlussdomäne durchgeführt
- Für das Routing wird eine globale Informationsbasis benötigt
- Diese globale Informationsbasis wird in GLIF zentral gehalten, um Synchronisationsaspekte zu vermeiden
- Der Anschluss-SP veranlasst das Switching bei allen weiteren SP-Domänen
- Es werden zwei Kommunikationsarten für die Signalisierung unterstützt: direkte Kommunikation mit allen beteiligten SP-Domänen oder in der Kette

2.3.4. Szenario 4: Dynamic Circuit Network (DCN)

Dynamic Circuit Network (DCN) ist ein von Internet2 gefördertes Projekt, mit dem Ziel der Entwicklung einer Technologie zur automatischen Schaltung von Punkt-zu-Punkt Verbindungen mit garantierter Bandbreite [DCN08, DCN09]. Die Verbindungen sollen sowohl *on-demand* als auch *scheduled* schaltbar sein und nach Bedarf von einigen Minuten bis hin zu mehreren Tagen bestehen. Die

automatische Schaltung der Verbindungen soll durch eine sog. *Control Plane* realisiert werden und eine Schaltung über mehrere administrative Domänen erlauben. Die Control Plane wird von den Partner-Projekten entwickelt. Zu den größten Kooperationspartnern gehören in der EU das Géant2 Projekt AutoBAHN [Aut08] und in USA das NSF geförderte Projekt DRAGON [DRA08] sowie das ESnet Program OSCARS [OSC08].

In AutoBAHN (*Automated Bandwidth Allocation across Heterogeneous Networks*) wird die Bandbreitenreservierung durch die Zuweisung von SDH-Kanälen zu einzelnen Verbindungen realisiert.

Im Gegensatz zu AutoBAHN basiert DRAGON (*Dynamic Resource Allocation via GMPLS Optical Networks*), auf GMPLS Technologie und hat – ähnlich wie GLIF – die Schaltung von Wellenlängen zum Ziel. Es wird allerdings gleichzeitig auch Packet-Switching angestrebt.

In OSCARS (*On-Demand Secure Circuits and Advance Reservation System*) wird die Bandbreitenreservierung in der eigenen Domäne mit Hilfe von MPLS und RSVP Protokollen bewältigt.

Alle Projekte streben Interoperabilität an, damit die Schaltung zwischen Netzen dieser Projekte möglich ist. Es wurden bereits erste erfolgreiche Versuche für Verbindungen zwischen Endpunkten in AutoBAHN und DRAGON/OSCARS Netzen durchgeführt und vorgestellt.

Alle DCN Projekte befinden sich derzeit in Entwicklungsphase.

2.3.4.1. Szenariobeschreibung

Die Control Plane ist hierarchisch aufgebaut. Um eine Verbindung zu beantragen, wendet sich z.B. der AutoBAHN-Kunde an den sog. Domain Manager (DM) – eine Managementkomponente – der eigenen Domäne mit der Anfrage, zwischen welchen Endpunkten und für welche Zeitperiode eine Verbindung benötigt wird. Falls der zweite Endpunkt außerhalb der eigenen Domäne liegt, leitet der DM die Kundenanfrage an den sog. Interdomain Manager (IDM) weiter, der für den Zusammenschluss von AutoBAHN-Netzen zuständig ist. Danach kontaktiert der IDM alle untergeordneten DMs und fragt nach den vorhandenen Kapazitäten zwischen den *Edge*-Punkten dieser Domäne. Basierend auf dieser Information bestimmt der IDM mit Hilfe von OSPF-Suchverfahren eine Multi-Domain-Route zwischen den Endpunkten. Anschließend kontaktiert der IDM alle DMs der beteiligten Domänen mit der Aufforderung, entsprechende Teildienste zu schalten. Falls ein Endpunkt außerhalb der AutoBAHN-Domänen liegt, wendet sich IDM an einen übergeordneten IDM, der die Koordinationsaufgabe zwischen IDMs unterschiedlicher DCN-Projekte übernimmt.

Derzeit können nur scheduled-Verbindungen für eine bestimmte Zeitperiode geschaltet werden. Normalerweise dauert es nur wenige Minuten, bis der Kunde ein Feedback erhält, ob die Dienstinstanz möglich ist oder die benötigten Ressourcen in der angeforderten Zeitperiode fehlen. Für die Inbetriebnahme einer Dienstinstanz werden allerdings mindestens 30 Minuten benötigt.

Für das Monitoring von bestehenden Verbindungen wurde das Konzept und das Monitoring-System von Géant2 E2E Links übernommen und dieses ist derzeit nur auf Up/Down Zustände beschränkt. Es ist geplant, das Géant2-Monitoring-System entsprechend zu erweitern, damit eine Überwachung und Darstellung von anderen relevanten Messwerten, wie z.B. Delay und Jitter, möglich ist.

2.3.4.2. E2E-QoS im Szenario

Die Kooperationspartner bei DCN sind unabhängige Organisationen. Sie fungieren als Service Provider, indem sie Teildienste zur Verfügung stellen, die für eine Verbindung benötigt werden. Die Teildienste sind horizontal verkettet. Somit liegt eine Dienstkette vor.

Neue Aspekte der E2E-Dienstgütezusicherung im Szenario sind:

Kundenperspektive (CSM und QoS):

- Der Zeitrahmen für die Dienstinstanz wird durch die Angabe einer erwünschten Zeitperiode gegeben
- Die Verbindungsdauer kann von einigen Minuten bis zu mehreren Tagen betragen
- Die Überprüfung der Realisierbarkeit kann einige Minuten in Anspruch nehmen
- Für eine Inbetriebnahme werden etwa 30 Minuten benötigt, die Zeit ist jedoch begrenzt und gut abschätzbar
- Das einzige derzeit unterstützte QoS-Merkmal ist die Bandbreite

Providerperspektive (Dienstrealisierung):

- Von den Partnerprojekten werden unterschiedliche Technologien zur Realisierung der Dienstgütezusicherung in eigener Domäne bevorzugt und eingesetzt
- Das Control Plane besteht aus baumartig verknüpften Multi-Domain Rollen, den Interdomain Managern (IDM)
- Die IDMs bestimmen das Routing durch die Domäne in ihrem Zuständigkeitsbereich

- Die Informationsbasis umfasst eine abstrahierte Sicht auf die vorhandenen Kapazitäten zwischen den Edge-Punkten einzelner Domänen
- Die Informationen über vorhandene Kapazitäten werden bei dem Bedarf von den SPs abgefragt. Dadurch wird auch die Aktualität der Informationen erreicht
- Das Switching wird von einem IDM angestoßen, in dessen IDM-Hierarchie der E2E-Pfad bestimmbar ist

2.3.5. Szenario 5: IntServ und DiffServ im Internet

Im Gegensatz zu Telefonnetzen, die auf Leitungsvermittlung beruhen, wird im Internet Nachrichtenvermittlung verwendet. Bei der reinen Datenvermittlung, die in Anfängen des Internets eine zentrale Rolle gespielt hat, bietet Nachrichtenvermittlung ein sehr gutes Kosten/Nutzen-Verhältnis und große Flexibilität bei der Realisierung. Mit der Entwicklung und Verbreitung von interaktiven Multimedia-Diensten, wie z.B. Videostreaming oder Internet-Telefonie, rücken unterschiedliche Qualitätsanforderungen wie z.B. niedrige Verzögerungszeiten in den Vordergrund. Diese können durch die konkurrierenden Nachrichtenströme im Internet nicht gewährleistet werden. Ende der 90er Jahre wurden daher zwei Verfahren zur Qualitätssicherung – DiffServ (Differentiated Services) und IntServ (Integrated Services) – entwickelt.

Bei DiffServ [NBBB98, BBC+98] kann der Sender alle IP-Pakete mit einer Prioritätsstufe versehen. So wird der IP-Verkehr in mehrere Klassen unterteilt. Die Router auf dem Weg zum Empfänger entscheiden allein anhand dieser Angabe, über welche Route und mit welcher Priorität die IP-Pakete weitergeleitet werden.

Bei IntServ [BCS94, SPG97, SW97] werden die Router-Ressourcen für einzelne Verbindungen und nicht Verkehrsklassen, wie es bei DiffServ der Fall ist, reserviert. Das Routing von IP-Paketen geschieht dann anhand ihrer Zugehörigkeit zu der Verbindung.

2.3.5.1. Szenariobeschreibung

Für die Priorisierung stehen bei DiffServ ausschließlich relativ grobe Prioritätsstufen zur Verfügung, die nichts über den tatsächlichen Endkundenbedarf (Bandbreite, Delay, etc.) aussagen. Pakete mit der gleichen Prioritätsstufe, die zu unterschiedlichen Verbindungen gehören, konkurrieren miteinander um die vorhandenen Ressourcen, wodurch Schwankungen der Qualität der einzelnen Verbindungen entstehen können. Andererseits ermöglicht dies die maximal mögliche Ausnutzung der vorhandenen Ressourcen, was im Sinne von Serviceprovidern ist. Da die Prioritätsvorgabe bei diesem

Verfahren seitens des Senders gemacht wird, besteht die Gefahr, dass der Sender dies missbraucht und immer die höchste Prioritätsstufe wählt.

Die Tatsache, dass das Routing von IP Paketen nur durch die Prioritätsstufen beeinflusst wird und keinen weiteren Verwaltungsaufwand seitens der Router braucht, macht dieses Verfahren gut skalierbar. Bei Ausfällen von Teilstrecken werden IP-Pakete automatisch über eine alternative Strecke umgeleitet. Da die Qualitätsanforderungen beim DiffServ direkt im IP-Paket kodiert sind, ist die Dienstgütezusicherung bei diesem Verfahren relativ robust gegen Ausfälle und Veränderungen im Netz. Allerdings müssen Ende-zu-Ende Verbindungen im Internet sehr oft über mehrere Domänen gehen, die u.U. die Prioritätsstufen unterschiedliche behandeln bzw. einfach ignorieren.

Das IntServ-Verfahren ist dagegen darauf angewiesen, dass jeder Knoten im Netz (Router, Switch, etc.) nach dem IntServ-Verfahren vorgeht und alle zur Verfügung stehenden Ressourcen verwaltet. Für die Pfadfindung und Reservierung der benötigten Ressourcen wird *Resource Reservation Protocol* (RSVP) verwendet. Das Problem mit IntServ liegt darin, dass sehr viele Verwaltungsinformationen an Routern gespeichert und bearbeitet werden müssen. Der erforderliche Verwaltungsaufwand führt dazu, dass dieses Verfahren in großen Systemen sehr schlecht skaliert, während es in kleinen Netzen i.A. gute Ergebnisse erzielt.

Obwohl sowohl IntServ als auch DiffServ darauf ausgelegt sind, die Dienstgüte in Multi-Domain Umgebungen zu sichern, bietet keine der beiden Technologien eine Möglichkeit an, die Einhaltung dieser Zusicherungen außerhalb der eigenen Domäne zu überprüfen. Deswegen sind die Dienstnutzer gezwungen, auf das im Internet übliche passive und aktive Monitoring zwischen zwei Endpunkten zurückzugreifen. Diese Verfahren bieten zwar kaum Möglichkeit, eine an einer schlechten E2E-Qualität schuldige Domäne ausfindig zu machen, erlauben es aber, die Dienstgüte aus der Endkundensicht zu messen.

2.3.5.2. E2E-QoS im Szenario

Bei den Verbindungen im Internet sind alle Provider grundsätzlich voneinander unabhängig. IntServ und DiffServ bieten Techniken, die es diesen SPs erlauben, innerhalb der eigenen Domäne die Einhaltung der Teildienste-QoS zu gewährleisten. Die Teildienste sind horizontal verkettet. Somit liegt eine Dienstkette vor.

Neue Aspekte der E2E-Dienstgütezusicherung im Szenario sind:

Providerperspektive (SLM):

- Der tatsächliche Kundenbedarf wird von Prioritätsstufen nicht angesprochen

- Die Prioritätsstufen geben keine Garantien für QoS-Werte und deren Einhaltung
- Die Kodierung der Prioritäten im IP Paket erhöht die Robustheit bei Ausfällen
- Prioritätsstufen können von unterschiedlichen Domänen unterschiedlich behandelt werden
- E2E-Monitoring wird nur von Dienstnutzern betrieben

Providerperspektive (Dienstrealisierung):

- DiffServ setzt auf die Nachrichtenvermittlung mit ihrer *in-band* Priorisierung
- IntServ realisiert eine Art der Leitungsvermittlung

2.4. Generische Betrachtung

In diesem Abschnitt werden alle aus den Szenarios gewonnenen Erkenntnisse generisch betrachtet. Alle für diese Arbeit relevanten Merkmale, die bei der Betrachtung der Szenarien aus fünf Perspektiven erkannt wurden, werden samt ihren in Szenarios vorkommenden Ausprägungen in einer Morphologie zusammengefasst (siehe Abbildung 2.6).

Der morphologische Kasten fungiert als Hilfsmittel, um Gemeinsamkeiten in den Szenarien zu identifizieren und auf dieser Basis ein verallgemeinertes Szenario für die Ende-zu-Ende Dienstgütezusicherung bei Verketteten Diensten zu erstellen.

Weiterhin werden anhand des morphologischen Kastens die Anwendungsfälle (Use Cases) und deren Zusammenhänge identifiziert, die für die E2E-Dienstgütezusicherung von Bedeutung sind.

Die unterstützten QoS-Parameter, das allgemeines Szenario und die Anwendungsfälle bilden die Grundlage für die Anforderungsanalyse, die im Kapitel 2.5 durchgeführt wird.

2.4.1. Morphologie der Szenarien

Im Folgenden wird die Szenario-Morphologie aufgestellt. Die Reihenfolge der Merkmale hat dabei keine Bedeutung und dient ausschließlich der besseren Lesbarkeit der Beschreibung. Die Merkmale werden samt ihren Ausprägungen in einer tabellarischen Darstellung zusammengefasst.

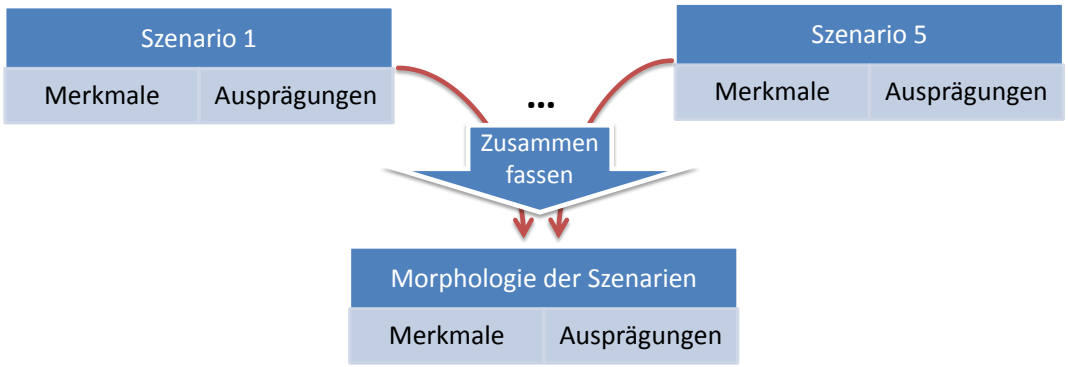


Abbildung 2.6.: Zusammenfassen von Erkentnissen zur Morphologie

Jede Merkmalausprägung wird dabei mit einer Reihe von "(Sx)" markiert, wobei "x" für die Nummer des Szenarios steht, bei dem diese Ausprägung zutrifft; "(S1)" steht somit für das Szenario 1 "Telefonnetz/PSTN".

2.4.1.1. Umfeld der Diensterbringung und -nutzung

Das Umfeld der Diensterbringung und -Nutzung besteht aus zwei Facetten: Aus den Eigenschaften der Service Provider, die den Dienst anbieten und ggf. sich bei der Diensterbringung beteiligen, sowie aus den Eigenschaften der Dienstnutzung der Kunden bzw. Nutzer. Die Morphologie der Szenarien aus dieser Perspektive ist in Tabelle 2.1 zusammengefasst.

Anzahl SPs	wenig (S3) (S4)	mittel (S2)	viele (S1) (S5)
SP-SP Kenntnisse	direkte Nachbarn (S1) (S2) (S3) (S4) (S5)	Kooperations-partner (S3)	Jeder jeden (S2) (S4)
SP-SP Verbindungen für die Teildienste	benachbarte SPs (S1) (S2) (S3) (S4) (S5)	sternförmig über zentrales Netz (S2)	
Von SPs angebotene QoS-Parameter	gleich (S3) (S4) (S5)	teilweise gleich (S1) (S2)	
Von SPs unterstützte QoS	unveränderlich (S3) (S4) (S5)	können sich ändern (S1) (S2)	
Anzahl Customer	wenig (S3) (S4)	mittel (S2)	viele (S1) (S5)
Gleichzeitige Verbindungsanfragen	wenig (S2)	mittel (S3) (S4)	viele (S1) (S5)
Gleichzeitig bestehende Verbindungen	wenig (S2)	mittel (S3) (S4)	viele (S1) (S5)

Tabelle 2.1.: Umfeld der Diensterbringung und -nutzung

In jedem der betrachteten Szenarios existiert ein Pool von Domänen, die als potenzielle Provider von Teildiensten fungieren. Dabei existieren enorme Unterschiede in der Anzahl dieser Domänen. So bewegt sich Anzahl der SP-Domänen, die den Telefondienst anbieten bzw. IntServ/DiffServ-Technologien einsetzen, im Bereich von mehreren hunderten, bei den E2E Links sind es knappe drei Dutzend, bei GLIF und DCN sind es – wegen des experimentellen Status dieser Projekte – nur einige ausgewählte Partner.

Die bei der Diensterbringung beteiligten SP-Domänen besitzen – bedingt durch die Kooperationseigenschaften – unterschiedliche Kenntnis von den anderen Domänen. In allen Szenarios existieren Beziehungen zwischen den direkt benachbarten Domänen. Bei DCN sind alle Domänen in eine Art von Gemeinschaften bzw. engen Kooperationspartnerschaften "gruppiert", die eng miteinander kooperieren. Bei E2E Links und GLIF bestehen Beziehungen zwischen allen beteiligten SP-Domänen.

Parallel zu dem Wissen der SP-Domänen übereinander existiert eine Reihe von Übergangspunkten zwischen den Domänen, an denen die Teildienste miteinander ver-

knüpft werden können. In allen Fällen kann es eine Verbindung zwischen den geographisch benachbarten Domänen geben, es kann aber auch benachbarte Domänen ohne Übergangspunkte geben, und es kann ggf. mehr als nur eine Verbindung zwischen den benachbarten SPs geben. Diese Art von Verbindungsmöglichkeiten ist in allen Szenarios zu finden. Eine weitere Verbindungsart wird parallel zu den oben beschriebenen durch das *Géant2* Backbone-Netz unterstützt, das sich geografisch über mehrere Länder erstreckt und eine Anbindung an alle in der Kooperation beteiligten nationalen Forschungsnetze hat. Dadurch entsteht eine sternförmige Verbindung zwischen Netzen mit dem Géant2 Backbone in der Mitte.

Zwei weitere Aspekte, die die Dynamik der Diensterbringung betrachten, beziehen sich auf die von den SP-Domänen unterstützten QoS-Parameter. Während sich die SP-Domänen in den Szenarios GLIF, DCN und IntServ/DiffServ auf die Zusicherung der Bandbreite beschränken, können SP-Domänen in den zwei weiteren Szenarios unterschiedliche QoS-Parameter unterstützen. Bei beiden, PSTN und E2E Links, existiert zwar eine gemeinsame Schnittmenge der Parameter – für PSTN ist das reine Sprachübertragung, bei E2E Links ist das die Bandbreite – im Übrigen kann die QoS-Unterstützung zwischen SP-Domänen stark variieren. Weiterhin können SP-Domänen bei PSTN und E2E Links ihre Unterstützung von QoS-Parametern jederzeit in Eigenregie ändern; in den anderen Szenarios ist dies momentan nicht der Fall.

Bei der Betrachtung der Aspekte in Bezug auf Dienstnutzer sei zunächst die Anzahl der Kunden angesprochen, die den Dienst nutzen bzw. nutzen wollen. Bei PSTN und IntServ/DiffServ kann man die Anzahl der Dienstnutzer und Kunden als sehr groß – oder sogar unüberschaubar – bezeichnen. Da sich GLIF und DCN derzeit erst im Entwicklungsstadium befinden, ist die Anzahl von Dienstnutzern gering. Die Kundenzahl von E2E Links ist moderat.

Im Bezug auf das Dienstnutzungsverhalten der Kunden und Nutzer müssen zwei weitere Aspekte angesprochen werden: Zum Einen die Anzahl der gleichzeitigen Verbindungsanfragen, die von den Customers gestellt werden bzw. auf die die jeweiligen Dienste ausgelegt sind; Zum Anderen die Anzahl der gleichzeitig bestehenden Verbindungen, die von den Dienstnutzern verwendet werden. PSTN und IntServ/DiffServ sind darauf ausgerichtet und optimiert, gleichzeitig viele Anfragen an den Dienstaufbau sowie viele gleichzeitig bestehende Verbindungen zu unterstützen. Da bei den E2E Links mehrere Managementoperationen manuell vom Betriebspersonal durchgeführt werden müssen, kann man diese zwei Merkmale bei diesem Dienst als eher gering einstufen. Obwohl GLIF und DCN noch nicht im Produktionseinsatz sind, nehmen sie mit ihrer durchgehenden Automatisierung eine mittlere Position ein.

2.4.1.2. Voraussetzungen für die Dienstinanspruchnahme

Um einen Dienst in Anspruch zu nehmen, müssen in den Szenarios verschiedene Voraussetzungen erfüllt werden (siehe Tabelle 2.2).

Anschluss an SP	erforderlich (S1) (S3) (S4) (S5)	nicht erforderlich (S2)
Global eindeutige Anschluss ID	erforderlich (S1) (S3) (S4) (S5)	nicht erforderlich (S2)
Anschluss realisiert durch	SP (S1) (S5)	Customer (S3)
Infrastruktur für Verbindung	Vorhanden und vorkonfiguriert (S1) (S3) (S4) (S5)	Kann (teilweise) fehlen (S2)

Tabelle 2.2.: Voraussetzungen für eine Dienstinanspruchnahme

So wird in allen Szenarios außer E2E Links ein bereits vorhandener Anschluss an die Infrastruktur der SP-Domäne vorausgesetzt; bei E2E Links ist es lediglich erforderlich, dass der Customer in der SP-Domäne bekannt ist. Analog setzen alle Szenarien außer E2E Links voraus, dass alle Anschlüsse mit einer global eindeutigen Anschluss ID versehen werden (für PSTN ist das eine Telefonnummer, bei den anderen ist das die IP Adresse); für die Bestellung E2E Links ist keine eindeutige ID erforderlich.

Bei der Realisierung des erforderlichen Anschlusses bestehen auch Unterschiede. So sind bei PSTN und IntServ/DiffServ dafür die Service Provider verantwortlich. Bei GLIF liegt es dagegen im Verantwortungsbereich des Customers, die eigene Netzinfrastruktur an die Infrastruktur des Providers anzuschließen.

Ein weiterer Unterschied besteht in den Voraussetzungen an die Infrastruktur in den SP-Domänen. In allen Szenarios außer E2E Links ist es erforderlich, dass die Infrastruktur, die für die Diensterbringung verwendet werden kann, bereits vorinstalliert und vorkonfiguriert ist. Bei den E2E Links dagegen geht man davon aus, dass bei Bedarf die fehlende Infrastruktur nachgerüstet wird, um entsprechend dem aktuellen Bedarf die Kundenwünsche erfüllen zu können.

2.4.1.3. Kundenperspektive (CSM und QoS)

Aus der Kundenperspektive sind grundsätzlich die QoS-Parameter und deren Grenzwerte für die E2E-Verbindung sowie die Managementfunktionalität interessant. Die Zusammenfassung dieser Merkmale ist in Tabelle 2.3 zusammengefasst.

Management-funktionalität	Negotiation (S2)		Ordering (S1) (S2) (S3) (S4) (S5)
	Monitoring (S1) (S2) (S3) (S4)		Reporting (S2)
	Change (S2) (S5)		Decomissioning (S1) (S2) (S3) (S4) (S5)
Verfügbarkeit der Mgmt. Funktionalität	24/7 (S1) (S3) (S4) (S5)		Zu Bürozeiten (S2)
Auftragserteilung	nach Verhandlung (S2)		gleich (S1) (S3) (S4) (S5)
Verbindungsbeginn	ab sofort (S1) (S5)		Zeitpunkt (S2) (S3) (S4)
Verbindungsende	open end (S1) (S5)	Dauer (S3) (S4)	Zeitpunkt (S2) (S3) (S4)
Kommunikationsrollen	eine für alle unterstützte SLM-Aufgaben (S1) (S3) (S4) (S5)		aufgabenbezogene Rollen, eine pro Aufgabe (S2)
Auftritt als Kommunikationspartner	Anschluss-SP (S1) (S2) (S3) (S4) (S5)		Multi-Domain Rolle (S2)
Zeit für Feedback	Sekunden (S1) (S5)	Minuten (S3) (S4)	Tage (S2)
Feedback beinhaltet	Ergebnis (S1) (S2) (S3) (S4) (S5)	Gründe (S2) (S4)	Alternativen (S2) (S4)
QoS-Anforderungen	Gegeben durch Vertrag (S1)	In *default settings* (S1)	Spezifizierbar pro Verbindung (S2) (S3) (S4) (S5)
Anzahl QoS-Parameter	1 (S3) (S4) (S5)		>1 (S1) (S2)
QoS-Kategorien (Usage Functionality)	Verfügbarkeit (S2)		Zuverlässigkeit (S2)
	Qualitative (S1) (S2)		Quantitative (S2) (S3) (S4) (S5)
	Wartungsarbeiten (S2)		Nicht-standardisiert (S2)
Abbestellung durch	Customer (S1) (S2) (S3) (S4) (S5)		jeden Nutzer (S1)

Tabelle 2.3.: Kundenperspektive (CSM und QoS)

Wenn man die Managementfunktionalität aus allen Szenarios zusammenfasst, entspricht sie den klassischen Aufgaben in unterschiedlichen Phasen des Dienstlebenszyklus. Allerdings werden bei manchen Szenarios den Kunden nicht alle Managementfunktionen angeboten. So werden Verhandlung und Reporting der QoS-Einhaltung nur bei E2E Links unterstützt. Das Monitoring der QoS-Einhaltung wird – zwar mit sehr großen Unterschieden – seitens des Service Providers für alle Dienste außer IntServ/DiffServ durchgeführt. In allen Szenarios sind die grundlegende Funktionen Bestellen und Abbestellen einer Dienstinstanz möglich.

Bei der Verfügbarkeit der Inanspruchnahme von Managementfunktionalität zeichnet sich der Unterschied zwischen den voll automatisierten und den manuell eingerichteten Diensten ab. So können die Kunden von E2E Links die erwünschten Aktionen nur zur Bürozeiten anstoßen, während bei den anderen Szenarios dies 24/7 möglich bzw. angestrebt ist.

Da beim Dienst E2E Links eine Verhandlungsmöglichkeit vorgesehen ist, besteht die Möglichkeit, einen Konsens zwischen dem Kunden den Service Provider in Bezug auf die benötigte E2E-QoS zu finden, bevor eine neue Dienstinstanz bestellt wird. Bei den übrigen Szenarios wird eine Dienstinstanz unmittelbar bestellt.

Bei der Spezifikation des Verbindungsbegins gibt es die Alternativen einer sofortigen Diensteinschaltung (bei PSTN und IntServ/DiffServ) bzw. die Bestellung einer Dienstinstanz ab einem bestimmten Zeitpunkt (bei den übrigen drei Szenarios).

Das Verbindungsende kann durch ein explizites Abbestellen (charakteristisch für PSTN und IntServ/DiffServ), die Angabe der erwünschten Verbindungsdauer (GLIF und DCN) oder die Angabe des erwünschten Zeitpunkts für das Verbindungsende (E2E Links, GLIF, DCN) angegeben werden.

Bei einem "Abruf" von Managementfunktionen hat der Kunden in allen Szenarien stets einen einzelnen Kommunikationspartner. In den meisten Fällen wird diese Rolle für alle Managementfunktionen von dem Anschluss-SP übernommen. Bei E2E Links allerdings wird diese Rolle für das Monitoring und Reporting von der zentralen E2ECU übernommen, für alle weiteren Funktionalitäten ist wiederum der Anschluss-SP der Kommunikationspartner.

Bei der Durchführung der Managementaufgaben wird dem Kunden ein Feedback geliefert. Das Feedback kann die reine Mitteilung der Ergebnisse einer Anfrage (in allen Szenarios), Gründe des Fehlschlagens (E2E Links und DCN) oder sogar mögliche Alternativen (wiederum E2E Links und DCN) beinhalten. Die Dauer, bis der Kunde das Feedback bekommt, variiert von Sekunden (PSTN und IntServ/DiffServ) über Minuten (GLIF und DCN) bis hin zu mehreren Tagen (E2E Links).

Bei der Bestellung einer neuen Verbindung bzw. bei der Änderung der Anforderungen an bestehenden Dienstinstanzen hat der Kunde die Möglichkeit, E2E QoS-Anforderungen an die Dienstinstanz zu spezifizieren. Beim Telefondienst sind die E2E-Anforderungen einerseits durch den Rahmenvertrag und andererseits durch die veränderbaren vordefinierten Einstellungen gegeben. In den übrigen Szenarios besteht für den Kunden die Möglichkeit, die erwünschte Dienstgüte und die Dienstgüteparameter frei zu wählen.

Dabei unterscheiden sich Dienste auch in Bezug auf die Anzahl gleichzeitig unterstützter Parameter. Für PSTN und E2E Links können das mehrere Parameter gleichzeitig sein, für die übrigen Szenarios nur einer.

Die in allen Szenarios unterstützten QoS-Parameter können zu einer Reihe von QoS-Kategorien zusammengefasst werden. So werden für E2E Links die klassischen QoS-Parameter Verfügbarkeit und Zuverlässigkeit der Dienstinstanzen dem Kunden angeboten. Bei PSTN und E2E Links kommen darüberhinaus auch QoS-Parameter vor, die als qualitativ bezeichnet werden können. Sie sagen etwas über das Vorhandensein eines gewissen Merkmals aus wie z.B., ob die Nummerweiterleitung oder die Konformität einer EU-Richtlinie unterstützt wird oder nicht. Von allen Diensten außer PSTN wird auch die Spezifikation von quantitativen Parametern unterstützt, wie minimale Bandbreite oder maximaler Jitter. Neben den beschriebenen, in SLAs üblichen QoS-Kategorien werden bei E2E Links noch zwei weitere Dienstgütemerkmale einer Dienstinstanz unterstützt. Zum einen ist das die Fülle der Parameter, die die Durchführung der Wartungsarbeiten an der Dienstinstanz regeln. Diese sind essentiell für Dienstinstanzen, die anspruchsvollen Kunden wie LHC oder DEISA angeboten werden. Weiterhin besteht für die Kunden die Möglichkeit, für sie relevante und von den SPs nicht standardisierte Parameter anzugeben, wie z.B. die Anforderung, für bestimmte E2E Links unterschiedliche Strecken der Glasfaser und unterschiedliche HW-Komponenten zu verwenden.

Zu guter Letzt ist zu berücksichtigen, wer die Dienstinstanz abbestellen darf. In allen Szenarios ist es möglich, dass der Kunde die Dienstinstanz abbestellt, der diese auch bestellt hat. Bei PSTN wird diese Möglichkeit auch dem zweiten Kommunikationspartner eingeräumt.

2.4.1.4. Providerperspektive (SLM)

Die Merkmale und Ausprägungen der SLM-Prozesse, die die SP-Domänen ausüben, um ihre Dienstgütezusicherungen zu gewährleisten, sind in Tabelle 2.4 zusammengefasst.

Aus der Providerperspektive weisen alle Szenarios zwei Gruppen von SLM-Anwendungsfällen auf. Die Anwendungsfälle, die sich mit der Kommunikation mit dem Customer befassen, können als "nach außen" orientiert bezeichnet werden. Diese Gruppe wurde bereits bei der Szenariobetrachtung aus der Kundenperspektive als "Managementfunktionalität" erfasst. Die andere Gruppe befasst sich mit der Realisierung dieser Funktionalität und orientiert sich "nach innen", da dabei die Kommunikation ausschließlich zwischen SP-Domänen und anderen bei der Diensterbringung benötigten Rollen existiert.

In den Szenarios kommen folgende Multi-Domain Use Cases nach innen vor. Bei E2E Links wird ein Angebot für die Verbindung anhand der Kundenanforderungen vorbereitet. Dies beinhaltet unter anderem eine grobe Routenplanung durch die SP-Domäne und eine Machbarkeitsstudie in den für die Diensterbringung vorgesehenen Domänen. In allen Szenarios wird eine genaue Routenplanung benötigt, diese wird i.d.R. nach der Auftragserteilung durchgeführt. Bei der Durchführung dieser Aufgabe

SLM Use Cases	Nach außen (zum Customer) (S1) (S2) (S3) (S4) (S5)		Nach innen (zu und zwischen SPs) (S1) (S2) (S3) (S4) (S5)
Multi-Domain Use Cases (nach innen)	Vorbereitung des Angebots (S2)		genaue Routenplanung durch SP-Domäne (S1) (S2) (S3) (S4) (S5)
	Aushandlung von Interconnection Points (S2)		Aushandlung von Verbindungsparametern (S1) (S2)
	Planung von QoS für SP-Abschnitte (Teildienste) (S2) (S3) (S4) (S5)		Teildienste-Monitoring Durchführen (S1) (S2) (S3) (S4)
	Monitoring der Teildienste aggregieren (S2) (S4)		Reporting erstellen (S2)
Aushandlung der Parameter	anhand eines allgemein unterstützten Protokolls (S1) (S3) (S4) (S5)		manuell (S2)
Kundenanforderungen an QoS bei der Planung	ignoriert (S1)		berücksichtigt (S2) (S3) (S4) (S5)
Planungsphasen	gleich detailliert (S1) (S3) (S4) (S5)		Schätzung und detailliert (S2)
Schätzung des Inbetriebnahmedatums	genau (S1) (S3) (S4) (S5)		ungenau (S2)
Dauer von Routing und Switching	kurz (S1) (S5)	zeitlich begrenzt (S1) (S3) (S4) (S5)	schwankt (S2)
Ausweichen auf alternative Route	möglich bei Planung (S1) (S2) (S3) (S4) (S5)	möglich bei Inbetriebnahme (S1) (S2) (S5)	möglich im Betrieb (S5)
QoS-Monitoring	Kunden-QoS (S3) (S4) (S5)		Ableitung Kunden-QoS von Geräte-QoR (S1) (S2)
E2E-Monitoring	direkte E2E-Messungen (S5)		Aggregation Teilstrecken Messungen (S2) (S4)
Monitoring-Strecken	E2E (S5)	Domain (S1) (S2) (S4)	Interdomain (S2) (S4)
Monitoring-Ziele	Ende der Dienstnutzung erkennen (S1)	Einhaltung Kunden-QoS (S2) (S4) (S5)	Erkennung Problem-SPs (S2)
Konsumenten von Monitoring-Infos	Kunde (S2) (S5)	SPs (S1) (S2) (S4) (S5)	Multi-Domain Rollen (S2) (S4)
Garantien (SLAs) für Teildienste	nicht gegeben (S1) (S2) (S4) (S5)		gegeben (S3)

Tabelle 2.4.: Providerperspektive (SLM)

wird in manchen Fällen auf zwei weitere Use Cases zurückgegriffen. Bei E2E Links wird dabei die Aushandlung von Verbindungspunkten zwischen zwei benachbarten SP-Domänen benötigt. Weiterhin findet zwischen den zu verbindenden Domänen bei PSTN und bei E2E Links eine Aushandlung von Verbindungsparametern statt. Wie die Teildienste von den SP-Domänen realisiert werden, ist in allen Fällen eine domäneninterne Angelegenheit. Allerdings müssen für alle Teildienste Schwellwerte der QoS-Parameter festgelegt werden, deren Einhaltung die Erfüllung der E2E-Anforderungen an die Dienstqualität gewährleistet. Dieser Use Case ist in allen Szenarios außer bei PSTN vorhanden. Die Einhaltung der an die Teildienste gestellten Anforderungen wird in den meisten Szenarios unterstützt. Zwei Ausnahmen bilden Intserv/DiffServ, da diese Technologien keine eingebaute Unterstützung für diese Monitoring-Art haben, und der Telefondienst, bei dem sich die Überwachung ausschließlich auf die reine Aufrechterhaltung der Verbindung beschränkt. Auf der Basis der QoS-Parameter einzelner Abschnitte wird bei E2E Links und DCN ein aggregierter E2E-QoS Wert errechnet. Dies erlaubt für den Kunden Berichte über die Einhaltung der vereinbarten Dienstgüte zu erstellen, was allerdings derzeit nur von E2E Links Dienst angeboten wird.

Bei der Durchführung vieler Managementaufgaben müssen zwischen Domänen eine Reihe von Parametern ausgehandelt werden. Mit Ausnahme von E2E Links, bei denen dies manuell geschieht, werden in den Szenarios für den Zweck von allen SPs unterstützte Protokolle verwendet und vorausgesetzt.

Wie man am Beispiel des Telefondienstes sieht, wird durch die reine Spezifikation der Kundenanforderungen ihre Einhaltung nicht garantiert. Die SP-Domänen, die sich bei der Diensterbringung beteiligen, dürfen diese Anforderungen ignorieren. Im Gegenteil dazu werden die Kundenanforderungen in den anderen Szenarios bei der Durchführung von SLM Aufgaben berücksichtigt.

Die Planung einer Verbindung kann in Phasen aufgeteilt werden. So wird bei E2E Links zunächst eine ungenaue Planung mit der Abschätzung der Machbarkeit und erst nach dem Vertragsabschluss die genaue Routenplanung mit der Festlegung aller Grenzwerte für die involvierten Teildienste durchgeführt. In den anderen Szenarios wird eine Schätzung weggelassen und gleich die genaue Planung durchgeführt.

Nachdem die Routenplanung abgeschlossen ist, muss die Dienstinstanz in Betrieb genommen werden. Dabei kann bei Diensten mit einer vorinstallierten und vorkonfigurierten Infrastruktur eine genaue Schätzung darüber gemacht werden, zu welchem Zeitpunkt die Dienstinstanz in Betrieb genommen werden kann. Bei E2E Links kann wg. fehlender oder noch nicht konfigurierter Infrastruktur i.d.R. nur eine ungefähre Schätzung gemacht werden.

Außer der Genauigkeit der Abschätzung weist die Dauer des Routings und des Switchings einer Dienstinstanz drei Ausprägungen auf. Während die Zeit für die Durchführung dieser Operationen bei E2E Links schwankt, sind sie bei den anderen Szenarios

zeitlich begrenzt. Bei PSTN und IntServ/DiffServ ist die Zeit für den Aufbau einer Dienstinstanz sehr kurz (im Bereich von *ms*).

In allen Phasen des Dienstlebenszyklus ist die Möglichkeit zum Ausweichen auf alternative Pfade interessant. In allen Szenarios ist ein Ausweichen während der Planung der Route für eine neue Dienstinstanz möglich. Weiterhin ist es bei PSTN, E2E Links und IntServ/DiffServ möglich, auch während der Inbetriebnahme auf eine alternative Route auszuweichen. Da die Qualitätsmerkmale bei DiffServ direkt in dem IP Header kodiert sind, ist es bei den auf dieser Technologie basierenden Diensten möglich, auch während des Betriebs ohne Qualitätsverlust auf eine Alternative auszuweichen.

Beim Monitoring von QoS-Parametern kann unterschieden werden, ob die dem Kunden angebotene QoS direkt gemessen (GLIF, DCN, IntServ/DiffServ) oder erst von den Statusmeldungen eingesetzter Geräten abgeleitet (PSTN, E2E Links) werden. Weiterhin können für die Überwachung von E2E-QoS entweder direkte E2E-Messungen zwischen zwei Endkunden (was bei dem Einsatz von IntServ/DiffServ üblich ist) oder durch die Aggregation der Messungen aller Teilstrecken (was bei E2E Links und DCN der Fall ist) eingesetzt werden. Die Monitoring-Strecken, aus denen eine E2E-Strecke besteht, kann in Domain- (komplett innerhalb einer SP-Domäne) und Interdomain-Teilstrecken (zwischen zwei benachbarten SP-Domänen) aufgeteilt werden. Während für den PSTN Dienst die Überwachung der Domain-Strecken ausreicht, müssen bei E2E Links und DCN auch Interdomain-Strecken überwacht werden, um eine aussagekräftige QoS-Aggregation zu bekommen.

Das Monitoring an sich ist kein Selbstzweck und wird eingesetzt, um das Eintreffen unterschiedlicher Ereignisse zu erkennen. Bei PSTN ist dies das Ende der Dienstnutzung; bei den übrigen Szenarios wird die Einhaltung der QoS-Zusicherungen überprüft. Bei E2E Links wird darüber hinaus auch das Ziel verfolgt, die SP-Domäne(n) zu identifizieren, die zum Verstoß gegenüber der Zusicherung geführt haben.

Als Konsumenten der Multi-Domain Monitoring-Informationen treten in den Szenarios die Kunden selbst (bei E2E Links und IntServ/DiffServ), die diensterbringenden Service Provider (in allen Szenarios außer GLIF) und auch Multi-Domain Managementinstanzen (bei E2E Links und in DCN) auf.

Das Monitoring der Einhaltung von QoS-Zusicherungen bedeutet nicht automatisch die Verbindlichkeit dieser Zusicherungen. So werden ausschließlich bei GLIF SLAs für die Teilstrecken und deren QoS-Parameter abgeschlossen, bei den restlichen Szenarios sind die Grenzwerte nicht verbindlich.

2.4.1.5. Providerperspektive (Dienstrealisierung)

Jeder der benötigten SLM-Prozesse kann auf unterschiedliche Art und Weise realisiert werden. Die in den Szenarios vorgekommene Realisierungsausprägungen und Aspekte sind in Tabelle 2.5 zusammengefasst.

Multi-Domain Routing durchgeführt von	SP (S1) (S2) (S3) (S5)		Multi-Domain Rolle(n) (S4)
Routing-Bezug und erforderliches Wissen	lokal (nächste SP-Domäne) (S1) (S2) (S5)	semi-global (Gruppe von SP-Domänen) (S4)	Global (für alle SPs in der Kette) (S3)
Routing-Reihenfolge	SPs in der Kette nacheinander (S1) (S2) (S5)		Gleichzeitig für alle SPs in der Kette (S3) (S4)
Routing-/Switching-„Verzahnung“	gleichzeitig mit dem Routing (S1) (S5)		nach dem vollständigen Routing (S2) (S3) (S4)
Inbetriebnahme	automatisiert (S1) (S3) (S4) (S5)		manuell (S2)
Kommunikation	in der Kette (S1) (S2) (S5)	im Baum (S4)	jeder mit jedem (S3)
Ressourcenzuweisung für die Verbindung	dediziert im Vorfeld (Leitungsvermittlung) (S1) (S2) (S3) (S4) (S5)		*on the fly* (anhand von Nachricht-Priorität) (S5)
Monitoring durch	Endnutzer (S5)		SPs für ihre Teildienste (S1) (S2) (S4)
Monitoring-Durchführung	Traps (S1) (S2) (S4) (S5)		Polling (S1) (S2) (S4) (S5)
Granularität der Messungen	identisch (S5)		unterschiedlich (S1) (S2) (S4)
Synchronisation der Messungen	nicht benötigt bzw. verwendet (S5)	anhand des Zeitstempels (S4)	gleichzeitiges Abholen (S2)
Abholen von Monitoring-Daten für E2E-Monitoring	Push (S1)		Pull (S2) (S4)

Tabelle 2.5.: Providerperspektive (Dienstrealisierung)

Das Routing durch mehrere Domänen wird in den meisten Szenarios – zwar auf unterschiedliche Art – von den SP-Domänen selbst bestimmt. Lediglich bei DCN wird diese Aufgabe von einer Multi-Domain Rolle (Interdomain Manager) übernommen.

Im Falle von PSTN, E2E Links und IntServ/DiffServ kann jede Domäne ausschließlich die nachkommende Domäne in der Route bestimmen. Diese Ausprägung und das

dafür benötigte Wissen kann man als "lokal" bezeichnen, da die Entscheidung anhand von SP-internen Kriterien und Routingtabellen getroffen wird. Bei GLIF wird die Entscheidung zwar von einer SP-Domäne getroffen, sie bezieht sich jedoch auf den kompletten Pfad über alle an der Diensterbringung beteiligten Domänen. Dafür wird "globales" Wissen über die bei allen Domänen vorhandenen freien Kapazitäten benötigt. Die Realisierung bei DCN nimmt eine Zwischenposition ein. Von jedem IDM wird eine Route durch mehrere, allerdings i.A. nicht alle SP-Domäne bestimmt, für die IDM verantwortlich ist. Das dafür benötigte Wissen sowie der Zuständigkeitsbereich können als "semi-global" bezeichnet werden.

Die Reihenfolge, in der das Routing für die einzelnen Abschnitte durchgeführt wird, unterscheidet sich in den Szenarios folgendermaßen: Bei PSTN, E2E Links und IntServ/DiffServ wird das Routing für die nächste Domäne erst dann angestoßen, wenn die Aufgabe bei der vorherigen abgeschlossen wurde. Bei GLIF und DCN kann diese Aufgabe gleichzeitig für alle Domänen in der Kette durchgeführt werden.

Die "Verzahnung" zwischen Routing und der Inbetriebnahme (bzw. Switching) kann auf mehrere Arten realisiert werden. So wird das Schalten einer Teilstrecke bei PSTN und IntServ/DiffServ gleich nach dem Abschluss des Routings gemacht. Bei den übrigen drei Szenarios wird zuerst auf den Abschluss des E2E-Routings gewartet.

Die Inbetriebnahme/Switching selbst geschieht in den meisten Fällen automatisiert. Lediglich bei E2E Links wird sie manuell durchgeführt.

Bei der Erfüllung von Multi-Domain Managementaufgaben müssen die Provider miteinander kommunizieren, um die für die Durchführung relevanten Informationen auszutauschen. In den Szenarios kommt Informationsaustausch entlang eines Pfades bzw. in der Kette (vertreten von E2E Links, PSTN und IntServ/DiffServ), in einer baumartig organisierten Managerstruktur (typisch für DCN) und "jeder mit jedem" (im Falle von GLIF) vor.

Um die zugesicherte Dienstgüte garantieren zu können, müssen für die Verbindung ausreichende Ressourcen reserviert werden. Lediglich bei DiffServ erfolgt eine *on the fly* Zuweisung von Ressourcen für die Nachrichten anhand ihrer Prioritätstufe. In den übrigen Fällen wird die Reservierung im Vorfeld dediziert für jede Verbindung gemacht, was für die Leitungsvermittlung typisch ist.

Das Monitoring der Dienstgüteeinhaltung wird beim Einsatz von IntServ/DiffServ grundsätzlich dem Endnutzer überlassen. Bei allen anderen betrachteten Diensten – zwar im unterschiedlichen Ausmaße – sind auch die Service Provider in der Überwachung involviert.

In allen betrachteten Szenarios können bei der Überwachung sowohl SNMP Traps als auch Polling von HW-Zählern zum Einsatz kommen. Im Fall von IntServ/DiffServ, wenn die Messungen von den Endnutzern durchgeführt werden, spielt der zeitliche Ablauf der Messungen keine Rolle, in anderen Fällen entstehen technologiebedingt

Synchronisationsprobleme, die auf unterschiedliche Weise adressiert werden. Im Falle von DCN werden Zeitstempel bei Messungen eingesetzt. Bei E2E Links wird das Problem durch das (fast) gleichzeitige Abholen der Messdaten aus allen beteiligten Domänen gelöst. In beiden Fällen bleibt allerdings das Problem von *spikes* (kurzfristigen Ausfällen zwischen Polling) nicht gelöst.

Die Verteilung der Messdaten an die daran interessierten Rollen wird mit Push- (im Falle PSTN) und Pull-Mechanismen (bei E2E Links und DCN) realisiert.

2.4.2. Generisches Szenario

Die im vorherigen Abschnitt aufgestellte Morphologie der Szenarien bildet eine Grundlage für die Ableitung eines allgemeinen generischen Szenarios. Das generische Szenario wird von den Gemeinsamkeiten in den untersuchten Beispielen abgeleitet. Es kann aber auch sein, dass in allen Szenarios dieselbe Voraussetzung zugrunde gelegt wird (siehe z.B. AN-QoSSemantik auf Seite 57) oder es in den Szenarios keine Schnittmenge bei der Herangehensweise an dasselben Problems existiert (siehe z.B. AN-EPIdentifikation auf Seite 57). Da in diesen Fällen dennoch Lösungsansätze existieren, die nicht als ein Teil des generischen Modells aufgefasst werden können, kann deren Lösung für diese Arbeit o.B.d.A. vorausgesetzt und als eine Annahme aufgefasst werden (siehe Abbildung 2.7). Für die bessere Referenzierbarkeit wird jede der getroffenen Annahmen mit einer mnemonischen Bezeichnung versehen, die mit "AN-" anfängt.

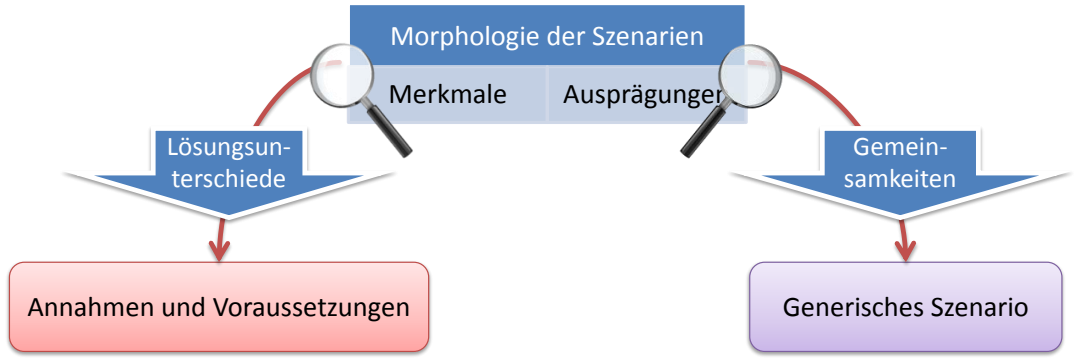


Abbildung 2.7.: Ableitung eines generischen Szenarios

Bei der Betrachtung der Morphologie des Umfeldes, in dem der Dienst erbracht und genutzt wird (siehe Tabelle 2.1), können folgende Verallgemeinerungen getroffen werden:

- Es existiert ein Pool von Service Providern, die als potenzielle Erbringer von Teildiensten auftreten. Alle SPs sind autonome, voneinander unabhängige Organisationen. Über ihre Anzahl und den gegenseitigen Bekanntschaftsgrad kann im Allgemeinen keine Aussage getroffen werden.

- Jede der SP-Domänen unterstützt eine Menge von Dienstgütemerkmalen und -Parametern. Bei der Erbringung von Teildiensten kann die Einhaltung der Grenzwerte ausschließlich für diese Merkmale garantiert werden. Die Unterstützung von einzelnen Parametern kann sich zwischen den Domänen unterscheiden und mit der Zeit ändern.
- Die Provider sind miteinander vermascht in dem Sinne, dass dadurch die Teildienste miteinander verknüpft werden können. Dies ist allerdings keine Vollvermaschung. Weiterhin kann zwischen je zwei Domänen mehr als eine Verbindung existieren. Diese Verbindungen können (durch die SP-Unterstützung) verschiedene Charakteristika – lies QoS-Unterstützung – aufweisen.
- Weder über die Anzahl der Dienstnutzer noch über deren Nutzungsverhalten in Bezug auf gleichzeitig gestellte Anfragen und/oder gleichzeitig bestehende Dienstinstanzen kann eine allgemeine Aussage getroffen werden. Aus diesem Grund kann in dem allgemeinen Szenario ausschließlich ein Kunde und seine Beziehung zu einer einzelnen Dienstinstanz betrachtet werden.

Annahme: für alle SPs gemeinsame QoS-Semantik

Auch wenn in allen Szenarios unterschiedliche QoS-Parameter unterstützt werden, so herrscht zwischen den SP-Domänen ein Konsens über die Semantik der QoS-Parameter. Da es eine verbreitete Praxis ist, die Semantik der QoS-Merkmale durch ITU-T, IEEE oder andere ähnliche Gremien eindeutig zu spezifizieren, wird folgende Annahme getroffen:

AN-QoSSemantik Die Semantik von QoS-Parametern und Merkmalen ist eindeutig definiert und wird von allen SP-Domänen gleich verstanden.

Aus der Morphologie der Voraussetzungen (siehe Tabelle 2.2) kann für das allgemeine Szenario lediglich eine Tatsache hinzugewonnen werden:

- Durch die prinzipielle Möglichkeit der SP-Domänen, ihre Infrastruktur zu erweitern bzw. auszubauen, kann man vorhandene Kapazitäten für QoS-Merkmale in zwei Gruppen aufteilen: bereits vorhanden bzw. potenziell.

Annahme: CSM sei gegeben

Aus der Morphologie können zwei weitere Voraussetzungen abgeleitet werden. So gibt es in den Szenarios keinen Konsensus darüber, wie und durch wen die Managementschnittstelle zwischen dem Kunden und seinem Service Provider realisiert wird. Da in allen Szenarios eine CSM-Schnittstelle existiert, wird sie in dieser Arbeit als gegeben vorausgesetzt:

AN-CSMExistiert Es existiert eine CSM Schnittstelle, über die der Customer den Zugriff auf die Managementfunktionalität seines Dienstes hat.

Annahme: EPs sind eindeutig identifizierbar

Weiterhin werden in allen Szenarios die Endpunkte einer Verbindung eindeutig identifiziert. Daraus leitet sich die folgende Annahme ab:

AN-EPIdentifikation Die Endpunkte einer Dienstinstanz können eindeutig identifiziert werden.

Die aus der Kundenperspektive erfassten Eigenschaften (siehe Tabelle 2.3) beziehen sich hauptsächlich auf die Ausprägungen der Managementfunktionalität und die den Kunden angebotenen QoS-Kategorien. Diese werden im folgenden Unterabschnitt genauer betrachtet. Für das allgemeine Szenario sind folgende Gemeinsamkeiten aufgefallen:

Rolle: Kommunikationspartner

- In allen Szenarios kommuniziert der Kunde bei allen Managementaufgaben jeweils mit einer einzelnen Rolle, die im Weiteren als *Kommunikationspartner* referenziert wird. Diese Rolle wird in den betrachteten Szenarios von unterschiedlichen Akteuren "besetzt", deswegen kann für das generische Szenario keine Aussage darüber getroffen werden. Im Allgemeinen kann man auch sagen, dass der Kunde jeweils einen Kommunikationspartner pro SLM-Aufgabe hat, da diese Rolle für unterschiedliche Aufgaben durch unterschiedliche Akteure besetzt werden kann.

- Weiterhin beziehen sich die Kundenanforderungen grundsätzlich auf eine Dienstinstanz. Die Kundenanforderungen beziehen sich auf einen oder mehrere QoS-Parameter, die übrigen (von SP-Domänen unterstützten) QoS-Parameter spielen für den Kunden keine Rolle.

Die Gemeinsamkeiten in der Morphologie aus der Providerperspektive (siehe Tabellen 2.4 und 2.5) liefern übrige Aspekte, die das generische Szenario bestimmen:

- Jede Dienstinstanz setzt sich aus den Teildiensten zusammen, die i.A. von mehreren SPs erbracht werden.

- Die E2E-QoS setzt sich aus den QoS der Teildienste zusammen, die deren Provider einhalten.

- Im Allgemeinen gibt es mehrere Wege über Domänen, die zwei Endpunkte verbinden. Nicht alle davon erfüllen aber E2E-Kundenanforderungen an die Verbindung.

- Die Einhaltung von E2E-QoS kann durch Monitoring unterstützt werden. Das Monitoring kann entweder Ende-zu-Ende oder auf Teilstreckenbasis durchgeführt werden. Es kann allerdings keine allgemeine Aussage darüber getroffen werden, wer und wie die Aggregation der Teilstrecken-QoS zu E2E-QoS durchführt.

Eine graphische Darstellung des generischen Szenarios ist in Abbildung 2.8) skizziert.

In der Wolke oben ist symbolisch die Kundenvorstellung der erwünschten Dienstinstanz und ihre E2E QoS-Werte dargestellt. Die horizontale Strich-Punkt-Linie in der Mitte des Bildes markiert die Tiefe des Kundeneinblickes in die Dienstrealisierung. Diese Linie trennt somit die Kunden- und die Multi-Domain Providersichten. Der

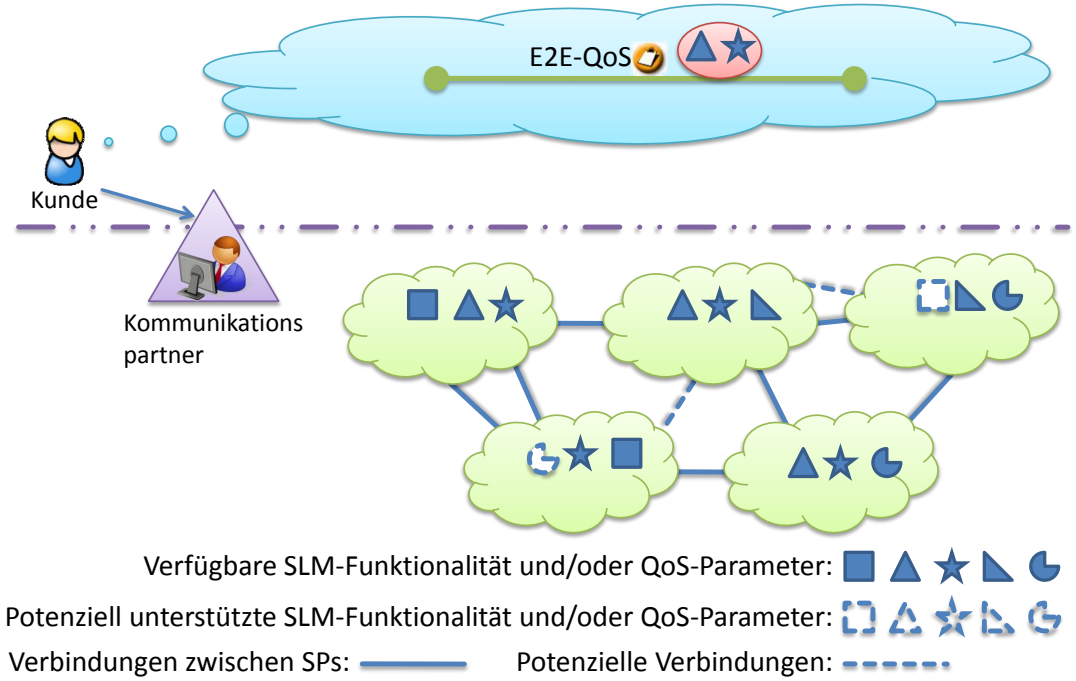


Abbildung 2.8.: Modell Concatenated Service

Kunde kann nur seinen Kommunikationspartner "sehen" und ansprechen. Der Kommunikationspartner stellt ein Verbindungsglied zwischen Kunden- und Multi-Domain Sichten dar.

Die Service Provider Domänen werden als eine Reihe von Wolken unterhalb der Strich-Punkt Linie gezeichnet. Die Verbindung zwischen der Rolle "Kommunikationspartner" und den Service Providern ist im generischen Szenario nicht festgelegt, deswegen existiert auch im Bild keine Verbindungslinie. Dafür existieren unterschiedliche Verbindungen zwischen den SP-Domänen selbst, die als durchgezogene – für bereits existierende – und als gestrichelte – für die potenziell möglichen – Linien dargestellt sind.

Die unterschiedlichen geometrischen Figuren in den Wolken symbolisieren QoS-Parameter und Managementfunktionalität, die von den SP-Domänen unterstützt werden bzw. (in der Wolke oben) die von dem Kunden erwünscht sind. Analog zu den Linien existieren dabei sowohl bereits unterstützte als auch potenziell unterstützte Parameter.

Bemerkung: Obwohl dies im Bild nicht explizit gezeichnet wurde, können die unterschiedlichen Verbindungen zwischen Domänen unterschiedliche QoS-Merkmale aufweisen. Das wird durch mehrere Verbindungen zwischen je zwei Domänen lediglich angedeutet.

2.4.3. Anwendungsfälle (Use Cases)

In diesem Abschnitt werden die CSM-Funktionalität und die Provider-internen SLM-Prozesse, die in den Morphologietabellen 2.3 und 2.4 zusammengefasst sind, in Verbindung miteinander gebracht. Die Use Cases werden generisch beschrieben, so dass sie die in den Szenarios vorgekommene Funktionalität umfassend abdecken. Das Zusammenspiel der Use Cases wird anhand von Ablaufszenarien mit Alternativpfaden sowie in der Form eines begleitenden UML-Diagramms erläutert.

Die Use Cases, für die unklar ist, wer sie ausführt, werden ohne Verbindung zu den Akteuren gezeichnet; die Zuweisung dieser Use Cases an Rollen und Akteure ist eine der Aufgaben des konstruktiven Teils dieser Arbeit.

2.4.3.1. Verhandlung und Bestellung

Verhandlung und Bestellung werden vom Customer initiiert. Da die Bestellung ohne vorangegangene Verhandlung ausgeführt werden kann, existieren in diesem Abschnitt zwei primäre Szenarioabläufe, die den erfolgreichen Fall beschreiben. Die sekundären Szenarioabläufe beschreiben den Fall, bei dem die Kundenanforderungen nicht erfüllt werden konnten. Die Zusammenhänge der Anwendungsfälle für Verhandlung und Bestellung sind in Abbildung 2.9 dargestellt.

Ablaufszenario: Primär I

Bezeichnung: Verhandlung mit anschließender Bestellung

Ablauf:

1. Der Customer teilt seinem Kommunikationspartner mit, dass er eine E2E Verbindung braucht. Dabei spezifiziert er, welche E2E Anforderungen diese Verbindung erfüllen soll. Diese Information dient als Grundlage für die Machbarkeitsstudie, ob die Kundenanforderungen realisierbar sind oder nicht.

2. Im Laufe der Machbarkeitsstudie wird einerseits eine grobe Routenplanung gemacht, um die Domänen zu identifizieren, die sich bei der Diensterbringung der neuen Verbindung beteiligen können. Zum anderen werden diese SP-Domänen gefragt zu prüfen, ob sie ihre Teildienste mit der erforderlichen Dienstgüte erbringen können oder nicht. Die Machbarkeit jeder Teilstrecke wird von der SP-Domäne geprüft, die diese später realisieren soll.

3. Falls die Realisierung mit den erforderlichen Parametern möglich ist, wird ein entsprechendes Feedback für den Kunden generiert.

4. Das Feedback wird vom Kommunikationspartner an den Kunden weitergereicht.

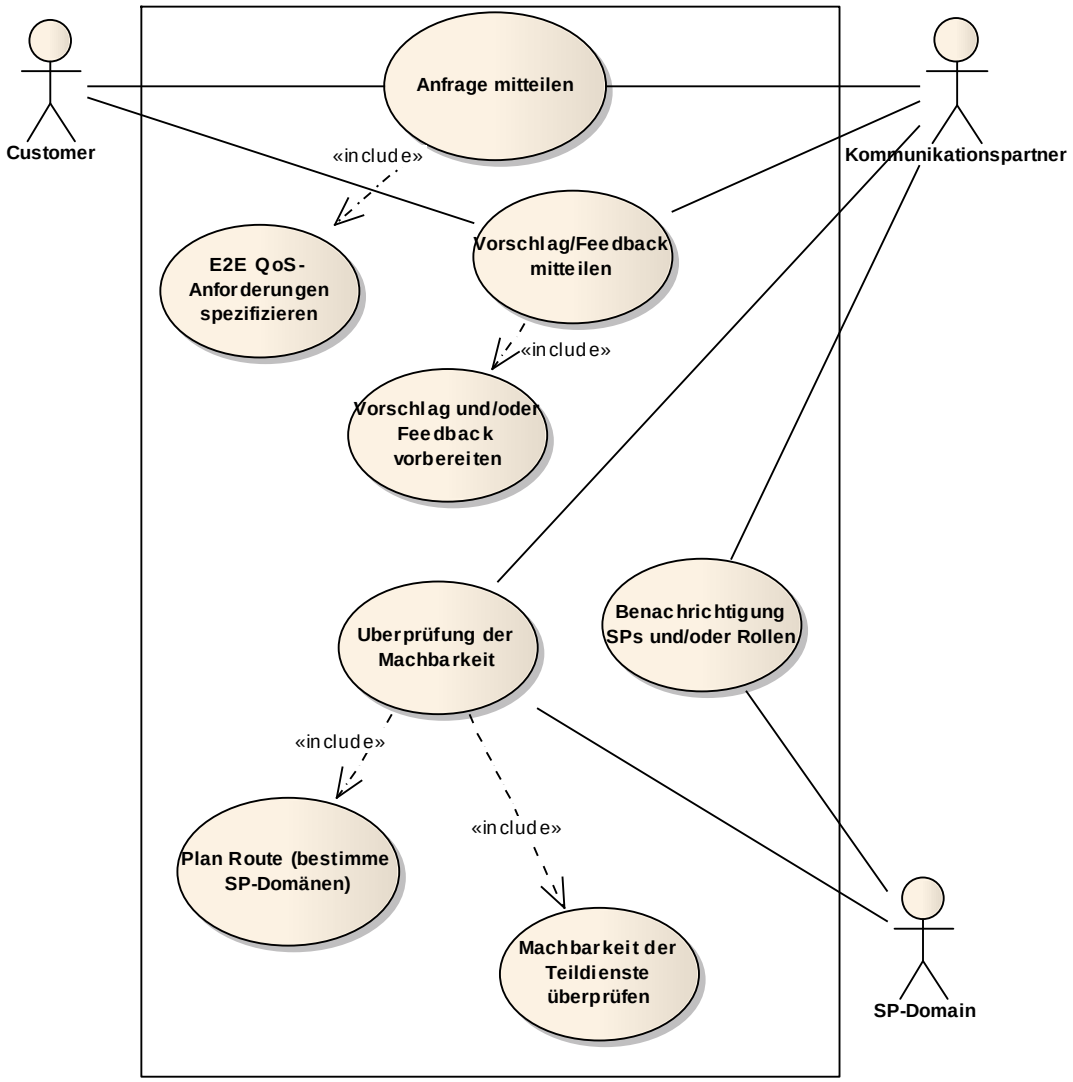


Abbildung 2.9.: Use Case: Verhandlung und Bestellung

5. Daraufhin entscheidet sich der Kunde, ob er die Verbindung mit den entsprechenden QoS-Parametern bestellen will oder nicht und teilt das dem Kommunikationspartner mit. In beiden Fällen benachrichtigt der Kommunikationspartner alle daran interessierten SPs und Rollen. Bei der Bestellung wird gleich danach der Inbetriebnahmeprozess gestartet.

Ablaufszenario: Sekundär I

Bezeichnung: Keine Route konnte gefunden werden, die E2E-QoS erfüllt

Ablauf:

1. Falls bei der Machbarkeitsstudie festgestellt wurde, dass die Kundenanforderungen nicht erfüllt werden können, wird ein entsprechendes Feedback vorbereitet. Das Feedback kann (je nach Umfang des Dienstes) außer der reinen Tatsache auch die Gründe für den Fehlschlag und/oder einen Alternativvorschlag beinhalten.

2. Das Feedback wird ähnlich wie in dem Primärfall von dem Kommunikationspartner an den Kunden gemeldet. Der Kunde kann dann entscheiden, ob er die Verhandlung weiter führt und dabei veränderte QoS-Anforderungen an die Dienstinstanz spezifiziert. In diesem Fall wird das primäre Ablaufszenario noch mal durchlaufen. Die Alternative wäre der Abbruch der Verhandlung.

Ablaufszenario: Primär II

Bezeichnung: Direkte Bestellung

Ablauf:

1. Im Falle, dass für den Dienst keine Verhandlung von vor Diensteinrichtung unterstützt wird, wird die Dienstinstanz unmittelbar bestellt; dabei werden wie im Primärfall I die E2E QoS-Anforderungen spezifiziert.

2. Daraufhin werden alle dafür zuständigen Rollen darüber benachrichtigt und die Inbetriebnahme der Dienstinstanz wird gestartet.

2.4.3.2. Inbetriebnahme

Die Inbetriebnahme wird gestartet, nachdem eine Dienstinstanz bestellt wurde. Das erwünschte Ergebnis ist der erfolgreiche Aufbau der Dienstinstanz, die im Anschluss vom Dienstnutzer verwendet werden kann. Die Zusammenhänge der Anwendungsfälle für die Inbetriebnahme einer Dienstinstanz sind in Abbildung 2.10 dargestellt.

Ablaufszenario: Primär

Bezeichnung: Inbetriebnahme verläuft erfolgreich und ohne Probleme

Ablauf:

1. Nachdem eine Verbindung bestellt wurde, beginnt die Inbetriebnahme. Diese beinhaltet zum einem das Routing, bei dem der Pfad bis ins letzte Detail definiert wird (inklusive Teildienste-QoS, Verbindungspunkte usw.), und zum anderen das Switching, bei dem die erforderlichen Teildienste in Betrieb genommen und zusammengeschaltet werden müssen.

2. Die Inbetriebnahme aller Teildienste wird von den SPs durchgeführt. Dabei sollen alle Teildienste den Festlegungen aus dem Routing entsprechen.

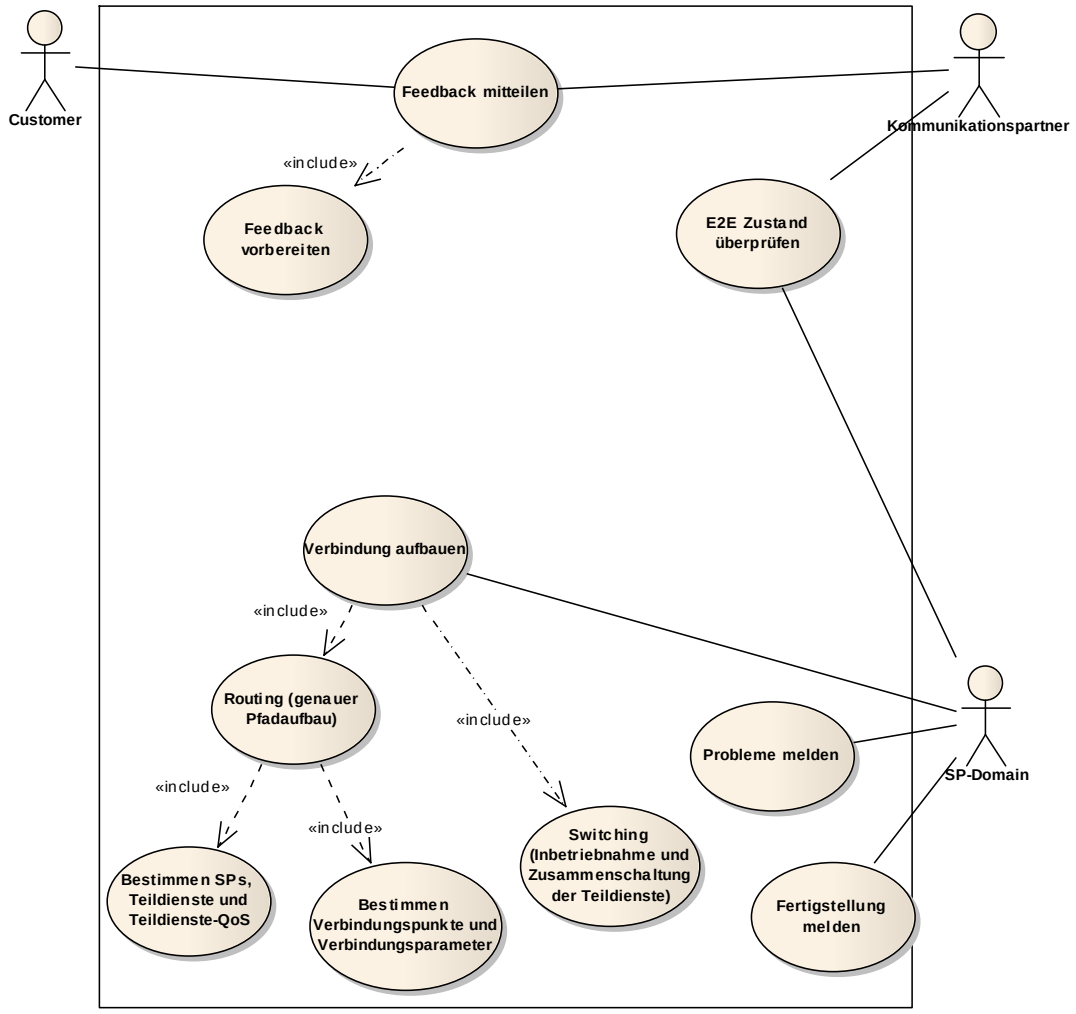


Abbildung 2.10.: Use Case: Inbetriebnahme

3. Nachdem die Teilstrecke der neuen Verbindung aufgebaut wurde und/oder zwei Teilstrecken zusammengeschaltet wurden, wird das von jedem SP gemeldet.

4. Diese Meldungen der SPs dienen der Überprüfung des E2E-Zustandes. Im Falle, dass alle Teildienste in Betrieb genommen und zusammen geschaltet werden konnten, wird ein entsprechendes Feedback vorbereitet, das von dem Kommunikationspartner an den Customer weitergereicht wird.

Ablaufszenario: Sekundär I

Bezeichnung: Probleme bei der Inbetriebnahme einzelner Teildienste können durch ein Re-Routing umgangen werden

Ablauf:

1. Wenn einzelne Teildienste nicht oder nicht entsprechend den Anforderungen in Betrieb genommen oder zusammengeschalten werden konnten, wird das von der SP-Domäne gemeldet.
2. Dieses Ereignis triggert ein erneutes Routing.
3. Falls der neue Pfad geschaltet werden konnte, wird das Feedback wie im primären Ablaufszenario generiert und an den Kunden weitergereicht. Ansonsten wird das Re-Routing abermals gestartet.

Ablaufszenario: Sekundär II

Bezeichnung: Probleme bei Inbetriebnahme einzelner Teildienste können durch das Re-Routing nicht umgangen werden

Ablauf:

1. Falls beim Routing kein geeigneter Pfad gefunden werden konnte, wird ein entsprechendes Feedback generiert.
2. Das Feedback wird analog zu dem Primärfall vom Kommunikationspartner an den Kunden ausgeliefert.

2.4.3.3. Monitoring und Reporting

Das Monitoring und Reporting sind einerseits Hilfsfunktionen, die im Betrieb bei der Dienstgüteeinhaltung verwendet werden, andererseits können sie als ein Teil der Managementfunktionalität angesehen werden, die dem Kunden und evtl. anderen Rollen angeboten werden kann. Die Zusammenhänge der Anwendungsfälle für das Monitoring und das Reporting der Dienstgüte einer Dienstinstanz sind in Abbildung 2.11 dargestellt.

Ablaufszenario: Primär I

Bezeichnung: E2E Monitoring seitens des Customers

Ablauf:

1. Bei der E2E Überwachung der Dienstgüte seitens des Customers besteht kein Bedarf, auf die Teildienste-Informationen zuzugreifen bzw. mit den Rollen und SP-Domänen zu kommunizieren, die die Dienstinstanz realisieren.

Ablaufszenario: Primär II

Bezeichnung: Das aggregierte E2E-Monitoring

Ablauf:

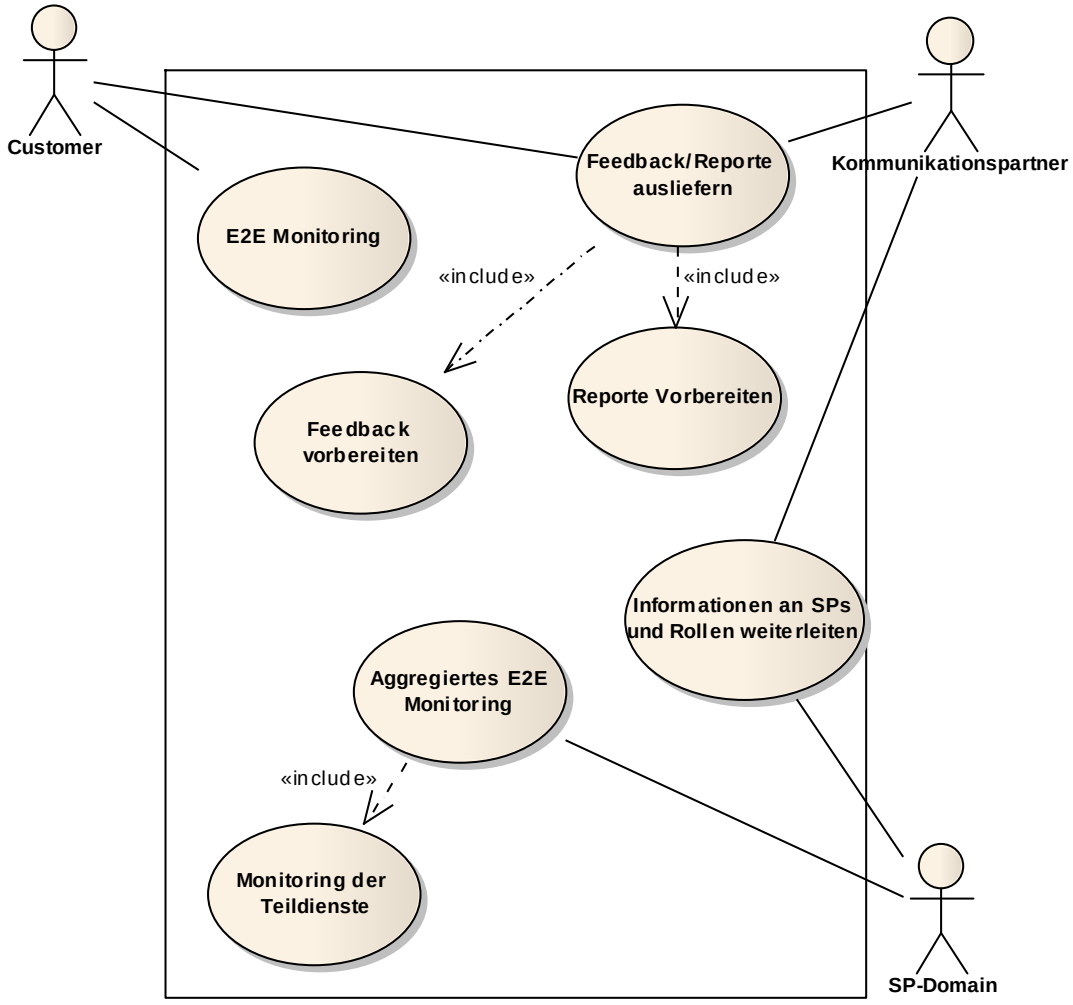


Abbildung 2.11.: Use Case: Monitoring und Reporting

1. Einzelne Teildienste werden von den Service Providern überwacht, die diese Teildienste erbringen.

2. Basierend auf der Dienstgüte der Teildienste wird ein aggregierter E2E-Zustand errechnet[2].

3. Die Monitoringinformationen werden für das Erstellen von Reports genutzt.

[2]Während der Vorbereitung eines Dienstangebotes werden die relevanten Aggregationsvorschriften und die dafür zuständige Rolle(n) entweder für alle Dienstinstanzen festgelegt, oder es werden Vorschriften für deren Bestimmung festgelegt. Im zweiten Fall beziehen sich die Aggregationsvorschriften, die Besetzung der Rollen durch die Akteure jeweils auf eine Dienstinstanz. Diese werden während der Verhandlungs- und Inbetriebnahme-Phasen in den jeweiligen Use Cases als Teil der Planung bestimmt. Die Klärung der Frage, welche der Varianten für die Verkettete Dienste sinnvoll wäre bzw. wer und wann diese Funktionalität festlegt, gehört zum konstruktiven Teil dieser Arbeit.

4. Beide Monitoring- und Reportingkomponenten stoßen die Erstellung eines Feedbacks an.
5. Das Feedback an den Customer wird von seinem Kommunikationspartner ausgeliefert.
6. Parallel dazu werden die Monitoring- und die Reportingdaten an die bei der Diensterbringung beteiligten SP-Domänen und weitere involvierte Rollen ausgeliefert.

2.4.3.4. Anpassung von E2E-QoS im Betrieb

Für den Fall, dass die für eine Dienstinstanz zugesicherte E2E Dienstgüte dem Dienstnutzer nicht mehr ausreicht oder umgekehrt reduziert werden kann, wird dem Kunden die Möglichkeit eingeräumt, die QoS-Anforderungen im Betrieb anzupassen. Bei dem Dienst E2E Links (dem einzigen Dienst aus den vorgestellten Szenarios, der diese Funktionalität anbietet) wird das durch das Abbestellen des alten und Bestellen eines neuen E2E Links realisiert. Dabei kann es durchaus sein, dass einzelne der bereits in Betrieb genommenen Teildienste für die Verbindung mit veränderter Qualität wiederverwendt werden können. Aus diesem Grund wird an dieser Stelle eine Mischung aus den Use Cases vorgeschlagen, die in den Originalszenarios bei Inbetriebnahme und Dienstauflösung vorkommen. Die Zusammenhänge der Anwendungsfälle für diese Managementaufgabe sind in Abbildung 2.12 dargestellt.

Ablaufszenario: Primär

Bezeichnung: QoS-Anpassung bei vorhandenen Teildiensten

Ablauf:

1. Der Customer teilt seinem Kommunikationspartner die veränderte QoS-Anforderungen an die bereits bestehende Dienstinstanz mit.
2. Daraufhin wird überprüft, ob der Kunde (entsprechend den Vertragsbedingungen) berechtigt ist, solche Anfrage zu stellen.
3. Bei vorhandener Berechtigung wird die Route durch die SP-Domäne samt der Teildienste-QoS neu berechnet.
4. Falls alle Teildienste wie vorher bleiben und ausschließlich ihre QoS-Werte angepasst werden müssen, übernehmen die betroffenen SP-Domänen diese Aufgabe.
5. Nach der Anpassung der Teildienste, die von jeder SP-Domäne gemeldet wird, wird ein Feedback für den Customer vorbereitet.
6. Das Feedback wird ähnlich wie in anderen Fällen an den Kunden über seinen Kommunikationspartner ausgeliefert.

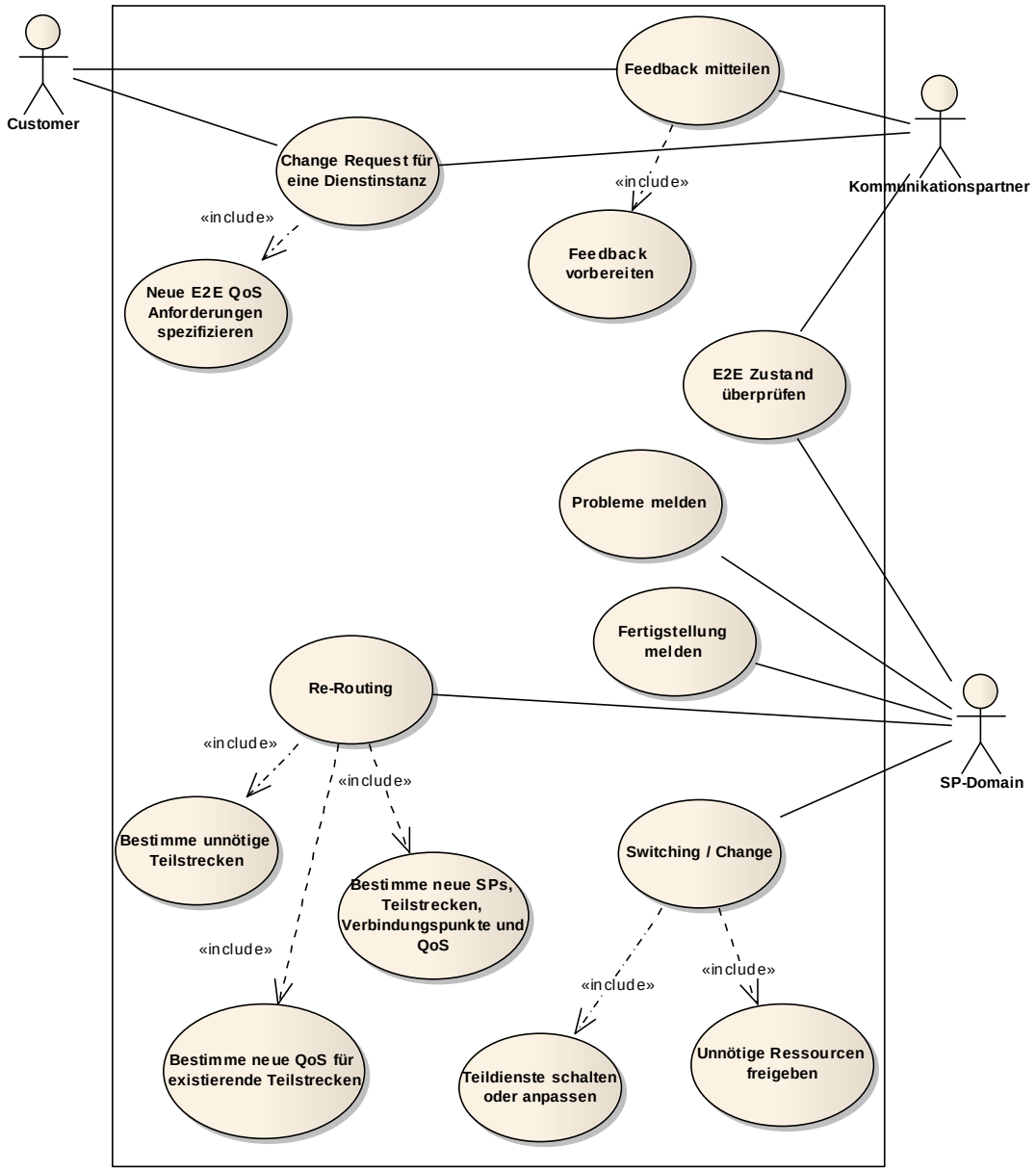


Abbildung 2.12.: Use Case: Anpassung von E2E-QoS im Betrieb

Ablaufszenario: Sekundär I

Bezeichnung: QoS-Anpassung erfordert andere Teildienste

Ablauf:

1. Falls beim Re-Routing festgestellt wurde, dass (teilweise) andere Teildienste bei der Diensterbringung der E2E-Verbindung eingesetzt werden müssen, wird den SP-Domänen der nicht mehr benötigten Teildienste mitgeteilt, dass die verwendeten Ressourcen freigegeben werden dürfen (siehe dazu auch Abbestellung im Abschnitt 2.4.3.5), und den SPs der neuen Teildienste werden der Bedarf und die QoS-Anforderungen mitgeteilt (siehe Inbetriebnahme im Abschnitt 2.4.3.2).
2. Die Teildienste, die "wiederverwendet" werden können, werden bei Bedarf von ihren Providern entsprechend neuer QoS-Anforderungen angepasst.
3. Nachdem alle Teildienste in Betrieb genommen und zusammen geschaltet wurden, wird ein entsprechendes Feedback generiert und an den Kunden ausgeliefert (identisch wie beim Primärfall).

Ablaufszenario: Sekundär II

Bezeichnung: Probleme bei der Anpassung

Ablauf:

1. Falls bei der Anpassung einzelner Teildienste Probleme auftreten, werden sie von den SPs gemeldet. Bei Bedarf kann das Re-Routing unter Berücksichtigung der veränderten Lage neu gestartet werden.
2. Falls keine geeignete Route gefunden und geschaltet werden konnte, die den neuen QoS-Anforderungen, wird ein entsprechendes Feedback generiert und ähnlich wie in dem Primärfall an den Kunden ausgeliefert.

2.4.3.5. Abbestellung

Falls eine Dienstinstanz nicht mehr benötigt wird, besteht bei einigen Diensten die Möglichkeit, die Dienstinstanz explizit abzubestellen. Die Zusammenhänge der Anwendungsfälle für diese Managementaufgabe sind in Abbildung 2.13 dargestellt.

Ablaufszenario: Primär I

Bezeichnung: Abbestellung durch Customer

Ablauf:

1. Der Customer teilt seine Entscheidung, die Dienstinstanz abzubestellen, dem Kommunikationspartner mit.

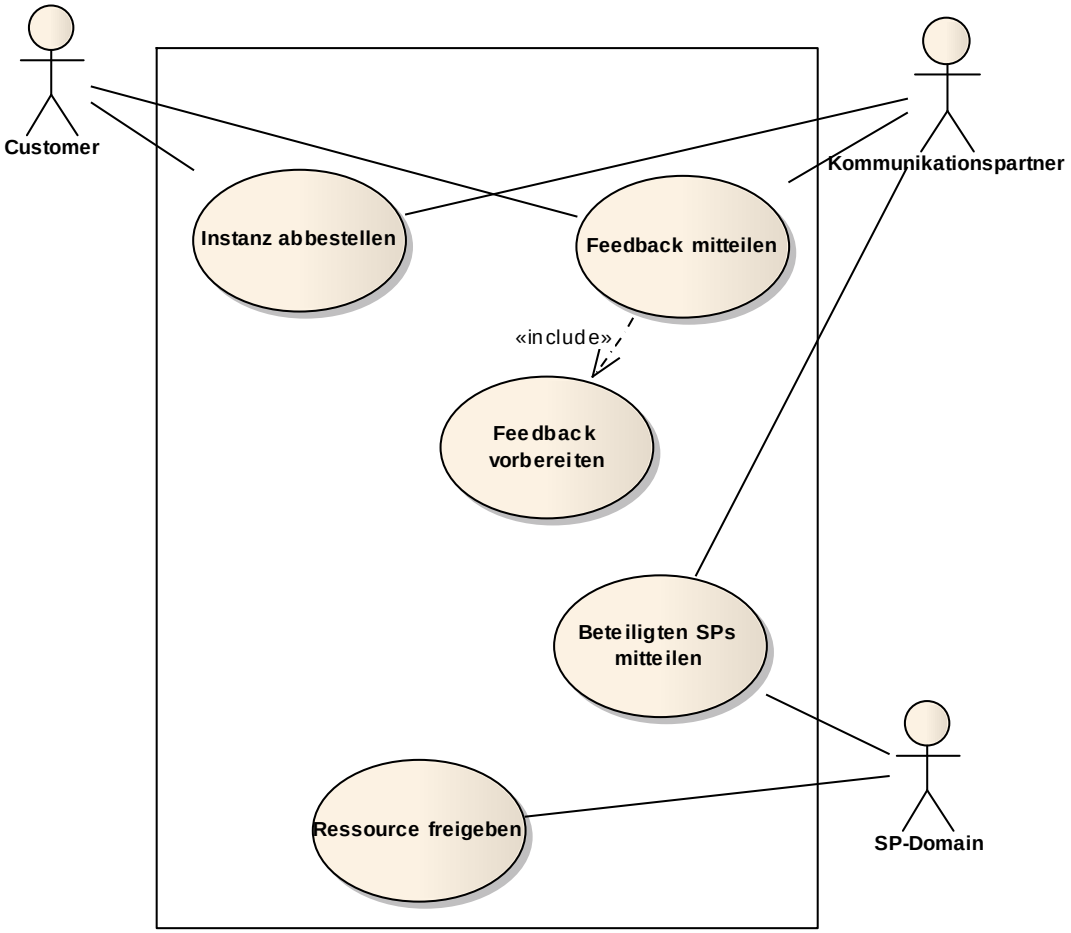


Abbildung 2.13.: Use Case: Dienstauflösung

2. Daraufhin wird überprüft, ob das für diese Dienstinstanz zulässig ist.

3. Falls die Berechtigung gegeben ist, werden alle in die Diensterbringung involvierten SP-Domänen darüber informiert. Sie können dann die verwendeten Ressourcen freigeben.

4. Gleichzeitig wird Feedback generiert, das an den Kunden von seinem Kommunikationspartner weitergereicht wird.

Ablaufszenario: Sekundär

Bezeichnung: Abbestellung durch Customer ist während der Vertragslaufzeit nicht erlaubt

Ablauf:

1. Falls die Abbestellung durch den Customer nicht erlaubt ist, wird ein entsprechendes Feedback generiert und wie beim Primärfall an den Kunden weitergereicht.

Ablaufszenario: Primär II

Bezeichnung: Dienstauflösung initiiert von Service Provider

Ablauf:

1. Falls die vereinbarte Dienstnutzungszeit abläuft oder eine der SP-Domänen (z.B. wegen einem Fehler) nicht mehr in der Lage ist, ihren Teildienst zu erbringen, wird die Dienstauflösung von SP initiiert.
2. Darauf werden alle weiteren beteiligten SPs darüber informiert, sodass sie die verwendeten Ressourcen freigeben können.
3. Gleichzeitig wird ein entsprechendes Feedback generiert, das an den Kunden ausgeliefert wird.

2.4.3.6. Vollständigkeit der Anwendungsfälle

Die anhand des morphologischen Kastens erkannten und in diesem Abschnitt beschriebenen Use Cases umfassen Verhandlung und Bestellung (Seite 60), Inbetriebnahme (Seite 62), Monitoring und Reporting (Seite 64), Anpassung von E2E-QoS im Betrieb (Seite 66) und Abbestellung (Seite 68) einer Dienstinstanz. Da in den vorgestellten Szenarios jeweils eine Untermenge der beschriebenen Anwendungsfälle unterstützt wird, stellt sich die Frage, ob die erarbeitete Liste vollständig und für alle möglichen Dienstausprägungen ausreichend ist.

Die erkannten Use Cases decken sich mit den SLM-Aufgaben überein, die von den Rahmenwerken ITIL und NGOSS für die Dienstgütezusicherung vorgeschlagen werden (siehe dazu auch Abschnitt 3.4). Deswegen kann davon ausgegangen werden, dass die Liste im Sinne dieser Arbeit vollständig ist.

Sollte durch die technische Entwicklung der Bedarf an neuen Use Cases entstehen, können sie auch zum späteren Zeitpunkt analog zu den bereits erfassten in die Anforderungsanalyse miteinbezogen werden, was wiederum evtl. eine Anpassung der erarbeiteten Lösung erfordern kann.

2.5. Anforderungsanalyse

Dieses Kapitel befasst sich mit der Ableitung der Anforderungen an die zu entwickelnde Lösung. Zunächst werden die allgemeinen Anforderungen an die QoS-Parameter und die SLM-Prozesse direkt aus der Morphologie der Szenarien abgeleitet. Weitere Anforderungen werden beim "Durchspielen" der Anwendungsfälle an dem generischen Szenario erkannt und erfasst. Die Analyse der Aspekte, die bei Verketteten Diensten die nichtfunktionale Anforderungen wie Skalierbarkeit und Robustheit beeinflussen, schließt die Anforderungsanalyse.

Alle Anforderungen werden für die bessere Referenzierbarkeit durchnummeriert. Die Nummer bestehen aus einem Präfix für den Typ der Anforderung und einer laufenden Nummer. Die funktionalen Anforderungen werden mit dem Präfix "FA-" und die nichtfunktionalen mit "NFA-" versehen. Bezeichner aller bei der Anforderungsanalyse getroffenen Annahmen werden weiterhin mit dem Präfix "AN-" gekennzeichnet.

2.5.1. Anforderungen an QoS und SLM

Wie man im morphologischen Kasten erkennen kann, werden in den betrachteten Szenarios unterschiedliche QoS-Parameter unterstützt (siehe dazu Tabelle 2.3). Das bezieht sich sowohl auf die QoS-Parameter selbst als auch auf deren dienstspezifischen Kombinationen. Eine Forderung nach einer Obermenge aller aus allen in den betrachteten Szenarios unterstützten QoS-Parametern würde die Frage nach der Vollständigkeit dieser Menge aufwerfen. Deswegen wird hier stattdessen eine generische Lösung gefordert:

Funktionale Anforderung FA-01 - Unterstützung beliebiger QoS-Parameter

Um beliebige QoS-Parameter zu unterstützen, wird eine generische Beschreibung der QoS-Parameter benötigt. Diese Beschreibung soll mindestens alle erfassten Kategorien beschreiben können. Die zu entwickelnde Lösung soll auf dieser Beschreibungsart operieren.

Eine ähnliche Überlegung gilt der Managementfunktionalität sowie deren Parametern (siehe dazu auch Tabellen 2.3 und 2.4). Die erfassten Ausprägungen zeigen deutlich, dass es zwischen unterschiedlichen Diensten große Unterschiede in Bezug auf die unterstützte Managementfunktionalität geben kann. Um der Gefahr der Unvollständigkeit bei einer expliziten Aufzählung entgegenzusteuern, wird auch für Managementfunktionalität eine ähnliche Anforderung benötigt:

Funktionale Anforderung FA-02 - Unterstützung beliebiger Managementfunktionalität

Um beliebige Managementfunktionalität sowie deren Parameter unterstützen zu können, wird eine generische Beschreibung der beiden benötigt. Die Beziehung zwischen der Managementfunktionalität und den zugehörigen Parametern soll dabei sichergestellt werden. Die Beschreibung soll mindestens alle in den Szenarios vorgekommenen Ausprägungen beschreiben können. Die zu entwickelnde Lösung soll auf dieser Beschreibungsart operieren.

Der Customer hat generell kein Interesse an allen möglichen QoS-Parametern, sondern stellt die Anforderungen ausschließlich an die für ihn relevanten QoS-Parameter. Dabei können sich diese QoS-Parameter sowohl auf die Dienstgüteeigenschaften und deren Grenzwerte als auch auf die Managementfunktionalität und deren Parameter beziehen. Weiterhin kann der Kunde i.A. an gleichzeitig mehreren Eigenschaften (d.h. QoS-Parametern und Managementfunktionalität) für seine Dienstinstanz interessiert sein (siehe Kapitel 2.4.2 bzw. die dieser Aussage zugrunde liegende Morphologie-Tabelle 2.3). Um dieses Kundenverhalten zu unterstützen, soll folgende Anforderung erfüllt werden

Funktionale Anforderung FA-03 - Gleichzeitige Unterstützung mehrerer Eigenschaften

Die Lösung soll in der Lage sein, gleichzeitig mit mehreren Eigenschaften (QoS-Parameter, Managementfunktionalität und Parametern der Managementfunktionalität) sowie mit beliebigen Kombinationen aus unterstützten Diensteigenschaften operieren zu können.

Die aufgestellten Anforderungen basieren auf einer in allen Szenarios angetroffenen und für diese Arbeit übernommenen Annahme, dass die Semantik der QoS-Parameter in allen SP-Domänen gleich ist (siehe AN-QoSSemantik). Dies entspricht auch den üblichen Bestrebungen nach Standardisierung, die die Interoperabilität zwischen Service Providern ermöglichen soll.

Da die SP-Domänen unabhängige Organisationen sind, ist die Unterstützung von QoS-Parametern und Managementfunktionalität für eigene Dienste individuell für jede SP-Domäne. Außerdem ist jede Domäne in der Lage, die Unterstützung von QoS-Parametern jederzeit ohne Absprache mit den anderen Domänen zu ändern. Diese Situation kann auch bei einem stark standardisierten Dienst wie Telefonie beobachtet werden. Aus diesem Grund wird folgende nichtfunktionale Anforderung aufgestellt:

Nichtfunktionale Anforderung NFA-01 - Autonomie der Service Provider in der Unterstützung von Diensteigenschaften

Die Lösung soll in der Lage sein, mit der individuellen Unterstützung von Diensteigenschaften durch die SP-Domänen zurechtzukommen. Dabei sollen auch Veränderungen in der Unterstützung berücksichtigt werden.

Am Beispiel von Géant2 E2E Links wurde gezeigt, dass es Dienste geben kann, die noch ohne eine vorhandene Infrastruktur angeboten werden. Die Dienstinstanzen solcher Dienste können nicht automatisch geschaltet werden. Allerdings können auch sie teilweise automatisiert werden, z.B. bei der Planung einer neuen Dienstinstanz. Um dies zu ermöglichen, soll folgende Anforderung erfüllt werden:

Nichtfunktionale Anforderung NFA-02 - Unterstützung potentiell möglicher Teildienste

Die Lösung soll in der Lage sein, auch potentiell mögliche (Teil-)Dienste und deren Eigenschaften zu unterstützen. Es muss auch möglich sein, zwischen existierenden und potentiell möglichen Teildiensten zu unterscheiden und zu wählen, welche davon bei allen Operationen berücksichtigt werden dürfen.

Da in der IT-Industrie die angebotenen Dienste ständig weiterentwickelt und erweitert werden, kann man davon ausgehen, dass alle bereits erfassten QoS- und SLM-Aspekte bereits nach einer relativ kurzen Zeitspanne geändert werden müssen. Aus diesem Grund muss folgende Anforderung erfüllt werden:

Nichtfunktionale Anforderung NFA-03 - Erweiterbarkeit in Bezug auf unterstützte Diensteigenschaften

Die zu entwickelnde Lösung soll in Bezug auf die unterstützten QoS-Parameter und Managementfunktionalitäten möglichst leicht erweiterbar sein.

Eine generelle und allgemeingültige Definition von SLM-Prozessen ist wegen ihrer Komplexität und Vielfältigkeit kaum möglich. Außerdem ist die Menge der etablierten SLM-Prozesse – im Gegensatz zu den unterstützten QoS-Parametern und Managementfunktionalitäten – leicht aufzählbar. Um eine größtmögliche Abdeckung zu erreichen soll folgende Anforderung erfüllt werden:

Funktionale Anforderung FA-04 - Unterstützung aller Use Cases

Die zu entwickelnde Lösung soll alle etablierten SLM-Prozesse unterstützen. Dadurch sollen mindestens alle in Abschnitt 2.4.3 identifizierten *Use Cases* realisierbar sein.

2.5.2. Anforderungen abgeleitet von Use Cases

Nachdem der Kunde seine E2E-Anforderungen (siehe Kapitel 2.5.1) über die CSM-Schnittstelle (siehe AN-CSMExistiert auf Seite 57) an seine Dienstinstanz spezifiziert hat, beginnt die Durchführung von Multi-Domain Managementprozeduren. Diese Prozeduren wurden in Kapitel 2.4.3 in Form von UML Use Case Diagrammen erfasst. In diesem Abschnitt werden die identifizierten Use Cases auf dem generischen Szenario (siehe Kapitel 2.4.2) durchgespielt (siehe Abbildung 2.14). Dabei werden die funktionalen und nichtfunktionalen Anforderungen identifiziert, die für einen reibungslosen Ablauf der jeweiligen Prozesse notwendig sind.

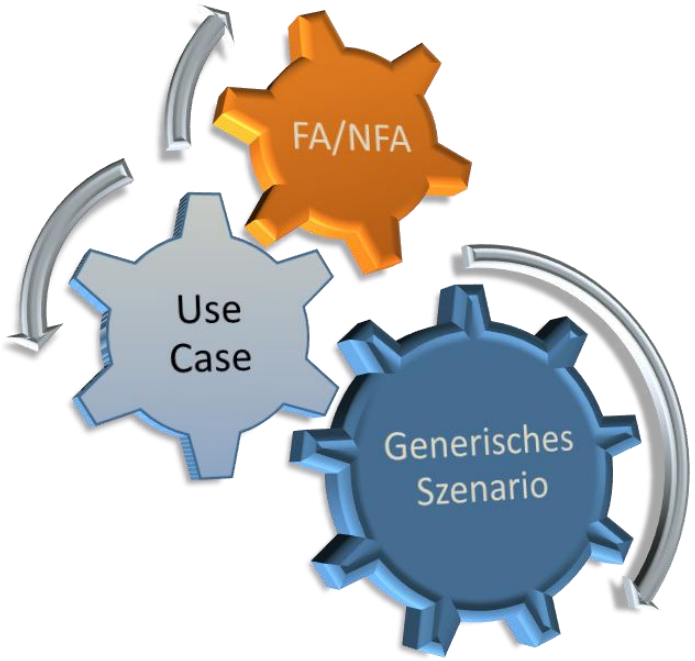


Abbildung 2.14.: Ableitung der Anforderungen von Use Cases

2.5.2.1. Verhandlung und Bestellung

Bei der Verhandlung (siehe Abbildung 2.9) wird durch die Kundenanfrage zunächst eine Machbarkeitsstudie ausgelöst. Ein Teil dieser Überprüfung besteht in der Definition des Pfades über mehrere SP-Domänen. Die zuvor definierte Anforderung FA-03 bedeutet in diesem Kontext zunächst, dass das Suchverfahren, der zur Pfadsuche eingesetzt wird, gleichzeitig mehrere Dienstgüteeigenschaften berücksichtigen soll. Weiterhin sollen zur Erfüllung dieser Anforderung auch die Informationen über alle realisierbaren Teildienste die Angaben über deren relevanten Eigenschaften beinhalten.

Die Informationen über alle möglichen Teildienste können ausschließlich von den SP-Domänen kommen, die diese Teildienste erbringen können. Da alle SPs unabhängige Organisationen sind, muss die Lösung folgende Anforderung erfüllen:

Nichtfunktionale Anforderung NFA-04 - Zugriffseinschränkung auf die Domain-Informationen

Bei Informationsabfragen darf kein direkter Zugriff auf die Infrastruktur der fremden SP-Domänen erfolgen. Jede SP-Domäne soll weiterhin in der Lage sein, die Informationsmenge nach eigenem Ermessen einzuschränken.

In Tabelle 2.3 wurde auch aufgezeigt, dass die Zeit, bis ein Feedback den Kunden erreicht, sehr stark zwischen den angebotenen Diensten variieren und im Falle von E2E Links nicht immer vorhersehbar lang sein kann. Die Dauer zwischen einer Anfrage und dem korrespondierenden Feedback entspricht der Prozessdurchlaufzeit. Um die Zeit bis zum Feedback an den Kunden begrenzen zu können, muss also folgende Bedingung erfüllt werden:

Nichtfunktionale Anforderung NFA-05 - Begrenzung der Prozessdurchlaufzeit

Die Dauer einzelner Aktionen sowie die komplette Prozessdurchlaufzeit sollen zeitlich begrenzbar sein.

2.5.2.2. Inbetriebnahme

Eine wichtige Voraussetzung für die Inbetriebnahme (siehe Abbildung 2.10) ist die Bestimmung aller SP-Domänen, die sich bei der Diensterbringung einer neuen Dienstinstanz beteiligen sollen, sowie der Teildienste, die diese SPs für die neue Dienstinstanz erbringen. Damit die Kundenanforderungen an die E2E-Dienstgüte erfüllt werden können, ist folgende Anforderung notwendig:

Nichtfunktionale Anforderung NFA-06 - Dekomposition der QoS-Parameter

Bei der Bestimmung der Teildienste muss es möglich sein, die E2E-Dienstgüteanforderungen an die Anforderungen der einzelnen Teildienste (d.h. Grenzwerte für einzelne QoS-Parameter) abzubilden.

Dies ist analog auf die erforderliche Managementfunktionalität anwendbar. Um domänenübergreifende Managementaufgaben für die Dienstinstanzen definieren zu können, muss folgende Anforderung erfüllt werden:

Nichtfunktionale Anforderung NFA-07 - Dekomposition der Managementfunktionalität

Bei der Bestimmung der Teildienste muss es möglich sein, deren erforderliche Managementfunktionalität sowie deren Funktionalitätsparameter zu bestimmen. Weiterhin muss es möglich sein, die Kommunikationswege zwischen einzelnen SP-Domänen für unterschiedliche Managementaufgaben zu definieren.

Nach der Bestimmung der erforderlichen Teildienste-QoS müssen die Teildienste in Betrieb genommen und zusammengeschaltet werden. Diese Aufgaben werden von den unterschiedlichen SPs jeweils für ihre Teildienste übernommen. Da aber zwischen Service Providern Heterarchie herrscht, darf es keine Rolle geben, die den SPs Anweisungen gibt. Somit darf die Teilnahme eines Service Provider bei der Erbringung einer Dienstinstanz ausschließlich auf freiwilliger Basis erfolgen. Das führt zu der folgenden Anforderung an die zu entwickelnde Lösung:

Nichtfunktionale Anforderung NFA-08 - Zustimmung der involvierten SPs

Die Beteiligung aller SP-Domänen an der Diensterbringung soll auf einer freiwilligen Basis passieren. Sollte die Lösung dedizierte Rolle(n) benötigen, die den Pfadverlauf bestimmen, dann soll dabei stets das SP-Einverständnis eingeholt werden, sich an der Diensterbringung zu beteiligen. Eine SP-Domäne darf jede Anfrage für die Dienstbeteiligung zurückweisen. Den SP-Domänen sollen für die Entscheidungsfindung (über ihre Beteiligung in der Diensterbringung) sowie für die Dienstinbetriebnahme alle dafür notwendigen Informationen (wie z.B. Zeitrahmen und die erforderlichen Teildienst-QoS) zur Verfügung gestellt werden.

Die Zusagen haben einen wichtigen Aspekt, der hier explizit angesprochen werden muss. Bei hierarchisch aufgebauten Diensten wird die Verbindlichkeit der Zusagen durch die Verträge (SLAs) festgehalten. Bei den betrachteten Szenarios wurde ausschließlich bei GLIF (siehe Tabelle 2.4) eine gewisse Form von Verbindlichkeit realisiert. Da diese Arbeit sich ausschließlich mit technischen Aspekten befasst, wird im Weiteren die Erfüllung folgender Annahme vorausgesetzt:

AN-Verbindlichkeit Alle Zusagen, die SPs und/oder andere Rollen machen, sind für diese verbindlich.

2.5.2.3. Monitoring und Reporting

Das in Abbildung 2.11 dargestellte Monitoring- und Reporting-Konzept sieht die Möglichkeit für eine Dienstgüteüberwachung sowohl durch den Customer als auch durch die beteiligten Service Provider vor. Aus der Providerperspektive ist das Monitoring

kein Selbstzweck. Wie man der Morphologie-Tabelle 2.4 entnehmen kann, müssen dadurch Situationen erkannt werden, die zu einer Verletzung der Vereinbarungen führen können. Aus technischer Sicht kann das als folgende Anforderung aufgefasst werden:

Nichtfunktionale Anforderung NFA-09 - Erkennung (drohender) E2E-Dienstgüteverletzungen

Die zu entwickelnde Lösung muss in der Lage sein, Verletzungen der E2E-Zusicherungen gegenüber dem Kunden zu erkennen, möglichst bereits im Vorfeld.

An dieser Stelle wird vorausgesetzt, dass die Planung einer E2E-Verbindung und vor allem die Abbildung der E2E-Anforderungen auf die Teildienste (siehe Anforderung [NFA-DekompositionQoS]) korrekt war. Unter dieser Voraussetzung kann die Verletzung der E2E-Anforderungen erst dann auftreten, wenn eine oder mehrere beteiligten SP-Domänen die für ihre Teildienste bestimmten Grenzwerte nicht einhalten. Zur Vereinfachung der Fehlerbehebung wird folgende Anforderung aufgestellt:

Nichtfunktionale Anforderung NFA-10 - Erkennung eines Verursacher-SP

Die zu entwickelnde Lösung muss in der Lage sein, die Verletzungen der Zusicherungen für alle Teildienste einer Dienstinstanz möglichst bereits im Vorfeld zu erkennen. Dabei sollen die SP-Domäne(n) identifizierbar sein, die Zusicherungen nicht einhalten.

Da es keinen direkten Zugriff auf die SP-Infrastruktur von außen geben darf (siehe dazu auch die Anforderung NFA-04), muss bei der Überwachung der Teilstrecken auf den Informationen aufgebaut werden, die von den jeweiligen SP-Domänen zur Verfügung gestellt werden. Aufgrund der fehlenden Möglichkeit, diese Informationen zu überprüfen, müssen deren Realitätstreue und Aktualität vorausgesetzt werden:

AN-WahreSPInfo Alle Informationen, die von den SP-Domänen nach außen zur Verfügung gestellt werden, sind aktuell und realitätstreu.

2.5.2.4. Anpassung von E2E-QoS im Betrieb

Für die Anpassung der Eigenschaften einer Dienstinstanz während der Betriebsphase (siehe Abbildung 2.12) kann es mehrere Gründe geben. Vor allem sind dabei veränderte Kundenanforderungen an die Dienstinstanz denkbar. Der Bedarf kann allerdings auch durch die Provider entstehen. So ist es denkbar, dass eine SP-Domäne häufig ihre zugesicherten Grenzwerte verletzt. Da bei einer Dienstinstanz die E2E-Dienstgüte im

Vordergrund steht, kann so eine Situation ggf. durch eine "Umverteilung" der erforderlichen Grenzwerte auf alle beteiligten SP-Domäne zunächst ohne, und wenn es nicht geht, dann mit einem Re-Routing gelöst werden. Weiterhin kann auch die Veränderung der Kommunikationswege bzw. der verantwortlichen Rollen zwischen den beteiligten SP-Domänen und involvierten Rollen, wie z.B. für ein E2E-Monitoring, notwendig sein. Der Grund dafür kann ein *Load Balancing* bzw. ein Ausfall der Überwachungsinstanz sein.

Um alle diese Fälle verfeinert (und nicht einfach pauschal) zu behandeln, wird folgende Anforderung spezifiziert:

Funktionale Anforderung FA-05 - Ziele der Anpassung im Betrieb

Während der Betriebsphase sollen folgende Anpassungen einer Dienstinstanz möglich sein:

- Erforderliche Diensteigenschaften und deren Grenzwerte bei den Teildiensten verändern (ohne Re-Routing)
- Erforderliche Managementfunktionalität (samt der zugehörigen Parameter) einzelner Teildienste verändern (ohne Re-Routing)
- Kommunikationswege bzw. -Verknüpfungen zwischen der Managementfunktionalität der Teildienste und der Multi-Domain Managementprozessen ändern
- Veränderung der Route

2.5.2.5. Abbestellung

Bei Abbestellung bzw. Abbau einer Dienstinstanz (siehe Abbildung 2.13) ist hervorzuheben, dass das nicht nur durch den Customer, sondern auch durch eine der SP-Domänen bzw. eine Rolle initiiert werden kann. Für die verfeinerte Unterscheidung zwischen diesen Fällen werden sie in einer eigenen Anforderung zusammengefasst:

Funktionale Anforderung FA-06 - Initiator der Abbestellung

Die zu entwickelnde Lösung soll unterschiedliche Quellen der Abbestellung einer Dienstinstanz unterstützen. Dazu gehören vor allem:

- Der Kunde dieser Dienstinstanz
- Die Bei der Diensterbringung beteiligten SP-Domänen

2.5.3. Allgemeine NFAs

Jede technische Lösung, unabhängig davon, wofür sie konzipiert wurde, ist immer mit einer Reihe von allgemeinen Anforderungen konfrontiert. Zwei davon, die in diesem Kapitel als erstes besprochen werden, sind die Anforderungen an Skalierbarkeit und die Anforderung an Robustheit. Dabei hängen diese beiden sehr stark sowohl von Nutzungsaspekten als auch vom Aufbau des Dienstes ab.

In Bezug auf Skalierbarkeit liefert der Telefondienst ein hervorragendes Beispiel mit vielen Teilaspekten. So sind bei der Erbringung dieses Dienstes tausende Service Provider aus unterschiedlichen Ländern beteiligt. Die Anzahl der Provider kann variieren, ohne dass jemand außer den direkten Nachbardomänen davon betroffen ist. Trotz der schlecht abschätzbaren Anzahl der Domänen, die sich bei dem Dienstangebot beteiligen, können zwischen Kunden dieser SPs Telefonverbindungen aufgebaut werden. Weiterhin können beim Telefondienst mehrere Kunden aus mehreren SP-Domänen gleichzeitig unterschiedliche Verbindungsanfragen stellen. Auch wenn diese Verbindungen über mehrere Domänen hinweg aufgebaut werden müssen, können diese Anfragen erfolgreich bearbeitet werden. Nachdem Verbindungen aufgebaut wurden, können sie erfolgreich betrieben werden. Das bezieht sich auch auf die kontinuierliche Überwachung der Aufrechterhaltung der Verbindung.

Am Beispiel von Géant2 E2E Links kann man einen weiteren Skalierungsaspekt illustrieren: Falls das Zeitfenster für eine Wartungsarbeit sehr eng gelegt ist, wie es z.B. bei E2E Links für das LHC Projekt der Fall ist, so müssen alle bei der Erbringung des Links beteiligten Domänen ihre Aktivitäten abstimmen und die Wartungsarbeit gleichzeitig durchführen. Bei einem E2E Link von der Schweiz nach Frankreich ist es kein großer Aufwand, Aktivitäten der zwei Domänen zu koordinieren; bei einem E2E Link nach USA müssen die Aktivitäten von mindestens 3-4 beteiligten Domänen koordiniert und dazu noch die Zeitdifferenz überwunden werden.

Somit kann die Anforderung an die Skalierbarkeit der zu entwickelnde Lösung für diese Arbeit wie folgt definiert werden:

Nichtfunktionale Anforderung NFA-11 - Skalierbarkeit

Die zu entwickelnde Lösung soll skalierbar in Bezug auf folgende Aspekte sein:

- Anzahl der Domänen, mit direkter Kundenanbindung
- Anzahl gleichzeitiger Verbindungsanfragen
- Anzahl gleichzeitig bestehender Verbindungen
- Anzahl der Domänen, die bei der Realisierung einer Verbindung beteiligt sind

Bei der Erbringung eines Dienstes sind mehrere Komponenten und – im Falle von Verketteten Diensten – i.A. auch mehrere Domänen beteiligt. Ein wünschenswertes

Kriterium ist es, beim Ausfall einzelner Komponenten den Dienst weiterhin erbringen zu können.

Auch wenn es bei unterschiedlichen Szenarien in verschiedenen Phasen des Dienstlebenszyklus vorkommt, müssen für jede Verbindung Routing und Switching durchgeführt werden. Beim Telefondienst und DiffServ geschehen Routing und Switching nacheinander bei jeder Domäne in der Kette. Das erlaubt auch Probleme beim Routing durch die Wahl eines alternativen Weges zu umgehen. Bei DCN und E2E Links kann zwischen Routing und Switching eine längere Periode liegen. Dadurch kann es auch möglich sein, dass der vorher gefundene Multi-Domain Pfad wegen in der Zwischenzeit aufgetretener Probleme nicht mehr geschaltet werden kann. Diese Situation erfordert, dass auch während des Switching die Suche nach einer alternativen Route möglich sein muss.

Alle erforderlichen Aktionen, wie z.B. Routing, Switching und Monitoring, werden von den funktionalen Komponenten ausgeführt. Ein Ausfall des Interdomain Manager (IDM) bei AutoBAHN in DCN oder des zentralen Wissens-Repository bei GLIF würde zur Beeinträchtigung des gesamten Dienstes führen und alle beteiligten Domäne betreffen.

Eine Multi-Domain Architektur ist immer auf die funktionalen Komponenten der beteiligten Domänen angewiesen. Somit kann die Anforderung an die Robustheit der angestrebten Lösung für diese Arbeit wie folgt definiert werden:

Nichtfunktionale Anforderung NFA-12 - Robustheit

Die zu entwickelnde Lösung soll möglichst robust auf folgende Ereignisse reagieren, die in unterschiedlichen Lebenszyklusphasen auftreten können:

- Probleme beim Routing
- Probleme beim Switching
- Ausfälle einzelner funktionaler Komponenten
- Ausfälle einzelner beteiligter SP-Domänen
- Ausfälle einzelner Teildienste einer Dienstinstanz

Neben Skalierbarkeit und Robustheit der Lösung gibt es noch einen weiteren generellen Aspekt – die Anpassbarkeit auf veränderte Anforderungen:

Nichtfunktionale Anforderung NFA-13 - Anpassbarkeit an veränderte Anforderungen

Die zu entwickelnde Lösung soll möglichst leicht an veränderte Anforderungen anpassbar sein.

Diese Anforderung ist insbesondere durch die hohe Entwicklungsdynamik im IT-Bereich bedingt. Ein weiterer Einflussfaktur, der diese Anforderung motiviert, sind unterschiedliche domänenspezifische Anforderungen, die eine Anpassung der entwickelten Lösung erfordern können.

2.6. Dienstketten und E2E QoS, Bewertung

Obwohl das Problem der E2E-Dienstgütezusicherung bei Dienstketten bereits seit langem bekannt ist, gibt es für dieses Problem nur wenige Lösungsansätze. Die im Abschnitt 2.3 ausführlich geschilderten Szenarios stellen dabei die derzeit bekanntesten und/oder die aussichtsreichsten Ansätze dar. Um dem Leser einen möglichst umfassenden Überblick zu geben, wurden bei den Szenarios absichtlich unterschiedliche Kategorien betrachtet: Szenario 1: PSTN – ein über mehrere Jahre hinweg bewährter Dienst; Szenario 2: Géant2 E2E Links – ein Forschungsprojekt, das langsam zu einem richtigen Dienst transformiert wird; Szenario 3: GLIF – ein internationales Forschungsprojekt mit mehreren Kooperationspartnern; Szenario 4: DCN – eine Kooperation von unabhängigen Forschungsprojekten, die Interoperabilität anstreben; und schließlich Szenario 5: IntServ/DiffServ – zwei Techniken für QoS-Zusicherung in Rechnernetzen. Die Bewertung aller Szenarios anhand der aufgestellten Anforderungen ist in Tabelle 2.6 in semi-graphischer Form zusammengefasst. Die zwei im Szenario 5 präsentierten Techniken werden getrennt bewertet, da sie in Bezug auf die aufgestellten Anforderungen unterschiedlichen Stärken und Schwächen aufweisen. Die einzelnen Protokolle, wie z.B. RSVP [BZB+97], LDP [ADF+01, AMT07] oder MPLS [RVC01, AMA+99], die bei der Umsetzung der Techniken zum Einsatz kommen, werden nicht gesondert bewertet. Das liegt daran, dass diese Protokolle sich bislang ausschließlich für den Einsatz in Single-Domain durchgesetzt haben, und aus diesem Grund nicht allein für die Lösung der E2E-Problematik eingesetzt werden können.

Bei der Bewertung der einzelnen Anforderungen wird immer von einer Verbindung über mehrere Domänen hinweg ausgegangen. Das Abschneiden der jeweiligen Dienste und/oder Technologien innerhalb einer Domäne wird dabei nicht berücksichtigt. Für die Bewertung werden vier Abstufungen des Erfüllungsgrades verwendet, die die Werte "gar nicht", "kaum", "größtenteils" oder "vollständig" annehmen können.

Um die Wiederholung der in diesem Kapitel ausführlich geführten Diskussion der Szenarien zu vermeiden, wird an dieser Stelle auf die explizite Begründung einzelner Bewertungen verzichtet.

Wie man der Tabelle entnehmen kann, werden zwar einzelne der aufgestellten Anforderungen von den existierenden Ansätzen "vollständig" oder "größtenteils" erfüllt, keiner der Ansätze schneidet aber zufriedenstellend über alle aufgestellten Anforderungen ab. Obwohl die vorgestellten Szenarios jeweils die fortschrittlichsten in der jeweiligen Kategorie sind, sind die Mängel in Bezug auf die aufgestellten Anforderungen zu groß, um sie durch kleine, punktuelle Erweiterungen ausgleichen zu können. Das macht die Entwicklung einer neuen Lösung notwendig, die sowohl die Lehren aus den existierenden Ansätzen zieht, als auch von vornherein sich auf die Erfüllung der aufgestellten Anforderungen fokussiert.

Szenario 1: Telefonnetz/PSTN	Szenario 2: Géant2 E2E Links	Szenario 3: GLIF	Szenario 4: DCN	Szenario 5/1: IntServ	Szenario 5/2: DiffServ		
						FA-01	Unterstützung beliebiger QoS-Parameter
						FA-02	Unterstützung beliebiger Managementfunktionalität
						FA-03	Gleichzeitige Unterstützung mehrerer Eigenschaften
						FA-04	Unterstützung aller Use Cases
						FA-05	Ziele der Anpassung im Betrieb
						FA-06	Initiator der Abbestellung
						NFA-01	Beachtung der Service Provider Unterstützung
						NFA-02	Unterstützung potentiell möglicher (Teil-)Dienste
						NFA-03	Erweiterbarkeit in Bezug auf unterstützte Diensteigenschaften
						NFA-04	Zugriffseinschränkung auf die Domain-Informationen
						NFA-05	Begrenzung der Prozessdurchlaufzeit
						NFA-06	Dekomposition der QoS-Parameter
						NFA-07	Dekomposition der Managementfunktionalität
						NFA-08	Zustimmung der involvierten SPs
						NFA-09	Erkennung (drohender) E2E-Dienstgüteverletzungen
						NFA-10	Erkennung eines Verursacher-SP
						NFA-11	Skalierbarkeit
						NFA-12	Robustheit
						NFA-13	Anpassbarkeit an veränderte Anforderungen

Erfüllungsgrad der Anforderungen:

gar nicht | bedingt/kaum | größtenteils | vollständig

Tabelle 2.6.: Bewertung anhand Kriterienkatalog

Teil II.

Lösungsvorschlag

3

Verwandte Arbeiten als Lösungsbausteine

Dieses Kapitel wird mit einem Abschnitt eingeleitet, in dem die Skizze der Lösungsidee präsentiert wird. Die Lösungsskizze besteht aus miteinander gekoppelten logischen Blöcken, die eine Reihe von unterschiedlichen Aspekte der Lösung abdecken. Der Rest des Kapitels beschäftigt sich mit der Analyse von Arbeiten und Ansätzen, die zu den aufgezeigten Lösungsteilen einen inhaltlichen Bezug haben. Bei der Analyse stehen vor allem zwei Aspekte im Vordergrund: "Lessons Learned"-Erfahrungen, um Defizite und Probleme existierender Ansätze zu vermeiden, und Lösungsbausteine und Ansätze, die als Teile der zu entwickelnden technischen Architektur verwendet werden können. Die Bewertung und Zusammenfassung dieser Aspekte wird für jedes Themengebiet im Unterabschnitt "Bewertung der Übertragbarkeit" durchgeführt.

Da Routing das Herzstück der angestrebten Lösung darstellt, werden Routingverfahren sowie Suchalgorithmen in Graphen in Abschnitten 3.2 und 3.3 genau betrachtet.

Die Abschnitte 3.4 bis 3.7 befassen sich mit Empfehlungen und Maßnahmen für das SLM, die zum Einsatz kommen, um die Dienstgüte zu garantieren. Im Abschnitt 3.4 werden die etablierten Rahmenwerke ITIL, ISO 20000 und NGOSS präsentiert. Abschnitt 3.5 zeigt, wie die E2E-QoS einer Dienstkette bei streng hierarchischen Organisationsbeziehungen garantiert werden. Im Abschnitt 3.6 werden Vorgehen präsentiert, die sich in Transportnetzen bewährt haben. Anschließend werden im Abschnitt 3.7 verschiedene Techniken und Maßnahmen besprochen, die innerhalb einzelner Service Provider zum Einsatz kommen, um die Dienstgüte für ihre Teildienste garantieren zu können.

Für die Bearbeitung domänenübergreifender SLM-Aufgaben ist der Austausch von Informationen in Multi-Domain Umgebungen erforderlich. Weiterhin besteht die Notwendigkeit, diese Informationen, wie z.B. Elemente einer Verbindung, global eindeu-

tig zu referenzieren. Die etablierten Ansätze, die diese Aspekte behandeln, werden entsprechend in Abschnitten 3.8 und 3.9 beschrieben.

Aspekte der Prozessmodellierung und -Beschreibung in Multi-Domain Umgebungen werden im Abschnitt 3.10 beschrieben.

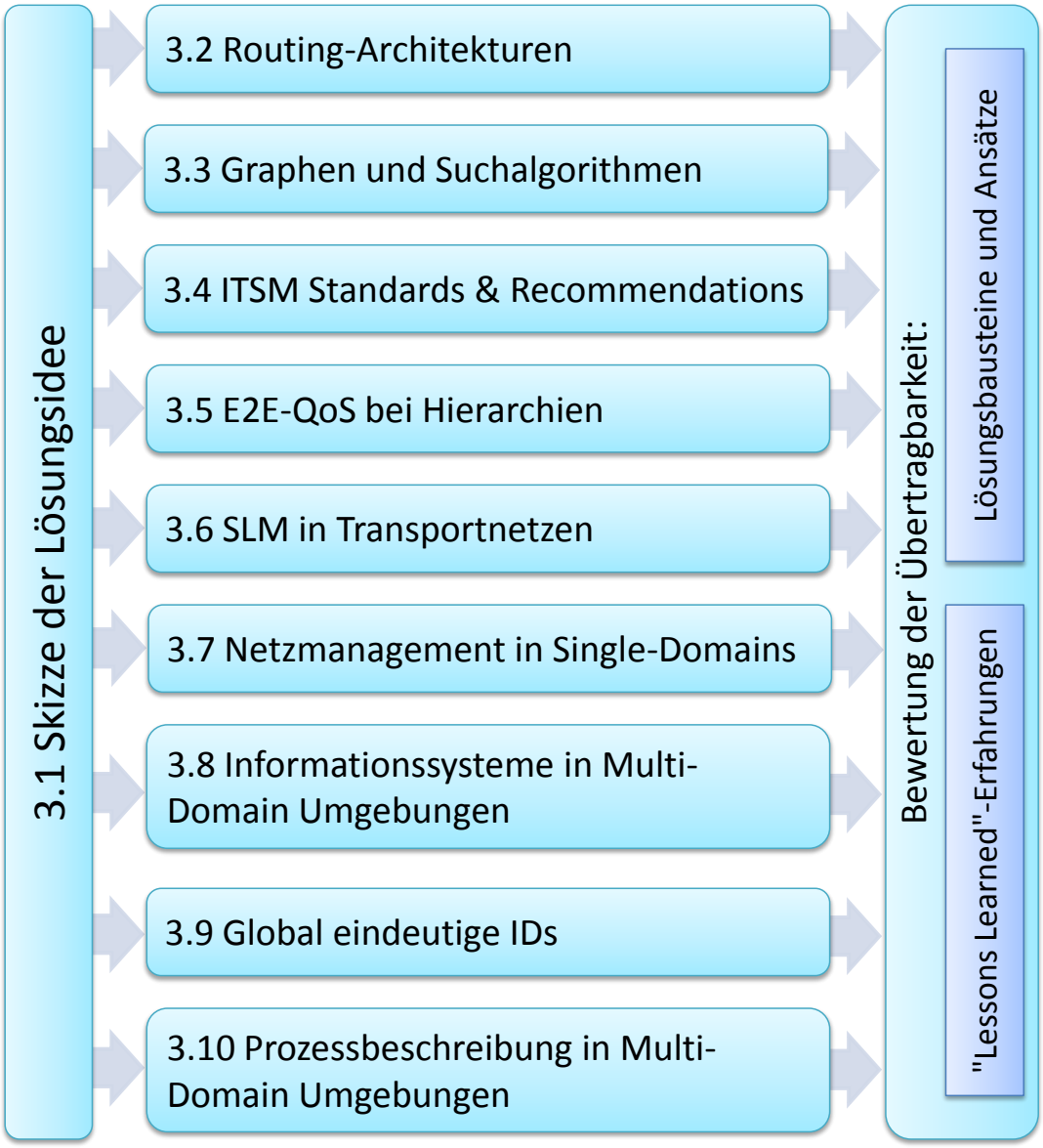


Abbildung 3.1.: Aufbau dieses Kapitels

3.1. Skizze der Lösungsidee

Die Einhaltung von erwünschten E2E-Eigenschaften – darunter werden sowohl die Dienstgüteeigenschaften (QoS) als auch die Managementfunktionalität verstanden – hängt direkt von den Eigenschaften der beteiligten Teildienste sowie deren Zusammenschluss ab (siehe Abbildung 3.2). Somit besteht der zentrale Aspekt zur Sicherung von E2E-Dienstgüteeigenschaften in der Festlegung aller Teildienste, aus der eine Dienstinstanz zusammengesetzt wird, sowie in der Festlegung der Dienstgüteeigenschaften, die diese Teildienste aufweisen sollen. Das Festlegen von Wegen für die Nachrichtenströme über Rechnernetze wird klassischerweise als *Routing* bezeichnet. Das Routing, bei dem QoS-Eigenschaften einzelner Teilstrecken und/oder Ende-zu-Ende berücksichtigt werden, wird in der Fachliteratur oft als *QoS-Routing* bzw. *QoS-aware Routing* referenziert.

QoS-aware Routing

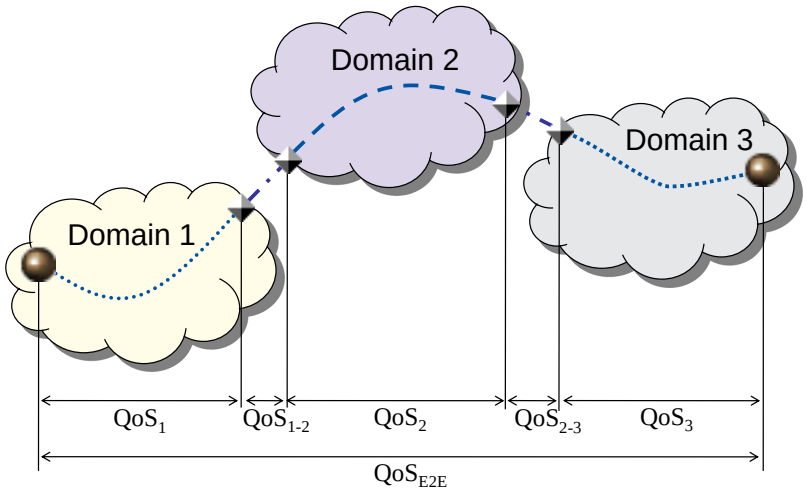


Abbildung 3.2.: Zusammensetzung der E2E-Dienstgüte

Um die Einhaltung der Soll-Werte einer Dienstinstanz garantieren zu können, muss deren Erbringung durch Service-Level-Management (SLM) Prozesse unterstützt werden. In Anlehnung an den Begriff "QoS-aware Routing" wird in dieser Arbeit das Routing als *SLM-aware* bezeichnet, falls sowohl QoS-Eigenschaften als auch Service-Level-Management-Aspekte beim Routingprozess berücksichtigt werden. Zu den Aufgaben der SLM-aware Routings gehört – zusätzlich zu den Aufgaben des QoS-aware Routings – die Festlegung der erforderlichen Managementfunktionalität aller involvierten Teildienste sowie der Zusammensetzung dieser Teildienst-Managementfunktionalitäten zu einem Multi-Domain SLM-Prozess.

SLM-aware Routing

Die angestrebte Lösung besteht aus drei aufeinander aufbauenden Teilen (siehe Abbildung 3.3), wodurch auch die Kapitelstruktur des Lösungsteils bestimmt wird.

Lösungsaufbau

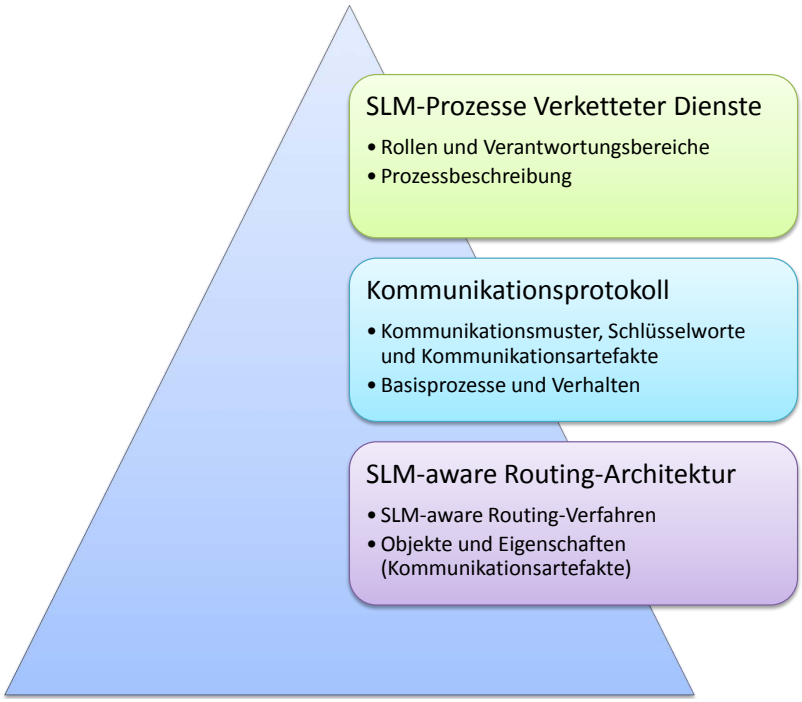


Abbildung 3.3.: Skizze des geplanten Lösungsaufbaus

SLM-aware Routing-Architektur

Die Basis dieses dreistufigen Aufbaus ist eine SLM-aware Routing-Architektur. Das Herzstück jeder Routing-Architektur bildet der Routing-Algorithmus, in dem die Entscheidung über den Routenverlauf getroffen wird. Der Suchalgorithmus muss dabei in der Lage sein, gleichzeitig mehrere Randbedingungen zu berücksichtigen, damit einem E2E-Dienst mehrere Eigenschaften garantiert werden können. Der Suchalgorithmus ist dabei direkt auf die Beschreibung der Objekte und Eigenschaften angewiesen, aus denen sich die Repräsentation der Netztopologie zusammensetzt. Diese werden zusammen mit dem Routing-Verfahren im Kapitel 4 definiert.

Kommunikationsprotokoll

Die Multi-Domain Netztopologie setzt sich aus der Netztopologie einzelner SP-Domänen und deren Verbindungen zusammen. Informationen über die entsprechenden Netztopologie-Objekte und -Eigenschaften einzelner SP-Domänen werden als Kommunikationsartefakte zwischen diesen Domänen ausgetauscht. Einen Rahmen dafür bildet das *Kommunikationsprotokoll* (in der Abbildung 3.3 in der Mitte), das von der Struktur der auszutauschenden Informationen unabhängig ist. Charakteristisch für ein Kommunikationsprotokoll ist die Festlegung eines Kommunikationsmusters sowie der Schlüsselworte, mit denen die (bereits definierten) Kommunikationsartefakte assoziiert werden. Weiterhin ist mit der Definition der Schlüsselworte, die die Anfragen für die unterstützten Aktionen signalisieren, die Festlegung der Basisprozesse sowie des Anfrage-spezifischen erlaubten Verhaltens verbunden. Die Schlüsselworte dienen zur Signalisierung, dass z.B. Informationen bzw. (Teil-)Dienste benötigt werden. Da alle SP-Domänen voneinander unabhängige Organisationen mit u.U. unterschiedlichen,

oft an die Vertrauensbeziehungen angelehnten Policies sind, muss in dem Protokoll auch die mögliche Ablehnung von Anfragen an Policies berücksichtigt werden. Alle diese Aspekte werden im Kapitel 5 definiert.

SL-Prozesse Verketteter Dienste

Die mit den Protokoll-Schlüsselworten assoziierten Basisprozesse können als Primitive betrachtet werden, aus denen komplexere Prozesse aufgebaut werden können. In dieser Arbeit sollen auf dieser Grundlage SLM-Prozesse für Verkettete Dienste definiert werden (siehe in der Abbildung 3.3 oben). Neben der eigentlichen Prozessdefinition werden dabei auch die notwendigen Rollen, deren Verantwortlichkeiten und die Rollenzuweisungsverfahren festgelegt. Dieser Teil der Gesamtlösung wird im Kapitel 6 beschrieben.

Beziehung zwischen verwandten Arbeiten und Lösungsteilen

Die Abbildung der ausgewählten verwandten Arbeiten auf die Teile der geplanten Lösung leitet sich wie folgt ab (vgl. Tabelle 3.1): Die Abschnitte 3.2 und 3.3 legen den Grundbaustein für die *SLM-aware Routing-Architektur*, vor allem für das Routing-Verfahren (siehe mehr dazu in Kapitel 4). Gleichzeitig werden in Abschnitt 3.2 die gängigen Routing- und Signalisierungsprotokolle sowie die etablierten Verhandlungsmuster diskutiert, die die Grundbausteine für die Definition des Kommunikationsprotokolls im Kapitel 5 liefern. Da der Routing-Prozess sowohl die E2E-Anforderungen als auch die Service-Level-Management-Prozesse unterstützen soll, werden diese Aspekte in Abschnitten 3.4 bis 3.7 besprochen. Diese haben ihren Einfluss einerseits auf die Definition der Kommunikationsartefakte im Kapitel 4 und andererseits auf die Definition der SLM-Prozesse in Kapitel 6. Die Diskussion der Multi-Domain Informationssysteme und global eindeutigen IDs in Abschnitten 3.8 und 3.9 hat eine Auswirkung auf die Definition der Kommunikationsartefakte und der Kommunikationswege im Kapitel 4. Schließlich hat die Wahl der Modellierungssprache im Abschnitt 3.10 einen unmittelbaren Einfluss auf die Definition der mit den Protokollschlüsselwörtern verbundenen Basisprozesse in Kapitel 5 sowie auf die darauf aufbauenden SLM-Prozesse in Kapitel 6.

	3.2 Routing Architekturen	3.3 Graphen und Suchalgorithmen	3.4 ITSM Standards & Recommendations	3.5 E2E-QoS bei Hierarchien	3.6 SLM in Transportnetzen	3.7 Netzmanagement in Single-Domains	3.8 Informationssysteme in Multi-Domain Umgebungen	3.9 Global eindeutige IDs	3.10 Prozessbeschreibung in Multi-Domain Umgebungen
SLM-Prozesse									
• Rollen und Verantwortung	—	—	√	√	√	√	—	—	—
• Prozessbeschreibung	—	—	√	√	—	√	—	—	√
Kommunikationsprotokoll:									
• Kommunikationsmuster	√	—	—	√	—	—	—	—	—
• Basisprozesse, Verhalten	√	—	—	—	—	—	—	—	√
Routing-Architektur									
• Routing-Verfahren	√	√	—	√	—	√	√	—	—
• Objekte und Eigenschaften	—	√	√	√	√	√	√	√	—

Tabelle 3.1.: Beziehung zwischen verwandten Arbeiten und Lösungsteilen

3.2. Routing-Architekturen

Der Prozess zur Bestimmung der Wege für die Nachrichtenströme wird in der Telekommunikation als *Routing* bezeichnet. Dabei wird zwischen dem sog. *Intradomain-* und dem *Interdomain-Routing* unterschieden. Während bei Intradomain-Routing die technisch effiziente(re) Nutzung der vorhandenen Netzinfrastruktur im Vordergrund steht (vergleiche Diskussion zum Traffic Engineering im Abschnitt 3.7.3), wird Interdomain-Routing sehr stark von anderen Faktoren, wie z.B. den Kosten des Routings über eine oder andere SP-Domäne, beeinflusst. Weiterhin wird der Umfang der zwischen den SP-Domänen auszutauschenden Informationen im Vorfeld zwischen den jeweiligen Service Providern ausgehandelt und vertraglich festgehalten, weswegen diese Art des Routings oft auch als *Policy-basiertes Routing* referenziert wird.

Da der Fokus dieser Arbeit auf interorganisationalen Aspekten liegt, werden in diesem Abschnitt ausschließlich Ansätze des Interdomain-Routings betrachtet. Zunächst werden in diesem Abschnitt unterschiedliche Konzepte und Begriffe eingeführt, die für die spätere Diskussion notwendig sind. Darauf aufbauend werden im nächsten Unterabschnitt die Routingarchitekturen, deren Zusammensetzung sowie die Abdeckung der Dienstgütezusicherung besprochen. Das Augenmerk wird vor allem auf die Prinzipien und die daraus resultierenden Vor- und Nachteile gelegt, die im letzten Unterabschnitt zusammengefasst werden.

3.2.1. Grundlegende Konzepte und Unterscheidungen

Routing und Forwarding

Zunächst soll zwischen zwei Prozessen unterschieden werden, die häufig miteinander vermischt und unter dem Begriff "Routing" referenziert werden – *Routing* und *Forwarding*. Unter Routing wird in der Nachrichtentechnik der Prozess zur Festlegung des gesamten Weges einer Nachricht bzw. eines Nachrichtenstroms über das Netz verstanden; bei Forwarding hingegen handelt es sich um eine lokale Entscheidung einer Netzkomponente, über welchen ihrer Nachbarn und wie technisch eine Nachricht auf dem Weg zum Ziel weitergeleitet werden soll.

Vermittlungsarten

Ein weiterer Aspekt bezieht sich auf die Fragen, wann, für welche Objekte und somit auch wie oft das Routing durchgeführt wird. In der Vermittlungstechnik wird zwischen zwei prinzipiellen Ansätzen unterschieden – der Leitungsvermittlung und der Paketvermittlung.

Leitungsvermittlung

Die *Leitungsvermittlung* (engl.: *Circuit Switching*, *Line Switching*) stellt das für die Telefonnetze übliche Vorgehen dar, bei dem ein exklusiver Nachrichtenkanal geschaltet wird. Die Dauer solcher geschalteten Verbindungen kann von relativ kurzfristigen Telefongesprächen bis hin zu dauerhaften Standleitungen variieren. Charakteristisch für die Leitungsverbindungen ist eine feste Vorauswahl aller Teilstrecken einer Verbindung, über die alle dazugehörigen Nachrichten übermittelt werden. Diese Festlegungen werden von den sog. *Vermittlungsstellen* getroffen, die gewisserma-

ßen die "Intelligenz" des Netzes verkörpern. Bevor der eigentliche Nachrichtenaustausch beginnen kann, muss bei dieser Vermittlungsart die Verbindung aufgebaut werden. Nach Beenden des Nachrichtenaustausches erfolgt ein Abbau der Verbindung. Zum Aufbau und Abbau einer Verbindung müssen zwischen den Vermittlungsstellen Steuerinformationen ausgetauscht werden, was als *Signalisierung* bezeichnet wird.

Paketvermittlung

Eine andere Vermittlungsstrategie wird bei *Paketvermittlung* (engl.: *Packet Switching*) verwendet. Robustheit gegenüber Ausfällen zählt zu den zentralen Designkriterien dieser Strategie.

Bei dieser Vermittlungsart wird die zu übertragende Information zunächst in einzelne Pakete aufgeteilt. Die Pakete werden dann einzeln über ein dezentrales, vermaschtes Netz übertragen. Außer den zu übertragenen Nutzinformationen, die sich in dem sog. *Payload*-Teil eines Pakets befinden, befindet sich im *Header*-Teil des Pakets eine Reihe von zusätzlichen Informationen (vor allem die Zieladresse), die sein Routing und Forwarding beeinflussen. Da die Entscheidung über die Route auf Paket-Basis getroffen wird, können unterschiedliche Pakete derselben Verbindung unterschiedliche Wege durchlaufen, was unter anderem zu unterschiedlichen Laufzeiten und falscher Ordnung der ankommenden Pakete führen kann.

Zellvermittlung

Die *Zellvermittlung* (engl.: *Cell Switching*, *Cell Relay*) stellt einen Spezialfall der Paketvermittlung dar, bei dem die Daten zwar weiterhin paketweise, diese jedoch auf fest definierten virtuellen Pfaden übertragen werden. Da bei dieser Vermittlungsart fürs Forwarding ausschließlich die Zugehörigkeit einer Zelle zum virtuellen Pfad benötigt wird, kann die Header-Größe wesentlich kleiner als bei der klassischen Paketvermittlung sein. Bei den ATM-Netzen (ATM steht für *Asynchronous Transfer Mode*), die wohl die bekanntesten Vertreter dieser Vermittlungsart sind, werden Zellen fester Größe verwendet. Während die feste Zellengröße die Verarbeitungsgeschwindigkeit wesentlich steigert, war die Wahl der Größe einer ATM-Zelle (5 Bytes Header und 48 Bytes Payload) eher politisch als technisch motiviert [Ste93]. Die gemeinsame Nutzung derselben physischen Verbindungen durch mehrere gleichzeitig bestehende virtuelle Verbindungen wird durch deren (im ATM-Fall zeitliches) Multiplexing realisiert.

Vermittlungsverfahren: Vor- und Nachteile

Alle diese Vermittlungstechniken haben ihre Vor- und Nachteile. So ist bei der Leitungs- und Zellvermittlung gewährleistet, dass die unterschiedlichen Verbindungen einander nicht beeinflussen, was bei der Paketvermittlung i.A. nicht garantiert wird. Auf der anderen Seite werden für diese Vorteile schlechtere Infrastrukturnutzung (bei Leitungsvermittlung) und aufwendige Multiplex-Verfahren (bei Zellvermittlung) in Kauf genommen. Die Paketvermittlung bietet dagegen wesentlich bessere Infrastrukturausnutzung und Ausfallsicherheit an.

Routingzeitpunkt und -Häufigkeit

Aus der Routing-Perspektive unterscheiden sich diese Verfahren nicht nur in Bezug auf Routing-Objekt (Pakete bei Paketvermittlung und Verbindung bzw. virtuelle Verbindung bei Leitungs- bzw. Zellvermittlung), sondern auch in Bezug auf den Zeitpunkt und die Anzahl der Routingentscheidungen. Während bei der Paketvermittlung das Routing durch Forwarding-Entscheidung pro Paket und somit im Laufe der ganzen Verbindung erfolgt, wird bei den beiden anderen Arten diese Entscheidung nur ein Mal in der Verbindungsaufbauphase getroffen. Forwarding bei der Zellvermittlung geschieht zwar auch auf Paket-/Zellenbasis, diese basiert jedoch auf der zuvor getroffenen Entscheidung über die Route.

Routing by Delegation

Eine andere, von der Vermittlungsart i.A. unabhängige Unterscheidung, besteht darin, von wem die Entscheidung über die Route getroffen wird. Klassischerweise entscheidet jede SP-Domäne, welche ihrer direkten Nachbardomänen den nächsten Abschnitt der Kette erbringen wird und legt den Verbindungspunkt (sog. NNI, *Network-Network Interface*) zu dieser Domäne fest. Danach wird diese Domäne über das ausgewählte NNI, das gleichzeitig auch als eine Kommunikationsschnittstelle dient, kontaktiert, um an sie die Routing-Aufgabe für den Rest der Kette zu delegieren. Diese Art des Routings, die im Weiteren als *Routing by Delegation* referenziert wird, findet sowohl bei Internet- als auch bei Telefonverbindungen statt.

Source Routing

Alternativ zum klassischen Routing (by Delegation) wird von *Source Routing* dann gesprochen, wenn der vollständige Pfad von der Quelle zur Senke über alle Netzkomponenten zentral getroffen wird. Üblicherweise wird diese Entscheidung vom Sender getroffen, wodurch auch der Name bedingt ist. Zur Entscheidungsfindung werden beim *Source Routing* wesentlich detailliertere Informationen über die Netzstruktur benötigt als das beim *Routing by Delegation* der Fall ist, weswegen dieses Verfahren hauptsächlich in lokalen Netzen Verwendung findet. Es gibt aber auch Alternativformen und Bestrebungen, dieses Verfahren auf Multi-Domain Umgebungen auszudehnen. Ein Beispiel dafür bietet die DCN-Kooperation (siehe Abschnitt 2.3.4), bei der die Entscheidung über den kompletten Pfad von den hierarchisch angeordneten Inter-Domain Managern (IDM) getroffen wird.

In-Band und Out-of-Band Kommunikation

Unabhängig davon, um welches Routingverfahren es sich handelt, wird ein Kommunikationsaustausch zwischen den involvierten SP-Domänen[1] benötigt. Dabei wird zwischen den sog. *In-Band* und *Out-of-Band* Kommunikationskanälen unterschieden. Bei der In-Band-Kommunikation werden Steuerinformationen und Nutzdaten über denselben Informationskanal ausgetauscht. Charakteristisch ist das vor allem für die Paket- und Zellvermittlung, bei denen die Dienstinformationen im Header kodiert werden. Diese Kommunikationstechnik kann jedoch auch bei einer Leitungsvermittlung verwendet werden, wie es z.B. bei den älteren Signalisierungssystemen in PSTN der Fall war. Das derzeit im Telefondienst eingesetzte Signalisierungssystem SS7 (*Signaling System Number 7*) verwendet für die Steuerung jedoch die Out-of-Band-Kommunikation.

[1] Im Bereich des Internets und insbesondere im Zusammenhang mit IP-Netzen wird dafür überwiegend der Begriff *Autonome Systeme* (AS) verwendet. Um die Allgemeinheit zu wahren, wird in dieser Arbeit jedoch der technologieübergreifende Begriff "SP-Domain" verwendet.

Die Gründe dafür sind sehr vielfältig. Zu den wichtigsten zählen z.B. die bessere Optimierbarkeit unterschiedlicher Kommunikationskanäle an die jeweilige Bedürfnisse sowie (telefondienstspezifisch) der Austausch von Steuerinformationen auch während der Verbindung und nicht nur bei deren Aufbau[Sig07].

3.2.2. Routing-Architekturen und QoS-Aspekte

Bestandteile einer Routing Architektur

Als die zwei wichtigsten Bestandteile einer Routingarchitektur werden das *Routing-Protokoll* und der *Routing-Algorithmus* angesehen, die sehr stark miteinander verzahnt sind. So gehört zum Aufgabenbereich des Routingprotokolls das Sammeln bzw. das Verteilen der Informationen, die für die Entscheidungsfindung – d.h. für den Routing-Algorithmus – benötigt werden, sowie die Kommunikation mit den ausgewählten Netzkomponenten, um die getroffene Entscheidung zu signalisieren, sodass die Infrastruktur entsprechend konfiguriert werden kann. Da die Möglichkeiten eines Routing Algorithmus sehr stark von den Informationen über das Netz abhängen, kann die Netzbeschreibung als ein dritter integraler Bestandteil einer Routing Architektur angesehen werden.

Statisches und Adaptives Routing

Bei Routing wird grundsätzlich zwischen sog. *statischem* und *adaptivem* Routing unterschieden. Beim statischen Routing, das z.B. in PSTN-Netzen Verwendung findet, werden die Tabellen mit den primären und Ersatz- bzw. Default-Routen vorkonfiguriert. Während bei kleinen Rechnernetzen diese Routingmethode auch eingesetzt werden kann, werden bei größeren Netzen adaptive Verfahren verwendet, die die Netztopologie automatisch erkennen und sich somit an die Veränderungen im Netz (wie z.B. Komponentenausfälle und/oder Bottlenecks) automatisch anpassen können. Die meisten im Internet vertretenen adaptiven Verfahren lassen sich auf die sog. *Link-State* oder *Distance Vector* Routing-Algorithmen bzw. -Protokolle zurückführen. Während bei dem Link-State Verfahren die Informationen über die tatsächliche Netztopologie (sog. *maps*) zwischen den Netzkomponenten (aus der Komponentensicht) ausgetauscht werden, werden bei Distanzvektor nur die Kosten fürs Erreichen bestimmter Zieladressen mitgeteilt. Abgesehen von den Unterschieden bzgl. der auszutauschenden Informationen kann die Netztopologie in beiden Fällen als ungewichtete bzw. (mit einem Wert) gewichtete Graphen dargestellt werden und somit die entsprechenden Suchverfahren anwenden (siehe mehr dazu im Abschnitt 3.3).

Berücksichtigung der QoS-Aspekte

Die Darstellung als ungewichtete bzw. gewichtete Graphen erlaubt allerdings ausschließlich die Anzahl der Hops bzw. die Kosten auf der Ende-zu-Ende Strecke zu minimieren, die QoS-Parameter (abgesehen von der reinen Erreichbarkeit) können jedoch nicht berücksichtigt werden. Insbesondere mit der zunehmenden Bedeutung von multimedialen Inhalten wurden immer wieder die Dienstgüteeigenschaften auch im Internet ins Visier genommen. Hier kann z.B. die in RFC 1992 spezifizierte *Nimrod Routing Architecture* erwähnt werden [CCS96]. Unter anderem wird für die Beschreibung der Netztopologie eine offene Liste von Dienstgüteeigenschaften angeregt, die mit den Verbindungen assoziiert werden kann. Dieser Ansatz liefert jedoch nur ein

relativ grobes Architekturkonzept. Weder ein Routingprotokoll noch ein Algorithmus, der gleichzeitig mit mehreren QoS-Parameter umgehen kann (mehr zu dem Thema siehe im Abschnitt 3.3.2), wurden spezifiziert.

Heutzutage werden mit den Begriffen Dienstgüte und Dienstgütezusicherung in Rechnernetzen hauptsächlich zwei Protokolle und deren Erweiterungen assoziiert: RSVP [BZB+97] und MPLS [RTF+01]. *Multi Protocol Label Switching* (MPLS) realisiert eine In-Band (im Paket-Header kodierte) Signalisierung an MPLS-fähige Router und Switches, über welche Route das Forwarding des Pakets geschehen soll. *Resource ReSerVation Protocol* (RSVP) ist ein Signalisierungsprotokoll, das auf existierenden Routing-Technologien aufbaut und sich ausschließlich auf die Reservierung der Netzinfrastrukturressourcen entlang eines gerouteten Pfades fokussiert. RSVP ist eine Implementierung der IntServ-Strategie (vgl. Abschnitt 2.3.5). Somit können RSVP und MPLS zur technischen Umsetzung getroffener Routing-Entscheidungen verwendet werden. Auch wenn aus der technischen Sicht die Verwendung dieser Protokolle in Multi-Domain Szenarios möglich ist, haben sie sich bislang ausschließlich im Single-Domain Umfeld durchgesetzt. Gründe dafür liegen hauptsächlich in Policy-bedingten Restriktionen, die die einzelnen Service Provider beim Informationsaustausch und dem Managementaccess anwenden.

Klasse	Bezeichnung	Beispiel einer Anwendung
CRB	Constant Bit Rate	Sprache
RT-VBR	Variable Bit Rate, Real Time	Videokonferenzen
NRT-VBT	Variable Bit Rate, Non Real Time	Video on demand
ABR	Available Bit Rate	Surfen im Internet
UBR	Unspecified Bit Rate	Dateitransfer

Abbildung 3.4.: Dienstklassen bei ATM (nach [Mey02])

Als einzige vollwertige Routing-Architektur, die Dienstgüteaspekte einer Verbindung berücksichtigt, kann beim derzeitigen Stand der Technik nur ATM erwähnt werden. Dienstgüteaspekte werden bei ATM auf der Basis von unterschiedlichen Dienstklassen zugesichert (siehe Abbildung 3.4). Dabei beschränkt sich die Wahl der QoS-Parameter, die diesen Klassen zugrunde liegen, auf Bandbreite, Delay und Jitter (Delay Variation). Interessant ist, dass moderne Forschungsprojekte, wie z.B. die im Kapitel 2.3 beschriebenen DCN und GLIF, sich ebenfalls auf die Bandbreite beschränken (eine Berücksichtigung von Delay und Jitter ist derzeit nur geplant[2]). Eine Ursache dafür ist, dass die Aggregatfunktion zur Berechnung der E2E-Bandbreite als "min"-Funktion realisiert werden kann, was die Ende-zu-Ende Betrachtung einer Verbindung überflüssig macht. Soll jedoch ein QoS-Parameter wie z.B. "*Packet Drops*" berücksichtigt werden, dessen Werte über alle Abschnitte aufsummiert werden müssen, dann wird eine direkte oder z.B. über eine Zwischensumme realisierte indirekte Ende-zu-Ende Betrachtung erforderlich. Das führt dazu, dass bei den Géant2 E2E Links – einem Verketteten Dienst,

[2] Stand Anfang 2009.

bei dem sowohl unterschiedliche QoS-Parameter als auch Managementfunktionalität unterstützt wird – alle Festlegungen durch persönliche Absprachen getroffen werden müssen.

Das Management domänenübergreifender Verbindungen, darunter auch Service-Level-Management, ist erst kürzlich in den Fokus der Aufmerksamkeit gelangt. Erst vor Kurzem wurde die Wichtigkeit dieses Themas erkannt. Derzeit wird an der Entwicklung technologiespezifischer Managementverfahren gearbeitet, wie z.B. *Ethernet* OAM! (*Operation, Administration, and Maintenance*), bei dem der Fokus auf der Verbindungsüberwachung und der Benachrichtigung bei Ausfällen liegt [Bro08].

Um Inkonsistenzen zu vermeiden, die in Multi-Domain Umgebungen durch die von verschiedenen SP-Domänen kommenden und i.A. miteinander konkurrierenden Service-Anfragen entstehen können, wurde eine Reihe von Techniken entwickelt. In diesem Kontext ist zunächst die Einführung eines Reservierungszustands zu erwähnen. Während bei RSVP die Reservierung bereits eine Zuweisung von Ressourcen zu einer gültigen Verbindung bedeutet, wird ein Zwischenzustand zwischen "Verfügbar" und "Verwendet" für die Diensterbringung benötigt. Oft wird auch gefordert, dass der Übergang zwischen "Verfügbar" und "Verwendet" nicht direkt, sondern ausschließlich über den "Reserviert"-Zustand möglich ist (siehe Abbildung 3.5). Der Zustand kann als eine Vorbestellung betrachtet werden, die ohne Konsequenzen widerrufen werden darf.

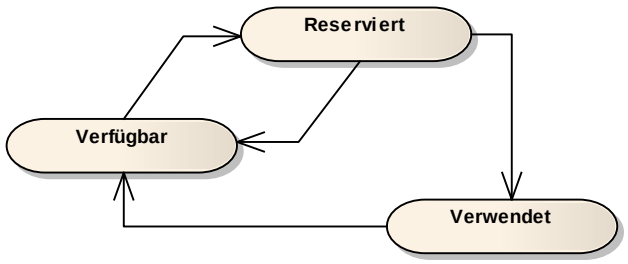


Abbildung 3.5.: Verwaltungszustände von Ressourcen

Weiterhin hat sich in Bezug auf die Verhandlung über den Dienstgütewert eine Reihe von sog. Verhandlungsmustern etabliert. Die dienstanfragenden und -anbietenden Kommunikationspartner (engl.: *Peers*) tauschen dabei Nachrichten aus, die sich auf einen erwünschten bzw. möglichen Wert beziehen. In Bezug auf diese Arbeit interessant sind vor allem die sog. *Bilateralen Peer-to-Peer* und *Trilateralen* Verhandlungsmuster. Im ersten Fall darf die angefragte SP-Domäne mit einem alternativen, schlechteren Vorschlag antworten (siehe Abbildung 3.6), im zweiten Fall hingegen darf die angefragte SP-Domäne ausschließlich bessere Dienstgüte als die angefragte erbringen [Ste00]. Sollte die Erfüllung der angeforderten Dienstgüte unmöglich sein, dann ist die angefragte SP-Domäne bei den Trilateralen Verhandlungen verpflichtet, die Anfrage mit der Fehlermeldung zurückzuweisen.

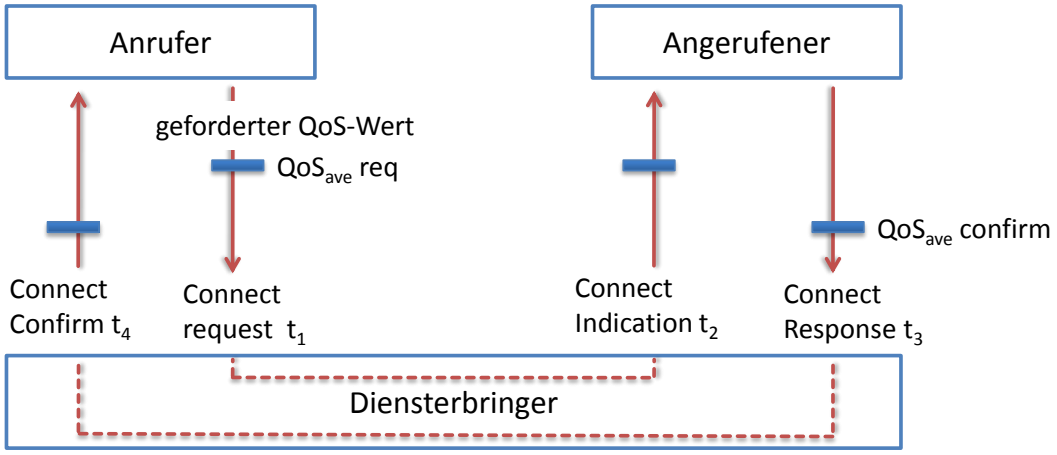


Abbildung 3.6.: Bilaterale Peer-to-Peer Verhandlung (nach [Ste00])

Die Bewertungen "schlechter" und "besser" werden abhängig vom jeweiligen QoS-Parameter definiert. So steht in Bezug auf die Bandbreite "besser" für "größer", bei der Fehlerrate dagegen für "kleiner". Da die existierenden Architekturen mit einer fest definierten und kleinen Menge an QoS-Parameter operieren, wurde für die Bewertung keine Verallgemeinerung getroffen.

3.2.3. Bewertung der Übertragbarkeit

QoS-Zusicherung innerhalb einer SP-Domäne ist gut ausgereift und kann daher i.a. als gegeben angenommen werden. Sollte eine E2E-Verbindung in Abschnitte mit festen Übergangspunkten zwischen SP-Domänen aufgeteilt werden, dann kann die Dienstgüte für jeden dieser Abschnitte von der jeweiligen SP-Domäne garantiert werden. Die Veränderung der Übergangspunkte während einer Verbindung, wie es z.B. bei der klassischen Paketvermittlung geschieht, ist zwar denkbar, würde aber einen erheblicheren Managementaufwand und eine ständige Neuberechnung der erforderlichen Dienstgüte der einzelnen Abschnitten bedeuten.

Eine Routingarchitektur umfasst Kommunikationsprotokoll, Netzbeschreibung und Routingalgorithmus. Bisherige Versuche, eine QoS-Routingarchitektur nicht nur zu entwickeln, sondern auch in Betrieb zu nehmen, sind hauptsächlich an administrativen Grenzen und erheblichen Restriktionen der notwendigen Informations- und Managementzugriffen gescheitert. Das macht erforderlich, dass die Informationsbeschreibung es einer SP-Domäne erlaubt, ihre vorhandenen Infrastruktur und Ressourcen beliebig zu verschatten. Weiterhin soll die Zurückweisung der Anfragen beliebiger Art ein integraler Teil des Kommunikationsprotokolls sein, sodass jede SP-Domäne ihre Souveränität beibehalten kann.

Die bestehenden Ansätze beschränken sich grundsätzlich auf die Unterstützung weniger ausgewählter QoS-Parameter. Das macht die Ausdehnung dieser Ansätze auf andere QoS-Parameter zu einer schwierigen Aufgabe. Um das zu vermeiden soll eine generische Beschreibung einer beliebigen Anzahl unterschiedlicher Parameter möglich sein. Eine generische Beschreibung der QoS-Parameter erfordert eine entsprechende Beschreibung der benötigten Aggregat- und Ordnungsfunktionen.Existierende Ansätze definieren parameterspezifische, feste Funktionen. Um eine variable Anzahl von QoS-Parametern zu unterstützen, erscheint die Out-of-Band-Kommunikation vor allem wegen ihrer Flexibilität als eine geeignete Wahl.

Die Behandlung von Managementaspekten wurde bei Dienstketten bislang fast komplett vernachlässigt. Das macht zunächst erforderlich, dass auch die Ansätze des IT-Service-Managements bei anderen Organisations- und Diensterbringungsformen untersucht werden (siehe Abschnitte 3.4 bis 3.7 in diesem Kapitel). Diese Aspekte können dann im Lösungsteil neben den Dienstgüteeigenschaften mit den Teilstrecken – als ihre Management-Eigenschaften – assoziiert werden.

Eine Ressourcenreservierung vor der eigentlichen Bestellung hat sich als eine sehr gute Strategie erwiesen, um die Inkonsistenzen bei miteinander konkurrierenden Bestellprozessen zu vermeiden. In diesem Zusammenhang ist insbesondere das Zusammenspiel der drei Ressourcen-Zustände (Verfügbar, Reserviert, Verwendet) mit den angesprochenen Verhandlungsmustern interessant. So kann bei der Reservierung auf dem Bilateralen Peer-to-Peer Verhandlungsmuster aufgebaut werden, was der dienstanfragenden SP-Domäne die Möglichkeit für die Suche nach einer Alternative eröffnet. Beim Übergang des Zustandes "Reserviert" nach "Verwendet" ist jedoch das Verhalten der Trilateralen Verhandlung erforderlich, um die vereinbarte Dienstgüte zu garantieren.

Es ist momentan unklar, ob *Source Routing* oder *Routing by Delegation* eine geeignete Strategie für Verkettete Dienste darstellt. In Bezug auf die E2E-Zusicherung und die Providerunabhängigkeit haben beide Strategien eine Reihe von Stärken und Schwächen. Deswegen sollen im Lösungsteil zunächst beide betrachtet werden (siehe Abschnitt 4.3). Unter Umständen kann auch eine Mischform der beiden Strategien interessant sein.

Genauso ist a priori nicht entscheidbar, ob die "Zusammenlegung" der Verbindungspunkte einzelner Teilstrecken mit der Managementschnittstelle, wie es z.B. bei UNI/NNI der Fall ist, eine für das Management Verketteter Dienste sinnvolle Lösung ist. Deswegen sollen diese zwei Aspekte im Lösungsteil zunächst getrennt voneinander betrachtet werden. Anschließend (siehe Abschnitt 4.5) soll diskutiert werden, ob oder unter welchen Bedingungen sie miteinander verknüpft bzw. getrennt implementiert werden sollten.

3.3. Graphen und Suchalgorithmen

Im Zusammenhang mit Routing-Verfahren gehört die *Graphentheorie* zu den wichtigsten Grundlagen. Aus diesem Grund wird die Beschreibung in diesem Abschnitt in zwei Unterabschnitte aufgeteilt: zunächst werden Grundbegriffe der Graphentheorie erläutert; dem folgt eine Beschreibung der speziellen Probleme sowie existierender Lösungsansätze, die für den Lösungsteil dieser Arbeit relevant sind. Die Übertragbarkeit der vorgestellten Ansätze auf die Problematik Verketteter Dienste wird im letzten Unterabschnitt diskutiert.

3.3.1. Terminologie und klassische Ansätze

Unter einem Graphen wird ein Tupel $G ::= (V, E)$ verstanden, wobei V für die Menge aller Knoten (engl.: *vertex/vertices*) und E für die Menge aller Kanten (engl.: *edges*) steht. Die Anzahl von Knoten bzw. Kanten wird entsprechend als $|V|$ bzw. $|E|$ gekennzeichnet. Bei der graphischen Darstellung werden Knoten als Punkte oder Kreise dargestellt, Kanten werden als Linien oder Pfeile dargestellt, die die Knoten miteinander verbinden (siehe Abbildung 3.7). Um die Knoten bei der Beschreibung voneinander unterscheiden zu können, werden sie üblicherweise mit Buchstaben oder Zahlen beschriftet.

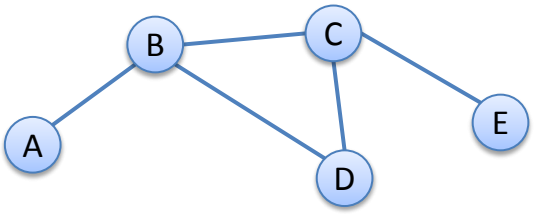


Abbildung 3.7.: Ein beliebiger Graph

Kategorisierungsmerkmale

Graphen werden anhand unterschiedlicher Merkmale kategorisiert. Zu den wichtigsten Unterscheidungskriterien gehören Kantenrichtung, Kantengewicht und die maximale Anzahl der Kanten zwischen je zwei Knoten. Bei sog. *ungerichteten* Graphen kann jede Kante zur "Bewegung" zwischen den verbundenen Knoten in beiden Richtungen verwendet werden, bei *gerichteten* dagegen nur in einer Richtung (die erlaubte Richtung wird durch die Pfeilspitze der Kante gekennzeichnet). Sind mit den Kanten keine Kosten bzw. Gewichte verbunden, dann spricht man von einem *ungewichteten*, ansonsten von einem *gewichteten* Graph. Bei gewichteten Graphen wird weiterhin unterschieden, ob die Gewichte ausschließlich positiv oder auch negativ sein dürfen. Ferner wird zwischen Graphen mit nur einem oder mehreren Gewichten unterschieden (siehe dazu Abschnitt 3.3.2). Bei der Anzahl der Verbindungskanten zwischen je zwei Knoten wird üblicherweise von maximal einer Kante ausgegangen. Solche Graphen werden als *einfache* Graphen referenziert. Sind mehrere Verbindungskanten

erlaubt, dann wird von *Multigraphen* gesprochen. Entsprechend diesen Klassifizierungen ist in der Abbildung 3.7 ein ungerichteter, ungewichteter, einfacher Graph dargestellt.

Graphen dienen als Beschreibungsmittel für unterschiedliche Aufgaben im alltäglichen Leben. So lassen sich geographischen Gegebenheiten mit Graphen gut beschreiben, dabei können die Knoten für die Städte, die Kanten für die Straßen zwischen den jeweiligen Städten und die Kantengewichte für die jeweilige Entfernung stehen. Genauso lassen sich auch Rechnernetze als Graphen mit Netzkomponenten wie Routers oder Switches als Knoten, direkten Verbindungen als Kanten und z.B. Delay oder Kosten als Knotengewichte beschreiben.

Begriffe und weitere Unterscheidungsmerkmale

Um unterschiedliche Aufgaben zu lösen, werden in der Graphentheorie weitere Begriffe und darauf aufbauende Unterscheidungsmerkmale eingeführt. Für die folgende Beschreibung ist vor allem der Begriff *Weg* von Bedeutung, der formal als die Knotenfolge $(v_1, ..., v_n)$ definiert ist, wobei für jedes in der Folge aufeinanderfolgende Knotenpaar (v_i, v_{i+1}) eine Kante in der Kantenmenge E existiert. Existiert zwischen beliebigen zwei Knoten ein Weg, dann wird ein solcher Graph als *zusammenhängend* klassifiziert, ansonsten als *unzusammenhängend*. Teile eines unzusammenhängenden Graphen, in denen zwischen je zwei Knoten ein Weg existiert, werden *Zusammenhangskomponenten* genannt. Ein Sonderfall eines Weges, bei dem alle Knoten voneinander verschieden sind, wird als *Pfad* referenziert. Ein weiterer Sonderfall stellt ein Zyklus dar, der formal als ein Weg mit identischem Start- und Endknoten definiert ist, d.h. $v_1 = v_n$. Auf dem Begriff baut eine weitere Unterscheidung auf: Graphen mit Zyklen werden *zyklisch*, ohne Zyklen *azyklisch* genannt.

Weg-Länge und -Gewicht

Zentrale Eigenschaften eines Weges sind seine *Länge* und sein *Gewicht*. Unter der *Länge* eines Weges wird die Anzahl seiner Kanten verstanden. In der englischsprachigen Literatur und insbesondere in Verbindung mit den Rechnernetzen wird oft auch von der Anzahl der *hops* (Knotenübergänge) gesprochen. Der Begriff Gewicht wird in Verbindung mit gewichteten Graphen verwendet. Bei den ungewichteten Graphen wird das Gewicht jeder Kante implizit auf 1 gesetzt. Unter dem Gewicht eines Weges wird die Summe der Gewichte aller Kanten in dem Weg verstanden. Bei den Graphen, die Rechnernetze repräsentieren, werden – je nach der repräsentierenden Größe – statt der Summe auch andere Aggregatfunktionen verwendet, wie z.B. die Multiplikation für die Wahrscheinlichkeit der fehlerfreien Übertragung oder die min-Funktion für die verfügbare Bandbreite.

Weg-Länge und -Gewicht spielen eine wichtige Rolle bei der Lösung unterschiedlicher Klassen von Aufgaben mittels der Graphentheorie. Dazu gehört vor allen die Findung eines beliebigen oder kostengünstigsten Weges zwischen zwei Knoten. Die Lösungen werden in Form eines Algorithmus spezifiziert. Unterschiedliche Algorithmen werden anhand ihrer Komplexität bewertet, die sich auf die Laufzeit und/oder den Speicherbedarf bezieht.

Breitensuche

Zu den wichtigsten Algorithmen gehören Breiten- und Tiefensuche. Bei der *Breiten-*

suche (engl.: *Breadth First Search*, BFS!) handelt es sich um ein Verfahren, bei dem ausgehend von dem Start-Knoten gleichzeitig in alle Richtungen nach dem Ziel-Knoten gesucht wird. Durch diese Art der Suche hat der gefundene Weg immer die kürzeste Länge von allen möglichen Wegen. Die Komplexität der Breitensuche – damit werden sowohl die Suchlaufzeit als auch der Speicherbedarf gemeint – beträgt $O(b^d)$, wobei "b" für den Verzweigungsgrad und "d" für Tiefe (Länge des Weges) bis zum Ziel stehen [Sas08a]. Somit schneidet dieses Verfahren dann sehr gut ab, wenn der Abstand zwischen Start- und Ziel-Knoten relativ klein ist.

Tiefensuche

Bei der *Tiefensuche* (engl.: *Depth-First Search*, DFS!) wird im Gegensatz zur Breitensuche immer nur ein einziger Weg verfolgt, dafür aber bis zur weitest möglichen Tiefe. Sollte auf dem Weg der Ziel-Knoten nicht gefunden werden, dann wird von dem letzten Knoten mit den noch nicht ausprobierten Alternativen ein anderer Zweig für die Tiefensuche gewählt. Diese Strategie erlaubt die Implementierung des Suchalgorithmus in Form eines rekursiven Funktionsaufrufes. Die Laufzeit der Tiefensuche beträgt $O(b^d)$, wobei "b" für den Verzweigungsgrad und "d" hier für die maximale Suchtiefe stehen [Sas08b]. Wenn ausschließlich der Weg abgespeichert werden muss (je nach Zielsetzung und Optimierung kann der Bedarf für weitere Informationen entstehen), entspricht der Speicherbedarf $O(d)$. Tiefensuche ist vor allem gut geeignet für die Wegesuche zu weit entfernten Knoten. Bei einer "unglücklichen" Wahl der Nachfolgeknoten kann es sein, dass der Algorithmus sehr lange braucht, bis ein nur wenige Hops entfernter Ziel-Knoten gefunden wird.

Bestimmung der Zusammenhangskomponenten

Wegen der einfacheren Datenverwaltung und Implementierung ist die Tiefensuche wesentlich schneller als die Breitensuche, weswegen sie sehr oft als die Grundlage für die anderen, an die spezifischen Aufgaben angepassten Algorithmen verwendet wird. Zu solchen Aufgaben zählt die Bestimmung der Zusammenhangskomponenten eines Graphs. Der DFS-basierte Algorithmus von TARJAN [Tar72] z.B. ist in der Lage, starke Zusammenhangskomponenten bei gerichteten Graphen in linearer Zeit von O(|E| + |V|) zu bestimmen.

Algorithmen von DIJKSTRA *u.a.*

Ein sehr gut untersuchter Teil der Graphentheorie beschäftigt sich mit der Suche der kürzesten Wege in vorwiegend ungerichteten, einfachen Graphen mit nur einem Kantengewicht. Als ein Klassiker soll in diesem Zusammenhang vor allem der Algorithmus von DIJKSTRA[Dij59] erwähnt werden. Der Algorithmus stützt sich auf die dynamische Programmierung und macht sich dabei die Eigenschaft zunutze, dass bei nur einem Kantengewicht (bei mehreren Gewichten sieht die Situation anders aus, siehe Abschnitt 3.3.2) jeder Teilweg eines kürzesten Weges selbst ein kürzester Weg ist. Die Komplexität des originalen DIJKSTRA-Algorithmus beträgt $O(|E|^2 + |V|)$. Bei der Verwendung von Fibonacci-Heap [FT87] als Datenstruktur kann die Komplexität bis $O(|E| \cdot \log |E| + |V|)$ reduziert werden. Es gibt aber auch eine Reihe von weiteren Algorithmen, wie z.B. der von BELLMAN und FORD, der einen Weg zwar in der höheren Laufzeitkomplexität von $O(|V| \cdot |E|)$ findet, dafür aber – im Gegensatz zum DIJKSTRA-Algorithmus – auch mit negativen Kantengewichten operieren kann. Es werden auch prinzipiell andere Optimierungsverfahren realisiert, wie z.B. Bidirektionale

Suche [Poh71], bei der ausgehend von Start- und Ziel-Knoten abwechselnd zu dem anderen Knoten gesucht wird, weswegen die Laufzeitkomplexität von $O(b^{d/2})$ erreicht wird.

3.3.2. Spezielle Graphen: Probleme und Lösungen

Umgang mit Multigraphen

Bei der Beschreibung von Rechnernetzen werden oft spezielle Graphen benötigt. So können u.U. zwischen zwei Knoten, die der Netzinfrastruktur wie z.B. Router oder Switches entsprechen, Verbindungen mit unterschiedlichen Eigenschaften (in Graphen als Gewichte modellierbar) existieren. Für die Beschreibung solcher Situationen werden *Multigraphen* verwendet (siehe Abschnitt 3.3). Da die meisten Suchalgorithmen ausschließlich mit einfachen Graphen arbeiten, müssen zur Anwendung dieser Algorithmen die Multigraphen zu einfachen Graphen transformiert. Für diese Transformation müssen lediglich alle Kanten in zwei Teile aufgeteilt werden und zusätzlich ein neuer Knoten "in die Mitte" als ihr Verbindungsglied hinzugefügt werden (siehe Abbildung 3.8).

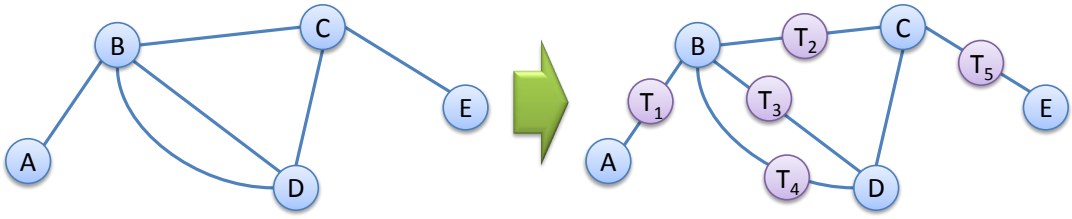


Abbildung 3.8.: Transformation von Multigraph zu einem einfachen Graph

Diese Vorgehensweise weist allerdings eine Reihe von Nachteilen auf. So steigt die Anzahl von Knoten und Kanten eines neuen Graphen ($|V_{new}| = |V_{old}| + |E_{old}|$ und $|E_{new}| = 2 \cdot |E_{old}|$), was sich auf die Suchlaufzeit und den Speicherbedarf auswirkt. Wie man in der Abbildung 3.8 deutlich sieht, werden alle Kanten transformiert, auch wenn das nicht immer notwendig ist. Damit ausschließlich mehrfache direkte Verbindungen "aufgebrochen" werden, wird eine komplexere Datenverwaltung sowie ein komplexerer Transformationsalgorithmus gebraucht. Ein anderer Aspekt, der ausschließlich bei gewichteten Graphen zum Vorscheint kommt, betrifft die Aufteilung des Kantengewichts bzw. die Bestimmung des Gewichts einer neuen Kante. Bei den additiven bzw. multiplikativen Aggregatfunktionen können das entsprechend 0 und 1 sein, bei den komplexeren Aggregatfunktionen und Typen von Gewichten, wie sie später im Kapitel 4 gebraucht werden, kann das eine Herausforderung darstellen.

Multi-Weighted Graphs

Eine wesentlich komplexere Herausforderung stellen Graphen mit mehreren Gewichten pro Kante (engl.: *Multi-Weighted Graphs*) dar. In Bezug auf Rechnernetze entspricht das der Situation, wenn gleichzeitig mehr als eine QoS-Eigenschaft für das

Routing relevant ist, wie z.B. Bandbreite, Delay und Fehlerrate einer Verbindung zwischen zwei Routern. Mehrfachgewichtete Graphen werden auch dann gebraucht, wenn neben den technischen Eigenschaften auch die Kosten einer Verbindung berücksichtigt werden sollen.

Darstellung im Vektorraum

Da die unterschiedlichen Eigenschaften i.A. voneinander unabhängig sind, hat sich in der Graphentheorie die Darstellung der Kantenwerte als Positionen in m-dimensionalen Vektorraum etabliert, wobei "m" für die Anzahl der mit jeder Kante verbundenen Eigenschaften steht. Somit werden auch die Operationen auf m-dimensionalen Werten, wie die Addition der einzelnen Kantengewichte auf dem Weg oder Vergleich miteinander, auf Operationen innerhalb einzelner Dimensionen zurückgeführt.

Aufgaben bei Multi-Weighted Graphen

In Bezug auf die Suche eines Weges in solchen Graphen wurde in der Graphentheorie eine Reihe von grundlegenden Aufgaben definiert, die in der Fachliteratur oft auch als *Probleme* referenziert werden. Für diese Arbeit sind vor allem die folgenden Probleme relevant:

Multi-constrained Path (MCP): Bei dieser Aufgabe muss ein beliebiger Pfad gefunden werden, der gleichzeitig mehreren Anforderungen genügt. Die Güte dieses Pfades (z.B. die Nähe oder Weite der Eigenschaften zu/von den spezifizierten E2E-Anforderungen) spielt dabei keine Rolle.

Constrained Shortest Path (CSP): Dabei wird ein nach nur einem Gewicht optimierter Pfad gesucht, der eine Reihe von E2E-Anforderungen erfüllt. Als das zu optimierende Gewicht spielen dabei oft die Anzahl der Hops oder die Verbindungskosten eine Rolle.

Multi-constrained Shortest Path (MCSP): In diesem Fall wird nach einem Pfad gesucht, der nicht nur wie bei CSP nach einem, sondern gleich nach allen relevanten Eigenschaften optimiert wird.

Alle diese Aufgaben sind NP-Vollständig [GJ79]. Um die Problematik zu verdeutlichen, eignet sich am Besten ein Beispiel mit zwei Gewichten, d.h. $m = 2$. In der Abbildung 3.9 werden die zweidimensionalen Gewichte der möglichen Pfade von Start- zum Zielknoten durch die Punkte repräsentiert. Die auf den kompletten Weg auferlegten Restriktionen L_1 und L_2 sind als Strichlinien eingezeichnet. Versucht man die für ein Gewicht optimierte Suchverfahren, wie z.B. das von DIJKSTRA, bei den Multi-Weighted Graphen wiederzuverwenden und bildet man dafür mehrere Gewichte mit Hilfe einer Funktion $d_1w_1(P) + d_2w_2(P)$ auf nur eines ab (in der Abbildung als parallele Linien angezeichnet), dann kann der so gefundene kürzeste Weg (im Bild – der umrandete Punkt) u.U. nicht alle Anforderungen erfüllen. Der Einsatz von anderen *m-zu-1* Abbildungsfunktionen ist auch möglich, ist jedoch immer mit einer Ungenauigkeit und einem Unsicherheitsfaktor verbunden. Der Rest des Abschnittes beschäftigt sich daher nur mit den exakten Lösungsansätzen.

Alle Aspekte der Multi-Weighted Graphen an dieser Stelle zu beschreiben würde wegen der Komplexität der Thematik den Rahmen dieser Arbeit sprengen. Ein sehr gu-

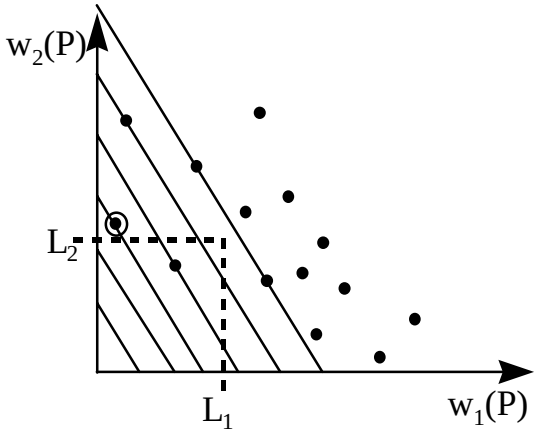


Abbildung 3.9.: Problem bei Abbildung von mehreren Gewichten auf einen [Kui04]

ter Überblick über die Entwicklung dieses Forschungsgebietes sowie eine Diskussion über die verwandten Probleme und Lösungsansätze kann z.B. in [Zie01] gefunden werden.

Non-dominance

Die Problematik der Suche in Multi-Weighted-Graphen entsteht vor allem dadurch, dass das der dynamischen Programmierung zugrunde liegende Optimalitätsprinzip von BELLMAN [Bel57] nicht mehr nur mit einem, sondern gleichzeitig mit mehreren Gewichten zurecht kommen soll. Das Prinzip besagt, dass, sollte ein Problem aus vielen gleichartigen Teilproblemen bestehen, dann setzt sich die optimale Lösung des Problems aus optimalen Lösungen der Teilprobleme zusammen. Übertragen auf die m-dimensionale Gewichte hat sich der Begriff von *non-dominance* etabliert: ein (Teil-)Weg W_1 ist nur dann non-dominant zu W_2 zwischen denselben Start- und End-Knoten, wenn für alle m Dimensionswerte gilt $w_{1,i} \leq w_{2,i}$, $\forall i : 1 \leq i \leq m$. Für einen Suchalgorithmus bedeutet das, dass nur ein non-dominanter Teilweg zu einem Zwischenknoten einen anderen Teilweg ersetzen darf, ansonsten müssen alle Alternativen als mögliche Teile des kompletten Weges betrachtet werden. Oft wird bei den Suchverfahren die Anzahl von solchen Alternativpfaden durch einen festen Wert "k" beschränkt, wodurch diese Methode der Komplexitätseinschränkung den Namen *k-shortest path* bekommen hat. Vergleichsweise muss bei dem DIJKSTRA-Algorithmus (siehe Abschnitt 3.3.1) an jedem Zwischenknoten immer nur ein Teilweg als optimaler betrachtet werden.

Mit der zunehmenden Bedeutung der multimedialen Dienste im Internet hat sich auch die Suche nach effizienten Algorithmen bei Multi-Weighted Graphen intensiviert. Viele solche Arbeiten sind unter den Schlagworten "QoS routing" und/oder "QoS aware routing" zu finden. Zu den Klassikern auf diesem Gebiet gehört der Algorithmus von JAFFE [Jaf84]. Aus den neueren Ansätzen kann z.B. der von KUIPERS entwickelte *SAMCRA* Algorithmus [Kui04] erwähnt werden, der sich der Lösung von MCP-Problem widmet. Es existieren auch weitere Ansätze, die sich auf dieses oder andere Probleme

der Multi-Weighted Graphen richten, wie z.B. der IDA*_MCSP-Algorithmus [LHH05] für das MCSP Problem. Um die Komplexität dieser spezialisierten Algorithmen zu illustrieren, wird in der Abbildung 3.10 der Pseudo-Code für SAMCRA-Algorithmus gezeigt; auf die Darstellung der dort verwendeten Hilfsfunktionen wird an dieser Stelle verzichtet.

```
SAMCRA(G, m, s, t, L)
1. INITIALIZE(G, m, s, t) → b⃗
2. while Q ≠ ∅
3. EXTRACT-MIN(Q) → u[i]
4. u[i] ← GREY
5. if u = t
6.     return path
7. else
8.     for each v ∈ adj[u]\{π[u[i]], s}
9.         FEASIBILITY(G, u, i, v, counter, d, w, maxlength)
           → dominated
10.        predicted_length ← l(d⃗[u[i]] + w⃗(u, v) + b⃗[v])
11.        if predicted_length ≤ maxlength
               AND dominated ≠ 1
12.            UPDATEQUEUE(Q, u, i, v, j, d, w, π, counter[v],
               predicted_length)
13.            if v = B AND
                   predicted_length < maxlength
14.                maxlength ← predicted_length
```

Abbildung 3.10.: Meta-code SAMCRA [Kui04]

3.3.3. Bewertung der Übertragbarkeit

Suchverfahren sind in der Graphentheorie immer noch ein spannendes Forschungsgebiet. Die bekanntesten Suchalgorithmen, wie z.B. von DIJKSTRA, können zwar einen besten Pfad in einer polynomialen Zeit finden, sind allerdings nur in der Lage höchstens mit einem additiven Gewicht zurechtzukommen. Die klassischen Verfahren können daher verwendet werden, um schnell eine prinzipielle Möglichkeit einer Verbindung zwischen zwei Knoten festzustellen. Bei relativ kleinen Graphen kann wegen ihrer Schnelligkeit und einfachen Datenverwaltung eine angepasste Tiefensuche verwendet werden, um eine akzeptable Lösung bei Berücksichtigung mehrerer Kantengewichte zu finden. Bei größeren Graphen kann der Einsatz von komplexeren Algorithmen wie SAMCRA notwendig werden. Weiterhin kann bei großen Graphen auch eine Re-

duktion der Komplexität vor der eigentlichen Suche wesentliche Abhilfe in Bezug auf Suchlaufzeit und Speicherbedarf schaffen.

Ein weiterer Aspekt hängt mit den Aggregat- und Ordnungsfunktionen zusammen. In der Graphentheorie werden bei der Berechnung des Pfadgewichtes ausschließlich additive Aggregatfunktionen und beim Vergleich der Pfade das kleinere Gewicht als das bessere angenommen. Diese Vorgehensweise kann nur für ein Teil der Dienstgüteeigenschaften angewendet werden. Dadurch entsteht der Bedarf für eine Verallgemeinerung dieser zwei Funktionen, die im Zusammenhang mit QoS-Parametern definiert werden müssen (vergleiche dazu auch die entsprechende Diskussion im Abschnitt 3.2). Weiterhin müssen auch die Suchalgorithmen so modifiziert werden, dass sie verallgemeinerte QoS-bezogenen Funktionen verwenden können.

3.4. ITSM-Standards und Recommendations

Das Management von IT-Diensten wird von einer Reihe von IT-Service-Management (ITSM) Frameworks adressiert. In diesem Abschnitt werden ITIL und NGOSS präsentiert, die eine De-facto-Standard Stellung haben und sich auf unterschiedliche Aspekte fokussieren. Andere bekannte Frameworks – wie z.B. MOF [MOF08] – gehen relativ ähnliche Wege und schlagen vergleichbare Ansätze und Herangehensweisen vor.

3.4.1. ITIL v.2, ITIL v. 3 und ISO20000

Die *IT Infrastructure Library* (ITIL) wurde im Auftrag der Britischen Regierung in den 1980er Jahren vom *Office of Government Commerce* (OGC), das damals noch *Central Computer and Telecommunications Agency* (CCTA) hieß, herausgegeben und bis Ende der 1990er von OGC weiterentwickelt [ITI08]. ITIL in der Version 2 wurde ab 1999 eingeführt. Die thematischen Module von *ITIL V2* wurden bis 2006 ständig aktualisiert und ergänzt, sodass diese Version zum Schluss aus sieben Bändern bestand, die sich unterschiedlichen Sachgebieten widmen. In dieser Periode hat ITIL sehr große Verbreitung und den Status eines De-facto-Standards erreicht. ITIL besteht aus einer Sammlung von Empfehlungen zur Strukturierung von ITSM-Prozessen, die sich in der Praxis bewährt haben. Im anglosächsischen Raum werden diese Empfehlungen als *best practice* oder auch *common practice* referenziert.

Um mit der Zeit voranzuschreiten und neuen Herausforderungen gerecht zu werden, wurde im Dezember 2005 eine komplette Überarbeitung der Version 2 angestoßen. Im Mai 2007 erfolgte die Publikation der fünf Bücher von *ITIL V3*, welche die vorherige Version ablösen. Während ITIL V2 sich auf die Definition einzelner ITSM-Prozesse konzentriert, ist das Blickfeld von ITIL V3 um einiges breiter ausgelegt. In V3 behalten die Prozesse aus Version 2 ihre Gültigkeit, werden aber ergänzt und in einem durchgängigen Lebenszyklus, beginnend mit der strategischen Planung von Diensten, eingebettet. Dies soll eine bessere Ausrichtung an den Business-Zielen ermöglichen.

Da ITIL kein formeller Standard ist, ist auch die Zertifizierung nur bedingt möglich. Es ist zwar möglich, die Mitarbeiter eines Unternehmens als "ITIL-compliant" zu zertifizieren, nicht aber Unternehmen selbst oder ihre ITSM-Prozesse. Die Zertifizierung der IT-Mitarbeiter und -Manager, die in der Form einer Prüfung durchgeführt wird, dient nur als Nachweis über ihre im Zusammenhang mit ITIL gewonnenen Fachkenntnisse. Um auch die Zertifizierung von Unternehmen zu ermöglichen, wurde im Dezember 2005 der Standard *ISO/IEC 20000* (oft auch *ISO 20000* oder *ISO 20k* genannt) verabschiedet. Der Standard definiert notwendige Mindestanforderungen an ITSM-Prozesse, die eine Organisation etablieren muss, um IT-Services in definierter Qualität bereitstellen und managen zu können.

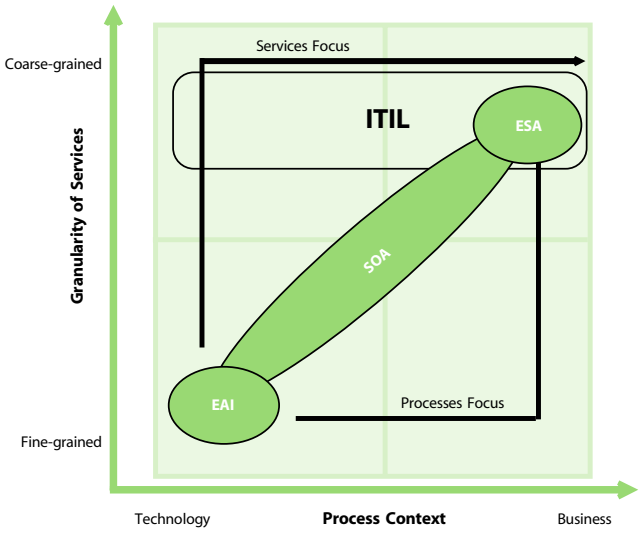


Abbildung 3.11.: Fokus von ITIL [Off07c]

OGC hat von Anfang an versucht, mit ITIL das IT-Service-Management allgemein und nicht für einen spezifischen Dienst anzusprechen. Aus diesem Grund werden die ITSM-Prozesse von ITIL und ISO 20000 relativ grobgranular beschrieben (siehe Abbildung 3.11). Es werden lediglich die Prozesse selbst, ihre Ziele und deren Zusammenspiel beschrieben; die konkrete Realisierung einzelner Prozesse wird von ITIL als zu szenariospezifisch angesehen und daher nicht spezifiziert.

Einer der zentralen Begriffe von ITIL und ISO 20000 ist der Dienstlebenszyklus. Die Phasen eines Dienstes werden dabei im Zusammenhang mit den Kundenbedürfnissen und den Phasen in der Kundenorganisation betrachtet (siehe Abbildung 3.12). Der Lebenszyklus beginnt damit, dass der Kunde den Bedarf identifiziert und Anforderungen an einen neuen Dienst formuliert. Erst dann wird der Dienst bei dem Service Provider bestellt. Daraufhin implementiert der Service Provider die bestellte Instanz eines Dienstes. In der Betriebsphase muss der Dienst überwacht werden, was eine Eingabe für Analyse-Reviews und für Dienstverbesserungsmaßnahmen liefert. Das Ende der Dienstinstanz wird durch die bei dem Vertragsabschluss ausgehandelten Bedingungen bestimmt.

Sowohl ITIL als auch ISO 20000 haben das kundenorientierte Servicemanagement als Hauptziel. Um dieses Ziel zu erreichen, werden alle ITSM-Prozesse zu unterschiedlichen Managementbereichen zusammengefasst. Diese Bereiche unterscheiden sich voneinander durch ihre Ausrichtung und die Ziele, die durch ihre Prozesse erreicht werden sollen. Das Zusammenspiel dieser Bereiche beim Design eines neuen Service ist in der Abbildung 3.13 dargestellt. Das Service-Level-Management (SLM) wird dabei als einer der zentralen Bausteine des gesamten Servicemanagements verstanden.

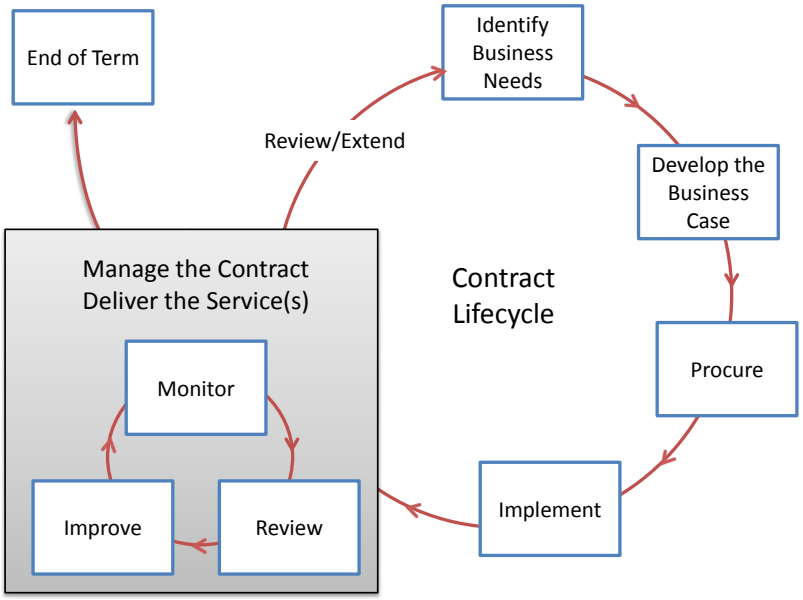


Abbildung 3.12.: Contract Lifecicle (nach [Off07d])

Bei der Beschreibung der Ziele und Aufgaben des Service-Level-Managements liegt bei beiden Rahmenwerken (ITIL und ISO 20000) der Fokus auf der Erbringung eines IT-Dienstes innerhalb einer Organisation. Als Abnehmer des erbrachten IT-Dienstes können sowohl organisationsinterne Abteilungen als auch externe Kunden auftreten. Es wird weiterhin davon ausgegangen, dass der Dienst entweder komplett basierend auf eigenen Ressourcen oder auch (teilweise) auf Basis der von anderen Service Provider eingekauften Teildienste realisiert wird. Auch wenn ITIL die Existenz anderer Formen der Zusammenarbeit erwähnt, bei der Prozessdefinition wird explizit davon ausgegangen, dass die Organisationsbeziehungen zwischen dem Serviceprovider und den u.U. miteinbezogenen externen Providern von Teildiensten hierarchisch aufgebaut sind. Über die Komposition eines kompletten Dienstes aus den Teildiensten wird dabei keine Aussage gemacht.

Als das Hauptziel des Service-Level-Managements wird das Einhalten der vereinbarten QoS-Wertebereiche für alle IT-Dienste verstanden. Dabei wird betont, dass alle Qualitätsziele erreichbar sein müssen. Dieses Ziel wird in einer Reihe von Teilzielen verfeinert, die wie folgt definiert sind:

- Definieren, Dokumentieren, Vereinbaren, Überwachen, Messen und Überprüfen der Grenzbereiche aller angebotenen IT-Dienste
- Verbessern der Beziehungen und der Kommunikation mit dem Business der eigenen Organisation sowie mit den Kunden
- Sicherstellen, dass ausschließlich messbare Parameter in die Entwicklung neuer IT-Dienste aufgenommen werden

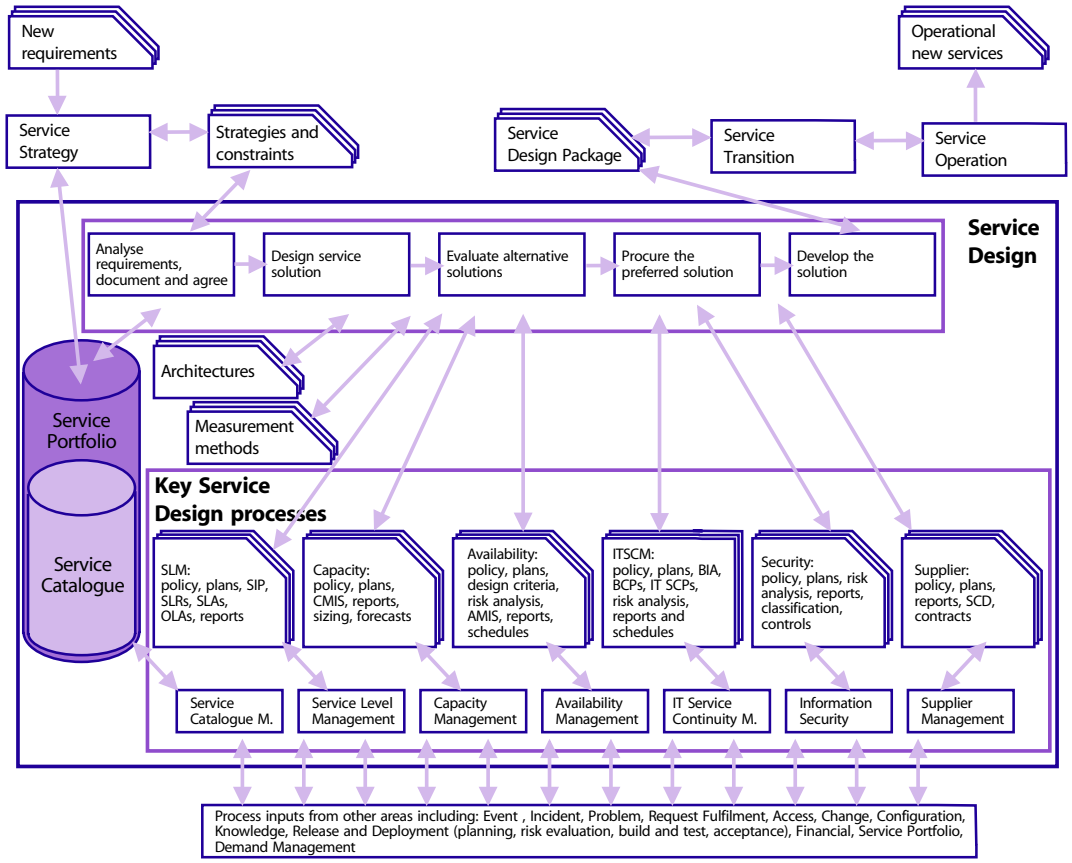


Abbildung 3.13.: Service Design – the big picture [Off07a]

- Überwachen und Verbessern der Kundenzufriedenheit mit der angebotenen Dienstgüte
- Sicherstellen, dass sowohl IT als auch Kunden klare unmissverständliche Vorstellungen und Erwartungen an die Dienstgüte haben
- Vorbereiten von proaktiven Maßnahmen zur kontinuierlichen Überwachung und Verbesserung des Dienstes und seiner Dienstgüte

In ITIL werden weiterhin eine Reihe von Aktivitäten von Prozessaktivitäten definiert, die für das Erreichen der gesetzten Ziele notwendig sind (siehe Abbildung 3.14):

- Erfassen, Vereinbaren und Dokumentieren neuer oder veränderter Anforderungen an den Dienst sowie die kontinuierliche Überprüfung dieser Ziele während des ganzes Lebenszyklus eines Dienstes

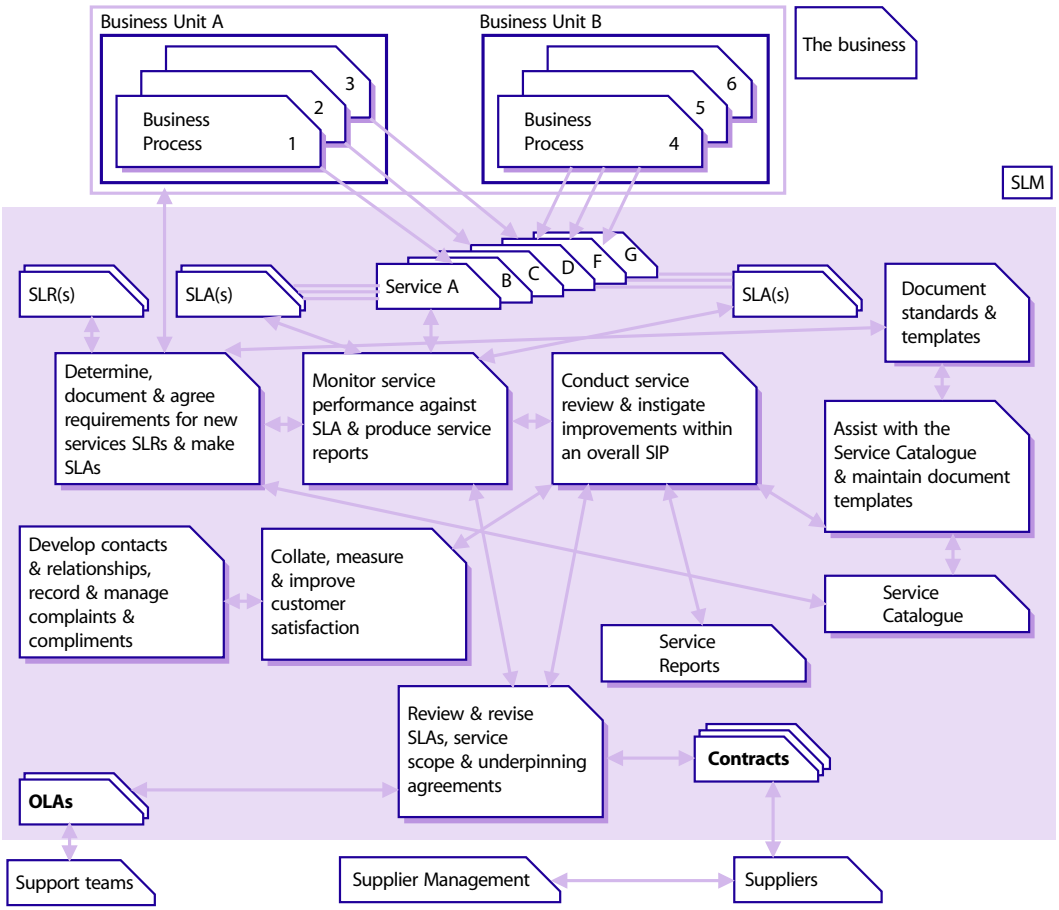


Abbildung 3.14.: The Service Level Management Process [Off07a]

- Überwachung der erzielten Servicequalität und Vergleich mit den im SLA festgelegten Zielen
- Erfassen und Verbessern der Kundenzufriedenheit
- Erstellen von Berichten
- Anhand der kontinuierlichen Dienstüberprüfung einen Plan erstellen, wie der Dienst verbessert werden kann
- Überprüfen und bei Bedarf überarbeiten des SLA und aller relevanten Verträge mit den organisationsinternen bzw. externen Anbietern der Teildienste
- Ausbauen und Dokumentieren der Kontakte mit Kunden sowie anderen interessierten Parteien
- Vorbereitung und Pflege von Prozeduren zur Erfassung der Beschwerden und zu deren Behebung

- Erfassen und Behandeln von Beschwerden
- Bereitstellen von Managementinformationen, die für die Verbesserung der Dienstgütemanagements und für die Demonstration der erreichten Ziele geeignet sind
- Pflegen und Bereitstellen der SLM-Dokumentation

Der Fokus der knapp 15 Seiten umfassenden Beschreibung des Service-Level-Managements liegt dabei ausschließlich auf Maßnahmen innerhalb einer Organisation, die einen IT-Dienst anbietet. Die Beschreibung beschränkt sich auf die grobe Auflistung der benötigten Aktivitäten sowie auf deren Zusammenspiel. Auf die mögliche Realisierung der Vorschläge wird dabei aus Gründen der Allgemeingültigkeit nicht eingegangen.

3.4.2. eTOM und NGOSS

Die *enhanced Telecom Operations Map* (eTOM) ist ein von *TeleManagement Forum* (TMF) entwickeltes Rahmenwerk, die Geschäftsprozesse von Telekommunikationsunternehmen und IT-Dienstleisten im Fokus hat. Die Zielsetzung von eTOM ist mit der von ITIL vergleichbar – die Schaffung eines gemeinsamen Verständnisses über die Geschäftsprozesse. Die Standardisierung dieser Prozesse soll dazu beitragen, die Effizienz dieser Prozesse sowohl innerhalb einer Organisation als auch bei der Kooperation zwischen Organisationen zu steigern.

Auch wenn die grundsätzlichen Ziele von ITIL und eTOM sehr ähnlich sind, bieten diese Frameworks in vielerlei Hinsicht unterschiedliche Konzepte. Das liegt sowohl an deren Entstehungsgeschichte als auch an deren Fokus. So liegt der Interessenfokus von ITIL auf Prozessen mit vielen menschlichen Interaktionen. Die Prozesse von eTOM sind dagegen für die TK-Branche konzipiert, die sehr stark auf eine durchgehende Automatisierung angewiesen ist. Alle Prozesse in eTOM sind entsprechend ihrer Ausrichtung in drei große Bereiche gruppiert (siehe Abbildung 3.15). Die Struktur sieht eine hierarchische Dekomposition vor, sodass eine Prozessschichtung ermöglicht wird, bei der Prozesse auf die Funktionalität der darunterliegenden Schicht aufbauen können.

Zusammen mit *Shared Information and Data Model* (SID) [TMF04b] und Richtlinien der *Technology Neutral Architecture* (TNA) [TMF04a] bildet eTOM eine der Säulen für das ehrgeizige TMF-Projekt NGOSS (*New Generation Operations Systems and Software*). In NGOSS soll eine herstellerunabhängige Architektur definiert werden, die den Aufbau kompletter Management-Lösungen aus Modulen mit standardisierten Schnittstellen erlaubt.

Das NGOSS SLA Management Handbook [TMF04c, TMF04d, TMF04e, TMF04f] legt das Hauptaugenmerk auf die Maßnahmen innerhalb eines Telekommunikationsunternehmens, die Dienstgütezusicherungen für die angebotenen Services ermöglichen. Den Kern jedes dieser Bücher bilden Überlegungen, wie die zugrundeliegenden Dienste

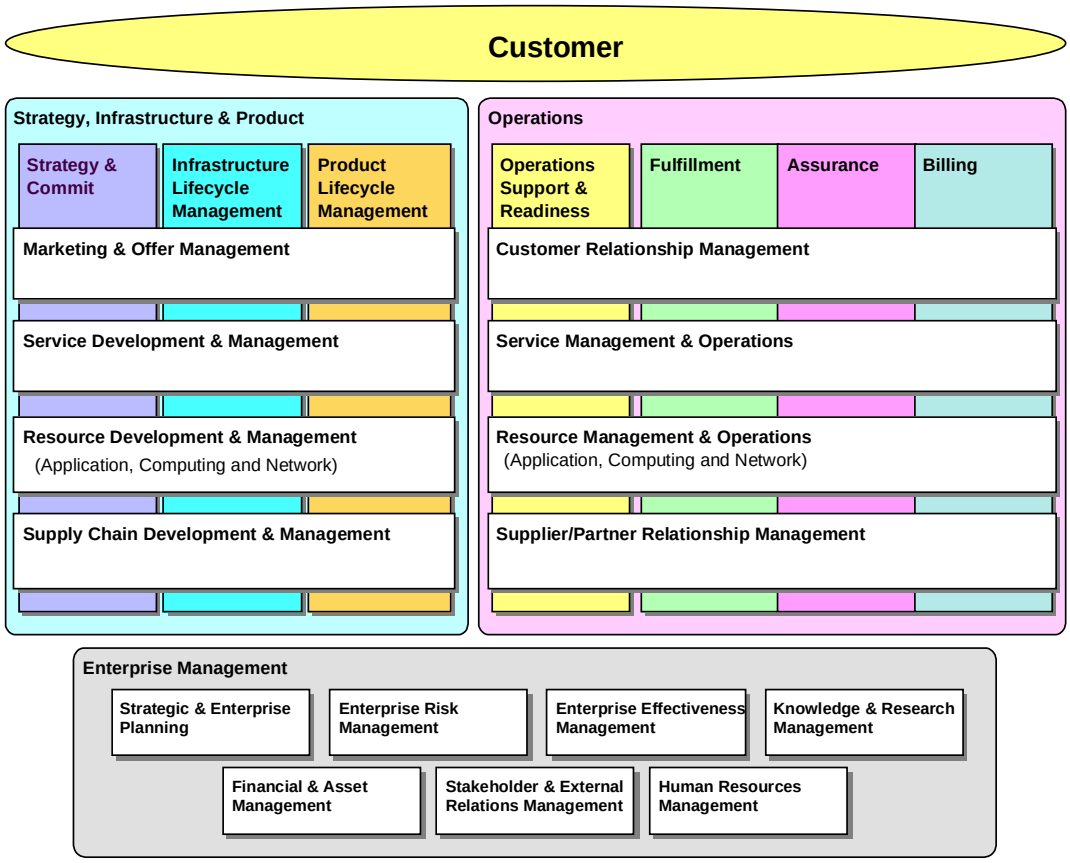


Abbildung 3.15.: eTOM Business Process Framework – Level 1 Processes [TMF07a]

und ihre messbaren KPIs (*Key Performance Indicators*) mit den darauf aufgebauten Diensten und dafür zugesicherten KQIs (*Key Quality Indicators*) zusammenhängen (siehe Abbildung 3.16).

Obwohl der Detaillierungsgrad des SLA Management Handbook um ein Vielfaches die Beschreibung dieser Thematik in ITIL übersteigt, bleibt NGOSS dennoch auf einem allgemeinen Niveau, so dass die besprochenen Zusammenhänge auf beliebige Dienste und Dienstzusammenhänge übertragbar sind. Abbildung 3.17 zeigt z.B. den Einfluss von SLAs auf die Dienstqualität aus Kundensicht.

Ähnlich wie bei ITIL spielt auch in NGOSS der Dienstlebenszyklus eine wichtige Rolle. Im Gegensatz zu ITIL und ISO 20000, die einen kundenzentrischen Lebenszyklus einführen, steht in NGOSS der Service Provider im Mittelpunkt. Der NGOSS-Lebenszyklus beginnt mit der Entwicklung eines neuen Dienstes. Weiter folgen die Lebenszyklusphasen Verhandlung und Verkauf, Inbetriebnahme, Betrieb, Anpassung und Dienstauflösung. Genauso wie in ITIL spielt auch hier das permanente Feedback eine wichtige

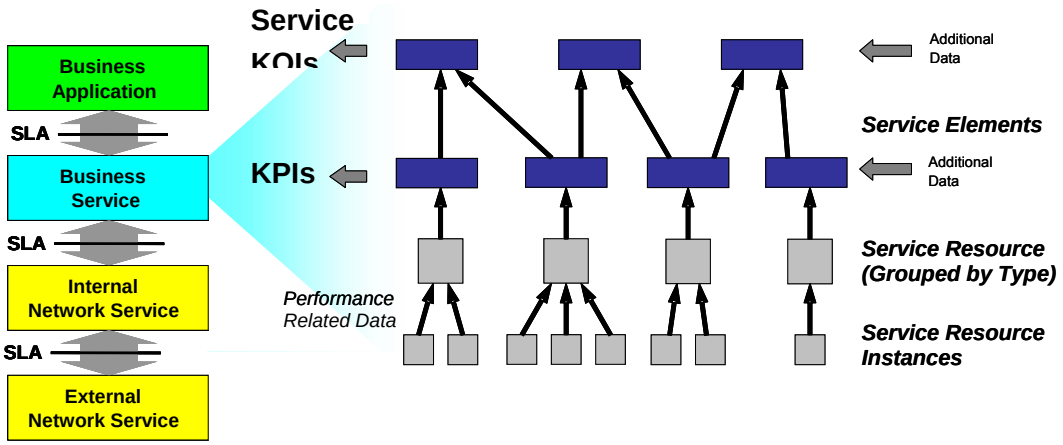


Abbildung 3.16.: Relationship between Service Resources, KQI, and KPI [TMF04f]

Rolle, um den Dienst und seine Eigenschaften – vor allem die zugesicherten QoS-Parameter –, bei Bedarf anzupassen.

Da NGOSS aus dem Telekommunikationsumfeld kommt, wird auch auf eine mögliche horizontale Kopplung der Teildienste und dadurch entstehende Dienstketten eingegangen. NGOSS geht davon aus, dass Dienste mit Hilfe sowohl vertikaler als auch horizontaler Kopplung von Teildiensten entstehen können. Bedauerlicherweise beschränkt sich NGOSS lediglich auf die Feststellung der Tatsache, dass die Ende-zu-Ende Dienstgüte aus den Teildiensten-QoS/SLAs zusammengesetzt wird (siehe Abbildung 3.18). NGOSS präsentiert allerdings weder einen Ansatz noch gibt es Vorschläge, wie die erforderliche E2E-QoS/SLA auf die Teildienste-QoS/SLAs abgebildet werden können.

3.4.3. Bewertung der Übertragbarkeit

Beide, ITIL und NGOSS, sind auf Maßnahmen innerhalb eines Service Providers fokussiert. In beiden Rahmenwerken werden die Maßnahmen, die in Bezug auf eine einzelne Dienstinstanz von dem Service Provider durchgeführt werden müssen, in das Lebenszyklus eingeordnet. Interessant ist vor allem der Fakt, dass die Zielsetzung einzelner Dienstlebenszyklusphasen den Aufgaben entspricht, die im Abschnitt 2.4.3 in Form von Use Cases zusammengefasst wurde.

Da beide Rahmenwerke sehr allgemein gehalten wurden, können sie nicht direkt als Teil der problembezogenen technischen Lösung übernommen werden. Dennoch identifizieren diese Rahmenwerke eine Reihe von Aspekten, die im Rahmen dieser Arbeit berücksichtigt werden müssen. Um ein Beispiel dafür zu nennen, spricht NGOSS davon, dass die Ende-zu-Ende Dienstgüte sich aus der Dienstgüte aller beteiligten Teil-

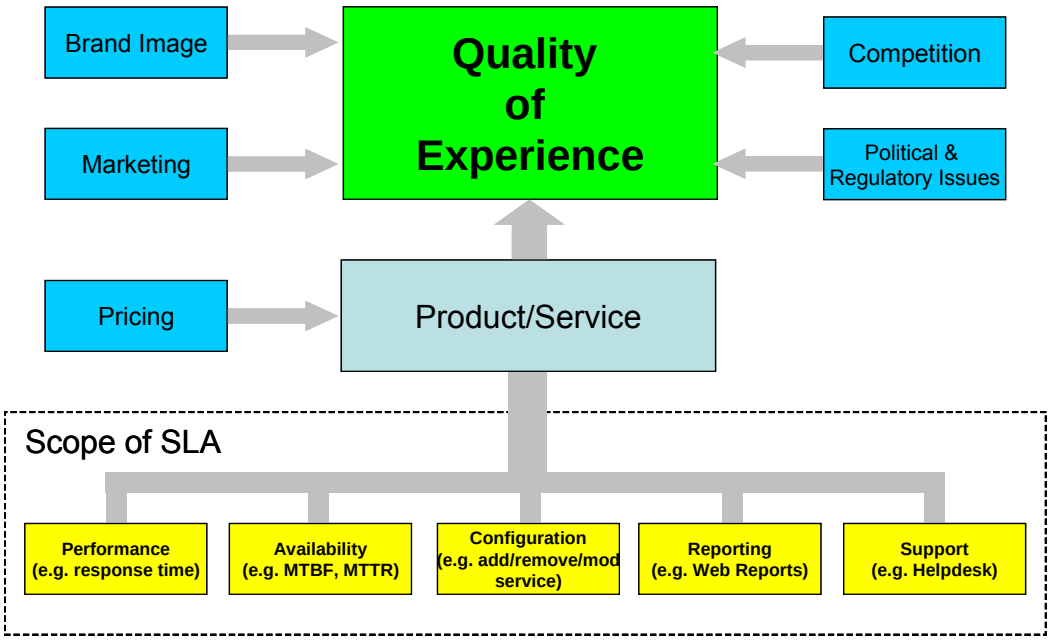


Abbildung 3.17.: Role of the SLA in the Customer Quality of Experience (QoE) [TMF04f]

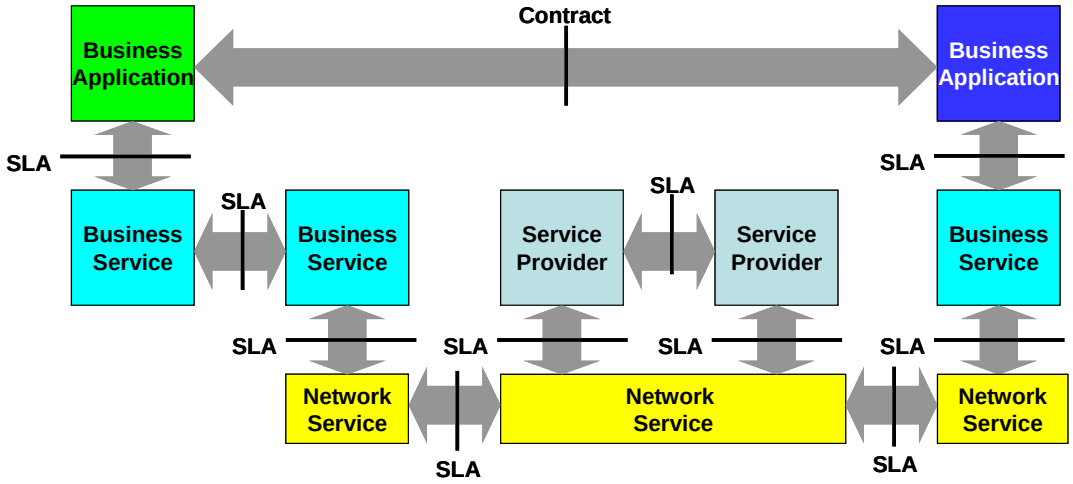


Abbildung 3.18.: Expanded View of SLA in Achieving the End-to-End SLA [TMF04f]

dienste zusammensetzt. Gleichzeitig mahnt ITIL ausschließlich erreichbare Dienstgütewerte zuzusichern.

SLM ist kein alleinstehender Managementprozess ist, sondern interagiert mit anderen Managementprozessen. So müssen die Dienstinstanzen sowie die beteiligten Teildienste nicht nur überwacht, sondern auch diese Informationen an andere Prozesse weitergereicht werden, wie z.B. an das *Incident&Problem Management* bei der Verletzung vereinbarter Grenzwerte.

3.5. E2E-QoS bei Hierarchien

Frage nach der E2E-Dienstgütezusicherung bei einer Dienstkette stellt sich auch dann, wenn diese dem Kunden als kompletter Dienst von einem einzigen Service Provider angeboten wird, bei der Erbringung der Teildienste aber mehrere Organisationen beteiligt sind. In diesem Abschnitt wird beschrieben, wie diese Situation bei hierarchischen Organisationsbeziehungen üblicherweise behandelt wird.

3.5.1. Maßnahmen zur Sicherung von E2E-QoS

Die Zusicherung von E2E-QoS bei Hierarchien zeichnet sich durch baumförmige Entscheidungs- und oft auch Kommunikationsstrukturen aus. Dabei durchläuft eine Dienstinstanz mehrere Lebenszyklusphasen, in denen verschiedene Managementaufgaben gelöst werden.

Als erstes werden Kundenanforderungen an eine neue Dienstinstanz geklärt. Dazu zählen sowohl Nutz- als auch Managementfunktionalität sowie die Grenzwerte für die E2E-QoS. Nachdem die Kundenanforderungen an die neue Dienstinstanz geklärt sind, beginnt der Service Provider mit der Analyse, was in Eigenregie erbracht werden kann und was als Teildienste von anderen Providern, die in dem Kontext als *Sub-Provider* agieren, hinzugekauft werden soll. Für die Identifikation der potenziellen Sub-Provider und deren Teildienste bestehen grundsätzlich zwei Möglichkeiten:

Identifikation der Sub-Provider

- Der Service Provider kann alle bekannten Sub-Provider direkt kontaktieren. Dabei wird entweder direkt gefragt, ob ein Teildienst mit den exakt definierten QoS-Parametern geliefert werden kann, oder es werden Randbedingungen für den Teildienst spezifiziert und der Sub-Provider kann daraufhin ein Angebot vorbereiten und dem Service Provider vorlegen.
- Eine Alternative zu einer direkten Kontaktaufnahme stellt eine Ausschreibung dar. In der Ausschreibung werden Bedürfnisse und Randbedingungen sowie die Frist für das Vorlegen des Angebots bekannt gegeben. Die Sub-Provider, die Interesse daran haben, können ein Angebot vorbereiten und dem Service Provider vorlegen.

Im öffentlichen Dienst sind solche Vorgänge gesetzlich geregelt, in vielen Fällen wird eine öffentliche Ausschreibung gefordert und der minimale Zeitrahmen dafür festgelegt (siehe [CIO08a], insbesondere [CIO08b]).

In beiden Fällen erfährt der Service Provider, welche Teildienste von welchen Sub-Providern erbracht werden können und welche QoS-Grenzwerte (in Bezug auf die erforderlichen Nutz- als auch Managementfunktionalitäten) diese Sub-Provider für ihre Teildienste garantieren können. Basierend auf diesen Informationen und eigenen

Kriterien entscheidet der Service Provider, welche der möglichen Teildienste für die Diensterbringung miteinbezogen werden sollen und welche QoS-Grenzwerte die Teildienste einhalten sollen, damit dem Endkunden die erwünschte E2E-Dienstgüte zugesichert werden kann.

Normalerweise werden erst nach dem Vorlegen eines Angebotes beim Kunden und seinem ausdrücklichen Einverständnis dazu zwischen dem Service Provider und seinen Sub-Providern entsprechende Verträge geschlossen. Die Zusicherungen der Sub-Provider werden in sog. *Underpinning Contracts* (UCs) festgehalten. Der Service Provider bestimmt auch, welche zusätzliche (nicht direkt mit den Kundenanforderungen korrelierende) Managementfunktionalität die Teildienste aufweisen sollen, sowie die Kommunikationswege zwischen Sub-Providern und u.U. anderen Rollen. Diese Festlegungen bilden einen integralen Teil von UCs.

Auch wenn die Kommunikation zwischen Sub-Providern u.U. direkt und nicht über den SP läuft und/oder die Monitoring- und Reporting-Daten von den Teildiensten an eine Drittorganisation gegeben werden sollen, wird die Entscheidung darüber immer von der beantragenden SP-Organisation getroffen. Genauso werden vom Service Provider Vorschriften festgelegt, wie kundenrelevante QoS-Werte aus Sub-Provider-spezifischen QoS-Werten errechnet werden sollen. Solche Berechnungsvorschriften, die oft auch als *Aggregatfunktionen* bezeichnet werden, werden normalerweise auch mit dem Kunden abgestimmt und im SLA festgehalten. Weiterhin legt der Service Provider noch während der Verhandlungsphase alle für die Dienstüberwachung relevanten Parameter fest wie z.B., zwischen welchen Messpunkten welche Messmethoden mit welcher Häufigkeit zum Einsatz kommen sollen. Dasselbe gilt auch für weitere Aspekte, die erst in den späteren Phasen des Dienstlebenszyklus relevant werden wie z.B., eine Berechtigung die QoS-Grenzwerte anzupassen oder die Dienstinstanz noch vor dem ursprünglich vereinbarten Termin abzubestellen.

Aggregatfunktion: Vorschrift zur QoS-Abbildung

Bei der Vertragsunterzeichnung mit dem Kunden, bevor UCs abgeschlossen werden, besteht ein gewisses Risiko, dass die gewählten Sub-Provider die angebotenen Teildienste nicht liefern können, z.B. weil die benötigten Ressourcen bereits für andere Teildienste verwendet wurden. Auf der anderen Seite garantiert der Abschluss einer Reihe von UCs noch nicht den Vertragsabschluss mit dem Kunden, was zu unnötigen Kosten beim Service Provider führen kann. Diese Situation wird von SP-Organisationen unterschiedlich angegangen. Als eine Alternative zu den zwei o.g. Vorgehensweisen kann auch ein Abschluss von vorläufigen Verträgen mit den Sub-Providern erfolgen, die dafür sorgen, dass die benötigten Ressourcen für die entsprechende Teildienste reserviert werden; erst nach dem Abschluss eines Vertrages mit dem Kunden werden daraus richtige UCs, ansonsten können die reservierten Ressourcen freigegeben werden.

Nach dem Vertragsabschluss beginnt die Inbetriebnahmephase. Wie die Provider der einzelnen Teildienste in dieser sowie in weiteren Phasen des Dienstlebenszyklus miteinander arbeiten, ist zu dem Zeitpunkt bereits festgelegt: Die Rollenzuweisung und

Aufgabenverteilung sowie die Informationen und die Informationskanäle für alle Aufgaben in späteren Phasen des Dienstlebenszyklus werden bereits während der Verhandlungsphase festgelegt. Viele technische Aspekte, wie z.B. exakte Parameter für die Zusammenschaltung benachbarter Teildienste (bei optischen Verbindungen wären das u.a. die Wellenlänge, Multimode/Monomode, Konnektor-Type), werden jedoch erst während der Inbetriebnahmephase bestimmt. So können evtl. notwendige Anpassungen bei der Zusammenschaltung erfolgen, etwa zur Kostenoptimierung.

Die Inbetriebnahmephase endet typischerweise mit einer Reihe von Abnahmetests, die in den Verträgen mit den Sub-Provider definiert wurden. Solche Tests sind nicht Bestandteil des Vertrages mit dem Customer, weil der interne Aufbau des Dienstes vor ihm so gut wie immer verborgen bleibt. Nachdem alle Teildienste in Betrieb genommen und zusammengeschaltet wurden, wird der komplette Dienst getestet. Bei Problemen werden Prozeduren gestartet, die die Ursache finden und beheben sollen. Die Inbetriebnahmephase endet mit einem erfolgreichen E2E-Abnahmetest.

Im Betrieb werden sowohl alle Teildienste als auch der komplette Dienst kontinuierlich überwacht. Die Art und Weise des Monitorings (Messmethoden, Messpunkte, usw.) sowie, wie diese Daten abgeholt und bearbeitet (z.B. aggregiert und mit den vordefinierten Zielsetzungen verglichen) werden, wird in den Verhandlungs- und Inbetriebnahmephasen festgelegt. Dasselbe trifft auch auf das Reporting und auf die Managementfunktionalität zur Anpassung im Betrieb und Abbestellung der Dienstinstanz zu.

3.5.2. Bewertung der Übertragbarkeit

Bei der Durchführung des technischen Service-Level-Managements im Rahmen hierarchischer Organisationsbeziehungen mit allen Providern der Teildienste müssen die in Abschnitt 2.4.3 als Use Cases erfassten Aktivitäten bewältigt werden. Gleichzeitig zeichnet sich auch eine Reihe von Abweichungen bei der Umsetzung der Aufgaben ab, die auf ihre Relevanz für Verkettete Dienste untersucht werden müssen.

So zeigt sich, dass nicht nur die Abbildung der Kundenanforderungen auf die Teildienste, sondern auch die Definition der Rollen und deren Zuweisung sowie die Festlegung einer Reihe von internen (für den Kunden nicht sichtbaren) Managementfunktionen bereits in der Verhandlungsphase geschieht. Diese Festlegungen bestimmen dann alle Prozesse und Interaktionseigenschaften in den darauffolgenden Phasen des Dienstlebenszyklus.

Die Aufteilung der Planung in zwei Phasen wurde bereits bei Géant2 E2E Links in Abschnitt 2.3.2 erwähnt, rückt jedoch noch stärker in den Vordergrund. Diese Aspekte können zwar nicht als technisch relevante Anforderungen betrachtet werden, werden bei der Erarbeitung der Lösung dennoch berücksichtigt.

Aus technischer Sicht wird auch eine Alternative zur direkten Abfrage der SP-Domänen gezeigt – eine Ausschreibung für die benötigten Teildienste. Verglichen mit den anderen im Kapitel 2 besprochenen Methoden räumt diese Möglichkeit wesentlich mehr Flexibilität den Service Providern ein. Sie erlaubt u.U. ein besseres Angebot für die benötigten Teildienste zu bekommen. Die Kehrseite der Medaille besteht dabei allerdings im wesentlich höheren Zeitbedarf.

3.6. SLM in Transportnetzen

Obwohl Transportnetze i.a. nicht direkt kundenorientiert sind, ist die zu bewältigende Problematik sehr ähnlich mit Verketteten Diensten. In diesem Abschnitt wird zunächst eine Netzbeschreibungstechnik präsentiert, die den Umgang mit der Komplexität des Problems erst ermöglicht. Weiterhin wird im Abschnitt gezeigt, welche Ansätze für das domänenübergreifende Monitoring entwickelt wurden. Eine Zusammenfassung der Ideen, die als Lösungsbausteine der SLM-Architektur wiederverwendet werden können, wird wie üblich im Bewertungsteil vorgenommen.

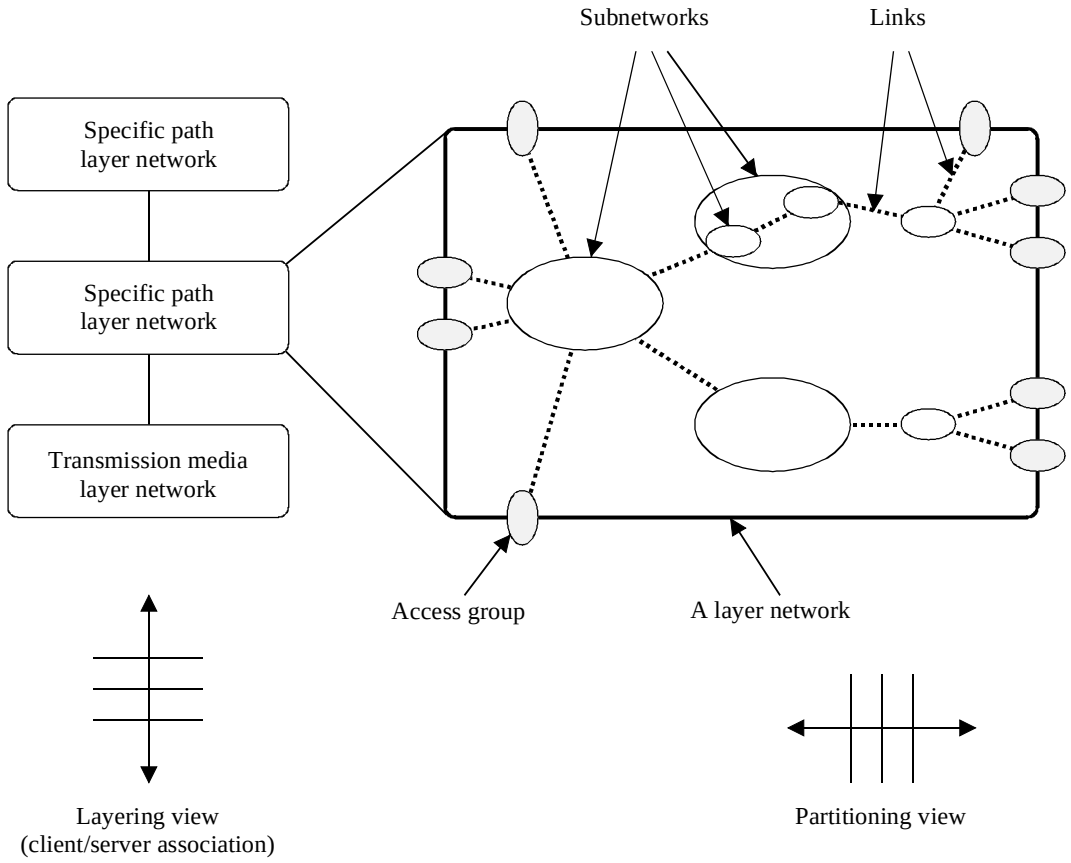
3.6.1. Layering und Partitionierung

Die ITU-T Empfehlung G.805 [ITU00] befasst sich mit der generischen Beschreibung eines Transportnetzes. Die Beschreibung in dieser Empfehlung geht von verbindungsorientierten Transportdiensten aus; eine an die Bedürfnisse verbindungsloser Dienste angepasste Empfehlung wird von ITU-T als G.809 [ITU03c] spezifiziert. In beiden Empfehlungen werden zwei Techniken – *Layering* und *Partitioning* – diskutiert, die im weiteren Verlauf dieses Abschnittes beschrieben werden.

Die *Schichtung* (engl.: *Layering*) erlaubt es, logische Verbindungen getrennt von den dafür verwendeten physischen Ressourcen und gewählten Routen zu betrachten. Schichtung baut auf dem Client/Service-Konzept auf, dabei wird ein Client-Signal vom Service transportiert. Das Client/Service-Konzept ist rekursiv und erlaubt den Aufbau von mehreren logischen Schichten (engl.: *stack of layers*). Jede Schicht ist dabei durch eine Reihe von Eigenschaften charakterisiert, die sich in G.805 auf die Signaleigenschaften beziehen, wie z.B. die Bandbreite und die Kodierung. Dadurch unterscheidet sich dieses Schichtenmodell vom OSI Schichtenmodell (ITU-T X.200 [ITU94a]), in dem Protokolle auf anderen (darunter liegenden) Protokollen aufbauen.

Ein so gewähltes Schichtenmodell trägt zur besseren Handhabung einer großen Anzahl von Signaleigenschaften bei, die durch die Vielfalt der eingesetzten Technologien und HW-Hersteller zu Stande kommen. Der Zugriff auf die jeweilige Schicht geschieht über sog. *Access Points* (APs). Das Schichtenmodell sieht vor, dass alle APs mit denselben Eigenschaften miteinander verbunden werden können. Um benachbarte Schichten zu verbinden, führt ITU-T drei Funktionen ein: *Adaptation*, *Termination* und *Connection*. Diese Funktionen sind dafür zuständig, die Nachrichtenströme zu identifizieren, die Signaleigenschaften an die Eigenschaften der jeweiligen Schicht anzupassen und bei bestehender Verbindung den Nachrichtenstrom innerhalb einer Schicht zu transportieren.

Auch wenn die Schichtung die Komplexität der Netzbeschreibung dramatisch reduziert, können in jeder Schicht beliebig komplexe Verbindungen zwischen Elementen



a) Layering concept **b) Partitioning concept**

Abbildung 3.19.: Layering and Partitioning [ITU00]

dieser Schicht existieren. Um auch diese Komplexität zu reduzieren, wird vorgeschlagen, logisch zusammenhängenden Komponenten zu Subnetzen bzw. Partitionen zusammenzufassen (siehe Abbildung 3.19).

Somit besteht ein *Layer Network* aus einer Reihe miteinander verbundener Sub-Netze. Die Zugriffspunkte zu dem Layer Network werden als *Access Groups* und die zu den Sub-Netzen als *Ports* referenziert. Einzelne Sub-Netze werden an ihren Ports über *Links* verbunden. Sub-Netze können bei Bedarf weiter verfeinert (*partitioned*) werden (siehe Abbildung 3.20). Der Partitioning-Prozess kann ähnlich wie Layering rekursiv angewandt werden bis ein Netz nur aus Elementen besteht, die nicht mehr weiter verfeinert werden können (siehe Abbildung 3.21).

Weiterhin wird in G.805 das Konzept der Partitionierung auch auf einzelne Links übertragen (siehe Abbildung 3.22). Dabei beschränkt sich die Empfehlung auf eine feingranulare Aufteilung der verfügbaren Bandbreite, damit den einzelnen Verbindun-

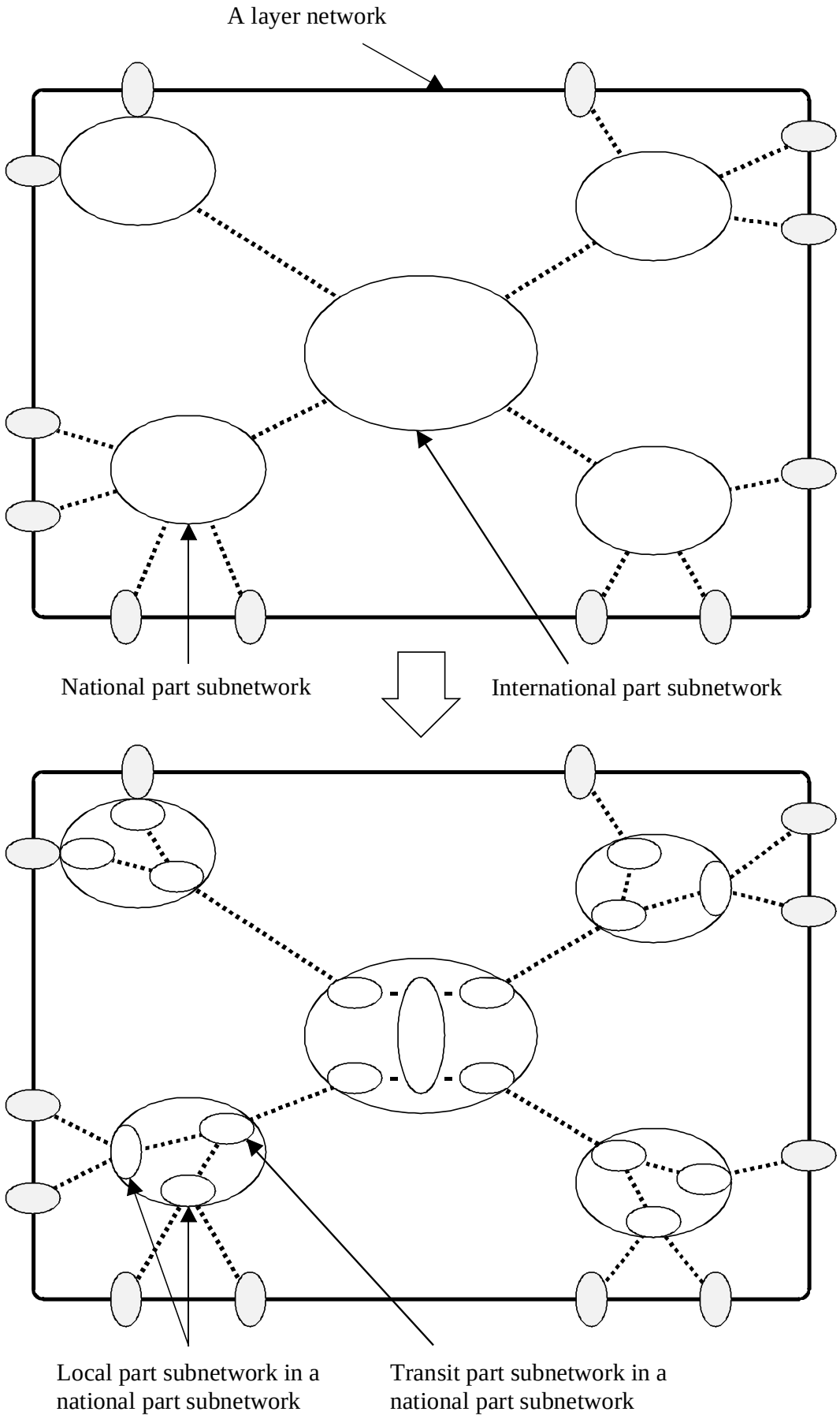


Abbildung 3.20.: Partitionierung von Layer Network [ITU00]

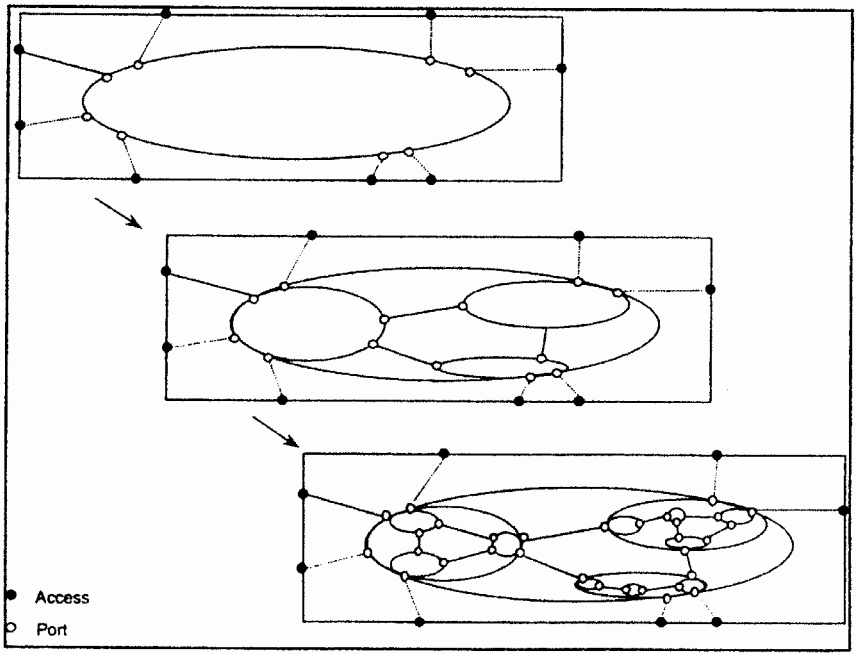


Abbildung 3.21.: Rekursive Partitionierung [Khu06]

gen nur ein Anteil und nicht die komplett verfügbare Bandbreite zugewiesen werden kann. Auf der anderen Seite sagt die G.805 Empfehlung, dass es auch möglich sein soll, die kleineren Kapazitäten für eine Verbindung mit einem größeren Bandbreitenbedarf zu bündeln.

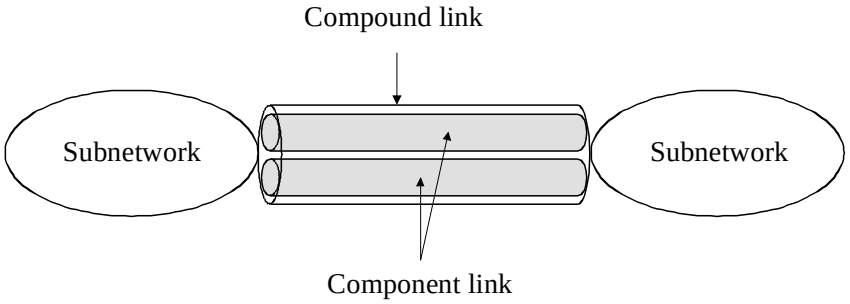


Abbildung 3.22.: Link Partitioning [ITU00]

Bei diesem Konzept signalisieren *Compound Links* die Existenz der Verbindung zwischen zwei Ports sowie beinhalten mindestens einen *Component Link*. Erst mit diesen *Component Links* werden die unterstützten Eigenschaften assoziiert.

3.6.2. Tandem Connection Monitoring

Ohne zu tief in technologiespezifische Details von optischen Transportnetzen zu gehen, werden in diesem Abschnitt zwei Methoden für die Verbindungsüberwachung vorgestellt, die in der ITU-T Empfehlung G.709/Y.1331 "*Interfaces for the Optical Transport Network (OTN)*" [ITU03b] spezifiziert sind.

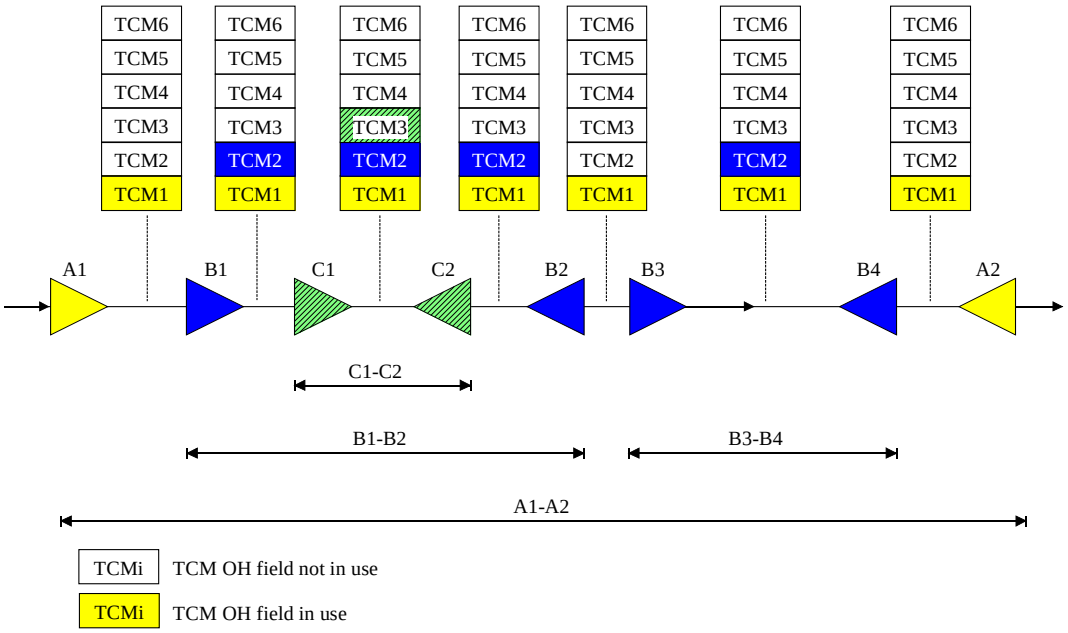


Abbildung 3.23.: Nested and cascaded monitored connections [ITU03b]

In der Empfehlung wird unter anderem eine Methode spezifiziert, wie die Monitoring-Informationen *In-Band* (d.h. zusammen mit den Nutzdaten) zwischen den Komponenten des Netzequipments ausgetauscht werden können. Dabei wird – durch den Headeraufbau bedingt – die gleichzeitige Überwachung von bis zu 6 Teilstrecken ermöglicht.

Neben der Überwachung von aneinander angeschlossenen Teilstrecken, die als *cascaded monitored connections* referenziert wird, werden in G.709 zwei komplexere Modelle für *Tandem Connection Monitoring* (TCM) unterstützt. Bei den sog. *nested monitored connections* können die überwachten Teilstrecken ineinander verschachtelt sein (siehe Abbildung 3.23). Sollen die Überwachungsstrecken einander nur teilweise überlappen, so spricht man von *overlapping monitored connections* (siehe Abbildung 3.24).

Unabhängig von Anordnungsmöglichkeiten zwischen allen überwachten Teilstrecken ist jede TCM-Teilstrecke durch zwei Access Points an den Endpunkten definiert. In G.709 werden die APs durch eindeutige numerische Bezeichner identifiziert, die innerhalb ihres Layer global eindeutig sein sollen. Der genaue Aufbau von IDs in G.709

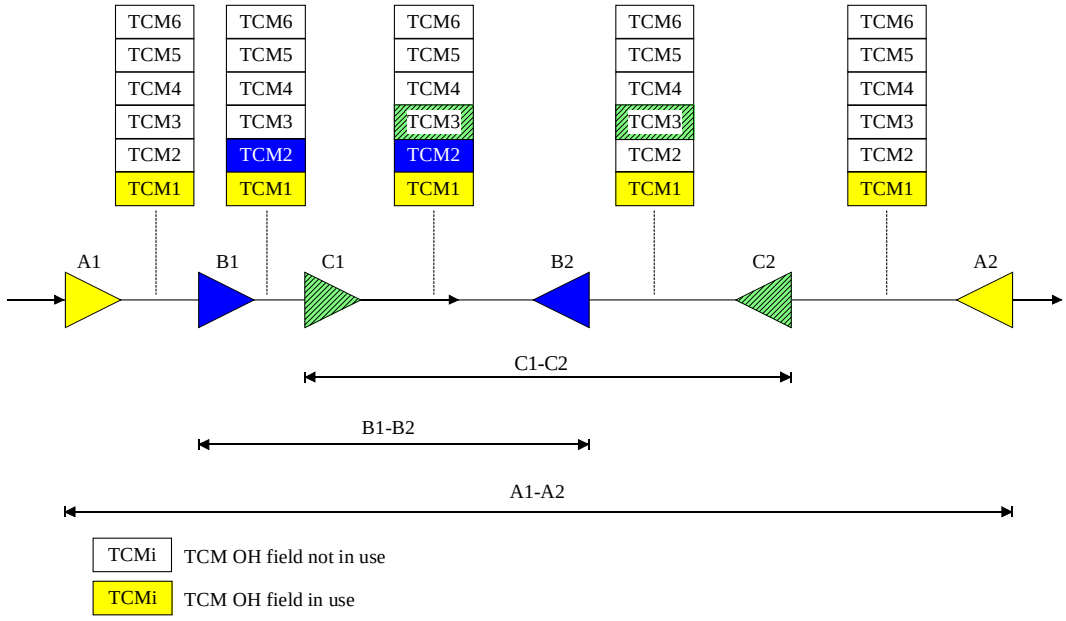


Abbildung 3.24.: Overlapping monitored connections [ITU03b]

ist protokollspezifisch und wird an dieser Stelle nicht beschrieben. Die sich in Multi-Domain Umgebungen etablierten Identifikationsmöglichkeiten werden später im Abschnitt 3.9 beschrieben.

3.6.3. Bewertung der Übertragbarkeit

Auch wenn das Schichtenmodell von G.807/G.809 auf die Problematik von Verketteten Diensten nicht direkt übertragbar ist, kann ein ähnliches Vorgehen bzgl. den QoS-Parametern angewendet werden. So kann die Ableitung der kundenspezifischen E2E-Dienstgütewerte in folgende Schritte aufgeteilt werden: Zunächst müssen die technologiespezifischen QoS-Parameter einzelner SP-Domänen durch geeignete Maßnahmen homogenisiert werden. Erst aus den homogenisierten QoS-Werten der einzelnen Teilstrecken kann mit Hilfe der Aggregatfunktion(en) der E2E-Wert berechnet werden. Dieser kann anschließend zu einer kundenspezifischen Darstellung konvertiert werden.

Das in G.805 präsentierte Partitionierungskonzept ermöglicht die Beschreibung eines globalen Netzes als ein Zusammenschluss von Netzen. Da SP-Domänen autonome Netze betreiben, ließe sich das Konzept auch auf Verkettete Dienste übertragen. Das Konzept lässt zu, die Verantwortungsbereiche anhand deren Verbindungspunkten (Ports) und den Verbindungen zwischen Ports zu beschreiben. Dadurch wird es möglich, vom Innenaufbau eines Netzes zu abstrahieren. Weiterhin kann bei dieser Beschreibungsart eines Verantwortungsbereiches auch ein Zusammenschluss mehrerer SP-Provider

verschattet werden, wodurch die Mischung aus hierarchischen und heterarchischen Kooperationsformen ermöglicht wird.

Interessant ist auch die Technik zur Beschreibung der Verbindungen zwischen einzelnen Ports. Die zweischichtige Aufteilung in *Component* und *Compound Links* kann ohne weiteres für die Beschreibung einzelner Teilstrecken übernommen werden. Dabei können *Compound Links* als Indikatoren einer prinzipiellen Verbindungsmöglichkeit dienen, mit den *Component Links* können unterschiedliche für diese Teilstrecke mögliche QoS- und Managementeigenschaften assoziiert werden. Die "Beschriftung" der Links, die Ports miteinander verbinden, muss jedoch an die Bedürfnisse Verketteter Dienste angepasst werden. Das trifft auch für die Benennung einzelner Verbindungspunkte zu. Eine Übersicht über die etablierten Identifizierungsmöglichkeiten in Multi-Domain Umgebungen kann im Abschnitt 3.9 gefunden werden.

Von den Monitoring-Techniken stellt die *Cascaded Monitored Connections*, bei der ausschließlich jede involvierte Teilstrecke von der diese Teilstrecke erbringenden SP-Domäne überwacht wird, die einfachste und fast immer mögliche Variante dar. Sollten alle Teilstrecken überwacht werden, dann kann durch eine geeignete Aggregatfunktion aus den individuellen Zuständen der entsprechende E2E-Wert berechnet werden. Bei den Ausfällen einzelner Überwachungsstrecken wird das allerdings bedeuten, dass der E2E-Wert nicht berechnet werden kann, wodurch auch *Overlapping Monitored Connections* interessant wird. Dies kann allerdings mit Problemen sowohl technischer als auch organisatorischer Natur verbunden sein, weil bei Overlapping Monitoring zwischen den – i.A. nicht direkt benachbarten – SP-Domänen Überwachungsinformationen ausgetauscht werden müssen. Da die SP-Domänen nicht unbedingt direkt benachbart sind, kann diese Art der Überwachung allein wegen zu niedriger Vertrauensbeziehungen zwischen den Domänen scheitern. Aus technischer Sicht setzt eine Umsetzung dieser Monitoring-Strategie den Austausch technologiespezifischer Informationen sowie die aufwendigen Synchronisierung der Informationen voraus. Aus diesem Grund wird im Lösungsteil ausschließlich das Cascaded Monitoring betrachtet, das Overlapping Monitoring bleibt allerdings als eine Erweiterung interessant (siehe Kapitel 10).

Bei der Überwachung wird die Identifizierung einzelner Überwachungsabschnitte benötigt, um z.B. bei Ausfällen das Fehlermanagement gezielt in der betroffenen Domäne starten zu können. Weiterhin sollen die Monitoring-Informationen zeitlich miteinander synchronisiert werden. Eine In-Band Übertragung einzelner Messwerte ist zwar sehr exakt und autosynchronisiert, muss allerdings in das jeweilige Übertragungsprotokoll integriert werden, was ihre Erweiterungsfähigkeit deutlich mindert. Alternativ dazu können die Monitoringinformationen mit Zeitstempeln (engl.: *time stamps*) versehen werden, oder – wie das z.B. bei der Überwachung von Géant2 E2E Links gemacht wird (siehe Abschnitt 2.3.2) – durch das gleichzeitige Polling der Domäneninformationen realisiert werden. Im ersten Fall wird eine Uhren-Synchronisation der beteiligten Domäne benötigt, was in der Multi-Domain Umgebung allein aus organisatorischen

Gründen sehr schwierig sein kann. Deswegen wird an der Stelle für eine Synchronisation durch eine zentrale Monitoring-Instanz entschieden. Wie die Monitoring-Instanz die Informationen bekommt – hier ist gemeint durch *push*, *pull* oder deren Kombination – soll beim Routing entsprechend den Kundenanforderungen entschieden werden. In Bezug auf den Übertragungskanal für die Monitoring-Informationen wird hier für die Out-of-Band Kommunikation entschieden, da die In-Band-Kommunikation insbesondere bei der beliebig großen Anzahl der überwachten QoS-Parameter weniger Flexibilität und Erweiterungsmöglichkeiten zulässt.

3.7. Netzmanagement Intra-Domain

Moderne Netze sind wegen ihrer Vielfältigkeit und Heterogenität sehr komplexe und daher auch schwer zu managende Systeme. Die Zusicherung der Dienstgüte ist dadurch auch innerhalb einer einzelnen administrativen Domäne eine Herausforderung. Um die Komplexität in den Griff zu bekommen, wurde eine Reihe von Techniken entwickelt, die in diesem Abschnitt präsentiert werden.

Zunächst wird erklärt, wie ein zu managendes Objekt durch eine *Management Information Base* (MIB) beschrieben und verwaltet werden kann. Dem folgt eine Beschreibung der möglichen Anordnungsformen zwischen den zu managenden Objekten und ihren Managern. Anschließend werden einige Aspekte des *Traffic Engineerings* und der dabei zu bewältigenden Herausforderungen diskutiert, die für die QoS-Zusicherung in Single-Domains eine wichtige Rolle spielen. Der Abschnitt schließt mit der üblichen Bewertung der Übertragbarkeit der diskutierten Ansätze auf Verkettete Dienste.

3.7.1. Management durch MIB-Zugriff

In einem Netz werden die tatsächlich verfügbare Funktionen in physischen Komponenten realisiert. Durch die Vielfalt der proprietären Technologien und oft auch Hersteller-spezifischen Realisierungen von Standards weisen diese Komponenten einen sehr hohen Grad an Heterogenität auf.

Von ISO/OSI eingeführt und durch andere Standardisierungsgremien, wie z.B. OMG und IAB (*Internet Activity Board*), getrieben hat sich die Idee durchgesetzt, Netzkomponenten als *Managementobjekte* (engl.: *Managed Objects*, MOs) zu betrachten und sie generisch anhand ihrer Eigenschaften und Managementfunktionen zu beschreiben. Dabei stellen *Managementobjekte* "die (Abstraktion der) Charakteristika von Ressourcen dar, auf denen das Management operiert"[HAN99]. Die Menge der von einem Manager- oder Agentensystem verwalteten MOs wird als *Management Information Base* (MIB) bezeichnet. Um Management-Interoperabilität gewährleisten zu können, sind die MIB selbst und das Interface zu ihr (sog. *MIB Access Interface*) standardisiert; die Entscheidung über die konkrete Realisierung in der realen Ressource kann proprietär gestaltet und dem jeweiligen HW-Hersteller überlassen werden.

Um in diesem Modell (siehe Abbildung 3.25) eine Ressource zu managen, muss sich ein Operator oder eine Applikation zunächst über das *User Interface* an einen sog. Manager wenden. Darauf schickt der Manager über ein *Management Protocol* einen entsprechenden Befehl entweder direkt an das zu managende Objekt oder an einen Management-Agent. Über das *MIB Access Interface* geschieht dann der Zugriff auf die entsprechende MIB. Diese Zugriffsmethode eignet sich sowohl für die Veränderung der MO-Einstellungen als auch für die reine Überwachung (Monitoring).

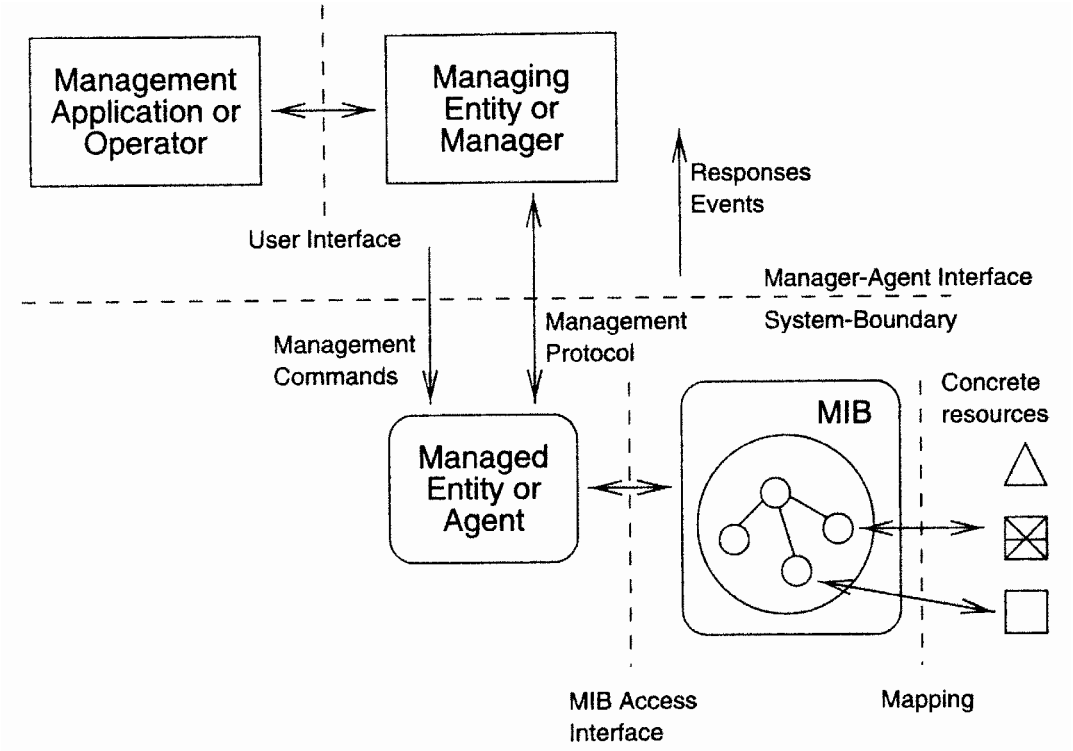


Abbildung 3.25.: Management durch MIB-Zugriff [HAN99]

3.7.2. Manager und Ressourcen, Anordnungsformen

Auch wenn der Managementzugriff von einer Applikation auf ein MO wie in dem vorherigen Abschnitt klar definiert ist, bestehen immer noch unterschiedliche Zuordnungsmöglichkeiten, welche Ressourcen von welchen Managern verwaltet und wie diese Manager-Einheiten miteinander verbunden sein können. Die Abbildung 3.26 präsentiert eine Reihe von möglichen Anordnungen zwischen Managementsystemen.

Die einfachste Anordnungsform stellt das *Central Management* dar. Dabei werden alle zu verwaltenden Ressourcen von einem einzigen Manager verwaltet. Der Manager ist dann auch für alle unterstützten Managementaufgaben zuständig.

Eine etwas komplexere Zuordnung bietet *Multipoint Control*. Bei dieser Anordnung werden Ressourcen nach unterschiedlichen (z.B. topologischen oder funktionalen) Kriterien zu Gruppen zusammengefasst, die jeweils von einem Manager verwaltet werden. Der Manager ist in diesem Fall auch für alle Funktionen zuständig, die von den verwalteten Ressourcen unterstützt werden. Die Anzahl von verwalteten Ressourcen pro Manager ist nicht definiert, somit kann im Extremfall ein Manager für eine einzige Ressource zuständig sein.

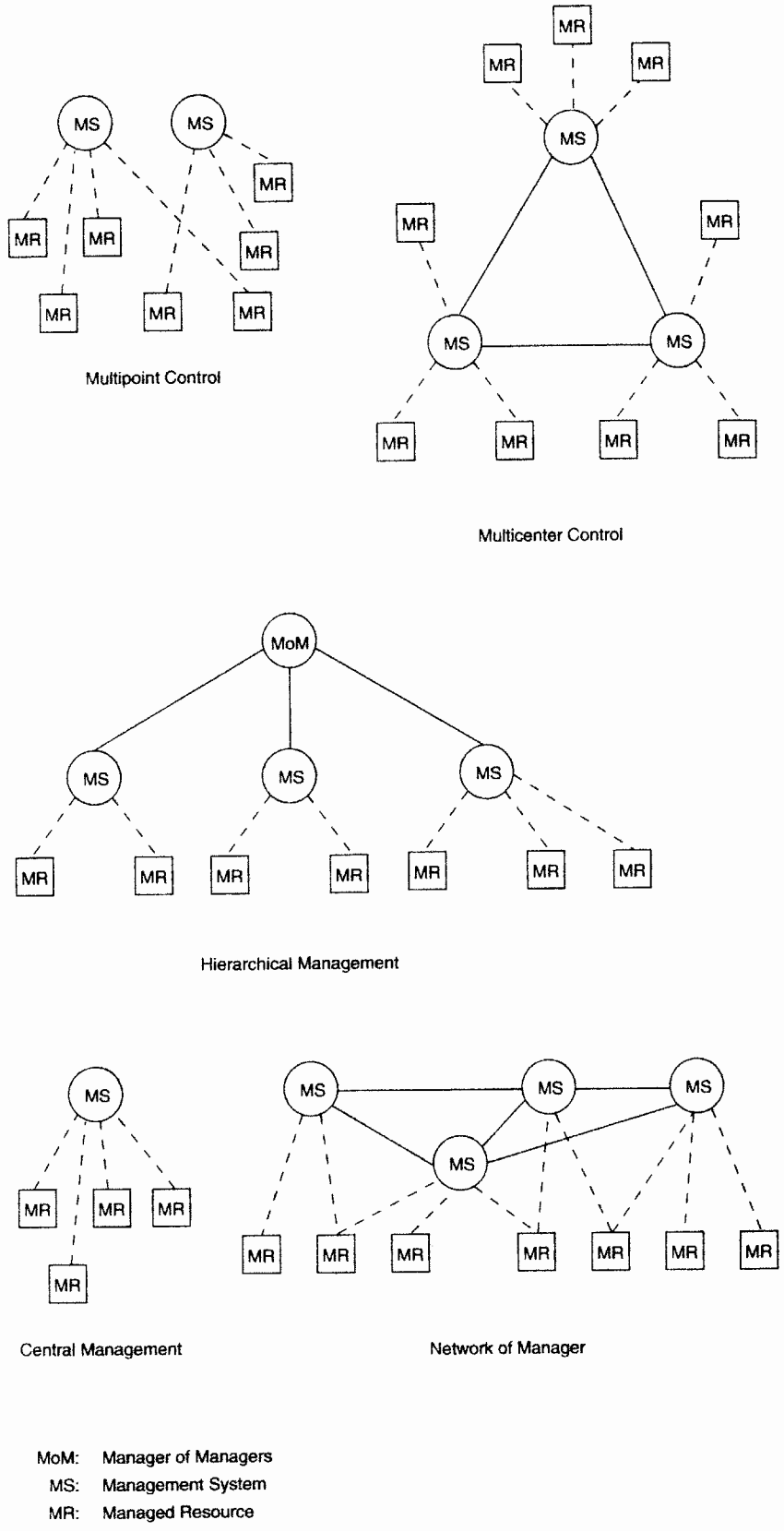


Abbildung 3.26.: Anordnungsformen von Managementsystemen und überwachten Ressourcen [HAN99]

Falls bei der Erfüllung der Managementaufgaben eine Koordination zwischen mehreren Managern erwünscht ist, können sie miteinander verbunden werden. Dabei sind je nach Kooperationsschema das *Multicenter Control* oder das *Hierarchical Management* denkbar. Das *Manager-of-Manager*-Konzept ist rekursiv und geeignet das hierarchische Management mit mehr als zwei Stufen zu bauen.

Bei den vier bereits beschriebenen Formen ist die Zuordnung zwischen einer Ressource und dem sie verwaltenden Manager eindeutig. Es kann aber auch sein, dass mehrere Manager für eine Ressource zuständig sind. Diese Form wird als *Network of Manager* bezeichnet. Die Gründe für eine solche Anordnung können verschieden sein. So können unterschiedliche Manager, die ein und dieselbe Ressource verwalten, für unterschiedliche Managementaufgaben zuständig sein. Weiterhin kann diese Anordnung für eine bessere Robustheit auf Ausfälle einzelner Manager verwendet werden.

3.7.3. Bottlenecks und Traffic Engineering

Ein Netz zeichnet sich unter anderem auch durch eine Vielzahl der möglichen Wege aus, auf denen Kommunikation zwischen zwei Knoten stattfinden kann. Die Wahl dieser Wege kann auch in einem einfachen Netz entscheidend für die Dienstgüte der Verbindungen sein. In der Abbildung 3.27 ist ein einfaches Beispiel mit drei möglichen Wegen zwischen Knoten A und C dargestellt. Die Routenwahl, die z.B. mit dem OSPF Algorithmus anhand der Gewichte getroffen wird, würde alle drei Verbindungen auf dem Weg ABC leiten. Ein Ausfall einer der Teilstrecken würde dann alle drei Verbindungen beeinträchtigen, was – bezogen auf die Anforderungen dieser Arbeit – eine schlechte Robustheit bedeutet.

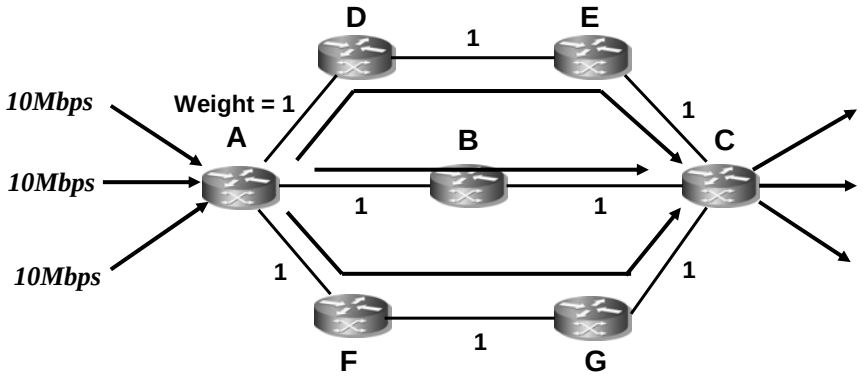


Abbildung 3.27.: Traffic Engineering [Pav07]

Ein weiterer Aspekt der lokalen Optimierung ist die Entstehung von unabsichtlichen *Bottlenecks*. Betrachtet man die Gewichte in der Abbildung gleichzeitig auch als Delays, so wird durch das Routing aller drei Verbindungen über ABC-Strecke der einzige Weg mit dem Delay 2 belegt. Würde jetzt eine weitere Verbindung benötigt, die außerhalb der Bandbreite noch die Anforderung "Delay <= 2 stellt", so wird es unmöglich diese zu schalten. Diese Situation würde dann – wieder übertragen auf die Anforderungen dieser Arbeit – sich in einer schlechten Skalierbarkeit bzgl. Anzahl der Verbindungen widerspiegeln.

Diese und ähnliche Probleme werden im Rahmen des *Traffic Engineerings*, das in der Telekommunikationsbranche sehr stark eingesetzt wird, durch eine geeignete Verteilung der Verkehrsströme auf unterschiedliche Wege gelöst. Im Falle von E2E-QoS spielt die Erfüllung der Zusicherungen auf dem Wege eine entscheidende Rolle. Im Beispiel der Abbildung 3.27 würde das zu einer Verteilung der Delay-toleranten Verbindungen auf die Wege ADEC, ABC- und AFGC führen. Um Pakete einer Verbindung über die ihr zugewiesene Route zu leiten wird häufig MPLS eingesetzt. Für die eigentliche Bestimmung der Route wird z.B. in [Pav07] vorgeschlagen, die Gewichtung einer Verbindung zwischen je zwei Knoten umgekehrt proportional zu deren Restkapazität zu definieren. Damit kann auch der Einsatz von OSPF auf dem Graphen mit veränderten Gewichten zu dem erwünschten Ergebnis führen.

3.7.4. Bewertung der Übertragbarkeit

Eine Standardisierung der Objektbeschreibung sowie der Kommunikationsschnittstelle hat sich durchgängig etabliert. Auch wenn der Dimensionsunterschied zwischen einem MO und einer SP-Domäne sehr groß ist, existiert auch eine Reihe von Parallelen. So können für die Realisierung eines Services in den SP-Domänen genauso wie bei Managementobjekten unterschiedliche Technologien zum Einsatz kommen. Die Beschreibung eines Services ist dadurch aber nicht beeinträchtigt und kann wie bei MOs in einer Form generischer Domain-MIBs geschehen. Bei den Funktionen, die auf einer Domain-MIB aufgerufen werden, muss jedoch berücksichtigt werden, dass sie sich auf eine unabhängige Organisation mit Entscheidungsfreiheit beziehen. Das bedeutet vor allem, dass bei der Kommunikation mit einer SP-Domäne keine Befehle, sondern ausschließlich Anfragen geschickt werden dürfen, die diese SP-Domäne ihrerseits auch zurückweisen darf.

Stellt man sich die SP-Domänen an der Stelle von Ressourcen aus dem Abschnitt 3.7.2 vor, dann kann man die Anordnungskonzepte auf die Szenarios aus dem Kapitel 2 übertragen. Z.B. das Domain-/Interdomain Manager Konzept aus DCN entspricht dem Hierarchical Management. Die Konzepte Multicenter Control und Network of Manager kommen in den Szenarios allerdings nicht vor. Es gibt unterschiedliche Einflussfaktoren, wie z.B. die Anzahl und Kooperationsform der beteiligten SP-Domänen, oder auch

die Managementaufgabe, die die Wahl einer der möglichen Anordnungen Szenario-spezifisch beeinflussen können. Für den Lösungsteil bedeutet das, dass keine Vorauswahl der Anordnungsform getroffen werden kann. Um beliebige Anordnungsformen unterstützen zu können, muss es bei Routing möglich sein, die Kommunikationswege für unterschiedliche Aufgaben zu definieren (vergleiche dazu auch entsprechende Diskussionen in Abschnitten 3.4 und 3.5).

Die im Abschnitt 3.7.3 angesprochenen Probleme, die durch lokale Optimierung auftreten können, sind auch auf die Multi-Domain Situation übertragbar. Die lokale Optimierung hat zwar auf die Erfüllung der E2E-QoS keinen negativen Einfluss, kann aber die Skalierbarkeit in Bezug auf die Anzahl der Verbindungen deutlich beeinträchtigen. Das angesprochene *Traffic Engineering* ist zwar darauf ausgerichtet, solche Probleme in den Griff zu bekommen, erfordert dafür aber eine Fülle an Informationen, wie z.B. Netztopologie und Auslastungsdaten, die von SPs grundsätzlich als sicherheitsrelevant und sensitiv betrachtet werden. Deswegen muss im Lösungsteil ein Weg gefunden werden, um bei der Wahl der Route solche Aspekte zu berücksichtigen, ohne zu viele sensible Informationen von den SP-Domänen abzufragen.

3.8. Informationssysteme in Multi-Domain Umgebungen

Die Erbringung von Verketteten Diensten erfordert eine enge Kooperation der beteiligten SP-Domänen. Das macht ein System zum Informationsaustausch zwischen diesen Domänen zu einem essentiellen Teil der Lösung. In diesem Abschnitt werden daher zwei Multi-Domain Informationssysteme besprochen, die sich im Laufe der Jahre als sehr robust und skalierbar erwiesen haben.

3.8.1. World Wide Web (WWW)

Das World Wide Web (WWW) wird von vielen in seiner Bedeutung mit dem Internet gleichgestellt. Die auf den sog. Webservern gespeicherte Informationsinhalte (Webseiten) können über HTTP (definiert in RFC 1945 [BFF96] und RFC 2616 [FGM+99]) oder HTTPS (definiert in RFC 2818 [Res00]) Protokolle prinzipiell von überall in der Welt abgefragt werden.

Informationsinhalte im Web kann man als relativ statisch betrachten, da im Vergleich mit der Anzahl der Lesezugriffe diese Inhalte i.a. relativ selten verändert werden. Die Veränderung der Inhalte kann sowohl vom Eigentümer der Webseite und/oder Webserver mit der Hilfe des Filesystems als auch – falls das erlaubt wurde – durch die HTTP-Befehle PUT und DELETE von den Web-Teilnehmern durchgeführt werden. Die Situation, dass auf eine Webseite gleichzeitig mehrere Web-Teilnehmer zugreifen können, kann zu Skalierungsproblemen führen, was bei populären Webseiten oft auch der Fall ist. Um dieses Problem zu umgehen, wurde eine Reihe von Techniken entwickelt, die die Belastung eines einzelnen Webservers wesentlich reduzieren.

Als erstes sei hier das Browsercaching erwähnt, das die Vorratsspeicherung der zuvor abgefragten Seiten erlaubt. Der HTTP-Befehl HEAD ermöglicht es dann, die Gültigkeit der lokal abgespeicherten Inhalte mit der "Master-Kopie" auf dem Webserver zu vergleichen. Die dadurch erreichte Entlastung kommt nicht nur dem eigentlichen Webserver zugute, sondern auch den Netzen, die die Kommunikation mit dem Webserver realisieren.

Das Browsercaching, das bei selten veränderbaren Webseiten gute Ergebnisse erzielt, kann bei den dynamischen Seiten, die z.B. Nachrichten oder Börsendaten darstellen, nur geringfügig helfen. Weiterhin schafft das Caching auch für mehrere Zugriffe seitens unterschiedlicher Nutzer keine Abhilfe. Um auch diese Situation in den Griff zu bekommen, wird das sog. *Server Load Balancing* (SLB) betrieben. Bei SLB werden die Daten redundant auf mehreren Webservern gespeichert und die Client-Anfragen auf diese Server ausgeglichen verteilt. Für die Verteilung können unterschiedliche Techniken angewendet werden, wie z.B. *DNS based SLB*. Der DNS-Server sorgt dabei dafür, dass die URL des Webservers auf die IP-Adresse eines der redundanten Server abgebildet wird.

Während Load Balancing sowohl eine Skalierbarkeit in Bezug auf die Anzahl der Clients und die Anfragerate als auch die bessere Robustheit gegen Serverausfälle mit sich bringt, muss auch eine Reihe von klassischen Problemen der redundanten Datenhaltung behandelt werden. In erster Linie gehört dazu die Gewährleistung der Konsistenz von Informationen auf den betroffenen Servern. Am Beispiel eines Online-Shops kann man es sich so vorstellen, dass die während der Verbindung mit einem Server in den Warenkorb gelegten Sachen auch bei der Umleitung der Verbindung zu einem anderen Webserver weiterhin verfügbar sein sollen. Das Auftreten und Behandeln solcher Probleme ist zwar nicht Bestandteil dieser Arbeit, diese müssen jedoch bei der Wahl der Komponenten und bei der Aufteilung der Zuständigkeitsbereiche berücksichtigt werden.

3.8.2. Domain Name System (DNS)

Eine weitere Form eines Multi-Domain Informationssystems stellt das *Domain Name Service* (DNS) dar. Das in RFC 1034 [Moc87c] und RFC 1035 [Moc87d] definierte DNS-System, dessen Aufgabe in der Übersetzung zwischen nutzerfreundlichen Webadressen (URLs) und IP-Adressen besteht, wird im Vergleich mit Webservern in WWW mit neuen Herausforderungen konfrontiert. Gleichzeitig mit der enormen Anzahl der Clients und der Kommunikationsdichte muss das DNS-System auch entsprechend große Mengen an Datensätzen verwalten können. Die Datensätze beziehen sich zudem auf mehrere administrative Domänen.

Um diese Aufgabe zu bewältigen, reicht die vergleichsweise einfache Replikation der Server mit dem Load Balancing nicht mehr aus. Die Abhilfe in dieser Situation schafft eine Aufteilung des gesamten Datenraumes in Zuständigkeitsbereiche (sog. *Zones*). Jede Zone (siehe Abbildung 3.28) umfasst einen Teil des hierarchisch angeordneten Adressraumes und bezieht sich i.A. auf mehrere organisatorische Domänen. Für jede dieser Zone ist eine Reihe von DNS-Servern zuständig, von denen einer die sog. *Master*-Rolle übernimmt. Alle weiteren sog. Slave-Server beinhalten nur die Kopie der Master-Datensätze und tragen dadurch zu einer besseren Lastverteilung und Ausfallsicherheit bei. Die Aufrechterhaltung der Datenkonsistenz bei Veränderungen wird durch den sog. *Zonentransfer* gewährleistet, bei dem eine Kopie der Master-Datensätze an die DNS Slave-Server übermittelt wird.

Die Aufteilung des ganzen Raumes auf Zonen verteilt zwar die gesamte Last auf mehrere DNS-Server, erfordert allerdings, dass jede Client-Anfrage für die Adressenumsetzung den für diese Adresse zuständigen DNS-Server erreicht. Bei der Menge der Zonen und den dafür zuständigen DNS-Servern ist es nicht zumutbar, dass jeder Client jeden DNS-Server (d.h. dessen IP-Adresse) kennt. Weiterhin können sich die Zonenaufteilung sowie die Zuständigkeit der Server für eine Zone mit der Zeit ändern. Abhilfe hierfür schafft die baumartige Anordnung der DNS-Server, die der Adressaufteilung auf Zonen entspricht. Dabei müssen alle DNS-Server ihre "Eltern" und "Kinder" im Baum kennen, damit die Client-Anfrage den zuständigen DNS-Server erreicht. Dabei werden

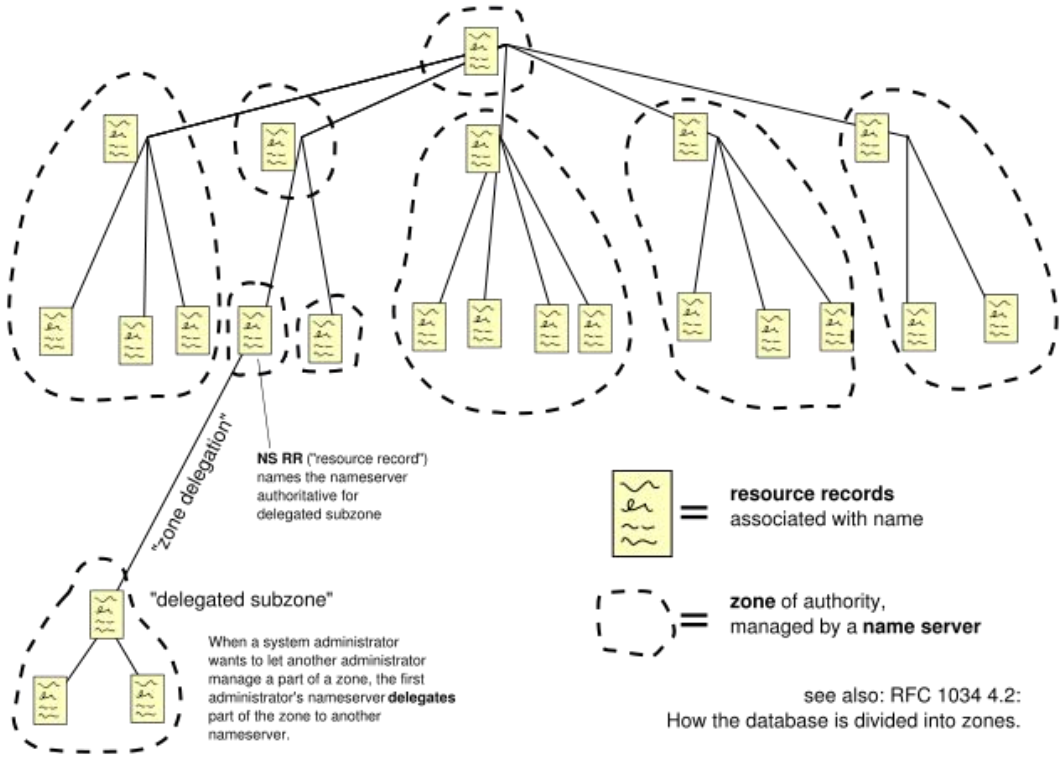


Abbildung 3.28.: Domain Name Space [WIK08]

zwei Methoden unterstützt. Der Client kontaktiert zuerst immer einen DNS-Server. Falls der DNS-Server für die angeforderte Adresse nicht zuständig ist, "wandert" bei der sog. rekursiven Namensauflösung die Client-Anfrage von einem DNS-Server zu einem anderen im Baum, bis sie den zuständigen Server erreicht. Die Antwort wird auf demselben Weg zurückgeschickt. Die rekursive Namensauflösung kann allerdings zu Abbrüchen wegen Zeitüberschreitung führen. Als Alternative kann der DNS-Server dem Client die Adresse des nächsten Server im Baum mitteilen. Der Client kontaktiert dann diesen, um die benötigte Adresse zu erfahren. Die letztere Methode erlaubt dem Client sein Wissen über DNS-Server sozusagen dynamisch zu erweitern und somit auf die benötigten Informationen zuzugreifen.

Auch wenn die Aufteilung des Namensraumes in Zuständigkeitsbereiche (Zonen) die Last auf die einzelnen DNS-Server deutlich reduziert, wird auch hier verstärkt das Caching eingesetzt. Dabei wird das Caching nicht nur bei den eigentlichen Clients, sondern auch bei den DNS-Servern selbst eingesetzt. Für den Client wirkt es sich durch die verkürzte Antwortzeit aus; bei den DNS-Providern trägt es dazu bei, die Kommunikation zwischen den DNS-Servern unterschiedlicher Zonen zu reduzieren.

Während Organisationen für die eigene Webpräsenz relativ leicht einen eigenen Webserver aufstellen können, werden DNS-Server – sowohl wegen ihrer Komplexität als auch

wegen deren Bedeutung für die Erbringung von anderen kundenorientierten Diensten – grundsätzlich von darauf spezialisierten Service-Providern betrieben, die eine Reihe von strengen Auflagen erfüllen müssen.

3.8.3. Bewertung der Übertragbarkeit

Die Techniken, die in diesem Abschnitt besprochen wurden, kann man grob in Domain-interne (von außen nicht sichtbare) und Multi-Domain-Techniken unterteilen. Bei den besprochenen Domain-internen Techniken sind vor allem der Einsatz von redundanten Servern für einen Domain-Dienst sowie das "Verstecken" dieser Server hinter einem *Load Balancer* von Bedeutung. Dies erlaubt die Skalierung und Robustheit eines Dienstes wirksam zu steigern. Dieses Vorgehen ist höchst ausgereift. Deswegen wird in dieser Arbeit ausschließlich von Diensten gesprochen und deren Verteilung auf mehrere Rechner als *bei-Bedarf-möglich* angenommen.

Von den Multi-Domain Ansätzen sollen zunächst das Caching und die damit eng verbundenen Aktualitätsabfragen erwähnt werden. Diese Techniken tragen sehr stark zur Erhöhung der Skalierbarkeit bei. Die Effektivität des Caching hängt allerdings sehr stark von den Häufigkeit der Datenabfragen und der Datenänderungen ab.

Am Beispiel von DNS sieht man auch, dass bei sehr großen Datenmengen eine Aufteilung in Verantwortungsbereiche sinnvoll sein kann. Dabei zeichnet sich der Trend ab, dass komplexe Dienste wie DNS – im Gegensatz zu relativ einfachen Webservern – von externen, extra darauf spezialisierten Organisationen erbracht werden.

Weiterhin scheint auch die in DNS umgesetzte Technik zur dynamischen Wissenserweiterung (Herausfinden des DNS-Servers, der für die erforderliche Adresse zuständig ist) für den Einsatz in einer Multi-Domain Umgebung vielversprechend. Besonders in Umgebungen mit einer unbestimmten bzw. variierenden Anzahl von beteiligten SP-Domänen kann diese Technik sehr hilfreich sein.

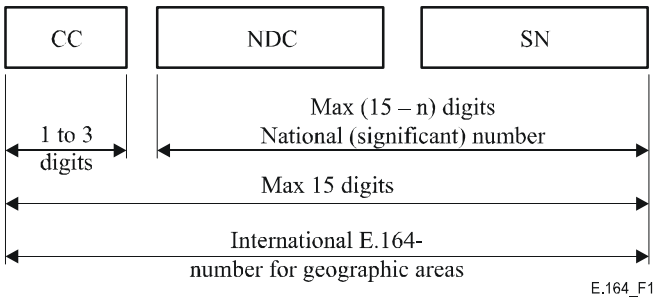
Lehrreich ist auch die Erfahrung mit der rekursiven Namensauflösung. So kann die Delegation der Aufgabe an einen anderen Server zwar die gestellte Anfrage lösen, aber führt u.U. zu Timeouts und einer gewissen Unwissenheit des Anfragestellers während der gesamten Zeit (vergleiche dazu auch die Diskussion über *Source Routing* und Routing-by-Delegation im Abschnitt 3.2).

3.9. Global eindeutige IDs

Damit die bei der Diensterbringung beteiligten SP-Domänen in der Lage sind, benötigte Objekte eindeutig zu referenzieren, werden *global-eindeutige IDs* erforderlich. In diesem Abschnitt werden deshalb bewährte Ansätze zur Identifikation in Multi-Domain Umgebungen besprochen. Im Bewertungsteil dieses Abschnitts werden die Stärken und Schwächen der jeweiligen Ansätze zusammengefasst.

3.9.1. Telefonnummerraum

Telefonnummern stellen wohl das bekannteste Beispiel von global eindeutigen IDs dar. Die ITU-T Empfehlung E.164 [ITU05] definiert Strukturierungsmöglichkeiten von Nummern für vier Kategorien: geographische Gebiete, globale Dienste, Netze und Ländergruppen. Die Struktur aller vier Kategorien ist sehr ähnlich aufgebaut und unterscheidet sich lediglich durch die Anzahl und die Größe der Nummernblöcke. Die Strukturierung nach geographischen Gebieten ist in der Abbildung 3.29 dargestellt.



CC	Country Code for geographic area
NDC	National Destination Code
SN	Subscriber Number
n	Number of digits in the country code

Abbildung 3.29.: Number structure for geographic areas [ITU05]

Interessant ist vor allem, dass eine global eindeutige Nummer aus mehreren Teilen besteht. Dabei wird jeder dieser Teile von unterschiedlichen Regulierungsbehörden definiert. Während Ländercodes von *Telecommunication Standardization Bureau* (TSB) verwaltet werden, ist die Verwaltung des Nummernraumes in jedem Land durch eine Behörde dieses Landes vorgesehen. In Deutschland wird diese Rolle von der *Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen*, kurz *Bundesnetzagentur* (BNetzA), ausgeübt. Die ITU-T Empfehlung beschreibt für den Länderteil lediglich einige Aspekte, die von den jeweiligen Behörden beachtet werden sollen.

Für ein Land wird eine ähnliche Vorgehensweise auch für die Ländernummer vorgesehen, bei der ein Teil (*Group Identification Code*) für die Identifikation eines Ortes bzw. eines TK-Providers und ein weiterer Teil für die Identifikation innerhalb dieses Providers vorgesehen ist. Der zweite Teil wird dann von dem entsprechenden TK-Provider verwaltet.

3.9.2. IPv4 und der Übergang zu IPv6

Der Aufbau von IP-Adressen, der Anfang 80er Jahre in RFC 791 [Pos81] spezifiziert wurde, ist ähnlich strukturiert wie die bereits besprochenen Telefonnummern (siehe Abbildung 3.30). Er zeichnet sich durch eine Aufteilung in autonome administrative Domänen (Netze) aus, die Nummern für lokale Hosts in Eigenregie verwalten.

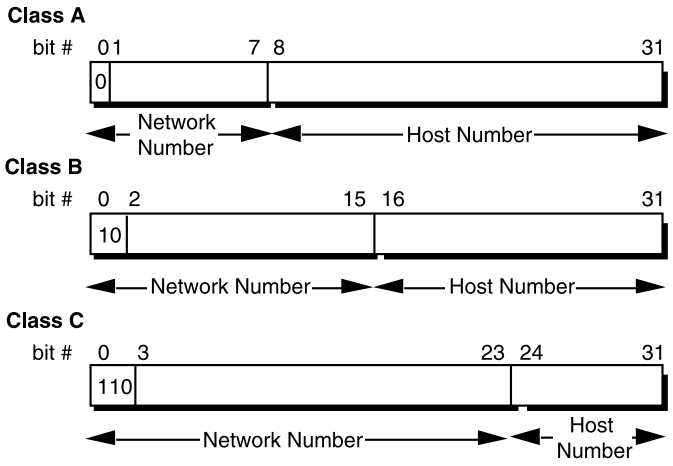


Abbildung 3.30.: IP Address Format [3CO08]

Der gravierende Unterschied besteht in einer festen Länge der IP-Adressen aus. Da Netze unterschiedlich groß sein können und somit eine unterschiedliche Anzahl Hosts haben, wurde der gesamte IP-Adressraum in Klassen unterschiedlicher Größe aufgeteilt. Die Netz- und Hostanteile dieser Klassen haben wiederum eine feste, für die Klasse festgelegte Größe. Eine feste Adressgröße und -Struktur hat zwar den Vorteil, dass sie sehr effizient in Hardware abgearbeitet werden kann, hat gleichzeitig auch eine Reihe von Problemen verursacht.

Da es kaum ein Netz gibt, das auf die vorgesehene Größe des privaten Raumes (für die Hosts) exakt passt, verursachte eine solche feste Aufteilung eine Adressenverknappung. Während die Class C Adressen für viele Organisationen zu klein waren, waren Class B Adressen mit ihren mit über 65 Tausend erlaubten Host-Adressen relativ schnell ausgeschöpft und oft nicht vollständig ausgenutzt. Auch wenn der Verknappung der

IP-Adressen mit Techniken wie *Network Address Translation* (NAT) und *Classless Inter-Domain Routing* (CIDR) entgegengewirkt wurde, wird zur Lösung des Adressierungsproblems im Internet ein neues Verfahren benötigt.

Als Lösung des Problems wird der Umstieg von IPv4- auf IPv6-Adressen angesehen, deren Adressraum in 128 statt 32 Bits kodiert wird. Interessant ist dabei nicht der Aufbau von IPv6-Adressen selbst (ähnlich wie bei IPv4 bestehen sie aus zwei Teilen für Netz- und Host-Adressen, die jetzt jeweils 64 Bit groß sind), sondern die Langwierigkeit des organisatorischen Übergangsprozesses. Der bereits in Dezember 1995 in RFC 1883 [DH95] vorgeschlagene IPv6-Standard[3] hat sich in mehr als 10 Jahren relativ wenig durchgesetzt. Die Gründe dafür sind weniger technischer Natur, sondern zeigen noch mal, wie schwer Änderungen bei einem laufenden Dienst durchsetzbar sind.

3.9.3. URL, URN und URI

Während die Telefon- und IP-Adressen die jeweiligen Objekte mit Nummern identifizieren, die für Menschen u.U. schwer zu merken sind, bieten *Uniform Resource Identifier* (URI), *Uniform Resource Locator* (URL) und *Uniform Resource Name* (URN) eine nutzerfreundlichere Variante, die zudem auch eine Reihe technischer Vorteile gegenüber bereits besprochenen numerischen IDs aufweisen.

Alle drei Identifikationsmöglichkeiten sind eng miteinander verwandt. Historisch gesehen kam zuerst die von Berners-Lee vorgeschlagene Definition der URLs zur Identifikation von Ressourcen in WWW. Diese ursprünglich in RFC 1738 [BMM94] definierte Methode erlaubt, sowohl einen Host im Internet als auch Ressourcen wie z.B. Webpages auf diesem Host zu lokalisieren. Da Ressourcen im Web periodisch umbenannt, gelöscht oder einfach verschoben werden können, entstehen mit der Zeit URLs, die auf nicht mehr vorhandene Ressourcen zeigen. Diesem Problem wurde mit der Entwicklung einer Reihe von Workaround-Techniken entgegengewirkt, wie z.B. *Persistent Uniform Resource Locator* (PURL) oder *Digital Object Identifier* (DOI). Als eine Lösung dieses Problems wurden Mitte 90er URNs entwickelt, die Ressourcen unabhängig von deren momentanen Position identifizieren. URIs wurden zunächst an der Stelle von URLs verwendet und sind um einiges genereller aufgefasst. Unter einer URI wird eine Identifizierungsmöglichkeit für "abstrakte oder physische Ressourcen"[BFM05] verstanden. URIs werden auch als eine Verallgemeinerung von URL und URN verstanden, die beides umfasst.

Obwohl URLs, URNs und URIs zur Identifikation unterschiedlichen Objekte genutzt werden, haben sie einen ähnlichen – wenn auch nicht identischen – Aufbau. Zunächst werden alle drei als Zeichenfolgen kodiert. Für die Strukturierung dieser

[3] Inzwischen durch RFC 2460 [DH98] abgelöst.

Zeichenfolge wird eine Reihe von Sonderzeichen verwendet, die semantisch unterschiedliche Blöcke einer ID voneinander trennen. Als erstes wird immer die Bezeichnung des Schemas eingegeben, die von dem restlichen Teil der ID durch das erste Sonderzeichen ":" getrennt ist (siehe Abbildung 3.31). Das Schema legt die Struktur des restlichen IDs fest. Nach RFC 2717 [PK99] ist die Registrierung von Schemas in mehreren Verwaltungsbäumen möglich. Die Registrierung wird von IETF durchgeführt.

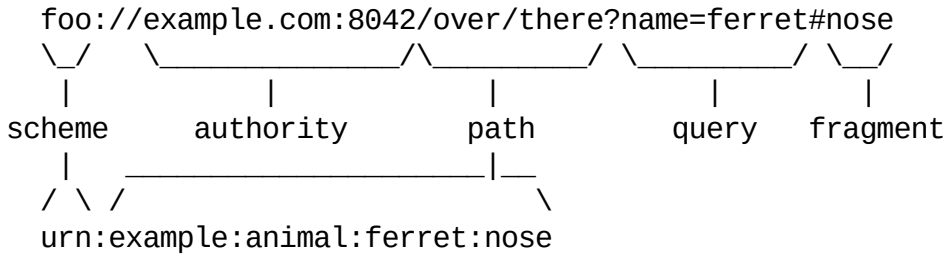


Abbildung 3.31.: URI Generic Syntax [BFM05]

Die Struktur des zweiten Teils einer ID hängt sehr stark vom Schema ab. Die meisten Schemas sehen auch für den zweiten Teil der ID einen strukturierten (hierarchischen) Aufbau vor. So können z.B. bei URLs mehrere Teile durch Sonderzeichen "/" voneinander getrennt werden. Interessant sind in dem Zusammenhang vor allem zwei Festlegungen: zum einen ist die Anzahl dieser Teile nicht beschränkt, und zum anderen kann das Verwaltungsrecht (engl.: *authority*) für den "Rest des IDs" an eine weitere Organisation delegiert werden. Diese Organisation kann es ihrerseits auch weiter delegieren. Diese zwei Eigenschaften erlauben es, eine ID sowohl beliebig erweiterbar zu machen als auch den Bedürfnissen der involvierten Organisationen zur Namensverwaltung zu entsprechen.

3.9.4. Internet Registrierungsbaum für MIBs

In einer Multi-Domain Umgebung, wie sie im Internet gegeben ist, ist es essentiell, Objekte nicht nur global eindeutig zu identifizieren, sondern auch genauso eindeutig beschreiben zu können, welche Funktionalität sie besitzen. Um diese Aufgabe zu bewältigen wurde von OSI und ITU-T ein sog. Internet-Registrierungsbaum eingeführt (siehe Abbildung 3.32).

Die Aufzählung und Benennung der registrierten Objekte geschieht anhand des Registrierungsbaumes, dessen Grundstruktur in RFC 1155 [RM90] definiert wurde. Jeder Knoten im Baum ist sowohl mit einer mnemonischen Bezeichnung als auch mit einer Nummer versehen, die ihn eindeutig identifiziert. Der eindeutige Knotenidentifikator besteht aus durch Punkt getrennten Namen bzw. Nummern aller Knoten auf dem

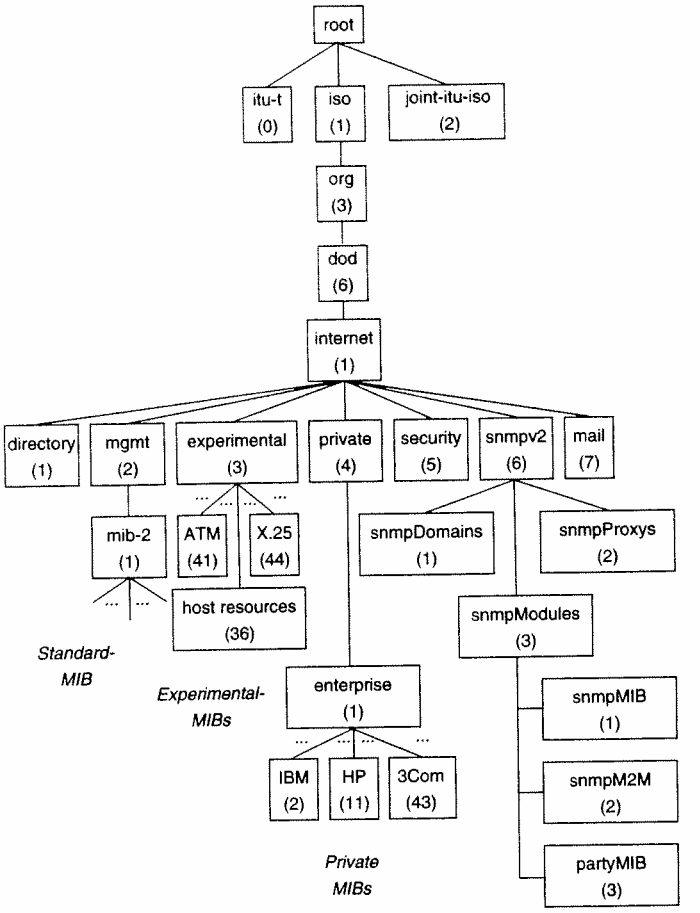


Abbildung 3.32.: Internet Registrierungsbaum [HAN99]

"Weg" zu diesem Knoten, angefangen von der Wurzel (*root*). Beide Bezeichnungsmöglichkeiten sind legitim, somit zeigen "1.3.6.1" und "iso.org.dot.internet" auf denselben Knoten.

Der Registrierungsbaum hat noch zwei wichtige Eigenschaften, die für diese Arbeit von Bedeutung sein können. Zu einem unterliegen unterschiedliche Zweige dieses Baumes der Verwaltung unterschiedlicher Organisationen. Diese können ihrerseits Unterzweige anlegen, deren Verwaltung sie an weitere Organisationen delegieren, wie z.B. es bei dem "enterprise"-Teilbaum der Fall ist, der für die Definition herstellerspezifischer Informationen reserviert ist.

Die zweite wichtige Eigenschaft, die den Registrierungsbaum von den anderen beschriebenen Identifizierungsmöglichkeiten unterscheidet, besteht darin, dass jedes Blatt dieses Baumes mit der Beschreibung eines Managed Objects (MO) assoziiert wird. Die Beschreibung selbst geschieht in der von ITU-T und ISO in X.680 [ITU94b] standardisierten Sprache *Abstract Syntax Notation One* (ASN.1).

Die Kombination des Registrierungsbaums, dessen Teilbäume von unterschiedlichen Organisationen erweitert werden können, und der Möglichkeit, die selbstdefinierte MIB-Beschreibung mit den Blätter in diesem Baum zu assoziieren, bietet nicht nur Vorteile. Neben dem wilden "Wachstum" des Baumes kann auch die Definition von semantisch identischen Beschreibungen in unterschiedlichen Teilbäumen als Nachteil angesehen werden. Das kann z.B. zu Interoperabilitätsproblemen zwischen Systemen unterschiedlicher Hersteller führen, die ihre Funktionalität anhand der IDs im Registrierungsbaum beschreiben. Zusätzlich muss als Nachteil gesehen werden, dass diese Form von Objektidentifikatoren bei der Programmierung von Managementanwendungen und in Hinblick auf Erweiterungen alle Nachteile eines absoluten Adressierung aufweist.

3.9.5. Bewertung der Übertragbarkeit

Charakteristisch für alle in diesem Abschnitt besprochenen Identifizierungsmöglichkeiten ist die Aufteilung einer ID in Verwaltungsbereiche, die von unterschiedlichen *Authority*-Organisationen unabhängig voneinander – und vor allem entsprechend organisationsinterner *Policies* – definiert werden können. Genau diese Eigenschaft macht sie geeignet für den erfolgreichen Einsatz in einer Multi-Domain Umgebung.

Die Verarbeitungsgeschwindigkeit einer ID ist umgekehrt proportional zu deren Komplexität (feste vs. variable Länge, feste vs. veränderbare Struktur). Aus Performancegründen wäre daher eine an den Einsatzort angepasste Wahl der Identifizierungsmethode angebracht. Aus den Schwierigkeiten bei dem Umstieg von IPv4 auf IPv6 soll allerdings eine Lehre gezogen werden, und die Wahl soll auch zukunftsorientiert getroffen werden. Auch wenn die Identifizierung von Domain-Objekten, wie z.B. Verbindungsorte, mit den zwei-geteilten IDs ("DomainID"-"LocalID") prinzipiell ausreichen würde, ist der Einsatz von URIs auf lange Sicht sinnvoller.

Ein globaler Registrierungsbaum ist dagegen für die eindeutige Definition von langlebigen und vor allem unveränderlichen Objekten gut geeignet. Die Identifikation von komplexen bzw. zusammengesetzten Objekten kann allerdings zur Inflexibilität und Schwierigkeiten bei Erweiterungen führen. Als eine Ausnahme von dieser Grundregel kann die Abspeicherung in Blättern von den Zusammenhängen zwischen den QoS-Parameter und deren Aggregat- und Ordnungsfunktionen (siehe entsprechende Diskussionen in Abschnitten 3.2 und 3.3) sowie die Versionen eines Kommunikationsprotokolls angesehen werden, da diese nicht verändert werden dürfen.

3.10. Prozessbeschreibung in Multi-Domain-Umgebungen

Die Spezifikation von ITSM-Prozessen setzt in jedem Fall die Auswahl einer geeigneten Prozessmodellierungssprache voraus. Deswegen wird in diesem Abschnitt zunächst ein kurzer Überblick über Methoden zur Prozessmodellierung beschrieben. Dem folgt eine detailliertere Beschreibung der *ITSMCooP* Modellierungsmethode, die für die Modellierung der Managementprozessen in Multi-Domain Umgebungen entwickelt wurde.

3.10.1. Prozessbeschreibungssprachen im Überblick

Seit den achtziger Jahren des letzten Jahrhunderts wurden unterschiedlichen Techniken zur Prozessmodellierung entwickelt. Hier werden kurz die bekanntesten Ansätze vorgestellt.

UML

Bei der Unified Modeling Language (UML) handelt es sich um eine semi-formale Modellierungsprache, deren Wurzeln im objektorientierten Software Engineering liegen. Die Version 1.1 der UML ist 1997 erschienen; die derzeit aktuelle Version ist 2.1.1. Die UML wird durch die Objects Management Group (OMG) standardisiert [OMG07b, OMG07a].

UML ist eine grafische Modellierungssprache, die – im Gegensatz zu unterschiedlichen anderen Modellierungssprachen – nicht in eine objektorientierte Modellierungsmethode eingebettet ist. Die UML-Spezifikation ist zwar äußerst detailliert, aber nicht formal. Die UML besteht aus insgesamt dreizehn Diagrammtypen, davon sechs Strukturdiagramme und sieben Verhaltensdiagramme. Die UML führt allerdings keine strikte Trennung der Diagrammtypen durch. So können die Notationselemente verschiedener Diagrammtypen in einem Modell miteinander verwendet werden.

In Bezug auf interorganisationale Prozesse sind insbesondere die Aktivitätsdiagramme relevant. Aktivitätsdiagramme enthalten keine spezifischen Notationselemente zur Modellierung interorganisationaler Prozesse. Dennoch gibt es eine Reihe von Arbeiten, die die Anwendung von Aktivitätsdiagrammen auf interorganisationale Szenarien demonstrieren.

XML-Sprachen

In den letzten Jahren wurden eine Reihe von Extensible Markup Language (XML) basierten Sprachen entwickelt, wie z.B. die *Business Process Execution Language for Web Services* (BPEL4WS) [OAS07] oder *XML Process Definition Language* (XPDL) [WfM09]. Diese Sprachen ermöglichen die maschinenlesbare Beschreibung von Prozessen und damit den Austausch von Prozessdefinitionen und die automatisierte Ausführung von Prozessen durch ein Workflow Management System (WfMS).

EPK

Weiterhin sollen hier die Ereignisgesteuerten Prozessketten [KNS92] erwähnt werden, eine vor allem im europäischen Raum verbreitete Modellierungstechnik. Insbesondere sind sie durch ihren Einsatz im SAP R/3 Referenzmodell der SAP AG bekannt.

Eine EPK ist eine Abfolge von *Funktionen*, die ein Objekt von einem Startzustand in einen Endzustand transformieren, und von *Ereignissen*, die den weiteren Verlauf des Geschäftsprozesses bestimmen können. Große Prozessmodelle können mit EPKs durch vertikale Hierarchisierungen und horizontale Unterteilungen strukturiert werden. Neben Ereignissen und Funktionen können auch Inputs und Outputs dargestellt sowie beteiligte Organisationseinheiten und Anwendungssysteme referenziert werden.

Bei EPKs werden allerdings Aspekte vernachlässigt, die sich auf die Kooperation von Unternehmen und Domänen-übergreifende Geschäftsprozesse beziehen. So wird durch EPKs die Darstellung organisationsspezifischer Aspekte, die Abstrahierung von Prozessinformationen sowie die Visualisierung von Schnittstellen zwischen Organisationen nicht unterstützt [KKS04]. Weiterhin gibt es in EPKs keine Darstellungsmöglichkeit für lokale Prozesse kooperierender Unternehmen, weswegen der Nachrichtenaustausch zwischen Organisationen nicht modelliert werden kann und Verantwortlichkeiten von Prozessteilnehmern nicht ausreichend modelliert werden können.

BPMN

Zum Abschluss dieses Überblicks soll noch die Business Process Modeling Notation angesprochen werden[4]. BPMN wurde ursprünglich von der *Business Process Management Initiative* (BPMI) entwickelt. Die Akzeptanz von BPMN ist schon wenige Jahre nach der Veröffentlichung der Version 1.0 im Jahr 2004 verhältnismäßig hoch [Ble07]. Im Jahr 2005 wurde BPMN für die weitere Pflege von OMG übernommen und ab 2006 wird diese Notation als OMG-Standard geführt.

Der Fokus von BPMN richtet sich auf die rein graphische Modellierung von Geschäftsprozessen. BPMN beschränkt sich auf die Darstellung des Kontroll- und Datenflusses. Andere Aspekte der Prozessmodellierung, wie z.B. die Beschreibung von Organisationsstrukturen, werden nicht unterstützt. Die Semantik der Notationslemente wird nur informell in Textform beschrieben. Dynamische Aspekte werden durch ein an Petri-Netze angelehntes Konzept des Token-Passings beschrieben [OMG09]. In der BPMN-Spezifikation werden allerdings bislang weder eine Formalisierung der beschriebenen syntaktischen Sprachelemente noch ein Metamodell vorgesehen.

Der Fokus von BPMN liegt auf Prozessen, die von menschlichen Akteuren durchgeführt werden und nicht notwendigerweise vollständig automatisiert werden sollen bzw. können. Die mit BPMN modellierten Prozesse sind daher nicht unmittelbar in einer der WfMS ausführbar. Dieses Ziel wird jedoch angestrebt. Bereits in der BPMN-Spezifikation wird ein Mapping von BPMN nach BPEL angegeben, das allerdings sehr umstritten ist [ODvdATH08, Sch08].

Im Gegensatz zu EPK adressiert BPMN explizit die Modellierung von interorganisationalen Prozessen. Im Unterschied zu den Partitionen des UML-Aktivitätsdiagramms, die lediglich eine Gruppierung der Notationselemente ohne bestimmte Semantik darstellen, unterscheidet BPMN zwischen Pools und Lanes. Ein Pool repräsentiert einen

[4] vgl. auch Darstellung in [Ham09]

Prozessteilnehmer. Durch die Verwendung von gleichzeitig mehreren Pools werden interorganisationale "business-to-business" Prozesse beschrieben. Ein Pool kann weiterhin in mehrere Lanes unterteilt werden. Die Lanes besitzen zwar keine feste Semantik, durch ihre Verwendung ist es z.B. möglich, mehrere Rollen zu beschreiben, die von einem Akteur übernommen werden.

Um die Prozesspartitionierung zu garantieren, verbietet die BPMN-Spezifikation, dass Sequenzfluss die Grenzen von Pools überschreitet. Die organisationsinterne Prozesse, die jeweils in ihren Pools bzw. Lanes definiert werden, laufen somit gleichzeitig. Zur Verknüpfung der in den einzelnen Pools ablaufenden Prozesse darf lediglich Nachrichtenfluss verwendet werden. Das entspricht der Aussage VAN DER AALSTS, dass Nachrichten das einzige Interaktionsprimitiv im interorganisationalen Prozessmanagement sind [vdA00].

3.10.2. Prozessbeschreibung mit *ITSMCooP*

HAMM [Ham09] analysiert die bereits erwähnten sowie weitere Modellierungsmethoden. Diese Arbeit befasst sich auch mit der Problematik *Verketteter Dienste*, allerdings mit dem Fokus auf die Definition domänenübergreifender IT-Service-Management-Prozesse.

HAMM stellt fest, dass die Beschreibungssprache BPMN für die Definition der ITSM Prozesse für Verkettete Dienste besser geeignet ist als die anderen betrachteten Alternativen. Aufbauend auf PMN und SID legt HAMM Vorgehensschritte für die Modellierung fest und definiert eine Reihe für die Eindeutigkeit der Beschreibung notwendigen Konventionen. Die Methodik wird als ITSMCooP bezeichnet.

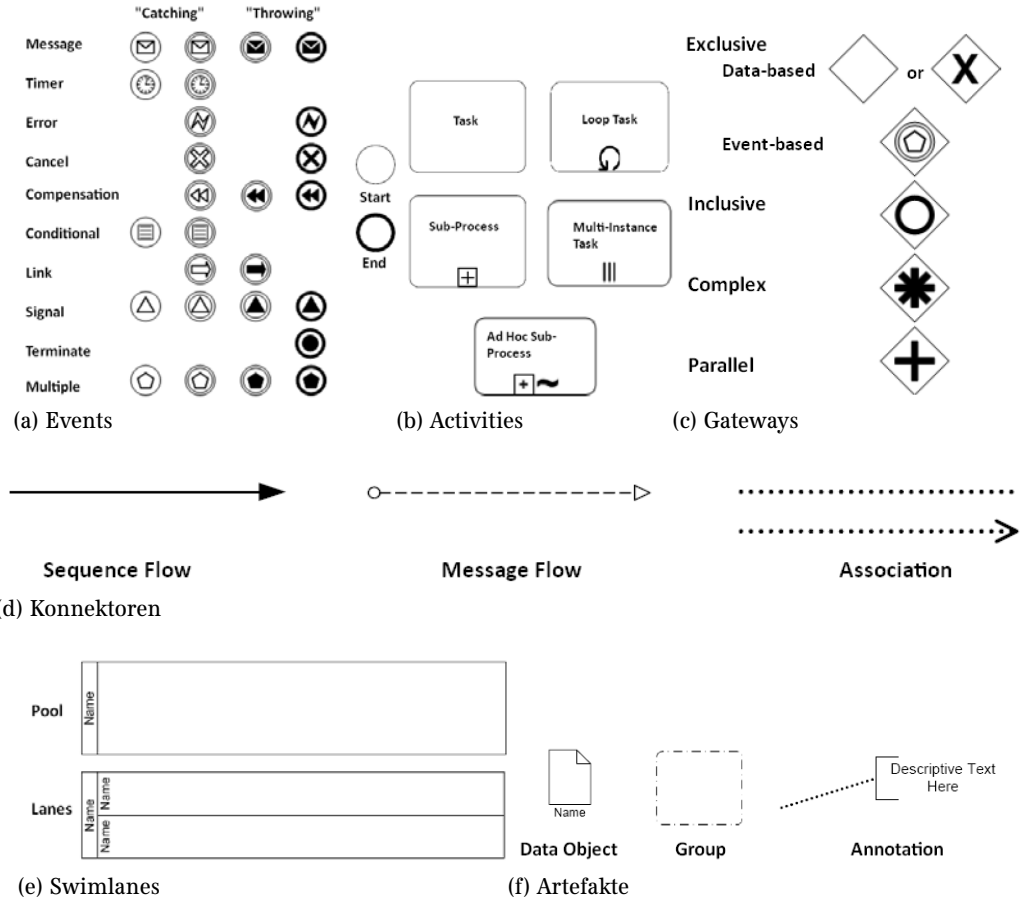
Die BPMN-Syntax [OMG09] unterscheidet vier Gruppen von Notationselementen:

Flussobjekte (engl.: *Flow Objects*) sind graphische Elemente zur Beschreibung des Verhaltens eines Geschäftsprozesses. Zu dieser Gruppe gehören *Events*, *Activities* und *Gateways* (siehe Abbildungen 3.33a, 3.33b, 3.33c).

Konnektoren (engl.: *Connecting Objects*) Es sind drei Möglichkeiten vorgesehen, wie die Diagramm-Objekte miteinander verbunden werden können: *Sequenzfluss*, *Nachrichtenfluss* sowie *Assoziationen* (siehe Abbildung 3.33d).

Swimlanes Alle Elemente sollen den *Pools* oder *Lanes* zugeordnet werden, die die Rollen repräsentieren, von denen die jeweilige Aktivität ausgeführt wird (siehe Abbildung 3.33e).

Artefakte Artefakte werden zur Darstellung zusätzlicher Informationen über den Prozess verwendet. Die BPMN-Spezifikation definiert drei Klassen von Artefakten, *Data Objects*, *Groups* und *Annotations* (siehe Abbildung 3.33f); es können jedoch weitere Artefakte bei Bedarf hinzugefügt werden.



(a) Events (b) Activities (c) Gateways

(d) Konnektoren

(e) Swimlanes (f) Artefakte

Abbildung 3.33.: BPMN Notation [OMG09]

Jede der drei *Flow-Objects*-Gruppen wird weiter verfeinert. So wird die Klasse *Events* in *Start*, *End* sowie eine Reihe *Intermediate Events* unterteilt. Activities werden in atomare *Tasks* und *Sub-Processes* unterschieden. Während die atomaren *Tasks* nicht weiter aufgegliedert werden, können für *Sub-Processes* eigene Prozessbeschreibungen spezifiziert werden. Weiterhin besteht die Möglichkeit, bereits definierte Prozesse zu referenzieren, wodurch auch die Möglichkeit der funktionalen Dekomposition gewährleistet ist. Activites werden nach ihrer Aktivierung standardmäßig nur einmal ausgeführt. Sollen Activities mehrfach hintereinander ausgeführt werden, können sie entweder als *Loop* oder *Multi-Instance Task* gekennzeichnet werden. Die Spezifikation der Reihenfolge oder der Anzahl der Durchläufe der Activities ist nicht vorgesehen. Gateways werden in weitere vier Typen eingeteilt: *Exclusive* (Entscheidung für genau einen Zweig des Sequenzflusses), *Inclusive* (Entscheidung für einen oder mehrere Zweige des Sequenzflusses), *Complex* (Kombination der anderen Typen), *Parallel* (Split und Join ohne Bedingungen). Die exakten Bedingungen werden erst durch die Gateway-Attribute spezifiziert.

Konvention K08 - Vermeidung impliziter Kontrollfluss

Der Kontrollfluss im globalen Prozessmodell ist explizit zu modellieren:

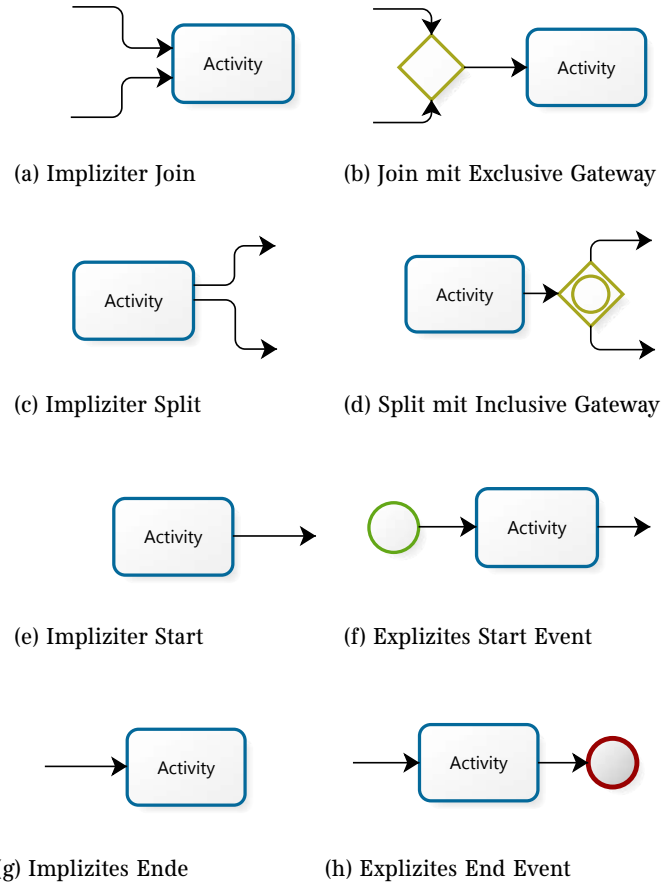
- Eine Activity darf nur je einen eingehenden und ausgehenden Sequenzfluss besitzen
- Jeder Prozess muss mindestens je ein Start- und End-Event besitzen

Abbildung 3.34.: ITSMCooP, Konvention K08 [Ham09]

Wie bereits erwähnt wurde, werden in ITSMCooP u.a. Konventionen zur Prozessmodellierung mit BPMN eingeführt. Ein Beispiel dafür ist in Abbildung 3.34 dargestellt. Entsprechend dieser Konvention soll der Kontrollfluss im Prozessmodell explizit ausmodelliert werden. Eine kurze Gegenüberstellung u.U. nicht eindeutiger – wenn auch nach dem BPMN-Standard erlaubter – und der korrespondierenden eindeutigen Beschreibungen ist in der Abbildung 3.35 dargestellt.

Ein weiterer Aspekt, der bei der Modellierung der Multi-Domain Prozesse eine zentrale Rollen spielt, ist die Zusammensetzung eines globalen Prozesses aus mehreren gleichzeitig ausgeführten Prozessen. Dieser Aspekt wird in Abbildung 3.36 illustriert. In die Durchführung des globalen Prozesses sind zwei Rollen involviert – ROLE A und ROLE B. Durch die vertikalen gestrichelten Blöcke werden in der Abbildung Zeitabschnitte gekennzeichnet, in denen die lokalen Aktivitäten der beiden Rollen gleichzeitig ausgeführt werden können. Über die Dauer der Ausführung – und somit auch dieser Zeitabschnitte – wird in der BPMN keine Aussage gemacht.

Die Ausführung des globalen Prozesses beginnt mit ACTIVITY 1 in ROLE A. Nach der Ausführung dieser Aktivität verzweigt sich der Prozessablauf in zwei parallele Prozessflüsse, die gleichzeitig in ROLE A ausgeführt werden. In einem dieser Flüsse wird ACTIVITY 3 ausgeführt. Im anderen Fluss wird eine Nachricht an die ROLE B geschickt. Da dies eine Ende-Nachricht ist, wird dieser Prozessfluss in ROLE A beendet. Die abgeschickte Nachricht, die von ROLE B empfangen wird, triggert die Ausführung von ACTIVITY 2. Aus Prozesssicht werden die ACTIVITY 2 und ACTIVITY 3 gleichzeitig ausgeführt. Nach der Beendigung der Ausführung von ACTIVITY 2 wird eine weitere Nachricht an ROLE B geschickt, womit der lokale Prozes in ROLE A beendet. Diese Nachricht wird von ROLE B empfangen und dient neben dem Beenden von ACTIVITY 2 als eine Eingabe für den *Parallel Gateway*. Laut der BPML-Spezifikation wird dieser Gateway erst dann geschaltet, wenn – in Petri-Netze-Sprache – auf beiden Eingängen Tokens vorliegen. Anhand von diesem Vorgehen wird die Synchronisierung zwischen lokalen Prozessflusen ermöglicht, die i.A. von unterschiedlichen Rollen ausgeführt werden. Der *Gateway* wird somit zu einem Synchronisationspunkt dieser Prozesse. Erst nachdem der *Gateway* geschaltet hat, kann in dem Beispiel die ACTIVITY 4 ausgeführt werden, nach der der globale Prozess abgeschlossen wird.



(a) Impliziter Join (b) Join mit Exclusive Gateway

(c) Impliziter Split (d) Split mit Inclusive Gateway

(e) Impliziter Start (f) Explizites Start Event

(g) Implizites Ende (h) Explizites End Event

Abbildung 3.35.: Explizite Modellierung des Kontrollflusses [Ham09]

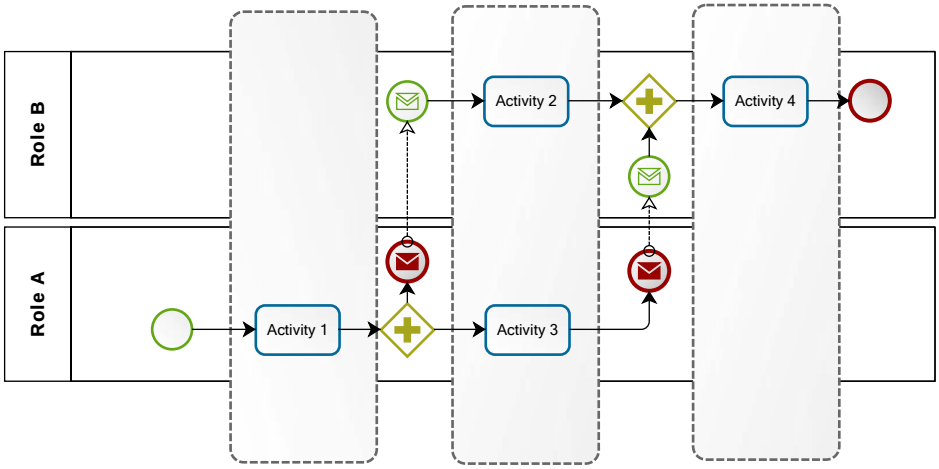


Abbildung 3.36.: Zuordnung globale Prozessinstanz – Beispiel [Ham09]

Die Kommunikationsartefakte, die zwischen den Prozessen ausgetauscht werden, sind in *ITSMCooP* aufbauend auf dem Shared Information/Data Model (SID) Modell des TMF definiert. Ausschlaggebend für diese Wahl war, dass das SID-Modell das derzeit einzige existierende Informationsmodell für IT-Service-Management darstellt [BSS09, Ham09]. Das Shared Information/Data Model wurde als Informationsmodell im Rahmen der NGOSS-Initiative des TMF entwickelt. Das SID-Modell beschreibt verschiedene Aspekte aus der Sicht des Telekommunikation-Service-Providers, wie z.B. Beziehungen zwischen Ressourcen- und Service-Sichten. Erweiterungen des Modells für Anwendungs-Szenarien sind explizit vorgesehen [TMF05]. In *ITSMCooP* wird das Modell erweitert, um Dienstzusammensetzung und Managementaspekte einzelner Dienstinstanzen Verketteter Dienste zu beschreiben.

3.10.3. Bewertung der Übertragbarkeit

Auch wenn *ITSMCooP* – genauso wie die zugrundeliegende BPMN – primär für die Definition manuell ausgeführter Managementprozesse konzipiert wurde, kann diese Modellierungstechnik auch bei automatisierten bzw. semi-automatisierten Prozessabläufen verwendet werden. Die in [Ham09] entwickelte Methodik und die Konventionen können sowohl bei der Definition von Basisprozessen, die mit den Protokollschlüsselworten assoziiert werden sollen, als auch von darauf aufbauenden SLM-Prozessen verwendet werden. Um den Bezug zum Protokoll sicherzustellen, müssen bei der Definition von Basisprozessen alle Aktivitäten, die ausgehende Protokollaufrufe produzieren, bzw. die ausgehenden Nachrichten selbst mit den entsprechenden Schlüsselworten beschriftet werden. Bei der Definition von SLM-Prozessen wird es zwangsläufig nötig sein, auf die zuvor definierten Basisprozesse zu verweisen. Solches Vorgehen wird in der BPMN-Spezifikation als *Reference Tasks* referenziert. Bei der Beschreibung von beiden, Basis- und SLM-Prozessen, soll die in *ITSMCooP* definierte Strukturierung beibehalten werden.

Die Interoperabilität der Prozesse soll einerseits anhand eines einheitlichen Protokolls und andererseits anhand einheitlicher Kommunikationsartefakte gewährleistet werden. Diese Aspekte (wie eine Anfrage signalisiert wird und wie die Daten strukturiert werden) sind weitestgehend voneinander unabhängig. Da ein Routing-Verfahren auf Daten operiert, die die vorhandenen Verbindungsmöglichkeiten und deren Eigenschaften beschreiben, werden die notwendigen Kommunikationsartefakte in Kapitel 4 von der Beschreibung der Transportnetze abgeleitet (siehe Abschnitt 3.6). Die Protokollanfragen sind dagegen eng mit den Basisprozessen verbunden, was ihre gemeinsame Definition im Kapitel 5 motiviert. Bei der Beschreibung der SLM-Prozesse im Kapitel 6 wird implizit davon ausgegangen, dass alle *Manager*-Rollen die Dienstinstanz-Informationen entsprechend den Definitionen in [Ham09] strukturieren.

4

SLM-aware Routing-Architektur für Verkettete Dienste

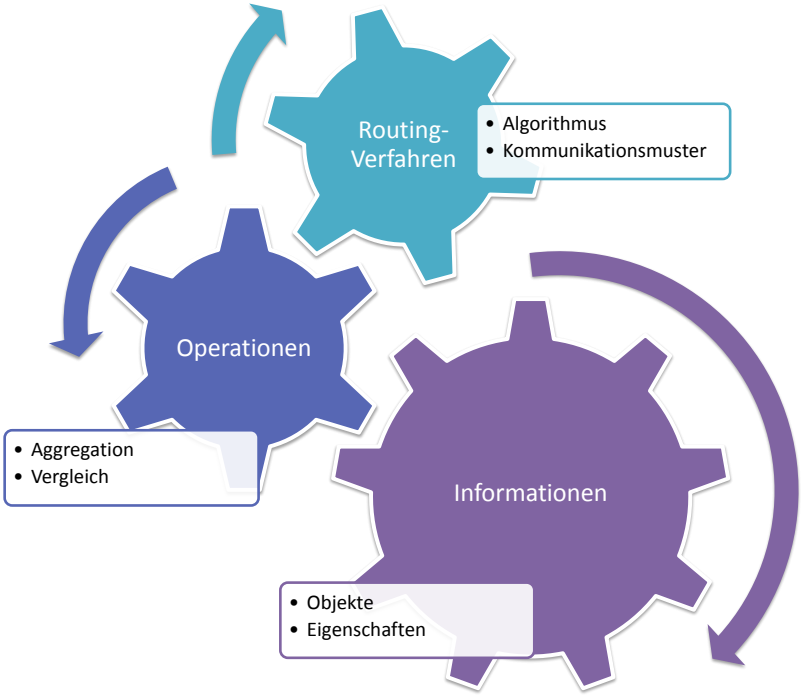


Abbildung 4.1.: Routing als Zusammenspiel von Routing-Verfahren, Informationen und Operationen auf den Informationen

Das Routing als Ganzes kann als ein Zusammenspiel dreier semantisch unterschiedlicher Teile beschrieben werden (siehe Abbildung 4.1).

Das Herzstück dieses Zusammenspiels bildet das *Routing-Verfahren*, das Entscheidungen über den Routenverlauf trifft. Dazu muss das Routing-Verfahren auf den vorliegenden *Informationen* über die *Objekte*, wie z.B. die Netztopologie, und deren *Eigenschaf-*

ten, wie z.B. die Qualität der Verbindung zwischen Netzelementen, operieren. Die dazu notwendigen *Operationen* sind einerseits die *Aggregation*, um aus den Eigenschaften einzelner vorhandener (Teil-)Strecken die Eigenschaften des resultierenden Pfads ableiten zu können, und andererseits der *Vergleich*, um zwischen alternativen Pfaden anhand ihrer Eigenschaften auswählen zu können. Alle diese *Operationen* auf den Informationen sowie die darauf basierenden Entscheidungen über den Routenverlauf werden vom *Routing-Algorithmus* ausgeführt bzw. getroffen.

In dieser Arbeit wird das Routing-Verfahren breiter aufgefasst als das reine Finden einer Route auf bereits vorliegenden Informationen. Um den kompletten Zyklus von Informationsabfragen bis hin zur Bestellung der gefundenen Route abdecken zu können, muss auch das Zusammenspiel des *Routing-Algorithmus*, der in der Fachliteratur oft auch als Suchalgorithmus referenziert wird, und *Kommunikationsmuster* zwischen den einzelnen SP-Domänen betrachtet werden. Unter einem *Kommunikationsmuster* wird dabei die Kombination aus dem Kommunikationsmodell und dem Timing verstanden. Das Kommunikationsmodell besagt, auf welchen Wegen die Kommunikation zwischen den Kommunikationspartnern stattfindet. Unter einem Timing wird an dieser Stelle verstanden, wann – im Verlauf des Routing-Algorithmus – welche Anfrage an welchen Kommunikationspartner geschickt wird. Neben dem Suchalgorithmus trägt das Kommunikationsmuster entscheidend zu Laufzeit und Güte des Routing-Verfahrens bei. An dieser Stelle soll bemerkt werden, dass das Kommunikationsmuster unabhängig ist vom Kommunikationsprotokoll, das die unterstützten Anfragen definiert. Das Kommunikationsprotokoll kann deswegen unabhängig von der Diskussion in diesem Kapitel definiert werden (für die Definition des Kommunikationsprotokolls siehe Kapitel 5).

Diese Begriffsabgrenzunden definieren auch die Grobstruktur für den Kern dieses Kapitels (siehe Abbildung 4.2). Im Abschnitt 4.1 werden zunächst die Zusammenhänge zwischen den Objekten und ihren Eigenschaften definiert, auf denen das Routing-Verfahren operieren soll. Im Abschnitt 4.2 wird diskutiert, welche Erweiterungen notwendig sind, um die benötigten Operationen auf diesen Objekten und Eigenschaften durchführen zu können. Anschließend werden im Abschnitt 4.3 unterschiedliche Routing-Verfahren diskutiert und deren Anwendbarkeit auf *Verkettete Dienste* diskutiert. Jeder Abschnitt ist mit einer separaten Einleitung versehen, die den internen Aufbau des Abschnittes beschreibt.

Während im Abschnitt 4.3 Routing-Verfahren bei einer homogenen Aufgabenzuordnung diskutiert werden, werden im darauffolgenden Abschnitt 4.4 Aspekte angesprochen, wie die Aufgaben dynamisch unterschiedlichen SP-Domänen zugeordnet werden können.

Entsprechend der im Abschnitt 3.2 getroffenen Entscheidung werden in den Abschnitten 4.1 bis 4.4 die Kommunikationsschnittstelle und die Verbindungspunkte einzelner Teildienste getrennt behandelt. Im Abschnitt 4.5 wird diese getrennte Betrachtungsweise den klassischen UNI/NNI-Schnittstellen gegenübergestellt. Dabei werden Aspek-

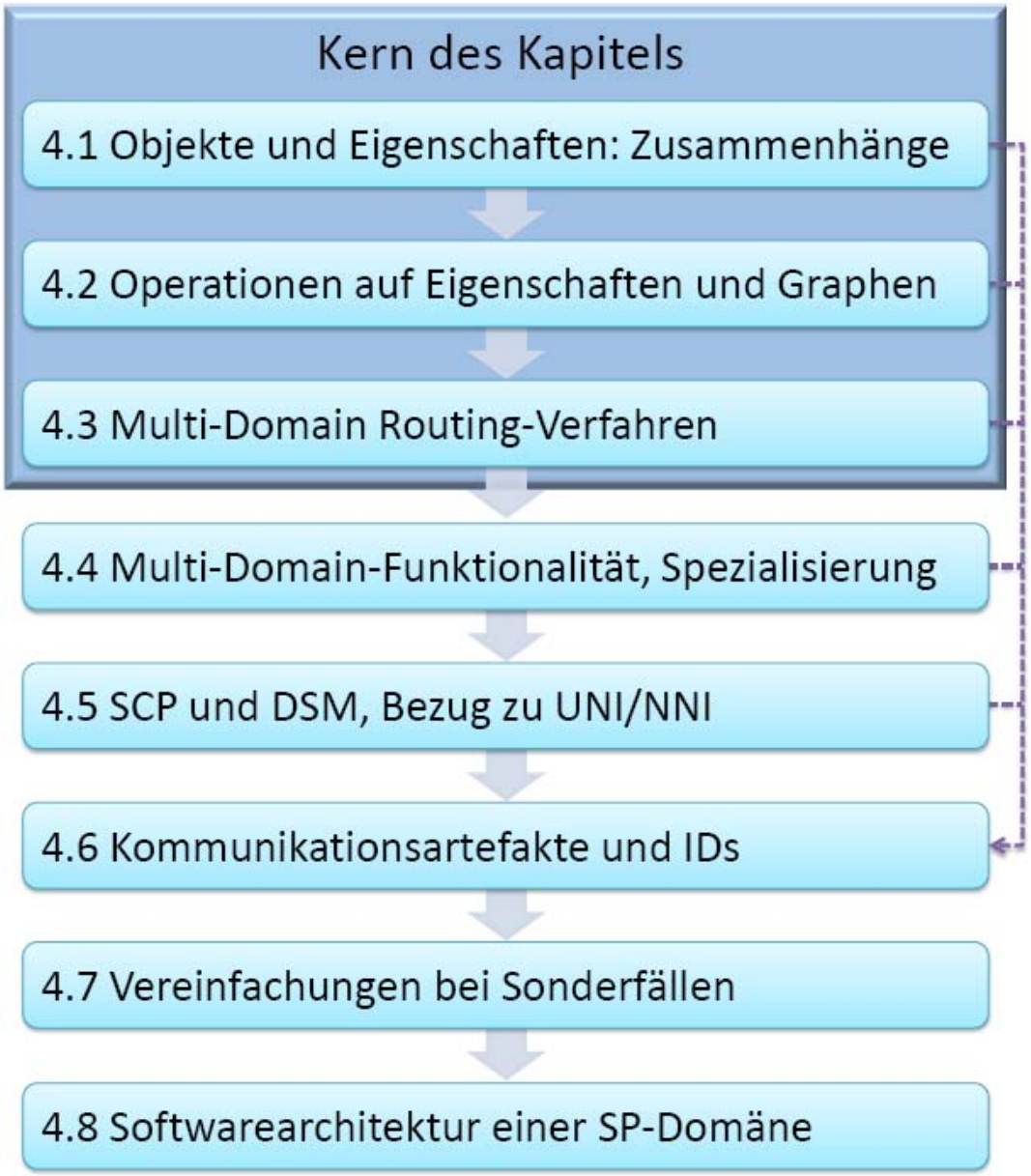


Abbildung 4.2.: Aufbau dieses Kapitels

te besprochen und Bedingungen aufgezählt, unter deren Berücksichtigung die Entscheidung zwischen den beiden Varianten getroffen werden soll.

Alle in Abschnitten 4.1 bis 4.5 getroffenen Festlegungen und Vorgehensweisen sollen durch die Informationen unterstützt werden, die in Form der Kommunikationsartefakte zwischen den SP-Domänen ausgetauscht werden. Um Abschnittgrenzenübergreifende Vorgaben, die durch die Kommunikationsartefakte abgedeckt werden sollen, werden sie in den o.g. Abschnitten hervorzuheben markiert. Die Vorgaben werden dabei in zwei Gruppen aufgeteilt – "Vorgabe (UML-Modellierung)" und "Vorgabe (Identifizierung)", um die unterschiedliche Natur dieser kapitelinternen Anforderungen besser zu betonen. Aufbauend auf diesen Vorgaben werden im Abschnitt 4.6 alle benötigten Kommunikationsartefakte definiert sowie die Art und Weise der Identifikation verschiedener Objekte festgelegt.

Es kann unterschiedliche Fälle geben, bei denen nicht alle der im Kapitel 2 auf die Lösung auferlegten Anforderungen und Randbedingungen erfüllt sein müssen. Im Abschnitt 4.7 werden daher die gängigsten Fälle diskutiert und dabei eine Reihe der dafür möglichen Vereinfachungen der entwickelten Lösung aufgezeigt.

Die im Abschnitt 4.8 aufgezeigte Skizze der Softwarearchitektur in einer SP-Domäne schließt dieses Kapitel ab.

4.1. Objekte und Eigenschaften: Zusammenhänge

Dieser Abschnitt beschäftigt sich mit den Zusammenhängen zwischen der in den SP-Domänen vorhandenen Netzinfrastruktur und den darauf realisierbaren Diensteigenschaften auf einer Seite und der abstrakten Beschreibung der Infrastruktur auf der anderen Seite. Das Ziel dieses Abschnittes besteht darin, Konzepte zu entwickeln und Begriffe zu definieren, die im weiteren Verlauf dieser Arbeit verwendet werden.

Im Abschnitt 4.1.1 wird zunächst eine Schnittstelle eingeführt, über die die Kommunikation zwischen gleichberechtigten SP-Domänen stattfinden soll. Bei der weiteren Diskussion wird gleichzeitig in zwei "Dimensionen" vorgegangen (siehe Abbildung 4.3). Die grobe Struktur wird durch folgendes dreistufiges Vorgehen gegeben: die Betrachtung geht von Single-Domain Aspekten im Abschnitt 4.1.2 über die Besonderheiten der Verbindungen zwischen zwei direkt benachbarten Domänen im Abschnitt 4.1.3 bis hin zu Multi-Domain Aufgaben im Abschnitt 4.1.4. Die zweite "Dimension" ist dadurch gegeben, dass in den ersten zwei Abschnitten die Innensicht auf die Domäneninfrastruktur einer Außensicht auf die Beschreibung der realisierbaren (Teil-)Dienste und deren Eigenschaften gegenübergestellt wird. Bei der Diskussion von Multi-Domain Aspekten wird gezeigt, wie aus mehreren Single-Domain Außensichten eine Multi-Domain Sicht abgeleitet werden kann. Im Abschnitt 4.1.5 werden anschließend weitere Aspekte diskutiert, die orthogonal zu den vorher betrachteten Dimensionen sind.

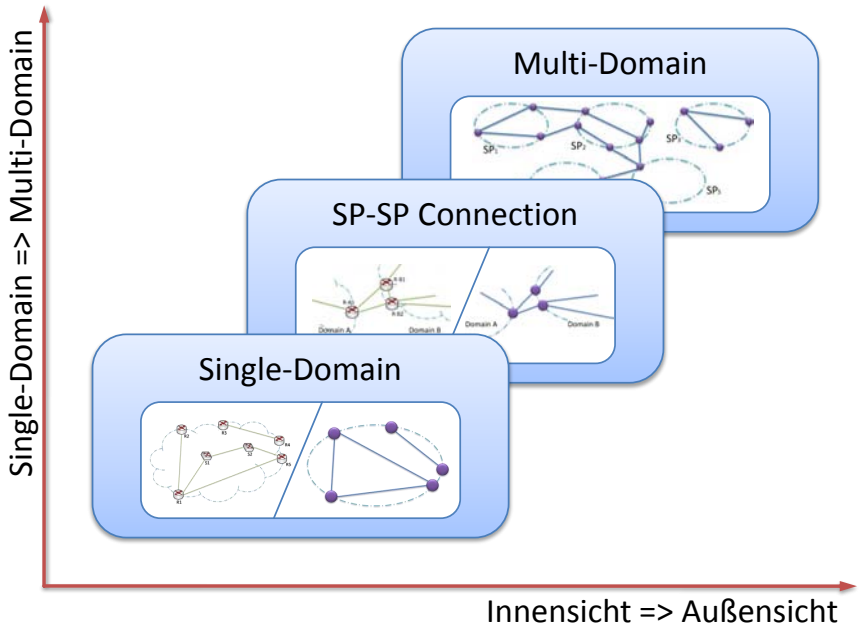


Abbildung 4.3.: Systematik dieses Abschnittes, zwei Dimensionen

4.1.1. DSM-Kommunikationsschnittstelle

Die Durchführung aller Multi-Domain Operationen setzt die Fähigkeit der SP-Domänen voraus, mit der "Außenwelt" zu kommunizieren. Diese Fähigkeit wird über die Kommunikationsschnittstelle(n) ausgeübt, die im Bereich des IT-Service-Managements (ITSM) zweckgebunden definiert werden. Bislang hat sich die Anbindung einer SP-Domäne an die "Außenwelt" – aus ITSM-Sicht – hauptsächlich auf bilaterale Kunden-Provider-Beziehungen fokussiert. Diese wird über die CSM-Schnittstelle abgewickelt. Die Nutzung dieser Schnittstelle setzt implizit hierarchische Inter-Organisationsbeziehungen voraus.

DSM-Schnittstelle

Zum Austausch der für das SLM-aware Routing relevanten Informationen und Service-Anfragen zwischen gleichberechtigten Service Providern wird eine bisher noch nicht definierte neuartige Schnittstelle benötigt, die in Anlehnung an CSM als DSM (*Domain Service Management*) bezeichnet wird (siehe Abbildung 4.4). Im weiteren Verlauf dieser Arbeit wird davon ausgegangen, dass über die DSM-Schnittstelle sowohl der Informationsaustausch als auch die Signalisierung aller unterstützten Anfragen abgewickelt wird (für die Definition des Kommunikationsprotokolls siehe Kapitel 5).

Um den SP-Domänen die Kommunikation über DSM-Schnittstellen zu ermöglichen, muss zunächst folgendes gewährleistet werden:

Vorgabe (Identifizierung) VI01 - DSM-Adresse

Jede DSM-Schnittstelle soll global eindeutig identifizierbar sein.

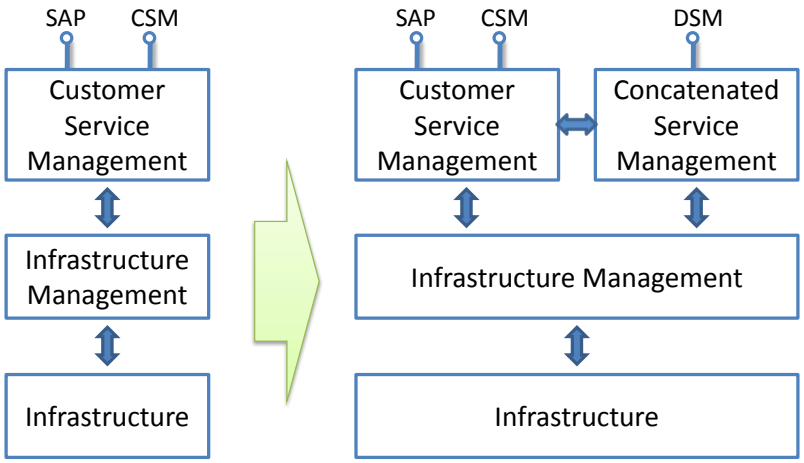
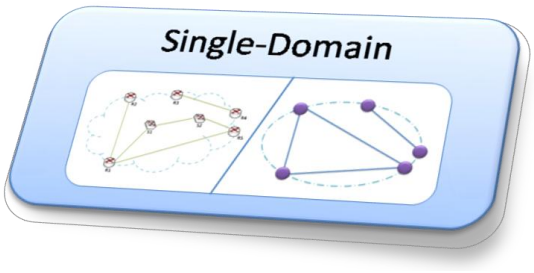


Abbildung 4.4.: Benötigte Erweiterung für die Kommunikation zwischen gleichberechtigten SP-Domänen

4.1.2. Single-Domain, Innen- und Außensicht

Um die Zusammenhänge zwischen der Infrastruktur und den darauf realisierbaren Diensteigenschaften zu verdeutlichen, wird ein einfaches Beispielnetz verwendet, das in Abbildung 4.5 dargestellt ist. Trotz seiner Einfachheit weist dieses Beispielnetz eine Reihe von Eigenschaften auf, die auch für große Provider-Netze charakteristisch sind.



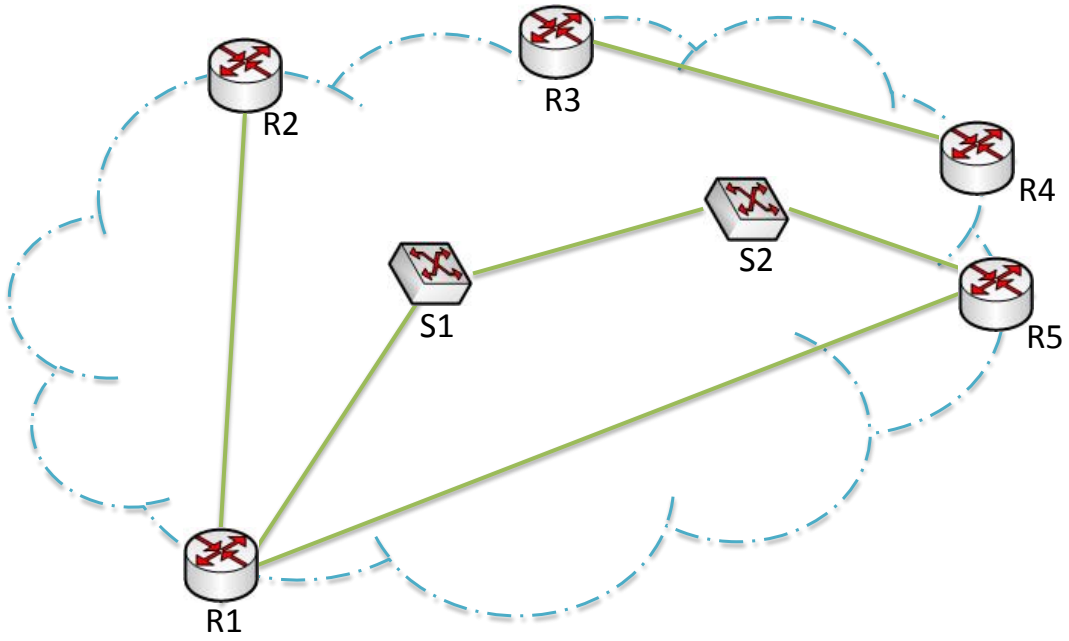


Abbildung 4.5.: Beispielnetz, Netzkomponenten Sicht

Zunächst sieht man auf der Abbildung eine Reihe von Routern und Switches, die miteinander physisch verbunden sind. Für die bessere Referenzierbarkeit werden die Router und Switches in dem Beispiel mit eindeutigen Bezeichnern versehen, die entsprechend mit den Buchstaben "R" oder "S" anfangen. Die Router werden an der Grenze der SP-Domäne platziert, die Switches dagegen ausschließlich innerhalb der Domäne, was eine typische[1] Situation darstellt. Die Verbindung zwischen Netzkomponenten ist bei weitem nicht voll vermascht. So existieren zwischen R1 und R2 sowie zwischen R3 und R4 direkte Verbindungen. Zwischen R1 und R5 existiert sowohl eine direkte als

[1] An dieser Stelle soll die klare Teilung nur betonen, dass die Infrastruktur an der Domänengrenze oft eine erweiterte Funktionalität aufweisen soll. Dem Einsatz von Routern als domaininterne Infrastruktur von IP-Netzen steht hauptsächlich der Kostenfaktor entgegen.

auch eine indirekte Verbindung über S1 und S2. Zwischen R2 und R5 ist ausschließlich eine indirekte Verbindung (über R1) möglich. Weiterhin, auch wenn das für die Providernetze eher untypisch ist[2], bildet die so zusammengeschaltete Netzinfrastruktur zwei physisch voneinander getrennte Sub-Netze (mit R3 und R4 in einem und der restlichen Infrastruktur in dem anderen Sub-Netz).

SCP: Service Connection Point

Aus Providersicht stellen alle Verbindungen, die zwischen der Infrastruktur an der Domänengrenze realisiert werden, einen Dienst dar. Da für die Erbringung eines Verketteten Dienstes mehrere solche von unterschiedlichen Domänen erbrachte Dienste miteinander verbunden werden müssen, werden im weiteren Verlauf dieser Arbeit die Verbindungspunkte an der Grenze einer Domäne als *Service Connection Points* (SCP) referenziert. Die SCPs stellen dabei die Außensicht auf die Verbindungspunkte einer Domäne dar und verschatten deren konkrete Realisierung. Die Außensicht auf das Beispielnetz ist in Abbildung 4.6 dargestellt. Die Domäne selbst wird durch ein Oval repräsentiert. Die SCPs werden durch ausgefüllte Kreise an der Grenze dieses Ovals gekennzeichnet. Die direkten sowie indirekten Verbindungsmöglichkeiten zwischen SCPs innerhalb einer Domäne werden im weiteren Verlauf als *Domain Links*[3] referenziert.

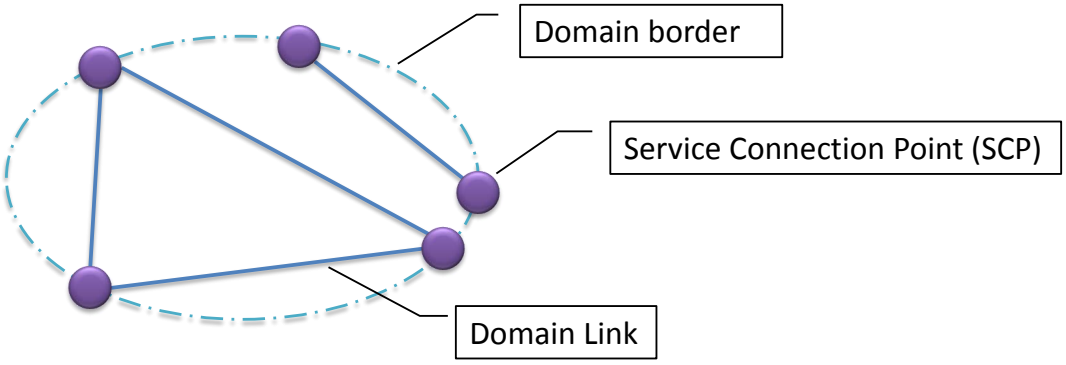


Abbildung 4.6.: Beispielnetz, Außensicht

Domänengrenze umreißt den Verantwortungsbereich des Service Providers

Bei der Domänengrenze handelt es sich um eine organisatorische Grenze, die den Verantwortungsbereich einer SP-Organisation für die Güte der von ihr erbrachten Diensten umreißt. Diese Definition schmälert keinesfalls die Möglichkeit eines Service Providers, einige benötigte Teildienste bei anderen Providern als Sub-Dienste hinzuzukaufen. Diese Aspekte werden durch die Domänengrenze von der Außensicht verschattet (vergleiche die Diskussion über Verantwortungsbereiche im Abschnitt 3.6).

[2] Gründe für diese Darstellung werden später im Abschnitt motiviert, wenn der Fokus der Beschreibung auf die für die Diensterbringung verfügbaren Ressourcen gelenkt wird.

[3] In der Fachliteratur werden Domain Links oft auch als *Intra-Domain Links* genannt.

Bemerkung: Da die Domänengrenze den Verantwortungsbereich des Service Providers umreißt, befinden sich an der Grenze sowohl die Infrastrukturkomponente, die den Anschluss an die Nachbardomäne realisiert, als auch die Infrastrukturkomponente, die den Service Access Point (SAP) für den Kunden realisiert. Das Beispielnetz spiegelt die Situation sowohl in Transit- als auch in Anschlussdomänen wider.

Eine Verbindung zwischen zwei SCPs kann unterschiedliche QoS-Parameter und deren Kombinationen unterstützen. Betrachtet man zunächst nur einen QoS-Parameter, wie etwa *Delay*, und setzt einfachheitshalber das Delay zwischen je zwei direkt miteinander verbundenen Netzkomponenten in der Abbildung 4.5 auf 1ms, so weisen die Verbindungen zwischen R1 und R2 sowie zwischen R3 und R4 jeweils 1ms Verzögerung auf. Zwischen R1 und R5 existieren zwei alternative Wege, die direkte Verbindung mit 1ms und die Verbindung über S1 und S2 mit 3ms Delay. Nach außen kann man das entweder als eine Verbindungsmöglichkeit beschreiben, die einen der beiden Werte aufweisen kann, oder als zwei mögliche Verbindungsmöglichkeiten, die unterschiedlichen QoS-Werte aufweisen können. Die Entscheidung darüber kann von jedem Service Provider entsprechend domaininterner Policies getroffen werden. Die Variante mit einer Verbindung hat z.B. den Vorteil, dass die interne Netzstruktur vollkommen verschattet wird; bei getrennten Beschreibungen ist es dagegen möglich, bei darauf referenzierenden Anfragen von Außen auf die Netzinfrastruktur rückzuschließen.

Betrachtet man mehr als nur einen QoS-Parameter gleichzeitig, so kann sich die Situation sehr schnell ändern. Nehmen wir an, dass die Ressourcenkapazität bei der direkten Verbindung zwischen R1 und R5 nur 2 Gbps mit 100Mbps Abstufungen beiträgt, die Verbindung über S1 und S2 dagegen bis zu 10Gbps mit Abstufung von 1Gbps (siehe Abbildung 4.7). In Kombination mit dem Delay aus der vorherigen Betrachtung bedeutet das für zwei alternative Pfade zwischen R1 und R5 folgende Möglichkeiten:

- R1-R5: 1ms, bis zu 2 Gbps, 100Mbps Abstufung
- R1-S1-S2-R5: 3ms, bis zu 10 Gbps, 1Gbps Abstufung

Würde man die möglichen Ausprägungen von QoS-Parametern auf den beiden Alternativpfaden bei der Beschreibung einer Verbindungsmöglichkeit zwischen zwei SCPs einfach "zusammenlegen" (1 oder 3ms Delay, bis zu 10 Gbps mit Abstufungen 100Mbps oder 1Gbps), so könnte der Eindruck entstehen, dass z.B. eine 8,3Gbps Verbindung mit 1ms Delay zwischen R1 und R5 möglich ist, was aufgrund der HW-Komponenten im Beispiel unmöglich ist.

Eine ähnliche Situation betrifft auch die Managementfunktionalität, die mit den Verbindungsmöglichkeiten zwischen SCPs assoziiert werden kann. So können u.U. unterschiedliche Überwachungstechniken oder Managementfunktionen auf unterschiedlichen Realisierungspfaden möglich sein. Beispielsweise könnte es sein, dass bei der

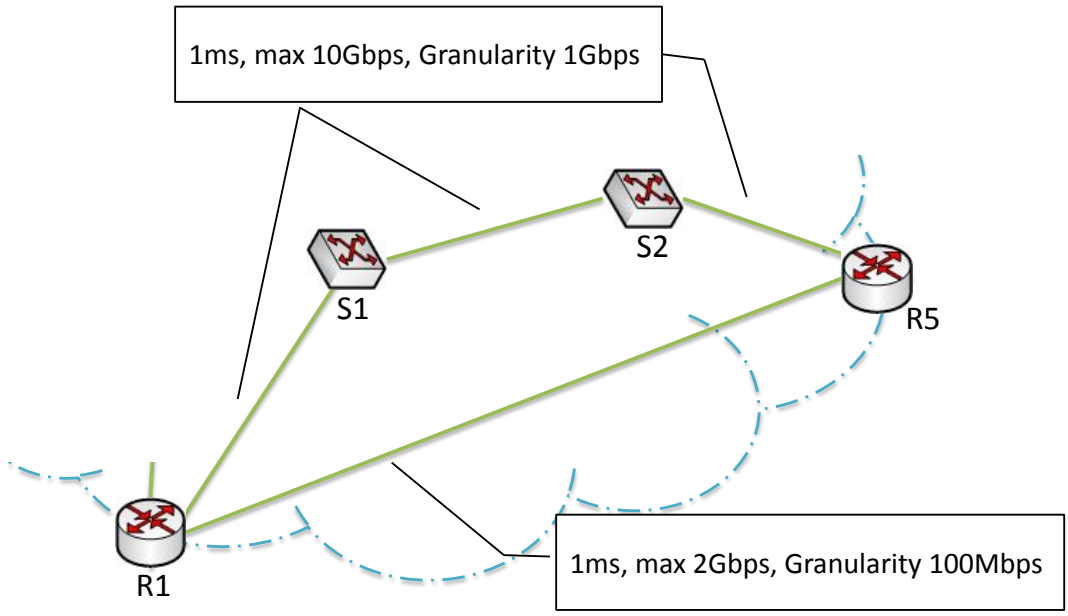


Abbildung 4.7.: Beispielnetz, Netzkomponenten Sicht mit 2 QoS-Parametern

direkten Verbindung zwischen R1 und R5 die Veränderung der vereinbarten Bandbreite im Betrieb unterstützt wird, bei der Route über S1 und S2 jedoch nicht (siehe Abbildung 4.8).

Die Auswirkungen von Unterschieden bei der unterstützten Managementfunktionalität, die auf alternativen Realisierungspfaden einer Verbindungsmöglichkeit zwischen zwei SCPs durch die Infrastrukturunterschiede bedingt sind, sind identisch mit den bereits besprochenen alternativen Realisierungspfaden mit mehreren QoS-Parametern. Um dieser Situation gerecht zu werden, werden die Verbindungsmöglichkeiten zwischen SCPs einer Domäne mit zwei Abstraktionsstufen modelliert (siehe Abbildung 4.9). Die Verbindungen zwischen SCPs auf diesen beiden Abstraktionsstufen werden in Anlehnung an die ITU-T Empfehlung G.805 (siehe dazu Abschnitt 3.6.1) als *Component* und als *Compound Links* referenziert.

Component Link

Unter einem *Component Link* wird eine Verbindungsmöglichkeit zwischen zwei SCPs verstanden, mit der eine Reihe von Eigenschaften (QoS-Parameter und Managementfunktionalitäten) samt ihren möglichen Wertebereichen assoziiert sind. Alle mit einem *Component Link* assoziierten Eigenschaften sind innerhalb der erlaubten Wertebereiche voneinander unabhängig, d.h. die Verbindung zwischen zwei SCPs mit jeder erlaubten Eigenschaftenkombination ist realisierbar.

Compound Link

Bei einem *Compound Link* zwischen zwei SCPs handelt es sich dagegen um einen Container, der alle *Component Links* zwischen diesen SCPs umfasst. Ein *Compound Link* soll mindestens einen *Component Link* beinhalten, somit kann er auch als ein

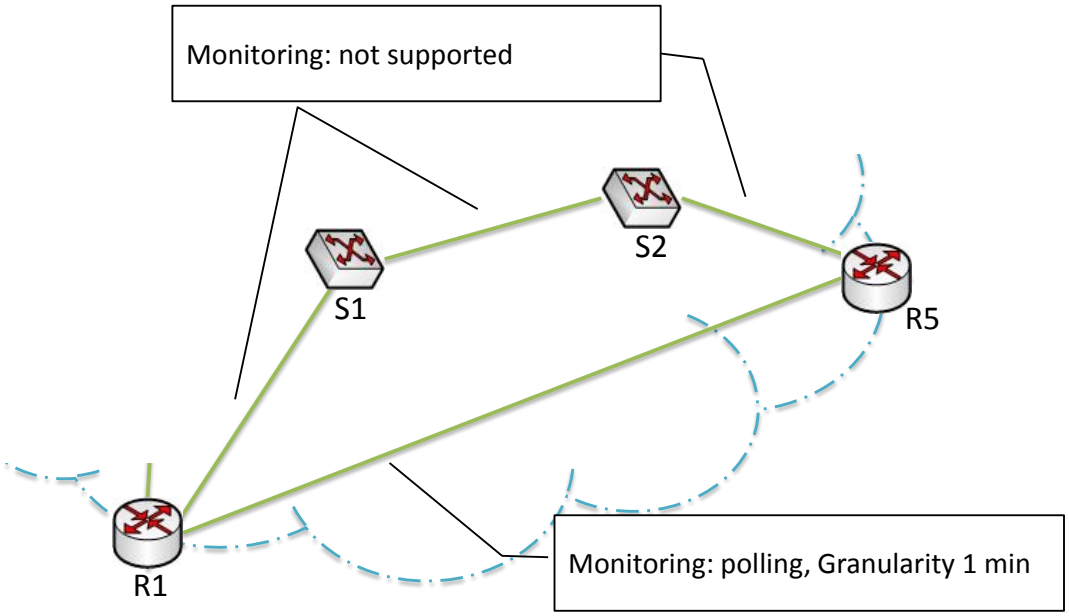


Abbildung 4.8.: Beispielnetz, Netzkomponenten-Sicht mit unterschiedlichen Überwachungsoptionen

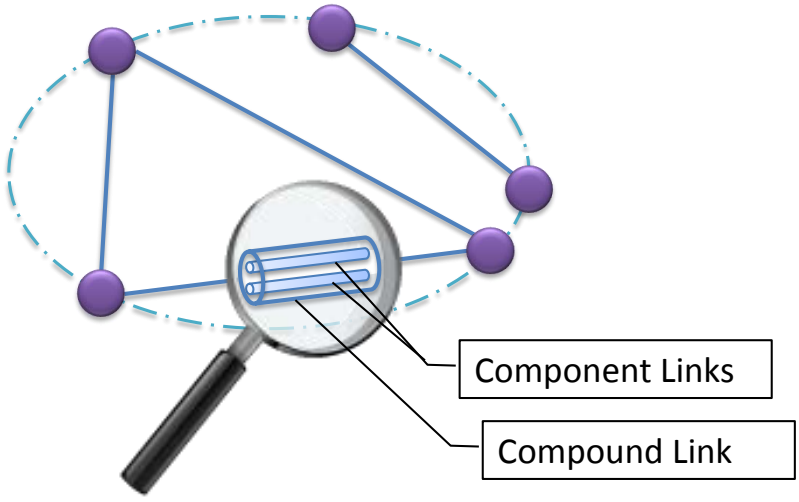


Abbildung 4.9.: Ein *Compound Link* unter der Lupe

Indikator für die grundsätzliche Verbindungsmöglichkeit zwischen zwei SCPs verwendet werden. Durch einen *Compound Link* werden keine Einschränkungen auf die darin enthaltene *Component Links* auferlegt. So können die darin enthaltenen *Component Links* bei ihrer Realisierung u.U. auf dieselbe Infrastruktur angewiesen sein und somit eventuell nicht gleichzeitig realisierbar sein.

Zusammenfassend können hier folgende Vorgaben für die Modellierung der Kommunikationsartefakte festgelegt werden:

Vorgabe (UML-Modellierung) VM01 - SCPs, Verbindungen und Eigenschaften

Jede SP-Domäne soll in der Lage sein, mehrere *Compound Links* zu definieren. *Compound Links* sollen anhand zwei SCPs, die sie verbinden, eindeutig identifizierbar sein. Jedes *Compound Link* soll mindestens ein *Component Link* beinhalten, mit dem die unterstützten Eigenschaften assoziierbar sein sollen. Unter Eigenschaften werden sowohl QoS-Parameter als auch Managementfunktionalität verstanden. Mit einem *Component Link* soll eine beliebige Anzahl sowie beliebige Kombinationen der Eigenschaften assoziierbar sein.

Durch die Festlegung, die *Compound Links* durch ihre zwei SCPs zu identifizieren, wird auch die Notwendigkeit der Identifizierung aller SCPs verursacht:

Vorgabe (Identifizierung) VI02 - SCPs

Jeder SCP soll mit einer ID versehen werden, die mindestens im Domain-Scope eindeutig ist.

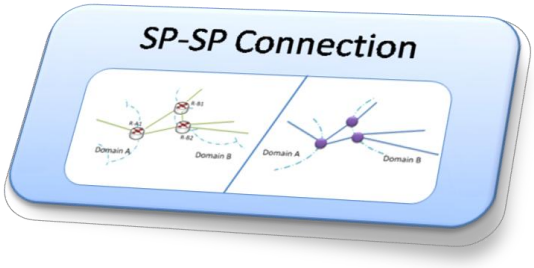
Um mit *Component Links* beliebig viele Dienstgüteeigenschaften assoziieren zu können, muss folgendes erfüllt werden:

Vorgabe (Identifizierung) VI03 - Identifikation der Eigenschaften

Jede unterstützte Eigenschaft soll global eindeutig identifizierbar sein.

Die entsprechenden Modellierungs- und Identifizierungsaspekte werden im Abschnitt 4.6 behandelt.

4.1.3. Anbindung an die Nachbar-Domänen



In diesem Unterabschnitt wechselt der Fokus der Beschreibung zu den Verbindungen zwischen aneinander angeschlossenen Service-Provider-Domänen. Bei der Beschreibung werden ausschließlich die Unterschiede zu domaininternen Verbindungen betont sowie die Lösungen für die dadurch entstehenden Herausforderungen beschrieben werden.

Aus technischer Sicht sind Verbindungen zwischen zwei benachbarten Service Provider Domänen nicht viel anders realisiert als Verbindungen zwischen SCPs innerhalb einer Domäne. Von einer Reihe technischer Besonderheiten der zwei prinzipiellen Verbindungsarten[4], die auf die Betrachtung von QoS-Eigenschaften keine Auswirkung haben, wird an dieser Stelle o.B.d.A. abstrahiert. Die Verbindung zwischen zwei SCPs benachbarter Domänen könnte prinzipiell genauso modelliert werden wie es für domäneninterne Verbindungen der Fall ist (siehe Abbildung 4.10).

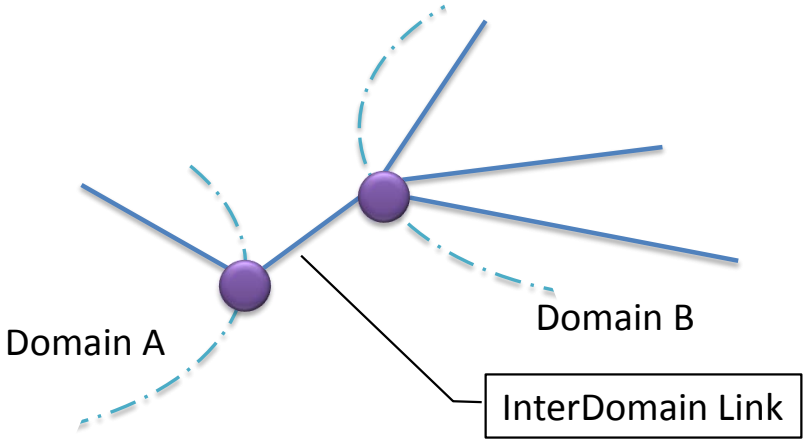


Abbildung 4.10.: Verbindung zwischen zwei SCPs benachbarter Domäne

In Anlehnung an den im Abschnitt 4.1.2 eingeführten Begriff "*Domain Link*", der als generelle Bezeichnung aller innerhalb einer Domäne liegenden Verbindungen verwendet wird, werden die Verbindungen zwischen zwei SCPs unterschiedlicher Domänen als *Interdomain Links* referenziert. Somit sind die Begriffe "*Domain Link*" und "*Interdomain Link*", die die Domainzugehörigkeit der SCPs an den Enden eines

[4]So werden Verbindungen über große Distanzen, die für domaininterne Verbindungen typisch sind, durch mehrere miteinander verkettete physische Strecken mit dazwischengeschalteten Netzkomponenten realisiert. Die physischen Verbindungen zwischen Domänen sind dagegen oft sehr kurz und werden häufig mit Hilfe der sog. *Patch Panels* zusammengeschaltet.

Links ansprechen, orthogonal zu den Begriffen "*Compound Link*" und "*Component Link*", die entsprechend die Möglichkeit mindestens einer Verbindung zwischen zwei SCPs bzw. die Verbindungsmöglichkeit samt der dafür erlaubten Eigenschaften bezeichnen.

Zwei Teil-Sichten auf ein Interdomain Link

Was *Interdomain Links* im Vergleich zu Domain Links besonders macht, ist die Tatsache, dass jede der beteiligten Domänen normalerweise Zugriff ausschließlich auf die eigene Netzinfrastruktur hat. Somit fehlt bei jeder SP-Domäne Information über das andere Ende einer Interdomain-Verbindung, geschweige denn der Managementzugriff auf die Netzinfrastruktur der benachbarten Domäne. Aus Modellierungssicht entsteht dadurch folgende Vorgabe:

Vorgabe (UML-Modellierung) VM02 - Aufbau von *Interdomain Links*

Es muss möglich sein, zwei getrennte Sichten auf ein und denselben *Interdomain Link* zu haben. Jede SP-Domäne soll in der Lage sein, ausschließlich ihre Teilsicht zu spezifizieren.

In Bezug auf die Problemstellung dieser Arbeit müssen folgende Herausforderungen gelöst werden, die durch die getrennten Teil-Sichten bedingt sind:

- Informationen aus zwei aneinander angeschlossenen SP-Domänen müssen miteinander in Verbindung gebracht werden (Matching) und
- Aus zwei Sichten auf die Verbindungseigenschaften soll eine korrelierte Aussage über die Verbindung gemacht werden können.

Teil-Sichten miteinander in Verbindung bringen

Die erste Aufgabe kann am Beispiel optischer Verbindungen verdeutlicht werden. So müssen sich beide SP-Domänen sowohl auf denselben Lichtwellenleiter als auch auf dieselbe Lichtwellenlänge einigen. Falls nur eins von beiden nicht übereinstimmt, würden sich die Aussagen auf zwei unterschiedliche optische Verbindungen beziehen.

An dieser Stelle wird folgende Lösung vorgeschlagen: Alle *Component Links* bei der Beschreibung der Teil-Sichten sollen sich ausschließlich auf physisch unterschiedliche Verbindungen beziehen. Weiterhin sollen diese *Component Links* mit IDs versehen werden, die bei beiden SP-Domänen für dieselben physischen Verbindungen stehen. Sollte das der Fall sein, können die Teilsichten der benachbarten SP-Domänen anhand dieser IDs in die Verbindung gebracht werden.

Abbildung 4.11 illustriert das Matchen einzelner Sichten auf dieselben Verbindungen anhand ihrer IDs ausschaut. Aus Sicht der Domäne A sind drei Verbindungen mit den IDs "Id1", "Id2" und "Id3" realisierbar; Domäne B sieht nur zwei Möglichkeiten, die mit "Id2" und "Id5" identifiziert werden. Die Gründe für diese Nichtübereinstimmung können unterschiedlicher Natur sein und sich von z.B. "Infrastruktur ist noch nicht installiert" über "Infrastrukturressourcen sind belegt" bis hin zu "Ausfall der Ressource"

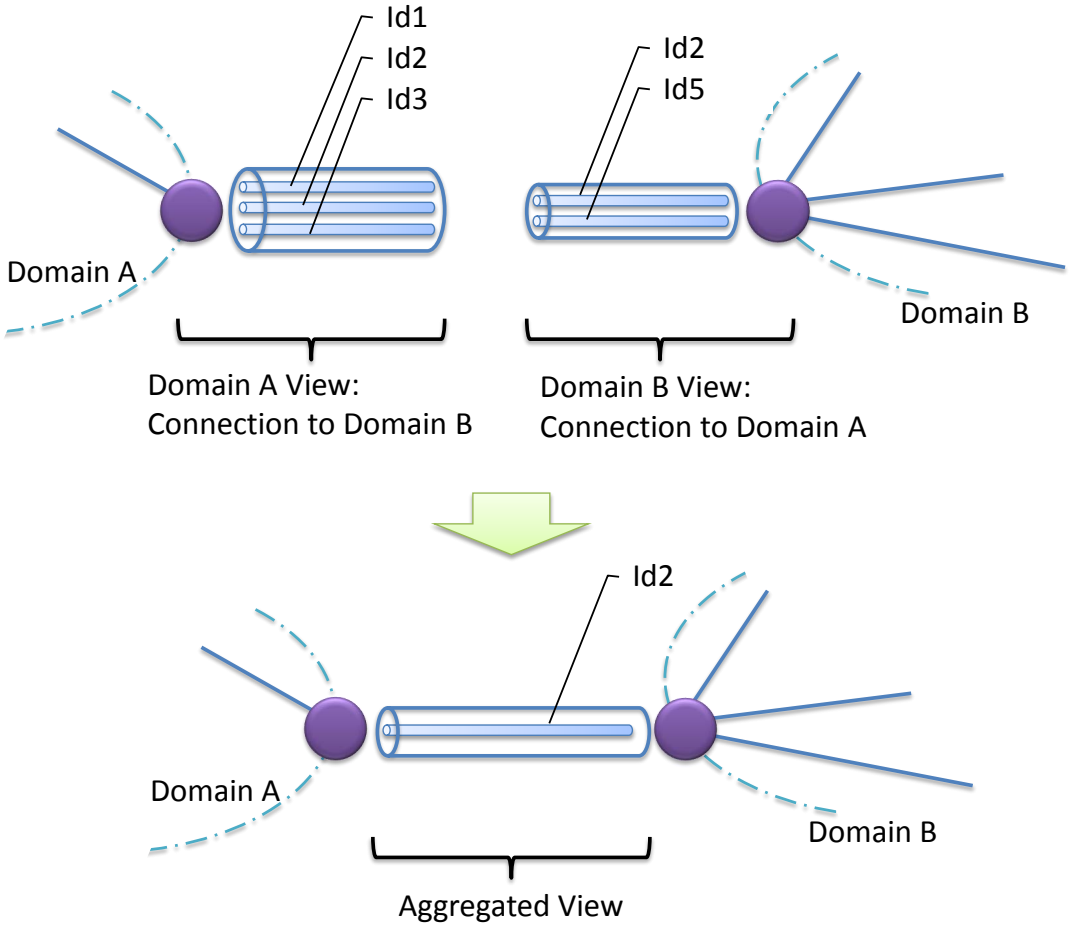


Abbildung 4.11.: "Verbindung" der Component Links durch ihre IDs

variieren. Im konkreten Beispiel ist daher nur ein Component Link mit "Id2" zwischen den beiden SCPs der Domänen A und B möglich.

Dieses Vorgehen führt zu folgender Vorgabe:

Vorgabe (Identifizierung) VI04 - *Component Links* bei *Interdomain*-Verbindungen

Zumindest bei *Interdomain Links* muss jeder *Component Link* mit einer ID versehen werden. Für diese IDs ist Eindeutigkeit zwischen zwei aneinander angeschlossenen SP-Domänen erforderlich. Das Vergabeverfahren für diese IDs soll in der Lage sein, der Dynamik der Veränderungen bei den realisierbaren Verbindungen und deren Verbindungseigenschaften zu genügen.

Während infrastrukturbezogene Informationen zwischen Nachbardomänen sowie in kleinen statischen Providerkooperationen üblicherweise aufgrund der bestehenden

Vertrauensverhältnisse gegenseitig ausgetauscht werden, soweit notwendig, kann eine Anfrage bzgl. einer Infrastruktur-Information von einer unbekannten bzw. einfach nicht direkt angeschlossenen SP-Domäne in großen, dynamischen SP-Kooperationen aufgrund domäneninterner Policies zurückgewiesen werden.

Ein Ausweg aus dieser Situation kann durch folgende Festlegung gewährleistet werden:

Festlegung: Infrastrukturbezogene Teilsichten auf die *Interdomain Links* dürfen ausschließlich von den unmittelbaren Nachbarn gesehen werden. Bei allen Multi-Domain Operationen, wie z.B. Informationsabfragen, Bestellung oder Monitoring, sollen die benachbarten SP-Domains die Proxy-Rolle für den kompletten *Interdomain Link* übernehmen.

Das bedeutet, dass z.B. bei *Interdomain-Link*-bezogenen Informationsanfragen eine Domäne ihre eigene Teilsicht mit der Teilsicht der benachbarten SP-Domäne aggregieren und der anfragenden SP-Domäne die bereits aggregierte Information mitteilen soll. Die aggregierte Informationen können eine abstrahierte – an die Anforderungen des Customers "zugeschnittene" und/oder an die Provider-Policies angepasste – Darstellung haben.

Während bei einem relativ selten auftretenden Anfragen für neue Dienstinstanzen *on-demand* Informationsanfragen ausreichen sollten, kann ein "Abonnieren" der aktuellen Informationen bei steigender Dynamik eine bevorzugte Lösung darstellen. Abonnieren beide Nachbardomänen A und B gegenseitig die Informationen über den Zustand ihrer Verbindung aus der Sicht des jeweils Anderen, so werden Benachrichtigungen bei Veränderungen in beide Richtungen geschickt (siehe Abbildung 4.12).

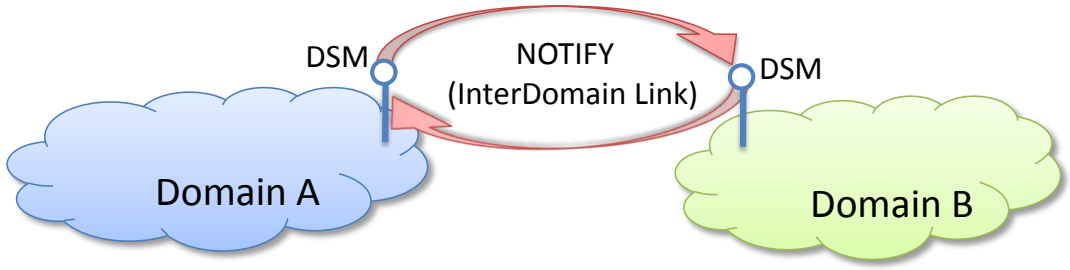


Abbildung 4.12.: Gegenseitige Benachrichtigung über Teilsicht

Analog wie bei Anfragen zu Informationen über *Interdomain Links* soll eine Domäne stellvertretend für die beiden Nachbardomänen auch Service-Requests entgegennehmen. Falls die Anfrage akzeptiert wird, soll die SP-Domäne, die als Stellvertreter (engl.: *Proxy*) agiert, eine infrastrukturbezogene Anfrage an die Nachbardomäne schicken.

Diese Festlegung verursacht die folgende Anforderung bzgl. der Modellierung:

Vorgabe (UML-Modellierung) VM03 - Aggregierte Sicht auf *Interdomain Link*

Zusätzlich zu einer getrennten Modellierung von Teilsichten muss es möglich sein, eine korrelierte Sicht auf *Interdomain Link* zu beschreiben.

Aggregation der Teilsicht-Eigenschaften

Die zweite in Bezug auf *Interdomain Links* identifizierte Aufgabe – Berechnung eines Aggregatwertes aus zwei Teil-Sichten – wird wegen ihrer Komplexität im Abschnitt 4.2 behandelt.

Dynamic der SCPs

Ein weiterer Aspekt hängt mit der eingesetzten Netzinfrastruktur und deren Kombination zusammen. Die am Anfang dieses Abschnittes in Abbildung 4.10 präsentierte Außensicht auf die Verbindung zwischen zwei SP-Domänen kann durch unterschiedliche technische Lösungen realisiert werden. In Abbildung 4.13 ist eine mögliche Realisierung dargestellt, bei der Domain A nur einen und Domain B zwei miteinander verbundene Router verwenden.

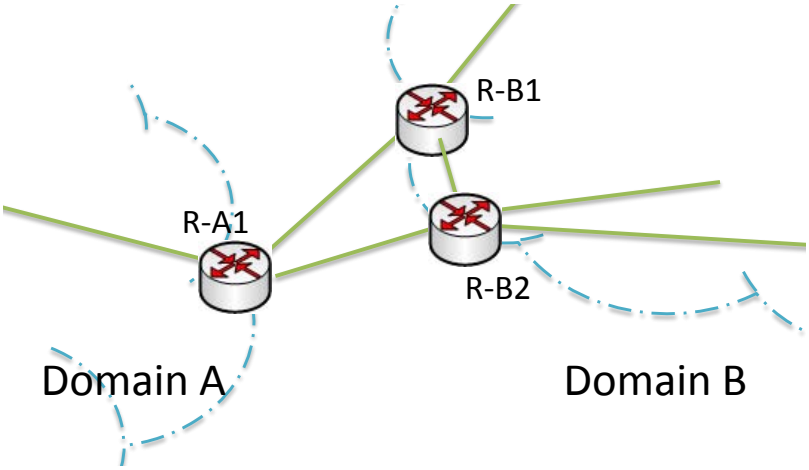


Abbildung 4.13.: Realisierung der Verbindung zwischen zwei Domänen

Solange die Verbindung zwischen den zwei Routern "R-B1" und "R-B2" existiert und die benötigten Eigenschaften aufweist, können die beiden für den Außenbeobachter als ein einziges SCP dargestellt werden. Sollte jedoch die Kapazität der Verbindung zwischen "R-B1" und "R-B2" durch die andere Verbindungen erschöpft werden oder nicht die benötigten QoS-Eigenschaften aufweisen, "zerfällt" ein logischer SCP in zwei (siehe Abbildung 4.14). Somit kann die Verbindung zwischen SCPs aus unterschiedlichen SP-Domänen als QoS-gebundener Systemschnitt betrachtet werden.

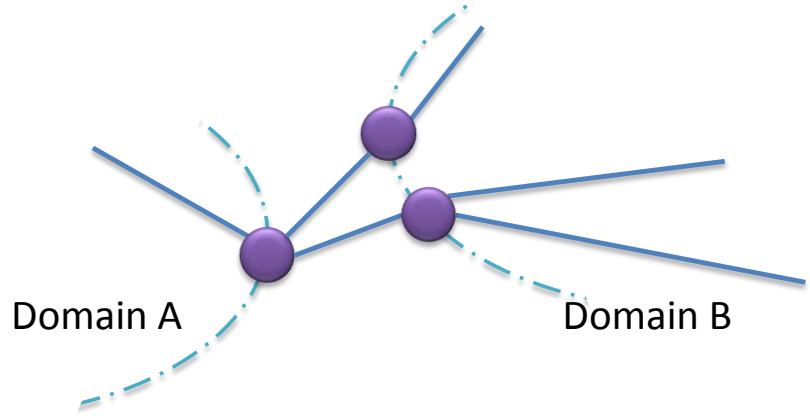


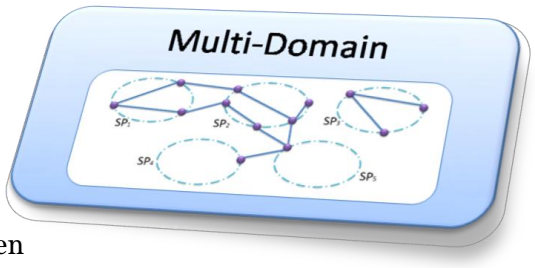
Abbildung 4.14.: Ein SCP "zerfällt" in zwei

Solche Veränderungen der Topologiebeschreibung einer Domäne können u.a. zu Inkonsistenzen bei der Multi-Domain-Sicht führen (für die Diskussion über den Aufbau dieser Sicht siehe Abschnitt 4.1.4). An dieser Stelle ist vor allem die Identifizierung der entstehenden SCPs interessant, die auch folgendes Designkriterium erfüllen muss:

Vorgabe (Identifizierung) VI05 - Dynamik von SCP-IDs

Die Identifizierungsart von SCPs soll es ermöglichen, die neuen IDs schnell zu vergeben.

4.1.4. Aufbau der Multi-Domain Sicht



Die Multi-Domain-Sicht ist für den Routing-Algorithmus eine essentielle Voraussetzung zur Bestimmung aller Teilstrecken eines Verketteten Dienstes. Die Multi-Domain-Sicht wird darüber hinaus auch im Betrieb einer Dienstinstanz benötigt, um z.B. ihren Zustand aus den Monitoring-Zuständen aller Teilstrecken bestimmen zu können (vergleiche entsprechende Diskussion und Festlegungen im Abschnitt 3.6).

In der Betrachtung dieser Arbeit sind alle Service Provider unabhängige, gleichberechtigte Organisationen. Das bedeutet vor allem, dass es i.A. keinen Einblick in die Netzinfrastruktur der einzelnen Provider geben darf. Die Multi-Domain-Sicht kann sich daher ausschließlich aus den Außensichten der einzelnen SP-Domänen zusammensetzen, wie sie in den Abschnitten 4.1.2 und 4.1.3 beschrieben wurden. Das setzt zunächst die Lösung der folgenden zwei Aufgaben voraus:

- Kommunikation mit den einzelnen SP-Domänen, um die Außensicht abzufragen und
- Das Ableiten einer Multi-Domain-Sicht aus den Single-Domain-Sichten

Da die Art der Kommunikation unabhängig von den übertragenen Informationen ist, wird das notwendige Kommunikationsprotokoll – vor allem wegen seiner Komplexität und seines Umfangs – in Kapitel 5 definiert. Die DSM Kommunikationsschnittstelle, über die die Kommunikation abgewickelt werden soll, wurde bereits im Abschnitt 4.1.1 eingeführt, um sie bei der Modellierung der Kommunikationsartefakte im Abschnitt 4.6 berücksichtigen zu können.

Aufbau der Multi-Domain-Sicht

Als eine Lösung für die zweite Aufgabe wird an dieser Stelle die Verwendung von *ID-Matching* vorgeschlagen, ähnlich wie das bereits für die Verbindung der Teilsichten auf *Interdomain Links* verwendet wurde (siehe Abschnitt 4.1.3). Graphisch ist das Verfahren zum Aufbau einer Multi-Domain-Sicht in der Abbildung 4.15 dargestellt. Die Betrachtung wird dabei auf zwei benachbarte SP-Domänen eingeschränkt, die ihre Außensicht auf vorhandene *Domain* und *Interdomain Links* mitteilen (in der Abbildung oben). Um die Erklärung möglichst einfach zu halten, wird an dieser Stelle davon ausgegangen, dass die aggregierte Sicht auf die Verbindungsmöglichkeit zwischen SP-Domänen nur von einem der verbundenen Nachbarn gemeldet wird (in der Abbildung – Domain A). Je nach dem Routing-Verfahren können beide benachbarte SP-Domäne Informationen über die sie verbindenden *Interdomain Links* mitteilen, dann wird jedoch der Ausschluss von Duplikaten benötigt (mehr dazu siehe im Abschnitt 4.3)

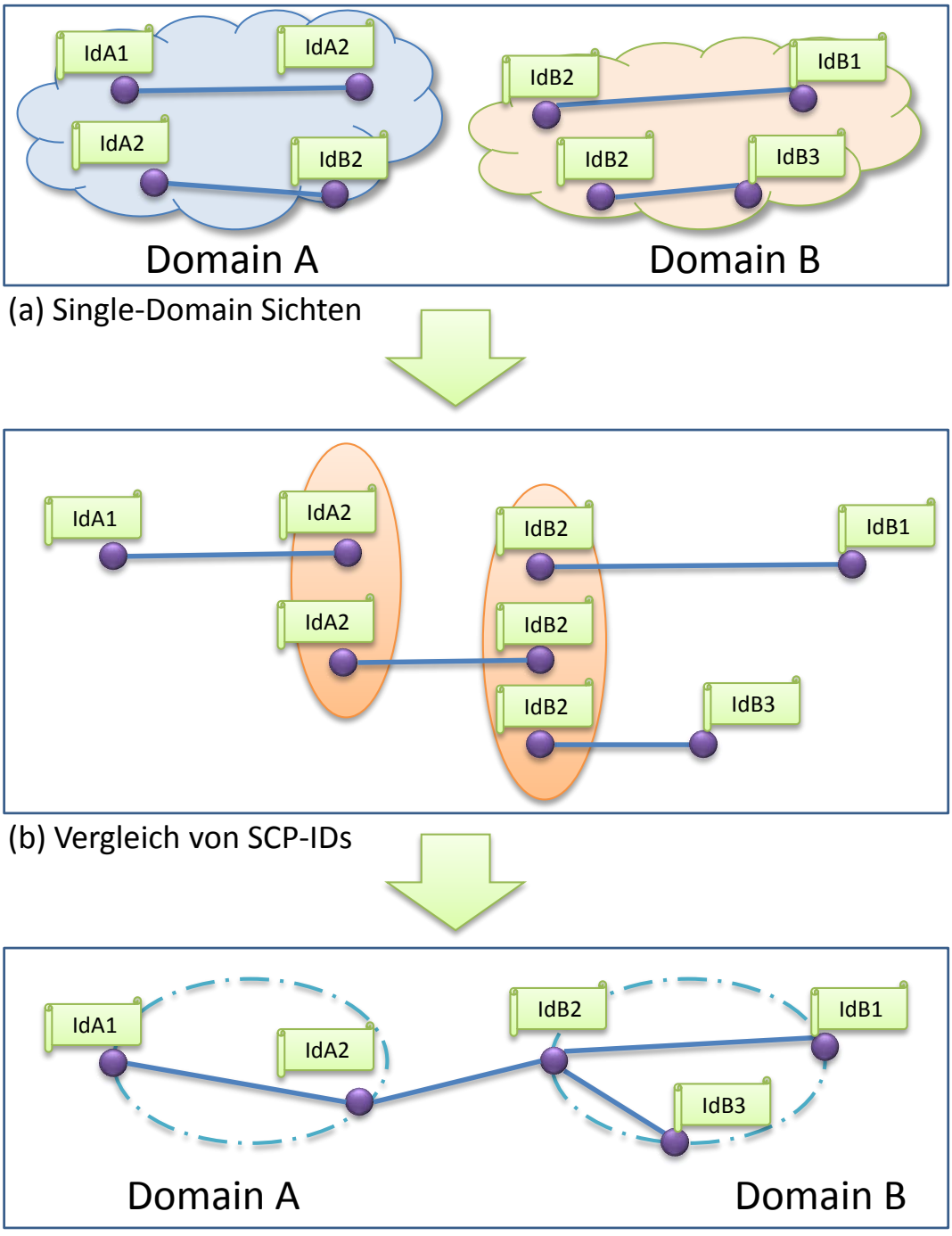


Abbildung 4.15.: Verbindungsmöglichkeiten, Ableitung der Multi-Domain Sicht

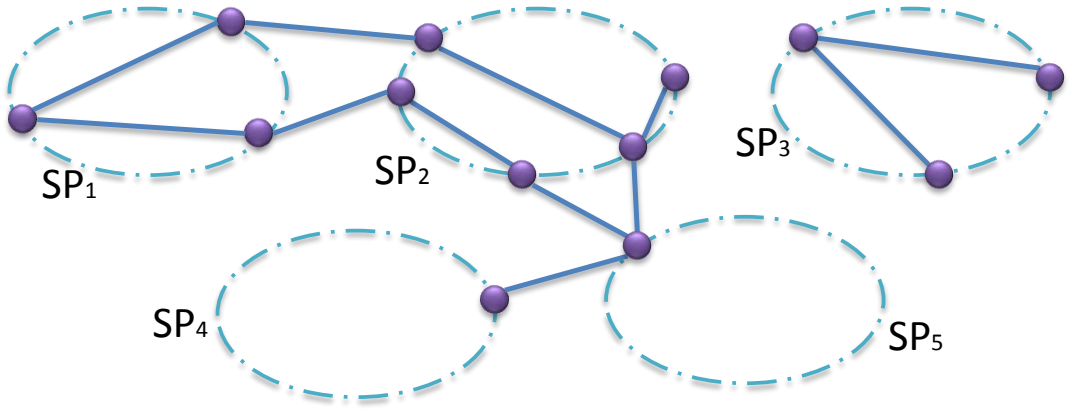


Abbildung 4.16.: Vorauswahl, Abstraktionsstufe *Compound Links*

Im nächsten Schritt können alle bekannten *Domain* und *Interdomain Links* an den SCPs miteinander verbunden werden, deren IDs übereinstimmen (siehe Darstellung in der Mitte der Abbildung). Dabei muss folgende Voraussetzung erfüllt werden:

Vorgabe (Identifizierung) VI06 - Globale Eindeutigkeit von SCP-IDs

Die ID jedes SCP muss global eindeutig sein.

Da laut der Definition im Abschnitt 4.1.2 jeder SCP an der Grenze der ihn erbringenden SP-Domäne "platziert" ist, ist das Ergebnis dieser Verbindung eine Multi-Domain Darstellung der möglichen Verbindungen und deren Eigenschaften, wie das graphisch unten in der Abbildung 4.15 unten dargestellt ist.

Wie eine Multi-Domain-Sicht mit fünf SP-Domänen aussehen kann, ist in der Abbildung 4.16 präsentiert. In dieser Abbildung sieht man deutlich, dass, um zwischen den einzelnen SP-Domänen unterschieden zu können, folgende Vorgabe erfüllt werden muss:

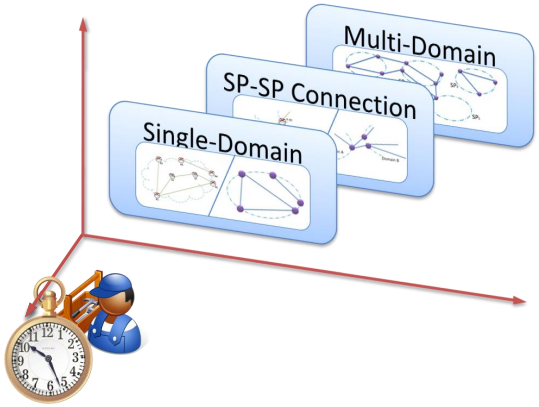
Vorgabe (Identifizierung) VI07 - Domain-IDs

Bei der Modellierung der Kommunikationsartefakte soll es möglich sein, jeder SP-Domäne eine global eindeutige ID zuzuweisen.

Wie bereits erwähnt wurde, wird eine Multi-Domain-Sicht auch im Betrieb einer Dienstinstanz benötigt. In dieser Arbeit wird davon ausgegangen, dass die beim Routing getroffenen Festlegungen über die Zusammensetzung einer Dienstinstanz auch im Betrieb bekannt sind. Sollte das nicht der Fall sein, kann auch da das ID-Matching-Verfahren die Abhilfe schaffen. Für eine Beschreibung darüber, wie dieses Verfahren beim E2Emon-Projekt eingesetzt wurde, siehe Abschnitt 8.1.

4.1.5. Berücksichtigung weiterer Aspekte

Die bislang geführte Diskussion fokussierte sich ausschließlich auf die Beschreibung der Zusammenhänge, die bei einem einzigen Dienst auf der vorhandenen Infrastruktur realisiert werden können. Diese idealisierte Sicht entspricht nur bedingt der Realität. In diesem Unterabschnitt werden deswegen die bislang ausgeblendeten Aspekte der Diensterbringung diskutiert und dadurch die notwendigen Erweiterungen des bisher sehr einfachen Modells motiviert.



Unterstützung unterschiedlicher Dienste

Netzkomponenten und physische Verbindungen können für die gleichzeitige Erbringung unterschiedlicher Dienste verwendet werden. So können z.B. bei ISDN sowohl Sprach- als auch Datenübertragungsdienste auf derselben Infrastruktur durchgeführt werden. Genauso können durch die Service Provider u.U. auf derselben Infrastruktur Dienste auf verschiedenen Schichten angeboten werden, wie z.B. das sog. *Lambda Switching* (zu Deutsch: Zusammenschalten der Wellenlängen bei optischen Verbindungen) auf ISO/OSI Schicht 1, über TCP/IP-Verbindungen auf Schichten 3 und 4 bis hin zu Verbindungen auf der Anwendungsebene (ISO/OSI Schicht 7). Für die Kommunikationsartefakte bedeutet das:

Vorgabe (UML-Modellierung) VM04 - Berücksichtigung unterschiedlicher Dienste

Bei der Modellierung möglicher Verbindungen muss berücksichtigt werden, dass sie zu unterschiedlichen Diensten gehören können.

Ressourcen Verwaltungszustände

Weiterhin verwendet ein Service Provider eine vorhandene Infrastruktur üblicherweise nicht ausschließlich zur Erbringung einer einzigen Dienstinstanz für einen einzigen Kunden, sondern versucht möglichst viele Dienstinstanzen für mehrere Kunden gleichzeitig zu erbringen. Das bedeutet, dass die bei den SP-Domänen vorhandenen Ressourcen für die Erbringung der Dienstinstanzen unterschiedlicher Kunden reserviert werden und nach der Abbestellung dieser Dienstinstanzen freigegeben werden. Sollte es bei der Bestellung eines Verketteten Dienstes möglich sein, ein in der Zukunft liegendes Zeitfenster zu spezifizieren (vergleiche dazu die Diskussion über DCN im Abschnitt 2.3.4), dann muss das auch bei den Kommunikationsartefakten berücksichtigt werden.

Vorgabe (UML-Modellierung) VM05 - Spezifikation von Zeitfenstern

Bei Informations- und Bestellanfragen muss es möglich sein, ein erwünschtes Zeitfenster für eine neue Dienstinstanz zu spezifizieren.

Berücksichtigung potentiell möglicher Teildienste

Ein weiterer Aspekt kommt durch die Möglichkeit hinzu, die Domäneninfrastruktur falls nötig auszubauen. Ob die Inbetriebnahme eines noch nicht vorhandenen Teils der Infrastruktur von der SP-Domäne bereits geplant wurde oder ob diese Infrastruktur für eine neue Dienstinstanz erst beschafft und installiert werden muss, spielt aus Kundensicht eine untergeordnete Rolle. Sollte die Installation und Inbetriebnahme der neuen Infrastruktur noch vor der geplanten Inbetriebnahme einer neuen Dienstinstanz möglich sein, kann die noch nicht vorhandene Infrastruktur für die Realisierung dieser Dienstinstanz reserviert werden.

Für den Kunden eines Dienstes, der auf eine noch nicht vorhandene Infrastruktur angewiesen ist, spielt allerdings der Unsicherheitsfaktor eine große Rolle. So ist die Wahrscheinlichkeit, dass die Inbetriebnahme der noch nicht vorhandenen Infrastruktur länger als geplant dauert, deutlich größer als die, dass eine bereits vorhandene ausfällt. Aus diesem Grund soll es möglich sein zu unterscheiden, welche Dienste eine SP-Domäne ausschließlich unter Verwendung der bereits vorhandenen Infrastruktur realisieren kann und bei welchen sie auf die noch nicht vorhandene angewiesen ist. Da der Unsicherheitsfaktor und dessen Bedeutung eher Kunden- und oft auch Dienstinstanz-spezifisch zu beurteilen sind, soll bei der Beschreibung realisierbarer Eigenschaften nicht nur signalisiert werden, dass Teile der benötigten Infrastruktur fehlen, sondern auch ein Datum angegeben werden, bis wann alle fehlende Infrastrukturkomponenten planmäßig in Betrieb genommen werden können. Im Abschnitt 2.3.2 wurde gezeigt, dass es Dienste wie Géant2 E2E Links geben kann, bei denen von den Kunden der Unsicherheitsfaktor in Kauf genommen wird. Um auch solche Situationen bei*Verketteten Diensten* zu unterstützen, muss bei den Kommunikationsartefakten folgendes erfüllt werden:

Vorgabe (UML-Modellierung) VM06 - Spezifikation des Unsicherheitsfaktors

Bei den Informations- und Bestellanfragen muss es möglich sein, zu spezifizieren, ob die Dienstinstanz ausschließlich auf der bereits vorhandenen Infrastruktur realisiert werden soll, oder auch die potentiell möglichen Ressourcen und deren Eigenschaften mit einbezogen werden dürfen.

Die Umsetzung dieser und weiterer Vorgaben für UML-Modellierung und Identifizierung findet im Abschnitt 4.6 statt.

4.2. Operationen auf Eigenschaften und Graphen

Jeder Routing-Algorithmus ist immer auf zwei Operationen angewiesen – die Aggregationsfunktion, um z.B. die Teilstrecken-Werte entlang der ausgewählten Route aufeinander zu summieren, und die Vergleichsfunktion, um z.B. die aggregierten Werten mit den E2E-Anforderungen zu vergleichen. Zunächst wird im Unterabschnitt 4.2.1 diskutiert, wieso existierende Ansätze aus der Graphentheorie nicht ohne weiteres in dieser Arbeit übernommen werden können. Dabei wird auch darauf verwiesen, in welchen weiteren Unterabschnitten die relevanten Anpassungen definiert werden. Anschließend wird in den Unterabschnitten 4.2.7 und 4.2.8 an Beispielen gezeigt, wie die getroffenen Festlegungen umgesetzt werden können.

Die Struktur dieses Abschnittes ist graphisch in der Abbildung 4.17 dargestellt.

Abbildung 4.17.: Aufbau dieses Abschnittes

4.2.1. Problematik im Überblick und Abschnitt-Zielsetzung

Aggregations- und Vergleichsfunktionen

Bei klassischen Suchverfahren in gewichteten Graphen wird davon ausgegangen, dass als Aggregatfunktion die Addition auftritt und beim Vergleich der kleinere Wert bevorzugt wird (siehe auch Abschnitt 3.3). Betrachtet man die Dienstgüteeigenschaften, die in dieser Arbeit berücksichtigt werden sollen, dann ist dieses Vorgehen bei weitem nicht allgemeingültig.

Bei qualitativen QoS-Parametern kann pauschal die Regel getroffen werden, dass als die Aggregatfunktion die logische AND-Funktion agiert und beim Vergleich "unterstützt" besser als "nicht unterstützt" ist. Als Beispiel kann hier die Unterstützung einer EU-Richtlinie dienen, die erst dann E2E erfüllt werden kann, wenn alle Teilstrecken sie unterstützen.

Bei quantitativen QoS-Parametern ist die Situation wesentlich komplexer und kann zwischen unterschiedlichen Eigenschaften stark variieren. So entsprechen z.B. die Aggregations- und Vergleichsfunktionen bei Delay dem klassischen Fall: die Summe wird für die Aggregation verwendet und der kleinere Wert als der bessere betrachtet werden kann. Bei der Bandbreite ändert sich die Situation: die Aggregation wird durch die min-Funktion gegeben und diesmal der größere Wert als der bessere betrachtet.

Diese Situation verkompliziert sich im Zusammenhang mit Managementfunktionalität nochmals. Am Beispiel eines Wartungsfensters kann die Aggregatfunktion als die Schnittmenge der möglichen Wartungsfenster definiert werden. Als die Vergleichsfunktion kann z.B. das Enthaltensein eines Zeitfensters in einem anderen dienen.

Sonderfall: Interdomain Links

Ein weiterer Aspekt bezieht sich auf die Aggregation der Teilsichten auf einen *Interdomain Link*. Auch wenn die Aussagen von beiden SP-Domänen über Delay sich auf dieselbe Verbindung beziehen, können sie u.U. unterschiedlich sein. Gründe dafür können unterschiedlicher Natur sein und von den Unterschieden bei der Delay-Schätzung bis hin zu unterschiedlichen *Store-and-Forward*-Verzögerungen der eingesetzten Infrastruktur variieren. Aus diesem Grund wurde bei der Bestimmung des Wertes für *Component Link* der maximale Wert der beiden *Component Link Parts* genommen. Diese Berechnungsvorschrift unterscheidet sich jedoch von der Aggregationsvorschrift für den Pfad bei demselben QoS-Parameter.

Daraus ergibt sich folgende Zielsetzung, für die in diesem Abschnitt eine Lösung definiert werden muss:

Zielsetzung (Operationen) I - Eigenschaften zu Operationen Assoziation

Es muss definiert werden, wie mit den Eigenschaften die für den Routing-Algorithmus notwendigen Operationen assoziiert werden können. Die Unterschiede zwischen Inter-Domain und Multi-Domain Fällen müssen dabei berücksichtigt werden.

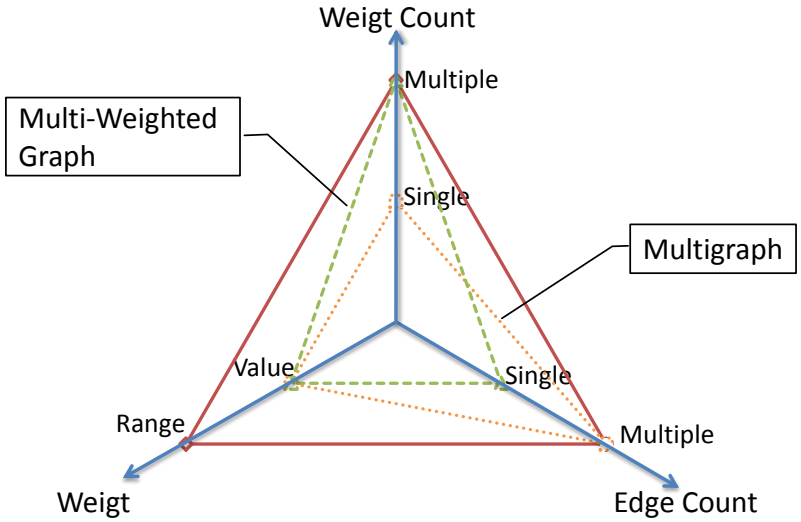


Abbildung 4.18.: Grapheneigenschaften, Einordnung

Um nicht nur die bereits angesprochenen, sondern u.U. auch weitere benötigten Funktionen gleichzeitig definieren zu können, wird eine Lösung für dieses Ziel erst im Abschnitt 4.2.6 präsentiert.

Graph-Zusammensetzung

Im Multi-Domain Fall setzt sich der Graph, in dem der Routing-Algorithmus nach einem geeigneten Pfad suchen soll, aus den Teilsichten einzelner SP-Domänen zusammen (siehe Abschnitt 4.1.4). Der Graph, der sich entsprechend den Festlegungen in Abschnitten 4.1 und 4.6 zusammensetzen lässt, weist einige Besonderheiten auf, die an dieser Stelle explizit angesprochen werden müssen.

Gesamtproblematik

Der Graph, in dem die Pfadsuche durchgeführt werden soll, kann anhand der drei Dimensionen aus der Abbildung 4.18 charakterisiert werden. Neben der sehr gut untersuchten einfachsten Variante – nicht mehr als eine Kante zwischen zwei Knoten mit jeweils nur einem ganzzahligen Gewicht pro Kante – sind im Bild gepunktet die sog. *Multigraphen* (Graphen bei denen mehr als eine Kante zwischen zwei Knoten möglich ist) sowie gestrichelt die sog. *Multi-Weighted Graphen* (jede Kante kann mehr als ein Gewicht haben) gekennzeichnet (vergleiche entsprechende Diskussion im Abschnitt 3.3). In Abhängigkeit davon, welche Informationen die SP-Domänen gemeldet haben (ein oder mehrere *Component Link*(s) sowie ein fester Wert oder ein Wertebereich bei der Beschreibung deren Eigenschaften) und wie viele welche Eigenschaften als E2E-relevant spezifiziert wurden (d.h. wie viele davon bei der Pfadsuche relevant sind), kann der Graph auch den komplexesten Fall aller drei Dimensionen aufweisen (in der Abbildung mit der durchgezogenen Linie gekennzeichnet). Im Übrigen wird von einem ungerichteten Graph mit nicht-negativen Gewichten ausgegangen. Die Zusammenhängigkeit des Graphen wird nicht vorausgesetzt.

Multi-Weighted Graphen

Wie im Abschnitt 3.3 bereits diskutiert wurde, kann die Abbildung mehrerer Gewichte auf nur einen zusammengesetzten Wert u.U. zu falschen Lösungen führen. Die dafür entwickelten Konzepte basieren jedoch auf den klassischen Aggregations- und Vergleichsfunktionen, weswegen für diesen Abschnitt auch folgendes Ziel gesetzt werden muss:

Zielsetzung (Operationen) II - Anpassung der Multi-Weight-Operationen

Die für die Multi-Weighted Graphen entwickelten Operationen müssen an die Verwendung der Eigenschaften-spezifischen Operationen angepasst werden.

Dieses Ziel wird separat für Aggregations- und für Vergleichsfunktionen in Abschnitten 4.2.2 und 4.2.3 verfolgt.

Multigraphen

Der klassische Umgang mit Multigraphen, wie er im Abschnitt 3.3 beschrieben wurde, besteht in dem Einfügen eines zusätzlichen Knotens in der "Mitte" jeder Kante. Rein theoretisch kann dieses Vorgehen auch bei mehreren *Component Links* ohne weiteres angewendet werden. Der Nachteil dieser Methode besteht allerdings darin, dass dadurch die Graphenkomplexität erheblich erhöht wird, was sich wiederum in der Suchlaufzeit widerspiegeln kann. Deswegen wird im Abschnitt 4.2.5 folgendes optionale Ziel verfolgt:

Zielsetzung (Operationen) III - Alternativer Umgang mit Multigraphen

Eine Alternative für den Umgang mit Multigraphen soll definiert werden. Diese Alternative soll auch die Anpassungen der Datenmodellierung sowie die Anforderungen an den Suchalgorithmus beinhalten.

Gewichte als Wertebereiche

Wertebereiche für Kantengewichte werden in der Graphentheorie nicht direkt behandelt. Die bereits besprochenen *Multigraphen* können als eine Art Workaround dafür betrachtet werden. Eine "Aufteilung" der Wertebereiche auf mehrere künstlich erzeugte Kanten würde die Graphenkomplexität und dadurch auch die Suchlaufzeit erheblich beeinträchtigen. Um solche Komplikationen zu vermeiden, wird im Abschnitt 4.2.4 folgendes Ziel verfolgt:

Zielsetzung (Operationen) IV - Umgang mit Wertebereichen

Es muss ein Verfahren definiert werden, wie Operationen auf festen Werten auf Wertebereiche übertragen werden können.

4.2.2. Multi-Weighted Graphen: Aggregatfunktionen und Pfadgewicht

Die Notwendigkeit der *Aggregatfunktionen* für die Teildiensteigenschaften (QoS-Parameter und Managementfunktionalität) wurde in diesem Abschnitt bereits angesprochen.

Da mit jedem Teildienst eine Reihe von Eigenschaften assoziiert ist, stellen die einzelnen Gewichte $\vec{W}_1$ bis $\vec{W}_n$ m-Dimensionalen Vektoren dar, wobei "m" für die Anzahl der relevanten Eigenschaften steht:

$$\vec{W}_i ::= (\mathrm{w}_{i,1}, ..., \mathrm{w}_{i,m})$$

$\mathrm{Aggr}_{\vec{v}}$ ist die Aggregatfunktion in dem Vektorraum, sie besteht aus m Aggregatfunktionen für die einzelnen Eigenschaften:

$$Aggr_{\vec{v}}(\vec{W}_i, \vec{W}_j) ::= (Aggr_1(\mathrm{w}_{i,1}, \mathrm{w}_{j,1}), ..., Aggr_m(\mathrm{w}_{i,m}, \mathrm{w}_{j,m}))$$

$\mathrm{Aggr}_{\vec{v}}$ kann somit nur dann assoziativ sein, wenn alle Aggregatfunktionen für die einzelnen Diensteigenschaften auch assoziativ sind.

Anzahl der Dimensionen m und deren Bedeutung können sich bei Verketteten Diensten von Fall zu Fall (von einer Dienstinstanz zur anderen) unterscheiden. Der Grund dafür sind die unterschiedlichen Eigenschaften, die der Endkunde als für seine Dienstinstanz relevant spezifiziert. Die Unterscheidung zwischen den einzelnen Diensteigenschaften geschieht anhand ihres Typs und der eindeutigen ID (QoS_ID, FUNCTIONALITY_ID, PROPERTY_ID), was auch Reihenfolgefreiheit erlaubt, in der diese Eigenschaften von jeder einzelnen SP-Domäne gemeldet werden.

Die Aggregatfunktionen, die die unterstützten Eigenschaften von *Interdomain Links* aus zwei "Informationshälften" miteinander verbundener SP-Domänen berechnen, müssen stets mit zwei Werten (Teilsichten) operieren und entsprechen somit der definierten binären Operation. Bei der Berechnung eines Pfadgewichtes müssen i.A. mehr als zwei Werte miteinander aggregiert werden. Damit die Berechnung mit Hilfe der Binärfunktionen durchgeführt werden kann, müssen folgende zwei Gleichungen erfüllt werden:

- $Aggr_{\vec{v}}(\vec{W}_1, \vec{W}_2, ..., \vec{W}_n) = Aggr_{\vec{v}}\ (Aggr_{\vec{v}}(\vec{W}_1, \vec{W}_2), ..., \vec{W}_n)$
- $Aggr_{\vec{v}}(Aggr_{\vec{v}}(\vec{W}_1, \vec{W}_2), \vec{W}_3) = Aggr_{\vec{v}}\ (\vec{W}_1, Aggr_{\vec{v}}(\vec{W}_2, \vec{W}_3))$

Grundsätzlich existieren für solche Berechnungen zwei Anwendungsfälle: bei der Wahl des Pfades zwischen zwei Endpunkten einer neuen Dienstinstanz, und zur Berechnung des E2E-Zustandes beim Dienstinstanz-Monitoring, falls ausschließlich die Überwachung von einzelnen Teildiensten möglich ist (siehe dazu "cascaded monitored connections" in Abschnitt 3.6.2). Diese Fälle unterscheiden sich grundsätzlich in zwei Aspekten: beim Monitoring werden die exakten Zustände aggregiert, bei der Pfadberechnung dagegen die erlaubten Wertebereiche, und – auch wenn das kein prinzipieller Unterschied ist – beim Monitoring werden ausschließlich die Wertezustände von quantitativen sowie das Vorhandensein von qualitativen QoS Parametern aggregiert, bei der Pfadberechnung muss bei der Aggregation noch die mögliche Managementfunktionalität und die dazugehörigen Parameter miteinbezogen werden. Somit wird für das Pfadgewicht eine Extradefinition gebraucht:

Pfadgewicht: als Pfadgewicht wird das Intervall von allen auf diesem Pfad realisierbaren Eigenschaften definiert: $\vec{\vec{W}}_{path} ::= [\vec{W}^{min}_{path}; \vec{W}^{max}_{path}]$.
Mögliche Abstufungen werden dabei nicht berücksichtigt. Wertebereiche beziehen sich sowohl auf QoS-Parameter als auch auf Managementfunktionalität und die zugehörigen Parameter.

Sollte die Schnittmenge eines so definierten Pfadgewichts mit den E2E-Anforderungen eine leere Menge ergeben, dann können durch diesen Pfad die Kundenanforderungen nicht erfüllt werden. Ansonsten existiert mindestens eine (nicht unbedingt optimale) zufriedenstellende Lösung.

Ableitung des E2E-Wertes

Die Berechnung eines Pfadgewichtes (abgesehen davon, ob es sich um den Monitoring-Wert oder die Ober- bzw. oder Untergrenze bei der Pfadsuche handelt) ist graphisch in Abbildung 4.19 dargestellt. Die einzelnen Werte-Vektoren sind in den Kästchen auf unterschiedlichen Ebenen abgebildet, zwischen den Ebenen sind symbolisch die für die Ableitung benötigten Operationen auf den Werten dargestellt. Die unterschiedliche Breite der Teildienste-QoS (unten im Bild) soll nur andeuten, dass die einzelnen Teildienste unterschiedliche geographische Ausdehnungen haben können, auf den eigentlichen Wert $\vec{W}_i$ hat das keine Auswirkung. Die Ableitungsrichtung ist von unten nach oben.

Eigenschaftstransformationen denen dazu, heterogene Informationen aus unterschiedlichen SP-Domänen auf eine gemeinsame Basis zu bringen, bevor die Einzelwerte aggregiert werden. Als ein Beispiel dafür kann die Berechnungsfunktion für Delay dienen, in der alle Delay-Werte zunächst in Mikrosekunden umgewandelt wurden. Es können allerdings – in Abhängigkeit von den QoS-Parametern – auch wesentlich kompliziertere Funktionen benötigt werden. Als ein Beispiel dafür kann der Unsicherheitsfaktor dienen, der sowohl als eine Erfolgswahrscheinlichkeit oder auch als Zeitangabe für eine geplante Infrastrukturinbetriebnahme angegeben wird. Die Berechnung eines E2E-Unsicherheitsfaktors bei "gemischten" Angaben beteiligter Domänen kann nur Policy-gesteuert geschehen. Denkbar wäre es allerdings, dass aus den Zeitangaben in

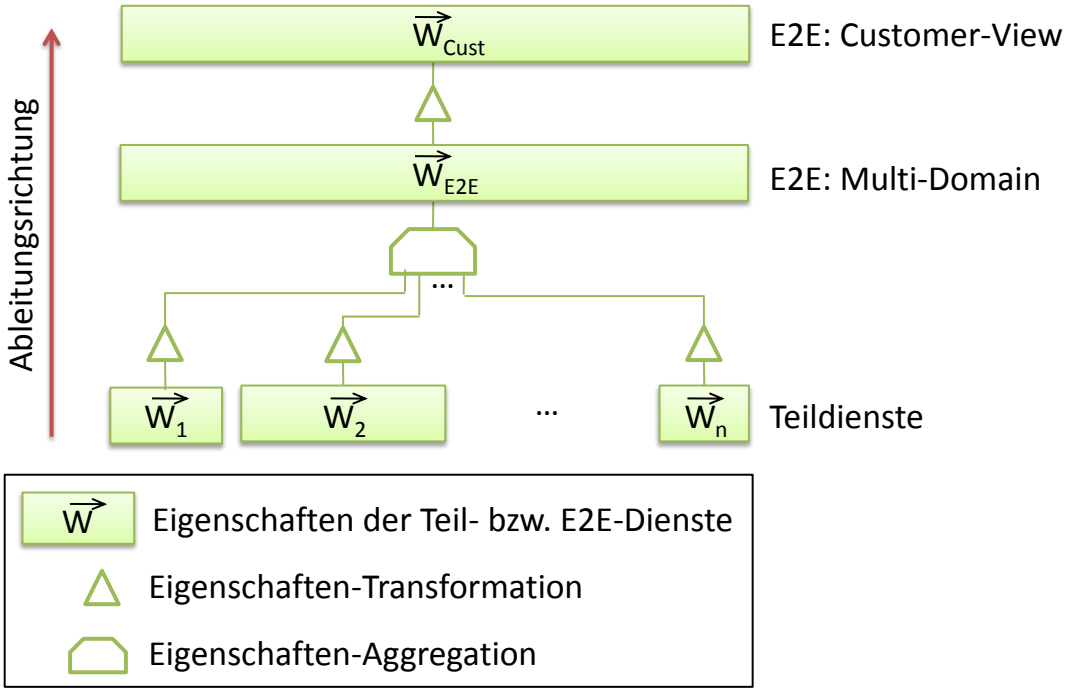


Abbildung 4.19.: Eigenschaften-Ableitung: von Teildiensten zu E2E

Abhängigkeit vom aktuellen Datum ein Wahrscheinlichkeitswert berechnet wird, der wiederum bei der Berechnung des E2E-Wertes[5] verwendet wird.

Nachdem die Eigenschaften zu einer gemeinsamen Basis transformiert wurden, können sie zu einem E2E-Wert $\vec{W}_{E2E}$ aggregiert werden. Unter Umständen wird danach eine weitere Transformation zu einem kundenspezifischen E2E-Wert $\vec{W}_{Cust}$ erforderlich. Als ein Beispiel dafür kann die Dienstverfügbarkeit dienen. Bei der Berechnung des Wertes $\vec{W}_{E2E}$ muss die Schnittmenge der Zeitintervalle aller Teildienste ermittelt werden, in denen die Teildienste verfügbar wären. Für den Customer muss die Verfügbarkeit dann prozentuell dargestellt werden, ausgehend von den mit dem Kunden definierten Verfügbarkeitszeiten.

[5] Für diese Berechnung sind wiederum unterschiedliche Alternativen denkbar, wie z.B. die bedingte Wahrscheinlichkeit oder der schlechteste Wert von allen Domänen.

4.2.3. Multi-Weighted Graphen: Vergleich im Vektorraum

Während die Aggregatfunktion (siehe Abschnitt 4.2.2) für die Berechnung des Pfadgewichtes und somit zur Findung eines zufriedenstellenden Pfades ausreicht, wird für die Suche nach einem optimalen Pfad eine *Vergleichsfunktion* benötigt. Außer der Pfadsuche kann die Vergleichsfunktion auch beim Monitoring verwendet werden, um die Tendenz der Zustandsveränderung (Verbesserung bzw. Verschlechterung) identifizieren zu können.

In der Graphentheorie werden als Gewichte grundsätzlich natürliche oder ganze Zahlen verwendet, wodurch auch eine natürliche Ordnung "eingeführt" wird. Als "bevorzugt" wird üblicherweise ein Pfad mit kleinerem Gewicht bezeichnet. Für mehrfachgewichtete Graphen wurde analog der Begriff von *non-dominance* wie folgt eingeführt: $\vec{W}_i$ ist nur dann non-dominant zu $\vec{W}_j$, wenn für alle k: $1 \leq k \leq m$ die Ungleichung "$w_{i,k} \leq w_{j,k}$" erfüllt ist (vergleiche die entsprechende Diskussion im Abschnitt 3.3).

Im Gegensatz zur klassischen Graphentheorie hängt die Bevorzugung eines Wertes gegenüber einem anderen auch vom QoS-Parameter und nicht nur vom Wertevergleich ab. Um ein Beispiel dafür zu geben, ist der kleinere Delay-Wert als der bessere zu betrachten, bei der Verfügbarkeit dagegen der größere Wert. Das macht die Einführung einer Ordnungsfunktion für jeden unterstützten quantitativen QoS-Parameter notwendig. Für qualitative Parameter ist diese Funktion nicht notwendig, denn für sie existiert – in Bezug auf erwünschte Eigenschaften – eine natürliche Ordnung: das Vorhandensein einer Eigenschaft ist bevorzugter als ihr Fehlen.

Bezeichnet man mit $\prec$ die bevorzugte Ordnung und mit $\succ$ das Gegenteil davon, d.h. in der Ungleichung "$w_{i,k} \prec w_{j,k}$" wird $w_{i,k}$ vor $w_{j,k}$ bevorzugt, dann kann in Analogie zu non-dominance die Ordnung in m-dimensionalen Vektorraum in Abhängigkeit von der Ordnung einzelner Dimensionswerte definiert werden. Sind k, q und p die Dimensionsindices, dann $\forall k : 1 \leq k \leq m$ und $\exists q, p : 1 \leq q, p \leq m$ ist die Beziehung zwischen zwei m-dimensionalen Werten $\vec{W}_i$ und $\vec{W}_j$ wie folgt definiert:

$$Order_{\vec{v}}(\vec{W}_i, \vec{W}_j) ::= \begin{cases} =, if & w_{i,k} = w_{j,k} \\ \prec, if & w_{i,k} \prec w_{j,k} \quad \vee \quad if w_{i,k} = w_{j,k} \\ \succ, if & w_{i,k} \succ w_{j,k} \quad \vee \quad if w_{i,k} = w_{j,k} \\ \neq, if & w_{i,q} \prec w_{j,q} \quad \wedge \quad w_{i,p} \succ w_{j,p} \end{cases}$$

Diese Beziehung sieht die gleichwertige Bedeutung aller QoS-Parameter vor. Es kann aber auch eine Priorisierung der relevanten QoS-Parameter erwünscht sein (die Verwendung dafür siehe in Abschnitt 4.2.8). Um diese Eigenschaft zu erfüllen, kann die Ordnungsformel leicht angepasst werden. Sind die QoS-Parameter in die Dimensionen

nach der absteigenden Priorität sortiert, dann kann die priorisierte Ordnungsfunktion wie folgt definiert werden:

$$\textit{PrioOrder}_{\vec{v}}(\vec{W}_i, \vec{W}_j) ::= \begin{cases} =, if & \forall k : 1 \leq k \leq m : & w_{i,k} = w_{j,k} & \\ \prec, if & \exists q : 1 \leq q, \leq m : & w_{i,q} \prec w_{j,q} & \wedge \\ & \forall p : p < q : & w_{i,p} = w_{j,p} & \\ \succ, if & \exists q : 1 \leq q, \leq m : & w_{i,q} \succ w_{j,q} & \wedge \\ & \forall p : p < q : & w_{i,p} = w_{j,p} & \end{cases}$$

Die Ordnungsrelationen einzelner QoS-Parameter bleiben dabei unverändert, was eine große Flexibilität und Anpassbarkeit an Dienstinstanz-spezifische Anforderungen garantiert. Als zusätzlicher Vorteil dieser Funktion kann auch das Fehlen des $\neq$-Zustandes angesprochen werden, weil dadurch die Wahl des besten Pfades aus allen zufriedenstellenden ermöglicht wird. Das kann jedoch nur auf E2E-Pfade angewendet werden und nicht auf Teilpfade (für die Begründung siehe die entsprechende Diskussion im Abschnitt 3.3).

4.2.4. Wertebereiche als Gewichte: Abbildung auf feste Werte

Der Übergang von Wertebereichen zu Werten kann verhältnismäßig leicht geschehen.

Bei E2E-Anforderungen (engl. *Constraints*) kann man davon ausgehen, dass sie die untere Schranke $\vec{C}_{E2E}$ für alle relevanten Eigenschaften darstellt. Eine Angabe der Anforderungen als ein Wertebereich ist zwar theoretisch möglich, ergibt aber wenig Sinn (z.B. Kundenanforderung "Die Eigenschaft XY soll besser als AA, aber nicht besser als BB sein") und wird daher nicht betrachtet. Bei dem Pfadgewicht, wie es im Abschnitt 4.6 definiert wurde, handelt es sich jedoch i.A. um einen Wertebereich, in dem die Eigenschaften eines Pfades variieren können.

Pfadsuche mit bestem Wert

Um feststellen zu können, ob ein Pfad die E2E-Anforderungen erfüllen kann, reicht der Vergleich zwischen dem bestmöglichen Pfadgewicht und den Anforderungen $\vec{C}_{E2E}$. Deswegen kann bei der Pfadsuche ausschließlich der bestmögliche Wert berücksichtigt werden, wodurch die Verwendung der Operationen auf festen Werten ermöglicht wird.

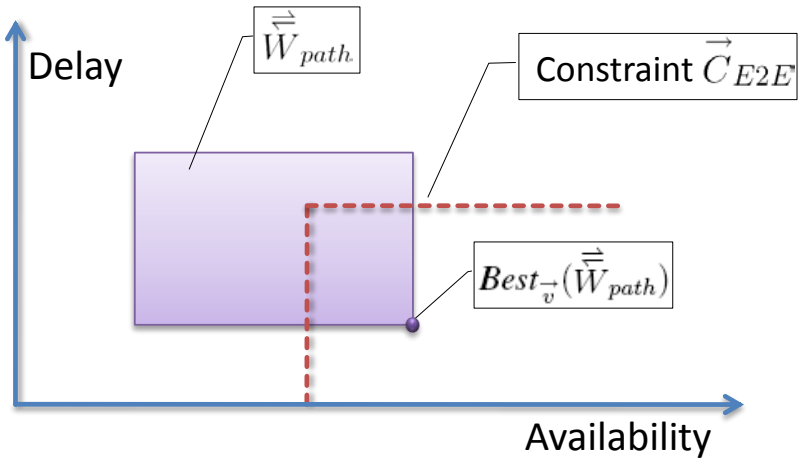


Abbildung 4.20.: Erfüllbarkeit der E2E-Anforderungen für einen Pfad

In der Abbildung 4.20 ist dies graphisch dargestellt. Für die Anschaulichkeit der Darstellung handelt es sich dabei nur um zwei QoS-Parameter, Delay und Verfügbarkeit. Die von $\vec{\vec{W}}_{path}$ aufgespannte Fläche der realisierbaren Eigenschaften ist durch das ausgefüllte Rechteck und die Anforderungsgrenze $\vec{C}_{E2E}$ durch die gestrichelte Linie gekennzeichnet. An dem Bild erkennt man die Problematik, die bereits bei der Definition der Ordnungsfunktionen zum Vorschein kam: ein kleinerer Delay ist als der bessere Wert zu beurteilen, bei der Verfügbarkeit ist dagegen der größere Wert besser. Um den bestmöglichen Wert eines Pfades (in der Abbildung durch einen Punkt hervorgehoben) bestimmen zu können, wird Funktion $Best_{\vec{v}}$ wie folgt definiert:

$$
\begin{aligned}
\textit{Best}_{\vec{v}}(\vec{\vec{W}}_{path}) &::= \textit{Best}_{\vec{v}}(\vec{W}^{min}_{path}, \vec{W}^{max}_{path}) \\
\textit{Best}_{\vec{v}}(\vec{W}_i, \vec{W}_j) &::= (Best(w_{i,1}, w_{j,1}), ..., Best(w_{i,m}, w_{j,m})) \\
Best(w_{i,k}, w_{j,k}) &::= \begin{cases} w_{i,k}, if\ w_{i,k} \prec w_{j,k}, & \forall k : 1 \leq k \leq m \\ w_{j,k}, otherwise \end{cases}
\end{aligned}
$$

Näherung an die E2E-Anforderungen

Die Erfüllung bzw. bestmögliche Erfüllung der E2E-Anforderungen ist nicht immer die beste Vorgehensweise: so muss der Kunde nicht unbedingt eine realisierbare 10Gbps-Verbindung bekommen, wenn er "mindestens 2Mbps" spezifiziert hat. Somit rückt (oft auch aus Kostengründen) die Aufgabe in Vordergrund, eine Verbindung zu finden, die den E2E-Anforderungen genügt, diese aber möglichst gering "übererfüllt" (siehe dazu auch die Diskussion im Abschnitt 3.3 über die Such-Probleme in Multi-Weighted Graphen).

In diesem Fall kann das Vorgehen in folgende grobe Schritte aufgeteilt werden:

1. Zunächst soll ein Pfad gefunden werden, der die E2E-Kundenanforderungen erfüllt, d.h. die Ungleichung $\textit{Best}_{\vec{v}}(\vec{\vec{W}}_{path}) \prec \vec{C}_{E2E}$ ist erfüllt.

2. Danach soll der für den gefundenen Pfad schlechtmöglichste Wert $\textit{Worst}_{\vec{v}}(\vec{\vec{W}}_{path})$ ermittelt werden. Da alle Teildienste des Pfades bekannt sein müssen, ist das ohne weiteres möglich, indem die $\textit{Worst}_{\vec{v}}$-Werte aller Teildienste aggregiert werden. Danach sollen zwei Fälle unterschieden werden:

   - Sollte auch der schlechteste Wert des gefundenen Pfades die E2E-Anforderungen erfüllen - d.h. "$\textit{Worst}_{\vec{v}}(\vec{\vec{W}}_{path}) \prec \vec{C}_{E2E}$" -, dann kann er als das gesamte Pfadgewicht verwendet werden. In diesem Fall sollen die SP-Domänen die ausgewählten Teilstrecken (d.h. *Component Links*) lediglich mit den schlechtesten für diese Strecken angebotenen Eigenschaften realisieren.

   - Falls jedoch der $Worst_{\vec{v}}(\vec{\vec{W}}_{path})$-Wert die E2E-Anforderungen nicht erfüllt (wie das in dem Beispiel aus der Abbildung 4.20 der Fall war), dann muss nach einer Näherung an die Grenzwerte gesucht werden.

3. Sollte der schlechtmöglichste Pfad-Gewicht die E2E-Anforderungen erfüllen (d.h. $\textit{Worst}_{\vec{v}}(\vec{\vec{W}}_{path}) \prec \vec{C}_{E2E}$) und dennoch - aus Providersicht - zu gut sein, kann nach einem alternativen Pfad gesucht werden. Dabei sollen die vorherig beschriebenen Schritte wiederholt werden.

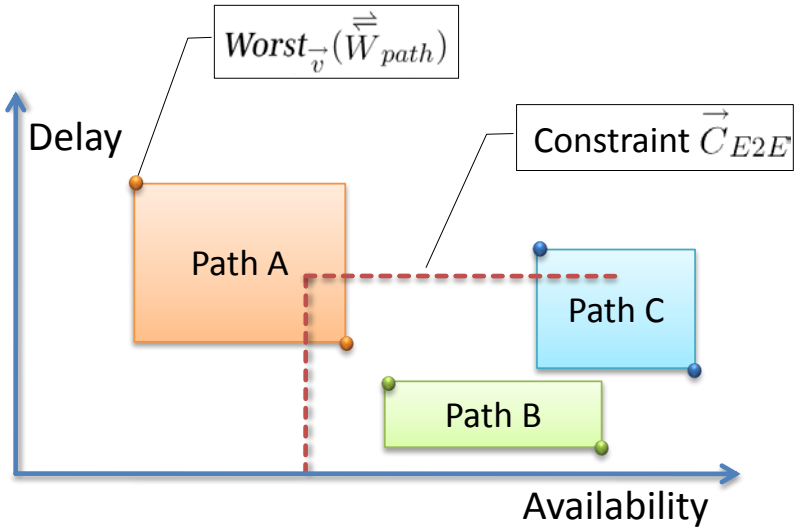


Abbildung 4.21.: Pfadgewicht und E2E-Anforderungen, mögliche Kombinationen

Dieses Vorgehen stützt sich auf die Funktion $Worst_{\vec{v}}(\vec{\vec{W}}_{path})$, die als Gegenteil zu $Best_{\vec{v}}(\vec{\vec{W}}_{path})$ definiert werden kann. Dazu muss in der Definition ausschließlich die Relationsbeziehung "$\prec$" durch "$\succ$" ausgetauscht werden:

$$
\begin{aligned}
Worst_{\vec{v}}(\vec{\vec{W}}_{path}) &::= Worst_{\vec{v}}(\vec{W}^{min}_{path}, \vec{W}^{max}_{path}) \\
Worst_{\vec{v}}(\vec{W}_i, \vec{W}_j) &::= (Worst(w_{i,1}, w_{j,1}), ..., Worst(w_{i,m}, w_{j,m})) \\
Worst(w_{i,k}, w_{j,k}) &::= \begin{cases} w_{i,k}, if\ w_{i,k} \succ w_{j,k}, & \forall k : 1 \leq k \leq m \\ w_{j,k}, otherwise \end{cases}
\end{aligned}
$$

Bei den Pfaden, die die E2E-Anforderungen erfüllen, können grundsätzlich drei Fälle bzgl. den $Worst_{\vec{v}}(\vec{\vec{W}}_{path})$-Werte auftreten. Diese sind graphisch in der Abbildung 4.21 dargestellt. Interessant sind vor allem der "Path A", bei dem im schlechtesten Fall keine der erforderlichen Eigenschaften erfüllt wird, und der "Path C", bei dem im schlechtesten Fall die E2E-Anforderungen nicht bei allen Eigenschaften erfüllt sein werden. Die Ermittlung einer Näherung an den Anforderungswert soll ausschließlich auf die Eigenschaften beziehen, bei denen die E2E-Anforderungen nicht erfüllt werden. Bei den übrigen können die schlechtesten Werte übernommen werden.

Bestimmen endgültiger Soll-Werte

Dieses Knappsack-ähnliche Problem kann relativ einfach mit den Mitteln der Graphentheorie gelöst werden. Da alle mit dem *Component Link* (der zugrunde einer Kante in dem betrachteten Graph liegt) assoziierten Eigenschaften voneinander unabhängig sind (siehe deren Definition in Abschnitt 4.1.2), kann die Näherung für jede der

m Dimensionen einzeln durchgeführt werden. Der gefundene Pfad kann einzeln für jede Dimension zu einem gerichteten Graphen transformiert werden. Dabei entsprechen die Knoten dieses Graphes den SCPs auf dem gefundenen Pfad. Die Anzahl von Kanten hängt von den erlaubten Zuständen des *Component Links* in der jeweiligen Dimension ab. Die Gewichte der Kanten variieren von dem besten zu dem schlechtesten Wert entsprechend den spezifizierten Abstufungen. Der so definierte Graph ist in Abbildung 4.22 dargestellt. Die Tiefensuche in dem gesamten so definierten Graphen kann zur Bestimmung der erforderlichen Gewichte jedes *Component Links* verwendet werden.

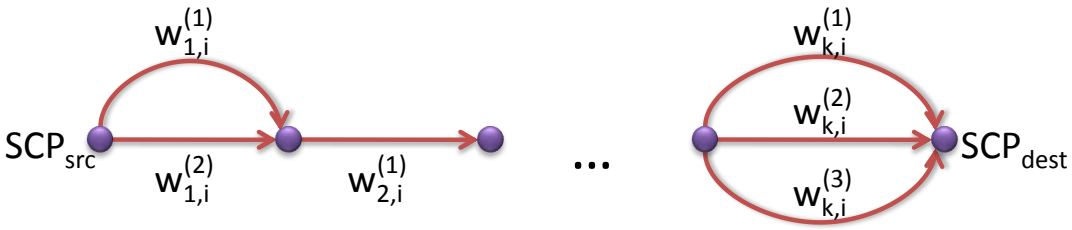


Abbildung 4.22.: DFS zur Bestimmung der Teildienstegewichte

Wie im Abschnitt 3.3 beschrieben wurde, beträgt die Laufzeit der Tiefensuche $O(b^d)$, wobei "b" für den Verzweigungsgrad und "d" für die maximale Suchtiefe stehen. Durch die Begrenzung der maximalen Anzahl der Abstufungen (Verzweigungsgrad) zwischen dem besten und dem schlechtesten möglichen Wert jedes *Component Links* kann die Begrenzung der Suchlaufzeit flexibel gestaltet werden. Wegen seiner Trivialität und großer Ähnlichkeit zur Bestimmung von MCSP (siehe Abbildung 4.27 im Abschnitt 4.2.8) wird dieser Algorithmus hier nicht extra ausgeführt.

4.2.5. Multigraphen: Alternatives Vorgehen

Der Zweck des Knoten-Einfügens beim klassischen Vorgehen mit *Multigraphen* (siehe Abbildung 3.8 sowie die zugehörige Diskussion im Abschnitt 3.3.2) besteht darin, die einzelnen Kanten im Graph voneinander unterscheiden zu können. Bei der Modellierung der Kommunikationsartefakte kann dieses Ziel auch dadurch erreicht werden, dass jeder *Component Link* mit einer global eindeutigen ID versehen wird. Der Suchalgorithmus muss dann entsprechend angepasst werden. Dazu müssen lediglich innerhalb der üblichen "für-alle-Nachbarn"-Schleife auch eine zusätzliche "für-alle-Kanten-zu-Nachbar"-Schleife eingebaut werden. Weiterhin soll bei der Gestaltung der Rückreferenz eines Pfades nicht nur den Knoten-, sondern auch die entsprechende Kante (bzw. Kanten-ID) berücksichtigt werden.

Um diesen Umgang mit den Multigraphen überhaupt zu ermöglichen, muss bei der Modellierung der Kommunikationsartefakte folgendes erfüllt werden:

Vorgabe (Identifizierung) VI08 - Identifizierung aller *Component Links*

Alle *Component Links* müssen mit einer global eindeutigen ID versehen werden. Das Vergabeverfahren für diese IDs soll in der Lage sein, der Dynamik der Veränderungen bei den realisierbaren Verbindungen und deren Verbindungseigenschaften zu genügen.

4.2.6. Definition der Operationen pro Diensteigenschaft

Notwendige Operationen

Bei der Diskussion in Abschnitten 4.2.2 und 4.2.3 zeigte sich, dass pro Diensteigenschaft mindestens die drei folgenden Funktionen definiert werden müssen: eine Vergleichs- und zwei unterschiedlichen Aggregationsfunktionen. Weiterhin wurde im Abschnitt 4.2.4 die Notwendigkeit von zwei weiteren Funktionen zur Bestimmung des besten bzw. des schlechtesten Wertes dargelegt. Die explizite Definition der letzteren zwei Funktionen kann man als optional betrachten, da deren Ergebnis ohne weiteres unter der Verwendung der Vergleichsfunktion erzielt werden kann. Wichtig ist vor allem, dass all diese Funktionen, die in Tabelle 4.1 zusammengefasst sind, für jede Diensteigenschaft definiert werden müssen, die bei der Pfadsuche berücksichtigt werden soll. Hier sind sowohl QoS-Parameter, als auch Managementfunktionalität und die einzelnen Eigenschaften der Managementfunktionalität gemeint.

Funktion	Zweck
`_Order_Compare`	Diese Funktion dient dem Vergleich zweier Werte des durch ID vorgegebenen Typs. Ergebnis dieser Funktion kann ausschließlich die Werte einnehmen, deren Bedeutung für die jeweilige Eigenschaft „`Besser`“, „`Schlechter`“ oder „`Gleich`“ ist.
`_Order_Best`	Dies ist eine Hilfsfunktion, die vom einfachen Vergleich abgeleitet werden kann. Diese Funktion soll den – im Sinne der Eigenschaft – besten Wert zurückliefern.
`_Order_Worst`	Dies ist eine Hilfsfunktion, die vom einfachen Vergleich abgeleitet werden kann. Diese Funktion soll den – im Sinne der Eigenschaft – schlechtesten Wert zurückliefern.
`_Aggregate_Links`	Diese Funktion definiert, wie die Werte auf der aneinander angeschlossenen `ComponentLinks` miteinander aggregiert werden können, um ein gemeinsames „Gewicht“ zu errechnen.
`_Aggregate_LinkParts`	Diese Funktion definiert, wie die Teilsichten zweier SP-Provider auf denselben von ihnen gemeinsam zu erbringenden `InterDomain Link` miteinander kombiniert werden können, sodass das `ComponentLink`-Gewicht errechnet werden kann.

Tabelle 4.1.: Erforderlichen ID-bezogene Funktionen

Bei den Aggregatfunktionen müssen, wie bereits erwähnt, zwei Funktionen definiert werden – für die Aggregation der Eigenschaftenwerte der unterschiedlichen Teildienste und für die Aggregation der Sichten aneinander angeschlossenen SP-Domänen

auf die Eigenschaften ein und desselben Links. Dabei muss betont werden, dass der Kontext bzw. Abstraktionslevel, in dem diese Funktionen zum Einsatz kommen, in dieser Arbeit strikt voneinander getrennt wurde. So sind die Teilsichten auf dieselben *Interdomain Links* ausschließlich für die aneinander angeschlossenen SP-Domänen möglich, für alle anderen Operationen werden sie von einer aggregierten View verschattet (siehe Abschnitt 4.1.3). Dieses Vorgehen mag zwar – aus Sicherheitsgründen – eine allgemeingültigere Lösung darstellen, die zudem auch eine wesentliche Vereinfachung der Prozesse ermöglicht, auf der anderen Seite fordert dies aber einen zusätzlichen Aufwand bei den SP-Domänen (für die Verschattung) sowie verursacht die Bildung eines zusätzlichen Kommunikationsschrittes. Aus diesen Gründen wird im Abschnitt 4.7 empfohlen, bei den kleinen und mittelgroßen Kooperationen mit guten Vertrauensbeziehungen zwischen den SP-Domänen auf diese Art der Verschattung zu verzichten.

Damit auf den Eigenschaften die definierten Operationen ausgeführt werden können, soll folgendes erfüllt werden:

Vorgabe (Identifizierung) VI09 - Operationen-zu-Eigenschaften Assoziation

Mit jeder unterstützten Eigenschaft sollen mindestens die drei erforderlichen Funktionen assoziiert werden.

Die entsprechende Lösung wird im Abschnitt 4.6.10 definiert.

4.2.7. Beispiel: Funktionendefinition für Diensteigenschaften

Durch den Aufbau der Eigenschaftenbeschreibung unter konsequenten Verwendung von IDs in Kombination mit der Assoziation der Funktionsdefinitionen ist es möglich, mehrdimensionale Operationen auf beliebige Eigenschaftenkombinationen zu unterstützen. In diesem Abschnitt soll illustriert werden, wie die einzelnen Funktionen für unterschiedliche Eigenschaften definiert werden können. Um an dieser Stelle keine Beschreibungssprache dafür einführen zu müssen, wird in dem folgenden Codebeispiel auf C/C++ zurückgegriffen, da diese Programmiersprachen sowohl sehr verbreitet sind als auch deren Syntax von vielen anderen Sprachen als Vorbild übernommen wurde. Für die Einführung in diese Sprachen empfehlen sich z.B. [KR88, Str00].

Funktionen für QoS-Parameter

Im Abschnitt 4.2.1 wurde bereits angesprochen, dass die Aggregatfunktion für Delay bei den Teilsichten auf denselben *Interdomain Link* sich von der Aggregatfunktion für den Multi-Domain Fall unterscheiden kann. In Abbildung 4.23 werden die notwendigen Typen (siehe Zeilen 1 bis 22) sowie die drei obligatorischen eigenschaftenbezogenen Funktionen (siehe Zeilen 24 bis 66) definiert. Wie man sieht, sind abgesehen von den Unterschieden zwischen zwei Aggregatfunktionen alle Definitionen in der Abbildung sehr einfach. Dies kann sich jedoch von einer Eigenschaft zur anderen sehr stark unterscheiden.

Funktionen für Managementfunktionalität

Auch wenn im Laufe des Kapitels hin und wieder betont wurde, dass die ID-bezogene Definition von Diensteigenschaften (und somit auch von Aggregat- und Ordnungsfunktionen) sich nicht nur auf Dienstgüteeigenschaften, sondern auch auf die Managementfunktionalität erstreckt, richtig illustriert wurde es bislang noch nicht. Der Grund dafür liegt einerseits daran, dass die Erklärungen anhand QoS-Parameter wesentlich intuitiver und daher auch leichter zu verstehen sind, und andererseits daran, dass die Definition entsprechender Funktionen für die Managementfunktionalität u.U. wesentlich aufwendiger und komplexer ist. Um dies zu verdeutlichen, wurden in Abbildungen 4.24 und 4.25 zwei der erforderlichen Funktionen für die Managementfunktionalität "Teilstrecken-Monitoring" definiert. Wie in dem vorangegangenen Beispiel in der Abbildung 4.23 handelt es sich um die Funktionen, die während des Routings eingesetzt werden sollen, wenn auch die getroffenen Entscheidungen die Managementfunktionalität und deren Eigenschaften beeinflussen.

Im Code-Beispiel in der Abbildung 4.24 ist die Komplexität nur unwesentlich höher als bei einem QoS-Parameter: es ist lediglich eine Aufzählung der möglichen Monitoring-Verfahren in einer SP-Domäne (vergleiche dazu Tabelle 2.5 im Abschnitt 2.4.1) dazugekommen, die weiter unten in der Ordnungsfunktion auch berücksichtigt werden. Die Aggregatfunktion in der Abbildung 4.25 sieht allerdings wesentlich komplexer aus. Das liegt daran, dass alle möglichen Kombinationen der Überwachungsmethoden einzelner Teilstrecken und deren Auswirkung auf die E2E-Überwachung berücksichtigt werden müssen.

```
typedef enum tagORDER
{
    BETTER,
    IDENTICAL,
    WORTHER

} ORDER;

typedef enum tagMETRICDELAY
{
    us  = 1,        // microsecond
    ms  = 10^3,     // milisecond
    sec = 10^6,     // second

} METRICDELAY;

typedef struct tagDELAY
{
    int         value;  // delay value
    METRICDELAY metric; // delay metric

} DELAY, *LPDELAY;

ORDER Delay_Order_Compare (LPDELAY lpPartA, LPDELAY lpPartB)
{
    if (lpPartA->value * lpPartA->metric == lpPartB->value * lpPartB->metric)
        return IDENTICAL;

    if (lpPartA->value * lpPartA->metric < lpPartB->value * lpPartB->metric)
        return BETTER;

    return WORTHER;
}

LPDELAY Delay_Aggregate_Links (LPDELAY lpPartA, LPDELAY lpPartB, LPDELAY lpResult)
{
    lpResult->value = lpPartA->value * lpPartA->metric +
                      lpPartB->value * lpPartB->metric;

    if (lpPartA->metric < lpPartB->metric)
    {
        lpResult->value  /= lpPartA->metric;
        lpResult->metric  = lpPartA->metric;
    }
    else
    {
        lpResult->value  /= lpPartB->metric;
        lpResult->metric  = lpPartB->metric;
    }

    return lpResut;
}

LPDELAY Delay_Aggregate_LinkParts (LPDELAY lpPartA, LPDELAY lpPartB, LPDELAY lpResult)
{
    lpResult->value  = lpPartA->value;
    lpResult->metric = lpPartA->metric;

    if (lpPartA->value * lpPartA->metric < lpPartB->value * lpPartB->metric)
    {
        lpResult->value  = lpPartB->value;
        lpResult->metric = lpPartB->metric;
    }

    return lpResut;
}
```

Abbildung 4.23.: Operationen für QoS-Parameter, Delay

```
typedef enum tagMONITORINGTYPE
{
    None,           // monitoring is not possible at all
    Polling,        // monitoring data is acquired by polling
    PollingOrTraps, // monitoring data is acquired by polling or traps
                    // as aggregat-value means that some sections are
                    // monitored with traps and other wit polling
    Traps,          // monitoring data is acquired by traps
    PollingAndTraps // combination of polling and traps is used

} MONITORINGTYPE;

typedef enum tagMONITORINGMETRIC
{
    us  = 1,        // microsecond
    ms  = 10^3,     // milisecond
    sec = 10^6,     // second
    min = 60*10^6   // minut

} MONITORINGMETRIC;

typedef struct tagMONITORINGACQUISITION
{
    MONITORINGTYPE   type;   // how monitoring is performed
    int              value;  // polling interval value
    MONITORINGMETRIC metric; // polling interval metric

} MONITORINGACQUISITION, *LPMONITORINGACQUISITION;


LPMONITORINGACQUISITION MonitoringAquisition_Order_Best (
    LPMONITORINGACQUISITION lpPartA,
    LPMONITORINGACQUISITION lpPartB,
    )
{
    if (lpPartA->type > lpPartB->type)
        return lpPartA;

    if (lpPartB->type > lpPartA->type)
        return lpPartB;

    // identical types - compare polling intervals
    switch (lpPartA->type)
    {
        case None:
        case Traps:
            return lpPartA;

        case Polling:
        case PollingOrTraps:
        case PollingAndTraps:
            if ( // smaller polling interval is better
                lpPartA->value * lpPartA->metric <
                lpPartB->value * lpPartB->metric
                )
                return lpPartA;

        default:
            break;
    }

    return lpPartB;
}

```

Abbildung 4.24.: Operationen für Managementfunktionalität, MonitoringAquisition (1/2)

```
65 LPMONITORINGACQUISITION MonitoringAquisition_Aggregate_Links (
66     LPMONITORINGACQUISITION lpAggregat,
67     LPMONITORINGACQUISITION lpNextPart,
68     )
69 {
70     // check whether E2E-Monitoring is possible at all
71     if (lpAggregat->type == Nonde || lpNextPart->type == None)
72     {
73         lpAggregat->type = Nonde;
74         return lpAggregat;
75     }
76
77     // if both rely on Traps - Traps remain as aggregated value
78     if (lpAggregat->type == Traps ||
79         lpAggregat->type == PollingAndTraps)
80         if (lpNextPart->type == Traps ||
81             lpNextPart->type == PollingAndTraps)
82         {
83             if (lpAggregat->type != lpNextPart->type)
84                 lpAggregat->type = Traps; // worst possiblity wins
85
86             return lpAggregat;
87         }
88
89     // at most one of arguments is Trap-based
90
91     if (lpAggregat->type == Traps ||
92         lpAggregat->type == PollingAndTraps)
93     {
94         lpAggregat->type   = PollingOrTraps;
95         lpAggregat->value  = lpNextPart->value;
96         lpAggregat->metric = lpNextPart->metric;
97
98         return lpAggregat;
99     }
100
101    if (lpNextPart->type == Traps ||
102        lpNextPart->type == PollingAndTraps)
103    {
104        lpAggregat->type   = PollingOrTraps;
105
106        return lpAggregat;
107    }
108
109    // both arguments rely on "Polling"
110    // only bigger (worther) polling can be guarantied for E2E
111
112    if (
113        lpAggregat->value * lpAggregat->metric <
114        lpNextPart->value * lpNextPart->metric
115        )
116    {
117        lpAggregat->value  = lpNextPart->value;
118        lpAggregat->metric = lpNextPart->metric;
119    }
120
121        return lpAggregat;
122 }
```

Abbildung 4.25.: Operationen für Managementfunktionalität, MonitoringAquisition (2/2)

Die Code-Beispiele, die in diesem Unterabschnitt präsentiert wurden, dienen ausschließlich zu Veranschaulichungszwecken und können nicht als eine endgültige Definition betrachtet werden. Die Wahl des zu unterstützenden Dienstes sowie der Implementierungskriterien (z.B. eine andere Programmier- bzw. Beschreibungssprache) können einen starken Einfluss auf die Funktionsdefinitionen haben.

4.2.8. Suchalgorithmen mit eingeführten Operationen

Obwohl es in diesem Abschnitt oft gesagt wurde, dass die definierten Aggregations- und Vergleichsfunktionsdefinitionen bei den Suchverfahren eingesetzt werden sollen, richtig illustriert wurde es bislang nicht. Da es unterschiedliche zu lösende Aufgaben geben kann, wird weiter in diesem Unterabschnitt exemplarisch gezeigt, wie die existierenden Suchverfahren an die Gegebenheiten Verketteter Dienste mit Hilfe der in den Abschnitten 4.2.2 und 4.2.3 eingeführten Funktionen angepasst werden können.

Aufgaben bei Multi-Weighted Graphen

Im Abschnitt 3.3 wurden drei Aufgaben präsentiert, die in Bezug auf Multi-Weighted Graphen am häufigsten gestellt werden. Diese Aufgaben, die in der Fachliteratur oft auch als Probleme referenziert werden, werden hier kurz in die Erinnerung gerufen:

Multi-constrained Path (MCP) : Bei dieser Aufgabe muss ein beliebiger Pfad gefunden werden, der gleichzeitig mehreren Anforderungen genügt. Die Güte dieses Pfades (z.B. die Nähe oder Weite der Eigenschaften zu/von den spezifizierten E2E-Anforderungen spielt dabei keine Rolle.

Constrained Shortest Path (CSP) : Dabei wird ein nach nur einem Gewicht optimierter Pfad gesucht, der eine Reihe E2E-Anforderungen erfüllt. Als das zu optimierende Gewicht spielen dabei oft die Anzahl der Hops oder die Verbindungskosten eine Rolle.

Multi-constrained Shortest Path (MCSP) : In diesem Fall wird nach einem Pfad gesucht, der nicht nur wie bei CSP nach einem, sondern nach allen relevanten Eigenschaften optimiert wird.

Übertragen auf die Aufgabenstellung kann jede dieser Aufgaben in Abhängigkeit von einer Reihe von Faktoren, wie z.B. von Verhandlungsart, Geschäftsmodell, Domain-Policies, Kundenanforderungen usw., relevant sein. So ist MCP für die Reaktionszeit optimal, CSP ist gut für die Kostenoptimierung. Das CSP-Problem kann auch leicht erweitert werden, indem nach einem kostengünstigsten Pfad gesucht wird, der dabei auch die schlechtesten, aber immer noch zufriedenstellenden QoS-Werte aufweist. Für MCSP sind zwei folgende Anwendungsfälle denkbar: konnte kein Pfad gefunden werden, der die aufgestellten E2E-Anforderungen erfüllt, dann kann der Ergebnis von MCSP als ein Alternativvorschlag für den Kunden verwendet werden; das kann auch dann als eine Alternative mit dem entsprechenden Aufpreis verwendet werden, wenn ein schlechterer zufriedenstellender Pfad z.B. mit CSP bereits gefunden werden konnte.

MCP mit DFS

Hier wird die Lösung des MCP-Problems auf Basis der einfachen Tiefensuche (engl.: *Deep First Search*, DFS!) präsentiert. Die problemspezifisch optimierten Algorithmen, wie z.B. der im Abschnitt 3.3.2 angesprochene SAMCRA-Algorithmus, sind wegen ihrer i.A. wesentlich höheren Komplexität für Illustrationszwecke weniger geeignet. Die

Berechnung eines Pfadgewichtes mit Hilfe von $Aggr_{\vec{v}}$-Funktion wurde im Abschnitt 4.2.2 beschrieben. Dieselbe Vorgehensweise ist auch bei der Berechnung der Teilpfadgewichte anwendbar. Sollten bereits beim Teilpfad die Erfüllung von allen E2E-Anforderungen nicht mehr möglich sein – d.h. die Bedingung "$Best_{\vec{v}}(\vec{\vec{W}}_{path}) \prec \vec{C}_{E2E}$" nicht mehr erfüllt ist – kann die Suche in dem Zweig als fehlgeschlagen abgebrochen werden. Sind die von SP-Domänen gemeldete Pfade in Abhängigkeit vom Ziel-SCP sortiert, dann liefert SCP auch den von SPs bevorzugten Pfad, der die E2E-Anforderungen erfüllt. Diese Eigenschaft kann als ein Teil der Lösungsidee im Abschnitt 4.3 wiederverwendet werden. Dieser Algorithmus wird in Pseudokode angegeben, um die Abweichungen vom Normalfall besser zu illustrieren (siehe Abbildung 4.26). Zu Gunsten der Verständlichkeit ist dieser Algorithmus nicht optimiert.

```
DFS_MCP (nodeCur, nodeDest, W_path^cur, C_E2E)

    if (nodeCur == nodeDest)
        BacktracePath (nodeCur, NULL);
        return TRUE;
    end if

    MarkNode (nodeCur);

    for every neighbor nodeNbr of nodeCur
        if (not Marked (nodeNbr))
            for every connection conNbr from nodeCur to nodeNbr
                W_path^nbr = Aggr_v (W_path^cur, Best_v(W_conNbr));
                if (W_path^nbr ≺ C_E2E)
                    if (DFS_CSP(nodeNbr, nodeDest, W_path^nbr, C_E2E) == TRUE)
                        BacktracePath (nodeCur, conNbr);
                        return TRUE;
                    end if
                end if
            end for
        end if
    end for

    UnmarkNode (nodeCur);

    return FALSE;
```

Abbildung 4.26.: Pseudokode für MCP mit Tiefensuche

Umgang mit Multigraphen und Wertebereich-Gewichten

Neben der Verwendung der neuen Funktionen zeichnet sich der Algorithmus durch den Einsatz einer "for every connection *conNbr* "-Schleife aus, die zum Umgang mit *Multigraphen* eingeführt wurde (siehe auch Abschnitt 4.2.5). Für den Umgang mit den als Wertebereiche spezifizierten Gewichten wurde die Funktion $Best_{\underset{v}{\rightarrow}}(\overrightarrow{\overleftarrow{W}}_{conNbr})$ verwendet, wie das im Abschnitt 4.2.4 definiert wurde.

MCSP mit DFS

Bei der Lösung des MCSP-Problems wird im Gegenteil zu MCP-Algorithmus auf den Abbruch beim Finden des ersten zufriedenstellenden Pfades verzichtet. Stattdessen fungiert er vorerst als der beste gefundene E2E-Pfad mit dem Pfadgewicht $\overrightarrow{\overleftarrow{W}}^{best}_{path}$. Das Gewicht jedes bei der kompletten Tiefensuche gefundenen E2E-Pfades wird mit dem bis dato besten verglichen. Ist der neue Pfad besser - d.h. $Best_{\underset{v}{\rightarrow}}(\overrightarrow{\overleftarrow{W}}^{cur}_{path}) \prec \text{Best}_{\underset{v}{\rightarrow}}(\overrightarrow{\overleftarrow{W}}^{best}_{path})$ -, dann nimmt er die Stelle des besten Pfades ein. Ein weiterer Unterschied zum MCP-Algorithmus besteht darin, dass der Pfad ständig mitgespeichert wird und nicht nach dem Finden einer Lösung durch Rückverfolgung rekonstruiert werden kann. Der Algorithmus in Pseudokode ist in der Abbildung 4.27 angegeben.

CSP mit DFS

Bei der Lösung des MCSP-Problems (siehe Abbildung 4.27) wurde von der allgemeingültigen Ordnungsfunktion $Order_{\underset{v}{\rightarrow}}$ ausgegangen (siehe Abschnitt 4.2.3). Werden die einzelnen Eigenschaften z.B. vom Kunden priorisiert, dann wird $PrioOrder_{\underset{v}{\rightarrow}}$ oder eine ähnliche, anforderungsspezifisch angepasste Funktion benötigt. Ein weiterer Grund für die Priorisierung ist das Traffic Engineering (siehe Abschnitt 3.7.3), das der ausbalancierten Nutzung der vorhandenen Ressourcen dienen soll. Dazu müssen die SP-Domänen jeden einzelnen *Component Link* mit dem quantitativen Parameter für "Kosten" versehen, der dann als der prioritätswichtigste Parameter in den Vergleich miteinbezogen wird. Die Anwendung der priorisierten Ordnungsfunktion ist jedoch auf den Vergleich von kompletten Pfaden beschränkt (im Algorithmus durch "if (nodeCur == nodeDest)"-Abfrage sichergestellt), da laut ihrer Definition (siehe Abschnitt 4.2.3) die Erfüllung aller Grenzwerte nicht garantiert ist. Falls keine Priorisierung vom Kunden vorgegeben wurde und die Optimierung nur auf die Pfadgewichte abzielt, dann entspricht der veränderte Algorithmus aus der Abbildung 4.27 der Lösung des CSP-Problems.

```
DFS_MCSP (nodeCur, nodeDest, W_path^cur, C_E2E)

    if (nodeCur == nodeDest)
        if (W_path^cur ≺ W_path^best)
            AddPathNode (nodeCur, NULL);
            SaveBestPath ();
            W_path^best := W_path^cur
        end if
        return;
    end if

    MarkNode (nodeCur);

    for every neighbor nodeNbr of nodeCur
        if (not Marked (nodeNbr))
            for every connection conNbr from nodeCur to nodeNbr
                W_path^nbr = Aggr_v (W_path^cur, Best_v(W_conNbr));
                if (W_path^nbr ≺ C_E2E)
                    AddPathNode (nodeCur, conNbr);
                    DFS_MCSP (nodeNbr, nodeDest, W_path^nbr, C_E2E)
                    RemoveLastPathNode ();
                end if
            end for
        end if
    end for

    UnmarkNode (nodeCur);

    return;
```

Abbildung 4.27.: Pseudokode für MCSP mit Tiefensuche

4.3. Multi-Domain Routing-Verfahren

Dieser Abschnitt wird mit der organisatorischen Einordnung eingeleitet. Die dabei festgelegten Rollen und Verantwortungsbereiche gelten für die ganze Arbeit. Dem folgt die Diskussion über verschiedene Routing-Verfahren und deren Anwendbarkeit auf die Verketteten Dienste. Zwei dieser Verfahren werden direkt von den etablierten Ansätzen abgeleitet. Basierend auf der Diskussion über deren Vor- und Nachteile wird ein drittes, hybrides Verfahren entwickelt, das die Stärken von beiden klassischen Ansätze in sich vereinen soll. Anschließend werden alle drei Verfahren miteinander verglichen und die endgültige Wahl für das Routing-Verfahren bei *Verketteten Diensten* getroffen.

Graphisch ist die Struktur dieses Abschnittes in der Abbildung 4.28 dargestellt.

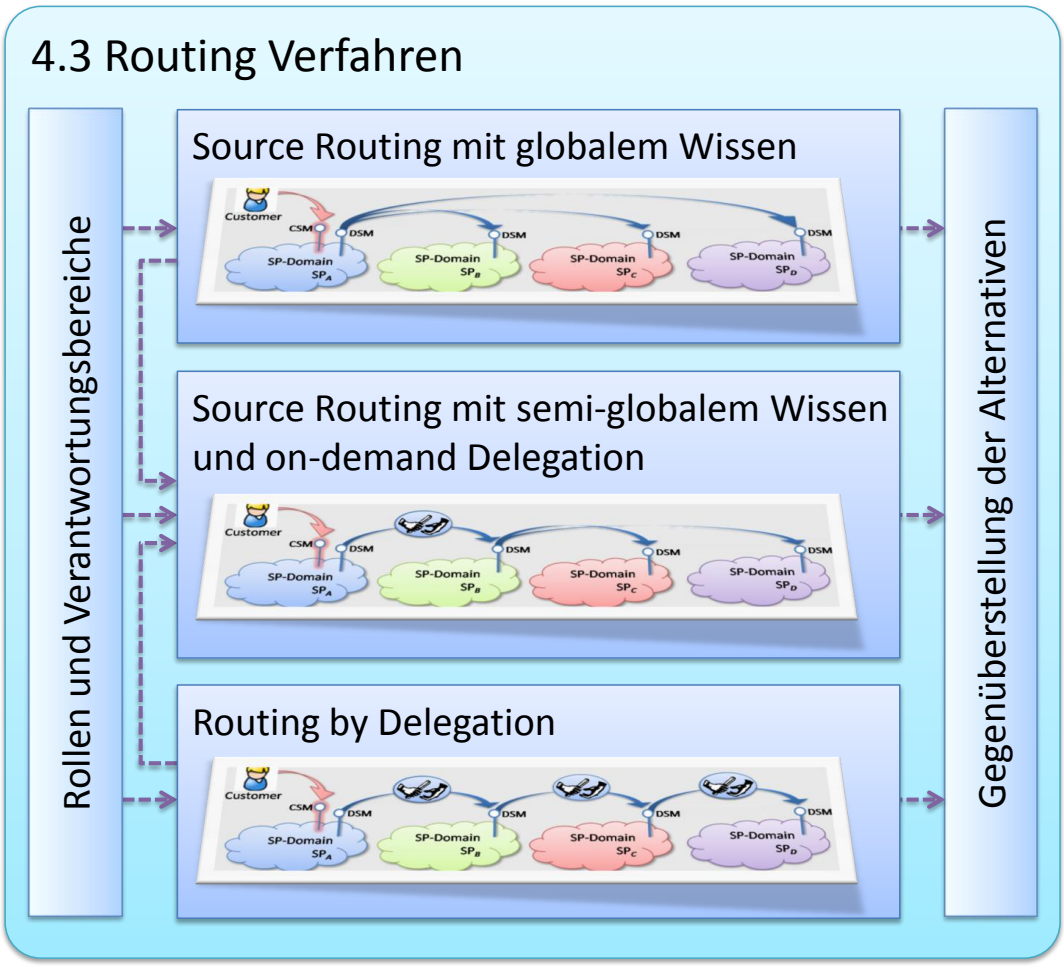


Abbildung 4.28.: Aufbau dieses Abschnittes

4.3.1. Rollen und Verantwortungsbereiche

Die organisatorische Einordnung wird anhand des Koordinationswürfels zusammengefasst [Ham09] (siehe Abbildung 4.29).

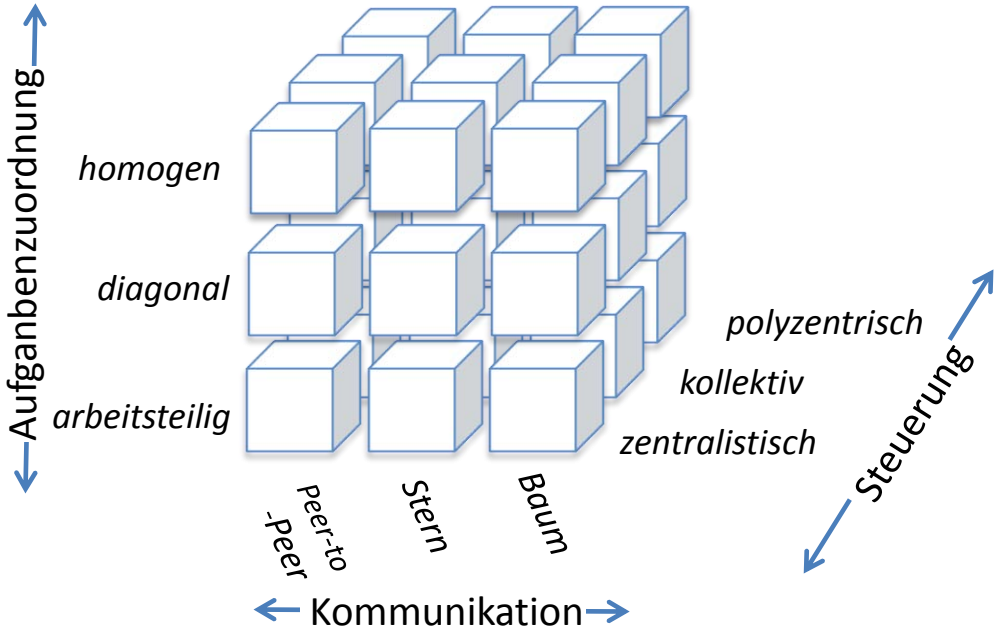


Abbildung 4.29.: Koordinationswürfel [Ham09]

Steuerung

Die Dimension der *Steuerung* legt fest, von welchen Organisationen welche Rollen und somit auch die Verantwortlichkeiten für alle Dienstinstanzen übernommen werden. Von *zentralistischer Steuerung* wird dann gesprochen, wenn alle Entscheidungen von einer für alle Dienstinstanzen gleichen SP-Domäne getroffen werden. Von *kollektiver Steuerung* wird dann gesprochen, wenn alle Entscheidungen darunter auch die Rollenzuweisung für eine Dienstinstanz) gemeinsam von allen SP-Domänen getroffen werden. Diese beiden Steuerungsformen zeichnen sich durch eine sehr klare Steuerungsstruktur aus, wodurch auch die im Vorfeld Etablierung der Konstellationen ermöglicht wird, die sowohl zur Dienstqualität als auch zur Kostenreduktion beitragen können (vergleiche dazu die Diskussion im Abschnitt 8 über E2ECU). Allerdings wird für ihren Einsatz ein Konsensus zwischen allen beteiligten SP-Domänen benötigt, was bei großen und/oder dynamischen Providerkooperationen sehr schwer durchzusetzen ist. Deswegen wird in dieser Arbeit generell für die sog. *kollektive Steuerung* entschieden, bei der alle Organisationen im weiten Sinne alle Entscheidungen selbst treffen und somit mehrere Machtzentren bilden.

Bei dem in dieser Arbeit gewählten Vorgehen geschieht die "Zuteilung" der beteiligten SP-Domänen (Akteuren) für die Rollen immer Dienstinstanz-bezogen. Die SP-

Domäne, bei der der Kunde eine neue Dienstinstanz des Verketteten Dienstes beantragt, übernimmt die Gesamtverantwortung und wird somit zum *Concatenated Service Provider* dieser Instanz. Bei Dienstrealisierung und Dienstmanagement tritt derselbe SP-Provider auch als *Concatenated Service Manager* auf, der die Verantwortung über das Management der gesamten Dienstinstanz trägt. Der *Concatenated Service Manager* darf – und muss u.U. auch – die Verantwortung für die Teile der Dienstinstanz bzw. der benötigten Managementfunktionalität an weitere SP-Domänen delegieren.

Die SP-Domänen können – in Abhängigkeit von den Diensten, die sie erbringen – i.A. gleichzeitig mehrere, Dienstinstanz-bezogenen Rollen einnehmen. Der Verantwortungsbereich einer SP-Domäne für eine Dienstinstanz umfasst die Ausübung aller Rollen und die Erbringung aller (Teil-)Dienste, die diese Domäne für die jeweilige Dienstinstanz übernommen hat. Der Erbringer einer Dienstinstanz-Teilstrecke hat für diese Dienstinstanz die Rolle *Partial Service Provider*, genauso wie die Erbringer der Routing- bzw. Monitoring-Funktionalitäten entsprechend die Rollen *Routing Manager* und *Monitoring Manager* einnehmen.

Aufgabenzuordnung

Bei der Diskussion über verschiedenen Routing-Verfahren wird in diesem Abschnitt zunächst von einer homogenen Aufgabenzuordnung ausgegangen. Das bedeutet, dass alle SP-Domänen alle benötigten Multi-Domain Managementfunktionalitäten besitzen. Im Abschnitt 4.4 wird gezeigt, wie die Delegation der Multi-Domain Managementfunktionalität realisiert werden kann, wodurch auch zwei weitere Aufgabenzuordnungsformen ermöglicht werden.

Kommunikation

Das Kommunikationsmuster zwischen den bei der Diensterbringung beteiligten SP-Domänen kann unterschiedliche Formen annehmen. Diese hängen sehr stark mit der Aufgabenzuordnung zusammen. Im einfachsten Fall, wenn alle erforderlichen Multi-Domain Managementaufgaben von der SP-Domäne übernommen werden, die auch als *Concatenated Service Provider* auftritt, entsteht zwischen dieser Domäne und allen Partial Service Providern eine sternförmige Kommunikation. Wird die Verantwortung (inklusive aller Managementaufgaben) für den Teil der gesamten Dienstinstanz an eine der SP-Domänen in der Kette delegiert (siehe Abschnitte 4.3.3 und 4.3.4, entsteht dadurch eine baumartige Kommunikationsform. Wenn die Multi-Domain Managementfunktionalität bei einer weiteren SP-Domäne – die i.A. nicht als Teildienstprovider auftreten muss – in Form eines Services bestellt werden kann (mehr dazu siehe im Abschnitt 4.4), kann u.U. zwischen den involvierten SP-Domänen eine *Peer-to-Peer Kommunikationsform* entstehen.

Für ein Beispiel, das unter anderem unterschiedlichen Aufgabenzuordnungs- und Kommunikationsformen illustriert, siehe Kapitel 7.

4.3.2. Source Routing mit globalem Wissen

In diesem Abschnitt wird die Übertragbarkeit des sog. *Source Routing* auf *Verkettete Dienste* analysiert. Das im Abschnitt 3.2 kurz eingeführte *Source Routing* ist ein etabliertes Routing-Verfahren. Abgesehen von dem BGP zwischen Autonomen Systemen, wird dieses Verfahren überwiegend beim Routing innerhalb einer einzelnen Domäne eingesetzt. In manchen Forschungsprojekten, wie z.B. bei GLIF und DCN (siehe entsprechend Abschnitte 2.3.3 und 2.3.4), wird dieses Verfahren mit einigen Anpassungen auf eine Multi-Domain Umgebung übertragen.

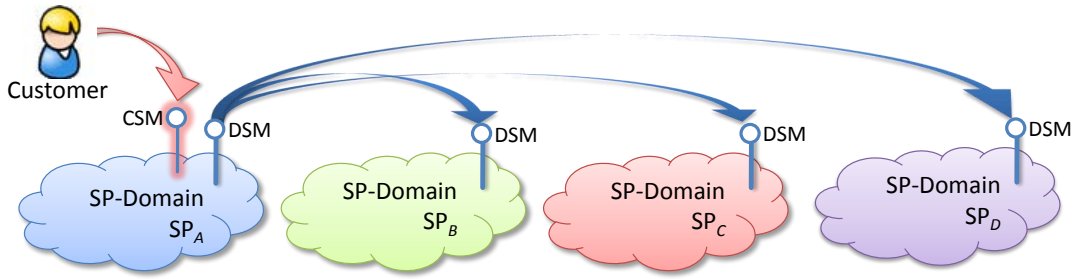


Abbildung 4.30.: *Source Routing*: Kommunikationsbeziehungen

Kommunikationsbeziehungen und Verantwortungsbereich

In Abbildung 4.30 sind die Kommunikationsbeziehungen beim *Source Routing* graphisch dargestellt. Dabei nimmt eine einzige SP-Domäne – in der Abbildung ist das SP_A – eine zentrale Stele bei der Bestimmung der E2E-Route ein und teilt allen anderen SP-Domänen mit, welche Teildienste sie für die neue Dienstinstanz verwenden sollen. Abgesehen davon, dass bei der im Abschnitt 4.3.1 beschlossenen kollektive Steuerung jede SP-Domäne die zentrale Stelle einnehmen kann, entspricht dieses Vorgehen dem sog. *Central Management* (vergleiche Abschnitt 3.7). Bei dieser Vorgehensweise liegt die Verantwortung für die Routenbestimmung ungeteilt bei einer einzelnen SP-Domäne, wie das in der Abbildung 4.31 durch einen Strichlinie-Oval gekennzeichnet ist.

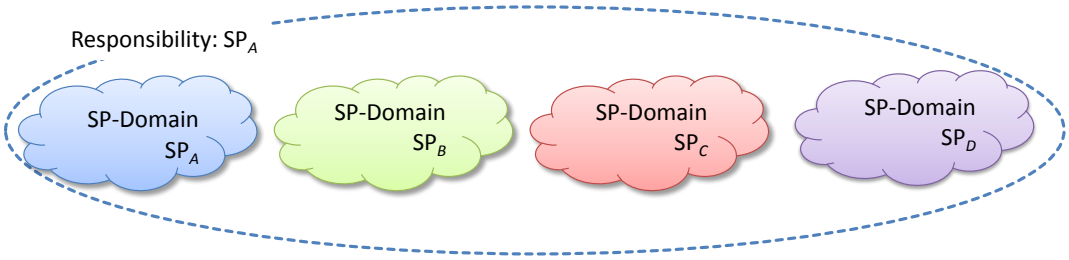


Abbildung 4.31.: *Source Routing*: Verantwortungsbereiche

Grundvoraussetzung: globales Wissen

Für diese Vorgehensart muss allerdings eine Reihe von Grundvoraussetzungen erfüllt werden. Eine der wichtigsten Voraussetzungen für das *Source Routing* ist das globale Wissen darüber, welche Teildienste (d.h. *Domain* und *Interdomain Links*) mit welchen Eigenschaften von den SP-Domänen erbracht werden können. Wie im Abschnitt 4.1.4 beschrieben wurde, setzt sich das globale Wissen aus dem Wissen einzelner SP-Domänen zusammen. Es kann sein, dass durch die Autonomie der Service Provider es unmöglich ist, eine oder mehreren Rollen einzuführen, die das zentrale Wissen sozusagen "verwalten" und allen SP-Domänen zur Verfügung stellen. In diesem Fall muss jede SP-Domäne mit jeder anderen auch bei Informationsabfragen direkt kommunizieren können, was wiederum den Kommunikationsbeziehungen in der Abbildung 4.30 entspricht.

Voraussetzungen: Kenntnis der DSM-Adressen und gute Vertrauensbeziehungen

Die Grundvoraussetzung für die direkte Kommunikation ist allerdings, dass jede SP-Domäne in der SP-Kooperation die Adresse der DSM-Schnittstelle jeder anderen SP-Domäne kennt. Weiterhin soll berücksichtigt werden, dass diese Art der Kommunikation eine Vertrauensbeziehung zwischen den einzelnen SP-Domänen voraussetzt, sodass Anfragen mit den Domänen-Policies vereinbar sind. Während bei kleinen, in sich geschlossenen Kooperationen das i.d.R. der Fall ist, können bei den großen und vor allem dynamischen SP-Kooperationen eventuell beide Annahmen nicht zutreffen.

Eine Abhilfe gegen das Fehlen der Kontaktinformationen kann die leicht angepasste Technik des DNS-Systems zum Weiterleiten an einen anderen DNS-Server schaffen (siehe Abschnitt 3.8). Angewandt auf die Problematik großer SP-Kooperationen für die Erbringung Verketteter Dienste wird ein Mechanismus benötigt, um bei jeder SP-Domäne die "Kontaktadressen" (DSM-Adressen) ihrer benachbarten Domänen abzufragen. Durch das rekursive Nachfragen bei bislang unbekannten SP-Domänen kann das globale Wissen über alle bei der Kooperation beteiligten Domänen, deren Nachbarbeziehungen sowie DSM-Adressen erworben werden. Dieses Vorgehen setzt voraus, dass SP-Domänen die DSM-Adressen ihrer Nachbarn weiter geben dürfen.

Bzgl. der Vertrauensbeziehungen ist die Situation wesentlich komplexer. Aus technischer Sicht kann diesem Problem z.B. durch die Kombination aus *föderierten Identitäts-Management* [Hom07] und *Trust-Based Access Control* [Bou09] begegnet werden, die sich mit der Identifizierung und den Vertrauensbeziehungen in Multi-Domain Umgebungen befassen. Sollte dennoch die Informationsanfragen zurückgewiesen werden, bleibt beim *Source Routing* der verantwortlichen SP-Domäne nichts anderes übrig, als das Routing auf dem vorhandenen (aber u.U. nicht vollständigem) Wissen über verfügbare Teildienste durchzuführen. Dadurch kann u.U. die E2E-Anforderungen erfüllende Route nicht gefunden werden, obwohl sie technisch realisierbar wäre.

Kommunikationsablauf

Sehr wichtig bei diesem Routing-Verfahren ist auch das Zusammenspiel der Kommunikation zwischen den SP-Domänen mit dem Routing-Algorithmus. In der Abbildung 4.32 ist ein vereinfachter Kommunikationsablauf dargestellt, der das Zusammenspiel

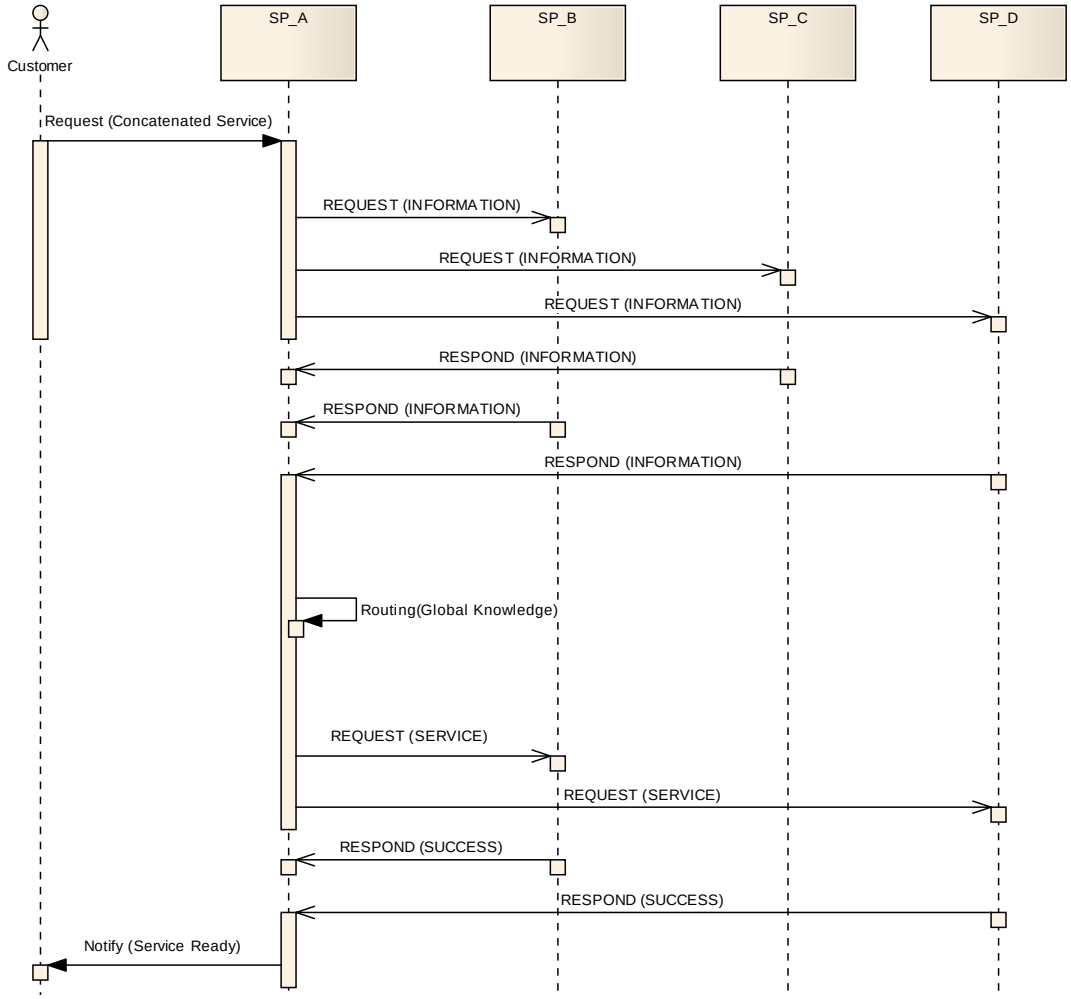


Abbildung 4.32.: *Source Routing*: Kommunikationsablauf (Vereinfacht)

illustriert. In der Abbildung schickt SP_A zunächst Informationsanfragen an alle anderen SP-Domänen. Bei der Realisierung können diese Anfragen entweder sequentiell oder auch gleichzeitig gesendet werden. In dem Beispiel wird davon ausgegangen, dass geeignete Vertrauensbeziehungen zwischen den Providern gegeben sind und alle angefragten SP-Domänen der SP_A die angefragten Informationen mitteilen. In der Abbildung ist auch deutlich zu sehen, dass die Antworten nicht unbedingt gleichzeitig oder in derselben Reihenfolge eintreffen. Erst nachdem die Informationen von allen SP-Domänen vorhanden sind, kann der Routing-Algorithmus ausgeführt werden. In dem Beispiel wird davon ausgegangen, dass die Route mit den erforderlichen Eigenschaften gefunden werden konnte. In diesem Fall können alle relevanten SP-Domänen – in dem Beispiel sind das SP_B und SP_D – mit der Bestellanfrage für die ausgewählte Teildienste kontaktiert werden. Diese Anfragen können wiederum gleichzeitig geschickt werden. Die Reihenfolge der Antworten auf die Bestellanfragen ist auch in

diesem Fall nicht gesichert. Erst nachdem die Bestätigungen für alle bestellten Teildienste vorliegen, kann der Kunde darüber benachrichtigt werden, dass die bestellte Dienstinstanz bereit ist.

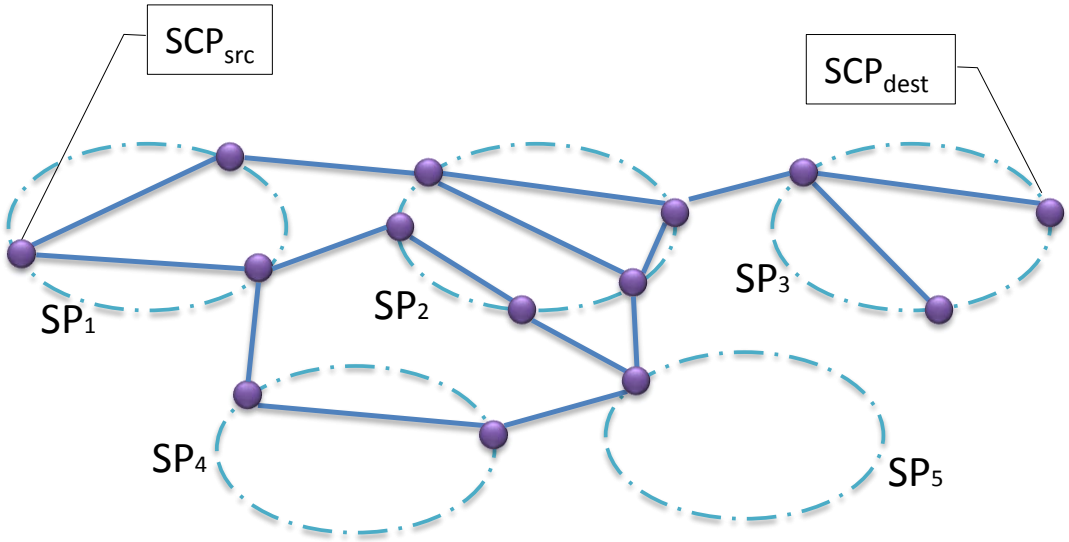


Abbildung 4.33.: Beispiel: Globales Wissen fürs Routing

Vor- und Nachteile des Verfahrens

Die Durchführung des Routings mit globalem Wissen hat sowohl Vor- als auch Nachteile. In der Abbildung 4.33 ist schematisch dargestellt, wie das globales Wissen bei nur fünf beteiligten SP-Domänen aussehen kann (für das UML-Objektmodell zur Beschreibung von Objekten und deren Eigenschaften siehe Abschnitt 4.6). In der Abbildung sind nur die *Compound Links* dargestellt, deren *Component Links* den E2E-Anforderungen genügen. Der Routing-Algorithmus soll in diesem Graph einen Weg zwischen SCP_{src} in SP_1 und SCP_{dest} in SP_3 finden.

In der Abbildung ist deutlich zu sehen, dass es mehrere Wege zwischen SCP_{src} und SCP_{dest} geben kann. Die Kenntnis aller möglichen Verbindungen erlaubt es, auf dem Graph unterschiedliche Routing-Anfragen zu bearbeiten, ohne dass zusätzliche Kommunikation zwischen SP-Domänen erforderlich ist. Als Beispiel dazu kann die Lösung des MCSP-Problems dienen, bei dem der kürzeste (bzw. der beste) Pfad von allen möglichen ausgewählt werden muss (vergleiche entsprechende Diskussionen in Abschnitten 3.3 und 4.2).

Auf der anderen Seite weist *Source Routing* auch einen u.U. wesentlich höheren Zeitaufwand bei der Pfadsuche auf. Dabei kann die Komplexität des Dijkstra-Algorithmus von $O(|N|^2 + |V|)$ als untere Schranke angegeben werden, weil bei diesem Algorithmus – im Gegensatz zur Problematik dieser Arbeit – nur ein einziger Parameter berücksichtigt werden muss. |E| steht dabei für die Anzahl der Knoten und |V| für die Anzahl der Kanten. Spricht man von der Kooperation der mittelgroßen und großen Service Provider (das Deutsche Forschungsnetz (DFN) hat z.B. ca. 130 Verbindungspunkte zu ande-

ren SPs [Adl09]) und soll dabei die Suche mit globalem Wissen durchgeführt werden, dann kann das u.U. zu Skalierungsproblemen führen.

Bei der Suche in sehr großen Graphen kann auf spezialisierte Algorithmen zurückgegriffen werden. Dazu gehört z.B. der im Abschnitt 3.3.2 angesprochene SAMCRA Algorithmus zur Lösung des MCP-Problems. Verglichen mit der Tiefensuche bieten solche Algorithmen eine bessere Suchlaufzeit. Auf der anderen Seite sind sie i.A. wesentlich komplexer aufgebaut, was die Integration der in diesem Abschnitt entwickelten Verfahren und Operationen u.U. komplizierter werden lässt.

Durch die u.U. lange Suchlaufzeit wird ein weiterer Nachteil des *Source Routings* verursacht. Da es i.A. mehrere Verbindungsanfragen von unterschiedlichen SP-Domänen geben kann, erhöht sich mit der steigenden Dauer der Pfadsuche auch die Wahrscheinlichkeit, dass gleichzeitige Dienstanfragen einander stören.

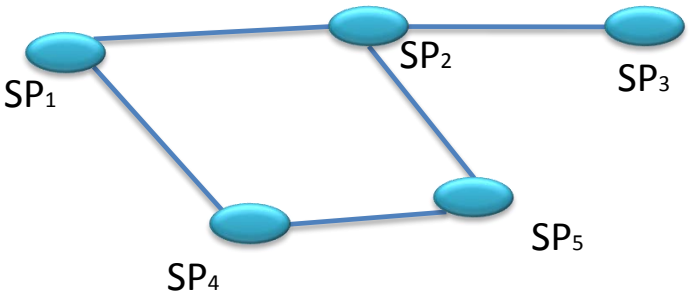


Abbildung 4.34.: SP-Nachbarbeziehungen

Reduktion der Komplexität

Eine Abhilfe kann eine Reduktion der Komplexität des Graphs schaffen, die vor der eigentlichen Pfadsuche durchgeführt werden kann. So könnte im Vorfeld der eigentlichen Routensuche ein höheres Abstraktionsniveau verwendet werden, um z.B. alle nicht zusammenhängenden Komponenten und vor allem Sackgassen zu eliminieren. In Abbildung 4.34 das Abstraktionsniveau von SP-DP-Verbindungen dargestellt. Das setzt auch voraus, dass alle Verbindungen innerhalb einer SP-Domäne "zusammengefügt" werden können, ansonsten kann z.B. ein Knoten eine Zusammenhangskomponente der SP-Domäne markieren. Die Verwendung dieses Abstraktionsniveaus bei den Informationsabfragen wird zwar die – nach dem Komplexitätsreduktionsverfahren – ausgeschlossenen SP-Domänen entlasten, auf der anderen Seite erfordert das ein komplexeres Kommunikationsprotokoll. Auf der anderen Seite birgt das Beibehalten einer einzigen Abstraktionsstufe bei den Anfragen andere Nachteile: zu einem bedeutet das unnötigen Kommunikationsaufwand der "irrelevanten" SP-Domänen und zum anderen beeinträchtigt das Verlagern der Abstraktionsaufgabe auf die Routing-Instanz u.U. die Suchlaufzeit.

4.3.3. Routing by Delegation

In diesem Abschnitt wird die Übertragbarkeit eines anderen Routing-Verfahrens auf die *Verkettete Dienste* diskutiert, das sich im Gegenteil zu *Source Routing* hauptsächlich in Multi-Domain Umgebungen durchgesetzt hat. Wegen des Grundprinzips, wie bei diesem Verfahren das E2E-Routing zu Stande kommt, wird es in dieser Arbeit als *Routing by Delegation* referenziert.

Kommunikationsbeziehungen

Das *Routing by Delegation*, wie es z.B. bei TK-Netzen stattfindet, ist in der Abbildung 4.35 graphisch dargestellt. Charakteristisch ist für dieses Vorgehen, dass die Entscheidungsgewalt jeder SP-Domäne sich ausschließlich auf das Routing innerhalb der eigenen Domäne und die Wahl der Nachfolgedomäne beschränkt (vergleiche auch Abschnitte 2.3.1 und 3.2).

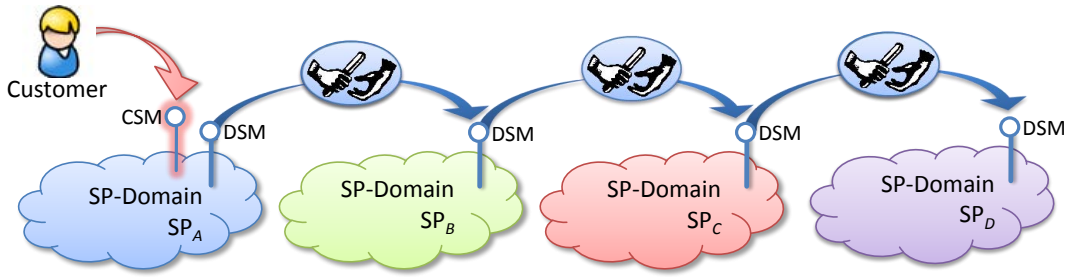


Abbildung 4.35.: *Routing by Delegation*: Kommunikationsbeziehungen

Verantwortungsbereiche

Da bei normalen Telefonverbindungen die E2E-Dienstgüte nicht berücksichtigt wird, kann bei der Aufgabendelegation – abgesehen von den technischen Verbindungsdetails – ausschließlich die Information über den zu erreichbaren Endpunkt sowie über den Verbindungsstatus (klingeln, besetzt, verbunden, aufgelegt) in der Kette ausgetauscht werden. Bei Verketteten Diensten hingegen muss zusätzlich auch die Verantwortung für die Dienstgüte des restlichen Abschnitts weitergereicht werden. In der Abbildung 4.36 sind die entsprechende Verantwortungsbereiche als die Domänen umschließende gestrichelte Ovale gekennzeichnet. Dabei übernimmt die SP_A dem Kunden gegenüber die Verantwortung für den gesamten E2E-Dienst; SP_B übernimmt die Verantwortung für die von den SP_B, SP_C und SP_D-Domänen erbrachten Teildienste usw.

Da auf die E2E-Dienstgüte auch die Dienstgüte der *Interdomain*-Verbindungen Auswirkung hat, müssen auch sie berücksichtigt werden. Diese Aufgabe kann von jeder SP-Domäne in der Kette für die Anbindung auf die Nachfolgedomäne erledigt werden. Am Beispiel der Abbildungen 4.35 und 4.36 würde SP_A die *Interdomain*-Verbindung zwischen SP_A und SP_B beantragen, SP_B ihrerseits die Verbindung zwischen SP_B und SP_C usw.

Bei der Delegation der Aufgabe an die Nachfolgedomäne kann ähnlich vorgegangen werden wie bei den im Abschnitt 4.2.8 beschriebenen angepassten Tiefensuche-

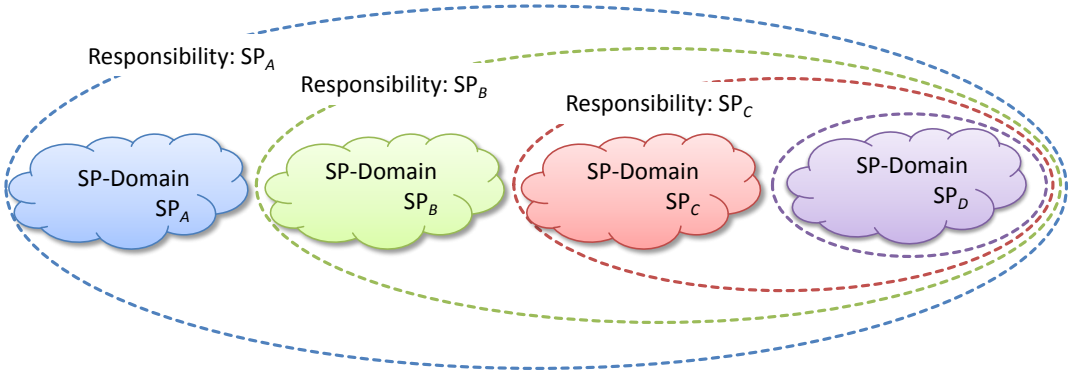


Abbildung 4.36.: *Routing by Delegation*: Verantwortungsbereiche

Algorithmen. Der Unterschied besteht nur daran, dass – nachdem die *Interdomain*-Verbindung zu der Nachbardomäne bestimmt und reserviert wurde – statt dem rekursiven Aufruf der DFS-Funktion die Delegation der Aufgabe an die ausgewählte SP-Domäne stattfinden soll. Die Funktionsparameter (*nodeCur*, *nodeDest*, $\vec{W}^{cur}_{path}$, $\vec{C}_{E2E}$) bleiben dabei dieselben. Die Notwendigkeit von SCP "*nodeCur*" ist dadurch bedingt, dass es zwischen zwei Nachbardomänen mehrere Verbindungspunkte geben kann und – im Gegenteil zu TK-Netzen – sie nicht implizit durch die Kommunikationsschnittstelle (NNI) implizit bestimmt sind. Die Verwendung von $\vec{W}^{cur}_{path}$ und $\vec{C}_{E2E}$ erspart die Notwendigkeit, die Obergrenze ständig zu verringern und dafür die entsprechende QoS-Parameter abhängige Funktionen definieren zu müssen. Stattdessen können hier die Aggregatfunktionen verwendet werden, wie sie im Abschnitt 4.2 definiert wurden.

Kommunikationsablauf

In der Abbildung 4.37 ist in der vereinfachten Form das Zusammenspiel zwischen der Inter-Domain Kommunikation und dem Routing-Algorithmus dargestellt. Das Routing wird jeweils anhand der lokal vorhandenen Informationen über die vorhandenen Kapazitäten, dem wiederum lokal vorhandenen Wissen über die Erreichbarkeit der Zieladresse hinter eigenen SCPs sowie den übergebenen Parametern ausgeführt. Nachdem der Verlauf der Route innerhalb der eigenen SP-Domäne bestimmt, die Wahl der nächsten SP-Domäne getroffen sowie alle relevanten Ressourcen reserviert wurden, kann die Aufgabe an die nächste SP-Domäne delegiert werden. Zuvor müssen *nodeCur* und $\vec{W}^{cur}_{path}$ aktualisiert werden.

Vor- und Nachteile des Verfahrens

Der wohl größte Vorteil dieses Verfahrens besteht in der potentiell höheren Akzeptanz der SP-Domänen, weil dabei kaum Informationen über die vorhandenen Kapazitäten preisgegeben werden müssen. Auch ist die Handhabung der Vertrauensbeziehungen viel einfacher als das bei *Source Routing mit globalem Wissen* erforderlich ist (vergleiche entsprechende Diskussion im Abschnitt 4.3.2), denn alle Kommunikationsbeziehungen beschränken sich ausschließlich auf die direkten Nachbarn-Domänen. Zu den Vorteilen dieses Vorgehens kann weiter der Einfluss der einzelnen

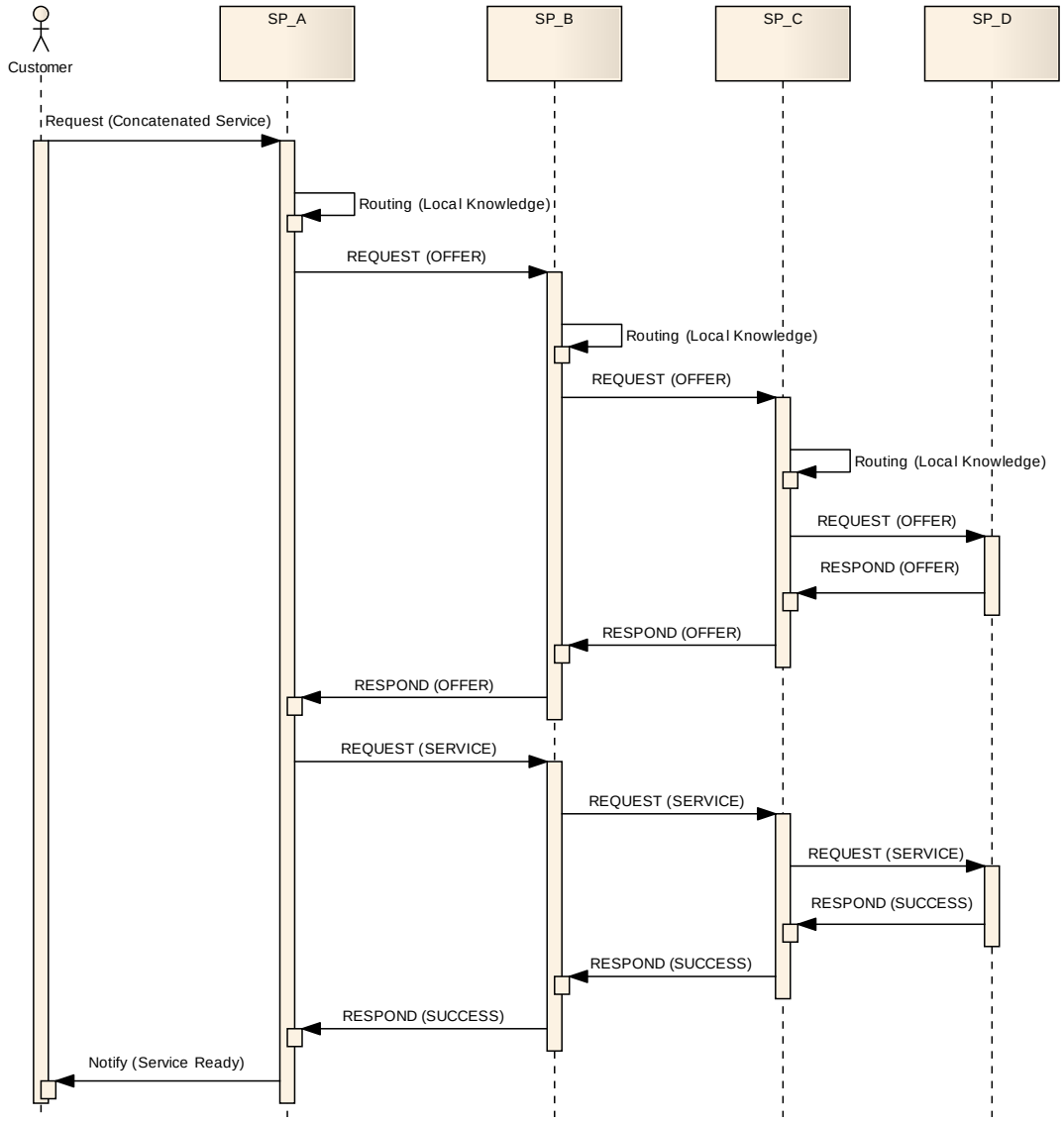


Abbildung 4.37.: *Routing by Delegation*: Kommunikationsablauf (Vereinfacht)

SP-Domänen auf den Routen-Verlauf gezählt werden, weil dadurch die internen – oft vertraglich und/oder monetär bedingten – Interessen besser berücksichtigt werden können.

Auf der anderen Seite geht durch die Delegation die E2E-Betrachtung verloren. Auch können Schleifen über dieselben SP-Domänen und dadurch unnötige Kommunikationsabfragen entstehen, was auf die Performance der Pfad-Suche Auswirkungen haben kann. Weiterhin entsteht durch die fehlende Multi-Domain Betrachtung eine Möglichkeit für Missbrauch (vergleiche z.B. die Diskussion über DiffServ im Abschnitt 2.3.5).

In der Abbildung 4.37 ist das *best-case* Szenario dargestellt, bei dem jede SP-Domäne die erforderlichen Teildienste schalten kann. Auch ein Fehlschlagen des Routings mit den spezifizierten Randbedingungen wird in der aufgebauten Kette zurückgemeldet. Bei einem Scheitern des Routings kann eine SP-Domäne auf die nächste mögliche Route, die u.U. über eine andere SP-Domäne führen kann, ausweichen und das Vorgehen wiederholen. Falls keine der in Frage kommenden Alternativen die erforderliche Dienstgüte für den Rest der Verbindung garantieren kann, wird das Fehlschlagen an die initiierende SP-Domäne gemeldet. Insbesondere wegen der Vielzahl der erforderlichen Interaktionen kann das ein sehr zeitintensives Vorgehen sein. Deswegen ist bei der Wahl dieses Verfahrens bei *Verketteten Diensten* eine zeitliche Beschränkung vorzugeben.

Ein weiterer Nachteil dieses Verfahrens, das in der Abbildung 4.37 zu sehen ist, sind die langen Kommunikationswege, die durch die Verschachtelung und die Delegation der Verantwortungsbereiche entstehen. In der Abbildung ist es z.B. bei der Bestellung des bereits gefundenen Pfades der Fall. Auch wenn es an dieser Stelle allein um das Routing geht, ist es dennoch wichtig zu berücksichtigen, dass diese langen Kommunikationswege auch bei den geschalteten Pfaden beibehalten werden, was u.U. zu unerwünscht langen Kommunikationszeiten bei allen Managementprozessen in weiteren Phasen des Dienstinstanz-Lebenszyklus führen kann.

4.3.4. Hybrides Routing-Verfahren

In diesem Abschnitt wird ein alternatives *hybrides* Routing-Verfahren entwickelt. Das neue Routing-Verfahren baut auf den beiden in den Abschnitten 4.3.2 und 4.3.3 diskutierten klassischen Verfahren auf. Das Ziel dabei ist, die unterschiedlichen Ansätze aus beiden Verfahren miteinander so zu kombinieren, dass die Anforderungen der *Verketteten Dienste* am besten abgedeckt sind.

Das neue Verfahren besteht aus zwei Teilen, was auch die Struktur dieses Abschnittes bestimmt. Zunächst wird im Unterabschnitt 4.3.4.1 eine veränderte Version von *Source Routing* vorgeschlagen, die mit Ideen aus TK-Netzen (siehe Abschnitte 2.3.1 und 3.2) angereichert wurde. Dem folgt im Unterabschnitt 4.3.4.2 die Beschreibung eines modifizierten *Routing-by-Delegation*-Verfahrens, das wiederum von Ideen des *Source Routings* profitiert. Das Zusammenspiel dieser beiden Teile sowie deren gegenseitige Übergänge werden in den jeweiligen Unterabschnitten erläutert.

4.3.4.1. Source Routing mit semi-globalem Wissen

Auch wenn das *Source Routing* mit globalem Wissen mehrere Vorteile hat, wie z.B. die Möglichkeit an die Kundenanforderungen angepasste Suchalgorithmen zu verwenden sowie mit mehreren SP-Domänen bei Informations-, Reservierungs- und Serviceanfragen parallel/gleichzeitig zu kommunizieren (für eine ausführliche Diskussion darüber siehe Abschnitt 4.3.2), weist diese Strategie eine Reihe von Nachteilen auf. Bei einer großen Anzahl von SP-Domänen und/oder Verbindungen bzw. Verbindungspunkten (SCPs) pro Domäne können sehr komplexe Graphen entstehen. Dadurch wird die Notwendigkeit einer Komplexitätsreduktion und komplexer Suchalgorithmen verursacht, was wiederum eine lange Suchlaufzeit nach sich ziehen.

Aus Sicht der einzelnen SP-Domänen liegt der größte Nachteil des *Source Routings* jedoch eher darin, dass dabei sehr viele Informationen über vorhandene Kapazitäten bekanntgegeben werden müssen, was insbesondere bei großen Kooperationen mit oft sehr restriktiven Policies nicht vereinbar ist. Bei *Routing by Delegation* dagegen werden die internen Kapazitäten von der Außenwelt verborgen, was eher dem Interesse der Service Provider entspricht. Weiterhin können die einzelnen SP-Domänen basierend auf ihrem eigenen Wissen über die Verbindungsmöglichkeiten zu unterschiedlichen Ziel-Domänen und aufgrund eigener – oft vertraglich bedingter – Präferenzen über den bevorzugten Routenverlauf entscheiden. Die Grundidee für die Entwicklung eines veränderten *Source Routings* besteht darin, diese – auf den ersten Blick miteinander nicht zu vereinbarenden – Eigenschaften miteinander zu kombinieren.

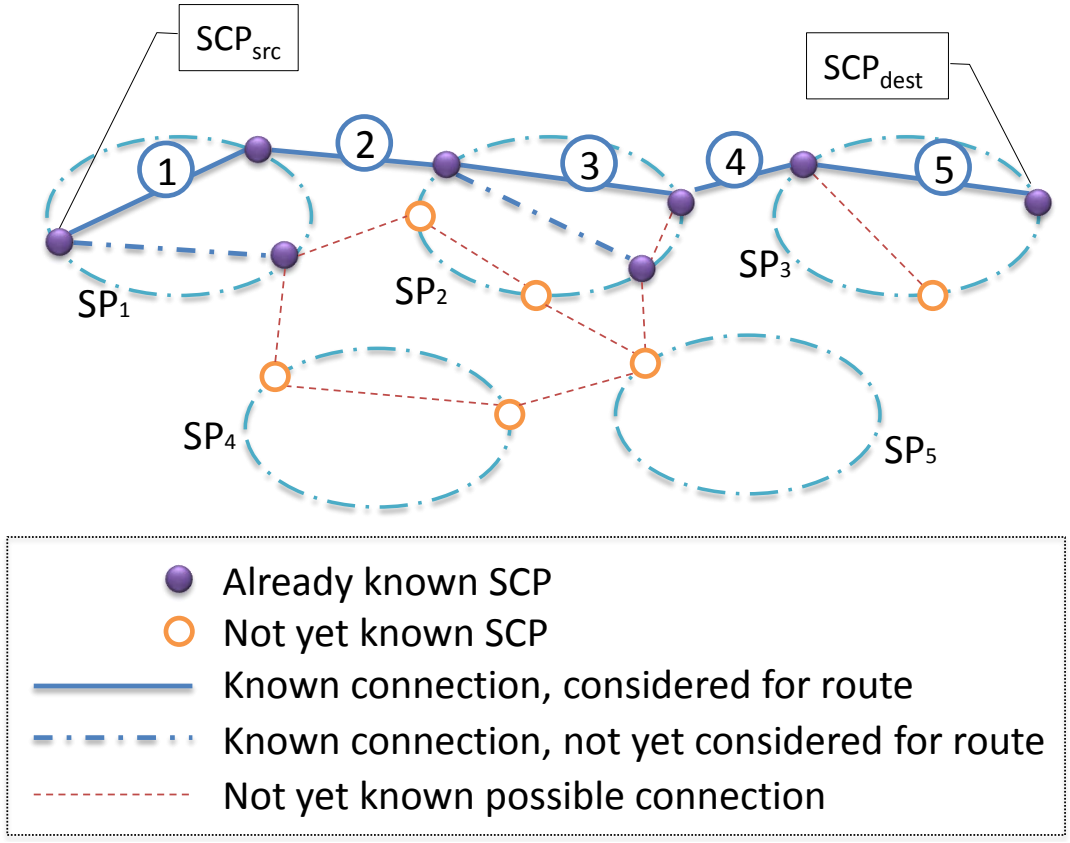


Abbildung 4.38.: Suche mit dem semi-globalen Wissen

Source Routing mit semi-globalem Wissen

Die angepasste Version des *Source Routings*, die im weiteren als *Source Routing mit semi-globalem Wissen* referenziert wird, ist graphisch in Abbildung 4.38 illustriert. Sollte ein Pfad zwischen SCP_{src} und SCP_{dest} gefunden werden, dann kann auf dem Wissen und den Präferenzen einzelner SP-Domänen aufgebaut werden. Wird jede SP-Domäne nach Informationen gefragt, welche Teildienste von dem vorgegebenen SCP_{cur} in die Richtung von SCP_{dest} gehen, dann kann die gefragte SP-Domäne als die Antwort eine Liste von *Compound* und *Component Links* von dem vorgegebenen Current-SCP zu den SCPs "in die Richtung" des Ziel-SCP zurückschicken. Ist diese Liste entsprechend den z.B. Policy- und/oder Netzauslastung-bedingten Präferenzen der jeweilige SP-Domäne sortiert, dann kann sie als Eingabe für den "MCP mit DFS"-Algorithmus (siehe Abschnitt 4.2.8) verwendet werden. Sollte die Aggregation der Eigenschaften der bevorzugtesten Teilstrecke in Verbindung mit dem berechneten Wert des Teilpfades die E2E-Anforderungen noch erfüllen, dann kann der zweite SCP der Teilstrecke bei dem nächsten Durchlauf dieses Vorgehens als Current-SCP betrachtet werden. Wenn die E2E-Anfordrungen beim Erreichen von SCP_{dest} erfüllt sind, können alle für den Pfad verwendeten Teilstrecken reserviert und anschließend bestellt werden. Sowohl die Reservierungs- als auch Bestellanfragen können entweder sequen-

tiell oder gleichzeitig an die jeweiligen SP-Domänen geschickt werden. Es ist auch denkbar, dass die Teilstrecken noch während der Pfadsuche gleich nach ihrer Auswahl reserviert werden. Jede dieser Vorgehensweisen hat ihre Vor- und Nachteile. Für die genauere Diskussion und die endgültige Festlegung siehe Kapitel 6, insbesondere Abschnitt 6.1 bis 6.4.

Die Abbildung 4.38 baut auf dem Beispielnetz aus der Abbildung 4.33 auf. Dabei wird von dem Best Case Szenario ausgegangen, dass alle als "erste" in der Liste angebotenen alternativen Verbindungen (in der Abbildung als durchgezogene dicke Linien dargestellt) auch reserviert und später geschaltet werden können. Die Reihenfolge, in der diese Teildienste gemeldet und reserviert werden, ist in der Abbildung mit Nummern in den Kreisen gekennzeichnet. Die alternativen gemeldeten Routen werden als dicke Strichpunktlinien dargestellt. Die Informationen über das globale Netz, die dem Suchalgorithmus "entfallen", sind in der Abbildung als dünne gestrichelte Linien (für *Compound Links*) und nichtausgefüllte kleine Kreise (für SCPs) dargestellt.

Wie man in der Abbildung leicht erkennen kann, braucht der Algorithmus für die Suche nicht das vollständige Wissen, sondern kann das nötige Wissen bei Bedarf durch die entsprechenden Anfragen beliebig erweitern (daher auch Bezeichnung als "semi-global"). Da dieser Algorithmus auf dem Hintergrundwissen der angesprochenen SP-Domänen aufbaut, kann man davon ausgehen, dass die Tiefensuche sehr schnell zum Finden eines Pfades führt, der die E2E-Anforderungen erfüllt. Daher eignet sich dieses Vorgehen hervorragend für die Lösung des relativ einfachen MCP-Problems. Zu den größten Vorteilen dieses Vorgehens kann auch die Berücksichtigung der SP-Präferenzen sowie der – verglichen mit dem klassischen *Source Routing* – wesentlich kleinere Informationsbedarf gezählt werden. Auf der anderen Seite eignet sich dieses Verfahren nur sehr schlecht für die Lösung anderer Aufgaben, wie z.B. des MCSP-Problems (siehe dazu insbesondere Abschnitte 3.3 und 4.2.8). Auch wird hier die Integration der Multi-Domain-fähigen Identitäts- und Trust-Managementsystemen notwendig.

4.3.4.2. Erweiterung: on-demand Delegation

Im Unterabschnitt 4.3.4.1 wurde das *Source Routing mit semi-globalem Wissen* präsentiert, das ein mit Ideen aus *Routing by Delegation* angereichertes *Source Routing* darstellt. Im Verlauf dieses Vorgehens kann es vorkommen, dass eine der direkt kontaktierten SP-Domänen eine Anfrage zurückweist. Der Grund dafür kann z.B. darin liegen, dass die Vertrauensbeziehung zu der SP-Domäne *Requesting Service* zu niedrig ist und die Policies der SP-Domäne vorschreiben, die Informationsanfragen im solchen Fall zurückzuweisen.

Diese Situation ist in Abbildung 4.39 graphisch dargestellt. SP_A kontaktiert zunächst die SP-Domäne SP_B direkt. Diese stellt die erforderlichen Informationen zur Verfü-

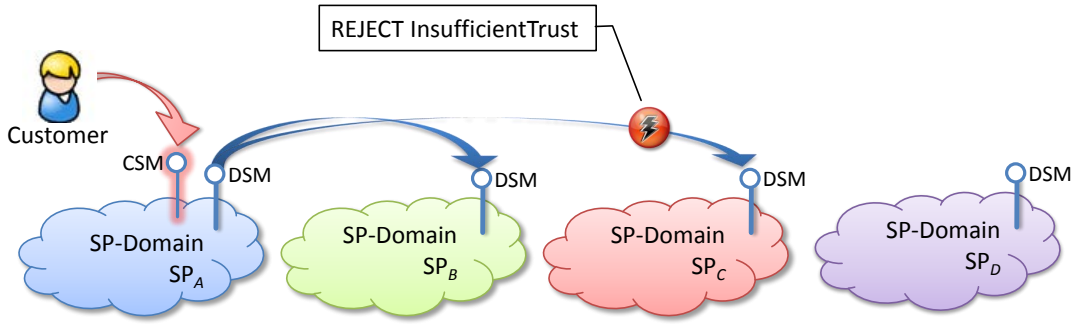


Abbildung 4.39.: Zentrales Management nicht möglich: Sicherheitsbedenken

gung und schlägt SP_C als die nächste Domäne auf dem Weg zum Ziel vor. Bei der direkten Anfrage bei SP_C wird diese jedoch zurückgewiesen.

Aus dieser Situation sind zwei Auswege denkbar. Zu einem kann es die Domäne SP_A mit einer alternativen Route über eine andere SP-Domäne probieren. Diese Möglichkeit schränkt aber die Anzahl der möglichen Routen zum Ziel ein, was wiederum die Wahrscheinlichkeit mindert, einen E2E-Anforderungen erfüllenden Pfad zu finden. Alternativ dazu kann die Delegation der Routingaufgabe an eine andere SP-Domäne sein. Sinnvoll ist dabei die Aufgabe an die letzte SP-Domäne zu delegieren, die die direkte Anfrage noch akzeptiert hat, weil sie u.U. durch die Nähe (direkte Nachbarschaft) zu der SP-Domäne mit restriktiven Sicherheitsregeln mehr Chancen hat, an eine Zusage von dieser SP-Domäne zu kommen (siehe Abbildung 4.40).

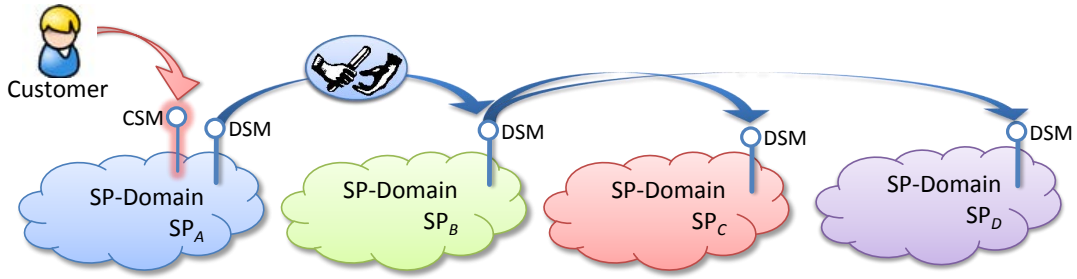


Abbildung 4.40.: Delegieren der Aufgabe

Die Art und Weise, wie die delegierte Aufgabe von der beauftragten SP-Domäne SP_B erledigt wird – d.h. ob SP_B für den Rest der Strecke als Zentraler Manager fungiert, wie es bei *Source Routing* der Fall ist, oder die Teilaufgabe(n) weiter delegiert – ist für die Domäne SP_A in Bezug auf das Routing und die Festlegung der Dienstgütegrenzen der restlichen Teildienste i.A. ohne Bedeutung. Die Verantwortungsbereiche für das Routing in diesem Fall sind in Abbildung 4.41 dargestellt.

Die Unterschiede können sich jedoch in Bezug auf die Managementfunktionalität ergeben. Während bei *Routing by Delegation* (siehe Abschnitt 4.3.3) die SP-Domäne, an die

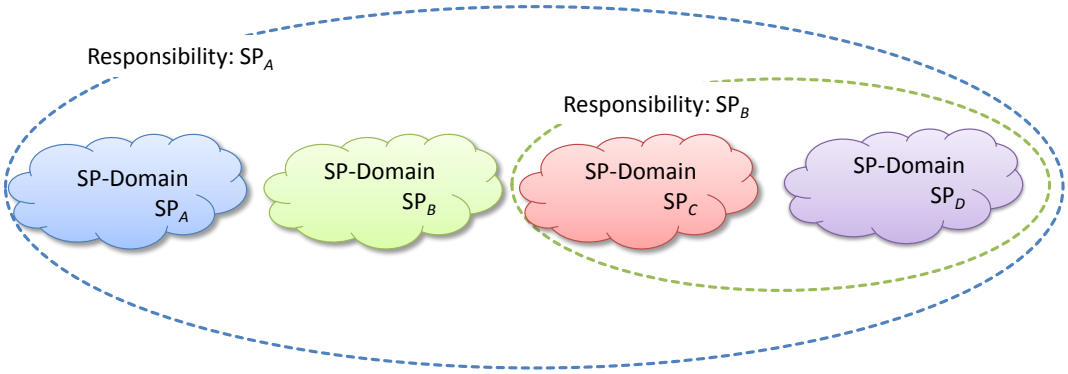


Abbildung 4.41.: *On-demand Delegation*: Verantwortungsbereiche

die Aufgabe delegiert wird, für alle Managementaufgaben als Proxy auftritt und die Zusammensetzung des restlichen Dienstes sowie die Managementaspekte komplett verschattet, wird bei *Source Routing* (siehe Abschnitt 4.3.2) eher das Gegenteil anvisiert – dass die vom Kunden beauftragte SP-Domäne alle Kommunikationswege zwischen den erforderlichen Managementkomponenten und allen beteiligten SP-Domänen selbst bestimmt.

Delegationsformen

Um auch bei der Aufgabendelegation die Festlegungen der vom Kunden beauftragten SP-Domäne beibehalten zu können, wird zunächst die Möglichkeit benötigt, dem Proxy-SP das zu signalisieren. Diese Option wird im Weiteren als TRANSPARENTPROXY referenziert. In diesem Fall müssen dem Proxy-SP auch alle Kommunikationsschnittstellen für alle erforderlichen Managementfunktionen mitgeteilt werden, wie z.B. für ein Monitoring. Insbesondere wird das bei Delegation der Managementfunktionalität wichtig (mehr dazu siehe im Abschnitt 4.4).

Unter Umständen kann jedoch – trotz der längeren Kommunikationswege – eine Delegationsform mit kompletter Verschattung aller Details hinter der Proxy-SP sinnvoll sein, wie sie bei *Routing by Delegation* verwendet wird. Diese Form wird im Weiteren als FULLPROXY referenziert. In diesem Fall agiert der Proxy-SP als der Provider aller in seinem Verantwortungsbereich sich befindenden Teildienste. Der Proxy-SP bildet alle Managementanfragen entsprechend ab und leitet sie an die involvierten SP-Domänen weiter. Der Proxy-SP braucht auch in diesem Fall alle Kommunikationsadressen für die Managementfunktionen.

An dieser Stelle soll noch kurz bemerkt werden, dass das hier angesprochene Management sich auf alle Phasen des Dienstinstanz-Lebenszyklus beziehen kann. Als ein für SLM typisches Beispiel kann das Monitoring dienen, bei dem die Überwachungsinformationen von den verschatteten Teildiensten durch den Proxy-SP aggregiert und im aggregierten Zustand an die übergeordnete Monitoring-Instanz weitergereicht werden sollen. Das entspricht weitgehend dem üblichen Vorgehen bei hierarchischen Organisationsformen.

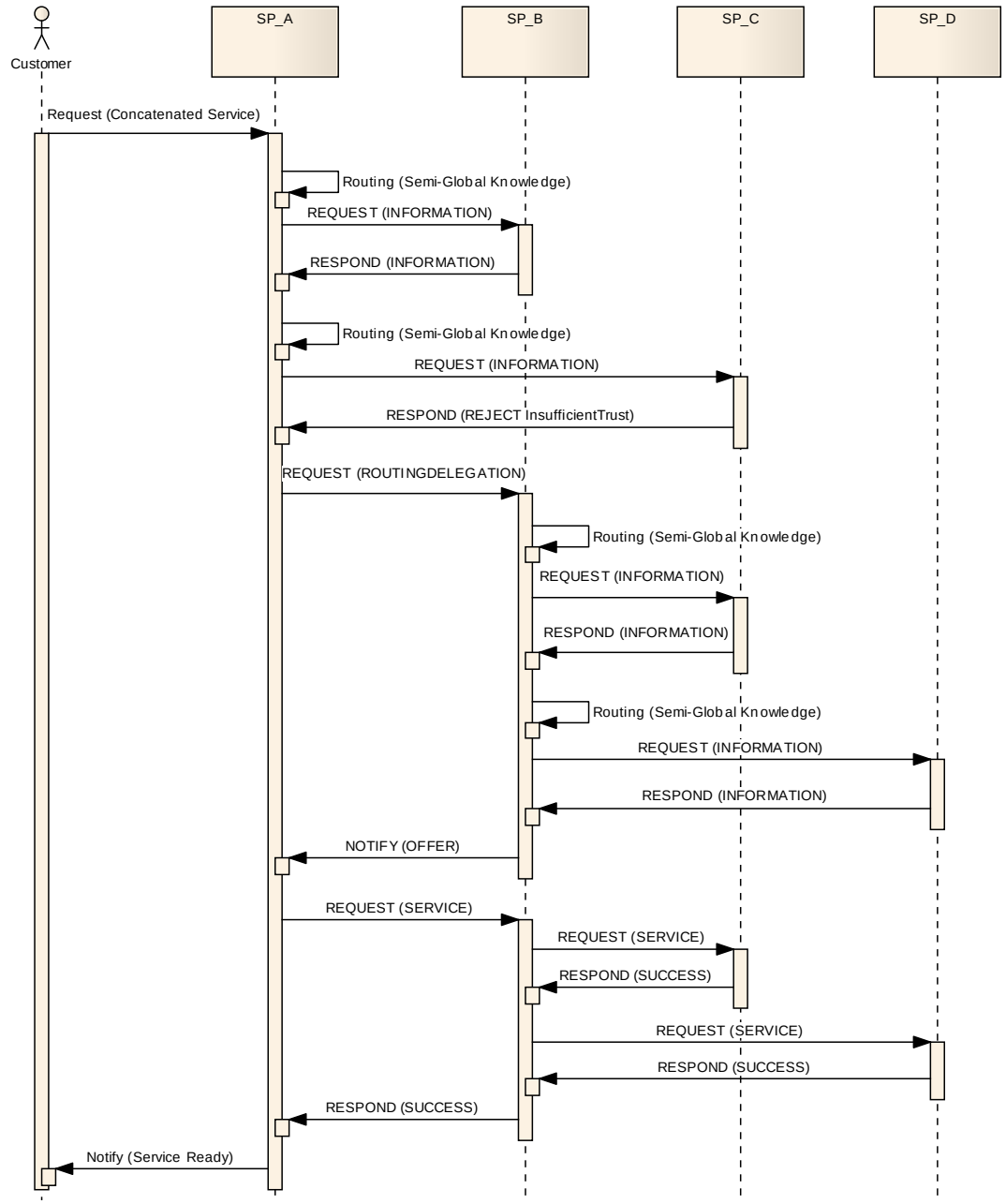


Abbildung 4.42.: Hybrides Verfahren *Source Routing mit mit semi-globalem Wissen und on-demand Delegation*: Kommunikationsablauf (Vereinfacht)

Routing nach der Delegation

Unabhängig davon, welche der Delegationsformen gewählt wurde, wird an den Proxy-SP vor allem die Verantwortung für das Routing für den Rest des Pfades übertragen. An dieser Stelle wird empfohlen, dass der Proxy-SP bei dieser Aufgabe wiederum entsprechend dem *Source Routing mit semi-globalem Wissen* vorgeht, wie dieses Verfahren im Unterabschnitt 4.3.4.1 beschrieben wurde. Die endgültige Entscheidung über das bevorzugte Vorgehen liegt allerdings beim Proxy-SP.

Delegation seitens Proxy-SP

Es kann sein, dass auch der Proxy-SP die Aufgabe weiter delegieren muss. In diesem Fall muss ein weiterer mit der Delegationsoption verbundener Aspekt berücksichtigt werden. Es kann sein, dass auch Proxy-SP die Aufgabe weiter delegieren muss. In diesem Fall muss ein weiterer mit der Delegationsoption verbundener Aspekt berücksichtigt werden. Während bei der FULLPROXY-Option der Proxy-SP selbst entscheiden darf, welche Delegationsart bei der erneuten Delegation verwendet wird, darf bei TRANSPARENTPROXY ausschließlich diese Proxy-Option wiederverwendet werden, um die Managementfestlegungen der beauftragten SP-Domäne weiter zu erhalten. Bei den Managementfestlegungen handelt es sich ausschließlich um Kontaktinformationen – d.h. DSM-Adresse(n) – sowie Bedingungen – wie z.B. die Grenzwerte, bei deren Verletzung eine Benachrichtigung erfolgen soll. Eine Reihe ähnlicher Kommunikationskanäle sind auch in umgekehrter Richtung – d.h. diesmal zu den involvierten SP-Domänenen – zu etablieren. Solche Kommunikationskanäle werden z.B. für das *Incident&Problem Management* gebraucht. Das heißt, dass die bei den Antworten einzelner SP-Domänen mitgeteilten Informationen vom Proxy-SP gebündelt und mit Verweisen auf die entsprechenden SP-Domänen und deren Teildienste an die anfragende SP-Domäne mitgeteilt werden müssen. Auch muss den jeweiligen SP-Domänen mitgeteilt werden, von wem solche Anfragen kommen können, damit sie nicht – z.B. wegen Security-Policies – automatisch zurückgewiesen werden.

Der Kommunikationsablauf aus dem in Abbildungen 4.39 und 4.40 eingeführten Beispiel ist in der Abbildung 4.42 als ein UML-Sequenzdiagramm dargestellt. Die Reservierungsschritte (anschließend nach der Informationsabfrage) wurden dabei zu Gunsten der Übersichtlichkeit weggelassen. Bei der Delegation mit TRANSPARENTPROXY-Option wäre es zwar technisch möglich, auch die abschließenden Serviceanfragen und die zugehörigen Antworten – und nicht nur die Managementkommunikation in den späteren Lebenszyklusphasen – direkt zwischen SP_A und den anderen Domänen auszutauschen. Die Zeitersparnis dabei ist allerdings eher als unbedeutend zu betrachten, insbesondere verglichen mit der Zeit für die eigentliche Pfadsuche. Die Realisierung dieser Option würde aber auch eine zusätzliche Verkomplizierung der Kommunikationslogik nach sich ziehen, weswegen diese Option nicht mehr weiter betrachtet wird.

Vor- und Nachteile des Verfahrens

Die Delegation der Aufgabe kann in vielerlei Hinsicht als eine Notlösung betrachtet werden, auf die nach einer zurückgewiesenen direkten Informationsanfrage zurückgegriffen werden kann. Es wird hier davon ausgegangen, dass, wenn die Vertrauensbeziehungen zu niedrig sind, gleich die Informationsabfrage und nicht eine

der späteren Reservierungs- und Bestellungsabfragen zurückgewiesen wird. Die Unterstützung von gleich zwei Delegationsoptionen hat sowohl positive als auch negative Konsequenzen. So wird dadurch das Verfahren komplizierter und dadurch die Beziehungen zwischen SP-Domänen schwerer nachvollziehbar. Auf der anderen Seite ermöglicht es den SP-Domänen mehr Flexibilität in der Wahl zwischen einfachen Kommunikations- sowie Verantwortungsbeziehungen auf einer Seite und den kürzeren Kommunikationswegen sowie besserer Multi-Domain Übersicht auf der anderen Seite.

4.3.5. Gegenüberstellung der Alternativen und Auswahl

Vergleicht man die in Abschnitten 4.3.2, 4.3.3 und 4.3.4 diskutierten Routing-Verfahren, so stellt man fest, dass sie alle eine Reihe von Vor- und Nachteilen aufweisen. Hier sollen kurz die wichtigsten zusammengefasst werden.

Bei *Source Routing mit globalem Wissen* ist es möglich, die Pfadsuche flexibel nach den Kundenanforderungen zu gestalten, bei Informations- und Service-Anfragen gleichzeitig mit mehreren SP-Domänen zu kommunizieren sowie die Wahl der Anforderungen für die Teildienste vollständig zu kontrollieren. Dazu ist es möglich, bei der Wahl der SP-Domänen während des Routing-Prozesses auch die Erfahrungswerte aus der Vergangenheit sowie die Vertrauensbeziehungen zu der jeweiligen SP-Domäne miteinzubeziehen. Auf der anderen Seite erfordert es oft einen tiefen Einblick in sensible Informationen, wie z.B. die in den SP-Domänen realisierbaren Teildienste und deren mögliche Dienstgüte oder auch die grobe Netztopologie.

Routing by Delegation bietet zwar eine sehr gute Verschattung der verfügbaren Ressourcen sowie – verglichen mit dem *Source Routing* – eine wesentlich bessere Kollisionsvorbeugung. Durch die Verschachtelung und Verschattung aller Managementprozesse werden im Gegenzug deren Laufzeiten jedoch wesentlich erhöht.

Das *Source Routing mit semi-globalem Wissen* versucht den Informationsbedarf so weit wie möglich einzuschränken. Der Informationsbedarf liegt jedoch immer noch über dem für *Routing by Delegation* üblichen. Die Informationsabfragen können bei dieser Routing-Methode nur sequentiell gestaltet werden. Die Kombination mit der *on demand Delegation* macht den Algorithmus zwar robust gegen zu niedrige Vertrauensbeziehungen und dadurch auch für große Providerkooperationen tauglich, auf der anderen Seite wird das Verfahren dadurch wesentlich komplexer als seine zwei Vorbilder.

Diese und weitere Vor- und Nachteile der angesprochenen Routingstrategien sowie deren Derivate sind in der Tabelle 4.2 kurz zusammengefasst. Für eine ausführliche Diskussion der Stichpunkte wird an dieser Stelle auf die entsprechende Abschnitte verwiesen, wo die jeweiligen Algorithmen beschrieben wurden.

Wahl des Routing-Verfahrens für Verkettete Dienste

Obwohl auch das im Abschnitt 4.3.4 entwickelte Routing-Verfahren eine Reihe von Nachteilen aufweist (siehe in der mittleren Zeile der Tabelle), sieht bei ihm das Verhältnis zwischen den Vor- und Nachteilen in Bezug auf die wichtigsten Eigenschaften wesentlich ausbalancierter aus als bei den klassischen Verfahren. Aus diesem Grund wird an dieser Stelle für das *Routing mit semi-globalem Wissen und on-demand Delegation* als die bevorzugte Routingform bei *Verketteten Diensten* entschieden. Das *Routing mit semi-globalem Wissen* Verfahren vereint eine verhältnismäßig gute Verschattung der Domain-Interna mit E2E-Kontrolle über alle wichtigen Entscheidungen und lehnt sich zudem an die Domain-Präferenzen über die bevorzugten Routen an. Sollte eine direkte Anfrage zurückgewiesen werden, kann als eine Notlösung auf das *Routing by Delegation* zurückgegriffen werden.

	Vorteile	Nachteile
Source Routing mit globalem Wissen	▪ Kundenangepasste Suche (beliebige Aufgaben Lösbar) ▪ Gleichzeitige Anfragen für: - Information - Reservierung - Service ▪ Berücksichtigung der SP-SP Vertrauensbeziehungen und Erfahrungen	▪ Hoher Detailierungsgrad der erforderlichen Informationen ▪ Erforderlich gute SP-SP Vertrauensbeziehungen ▪ Lange Suchlaufzeit ▪ U.U. Notwendigkeit für - Komplexitätsreduktion - Komplexe Suchalgorithmen ▪ Hohe Wahrscheinlichkeit der Kollisionen bei konkurrierenden Anfragen
Source Routing mit semi-globalem Wissen und on-demand Delegation	▪ Gleichzeitige Kommunikation bei: - Reservierung - Service-Request ▪ Mittlere Verschattung der Domain Ressourcen ▪ Nutzen von SP-Wissen über mögliche Route (Kommunikation nicht mit allen Domänen notwendig) ▪ Einfache Suchalgorithmen (z.B. CSP mit DFS) ▪ Mittlere Suchlaufzeit ▪ Bei Bedarf Ausweichen auf Delegation möglich ▪ Kollisionswahrscheinlichkeit ist gering und kann gleich berücksichtigt werden	▪ Verfahren ist relativ komplex ▪ Sequentielle Kommunikation bei: - Information ▪ Algorithmen geeignet nur für CSP-spezifischen Aufgaben ▪ Verbeugung des Missbrauchs nur im Bereich der direkten Kommunikation möglich ▪ Ausfall einer Proxy-SP verhindert die Kommunikation mit allen dahinterliegenden Domänen
Routing by Delegation	▪ Keine sensible Informationen nötig ▪ Nutzen von SP-Wissen über mögliche Route ▪ Einfache Suchalgorithmen (z.B. CSP mit DFS) ▪ Kommunikation beschränkt auf die Nachbardomänen (SP-SP-Vertrauen gegeben) ▪ Reservierung/Ordering ohne zusätzliche Kommunikation möglich	▪ Keine Kontrolle über die Entscheidungen einzelner Domäne (Missbrauch möglich) ▪ Mehrmaliges durchsuchen selber (Teil-)Pfade und in der Schleife nicht ausgeschlossen ▪ Lange Durchlaufzeiten bei allen Managementprozessen (hängt von der Kettenlänge ab) ▪ Ausfall einer Proxy-SP verhindert die Kommunikation mit allen dahinterliegenden Domänen ▪ Abbruche durch Timeouts bei Managementoperationen möglich

Tabelle 4.2.: Routing-Verfahren: Gegenüberstellung der Alternativen

Modellierungs- und Identifikations-Vorgaben

Durch die Wahl des Routing-Verfahrens ist auch eine Reihe von Voraussetzungen bedingt, die bei der Inter-Domain Kommunikation erfüllt sein müssen. Bei der Kommunikation zwischen SP-Domänen müssen unterschiedliche Anfragen signalisiert werden. Für die reibungslose Zusammenarbeit zwischen SP-Domänen muss die globale Eindeutigkeit dieser Anfragen gewährleistet werden:

Vorgabe (Identifizierung) VI10 - Kommunikationsprotokoll

Ein global eindeutiges Kommunikationsprotokoll soll definiert werden, das alle erlaubten Anfragen unterstützt.

Weiterhin soll es für den definierten Ablauf des *Source Routings mit semi-globalem Wissen* möglich sein, folgende Informationseinschränkung bei den Informationsabfragen zu spezifizieren

Vorgabe (UML-Modellierung) VM07 - Topology-Einschränkung

Es muss möglich sein, eine topologische Einschränkung anhand zweier SCPs (einem Ausgangs- und einem Zielpunkt) anzugeben.

Für die *on-demand Delegation* werden weiterhin folgende Kommunikationsartefakte benötigt:

Vorgabe (UML-Modellierung) VM08 - Zwischensumme und E2E-Anforderungen

Es muss möglich sein, dem Proxy-SP sowohl das Gewicht des bisher gefundenen Teilpfades als auch die E2E-Anfordrungen mitzuteilen.

4.4. Multi-Domain-Funktionalität, Spezialisierung

Alle bisherigen Überlegungen im Abschnitt 4.3 gingen von der Annahme aus, dass alle SP-Domänen immer alle benötigten funktionalen Komponenten haben. Da die Bereitstellung und der Betrieb jeder funktionalen Komponente mit Kosten verbunden ist, haben sich in der Praxis zwei eng miteinander verbundene Aspekte durchgesetzt: Spezialisierung und Sharing. Ein gutes Beispiel dafür stellt der DNS-Dienst dar (siehe Abschnitt 3.8.2). Die DNS-Server werden oft von darauf spezialisierten Service Providern betrieben und der Dienst wird gemeinsam von den anderen Service Providern genutzt.

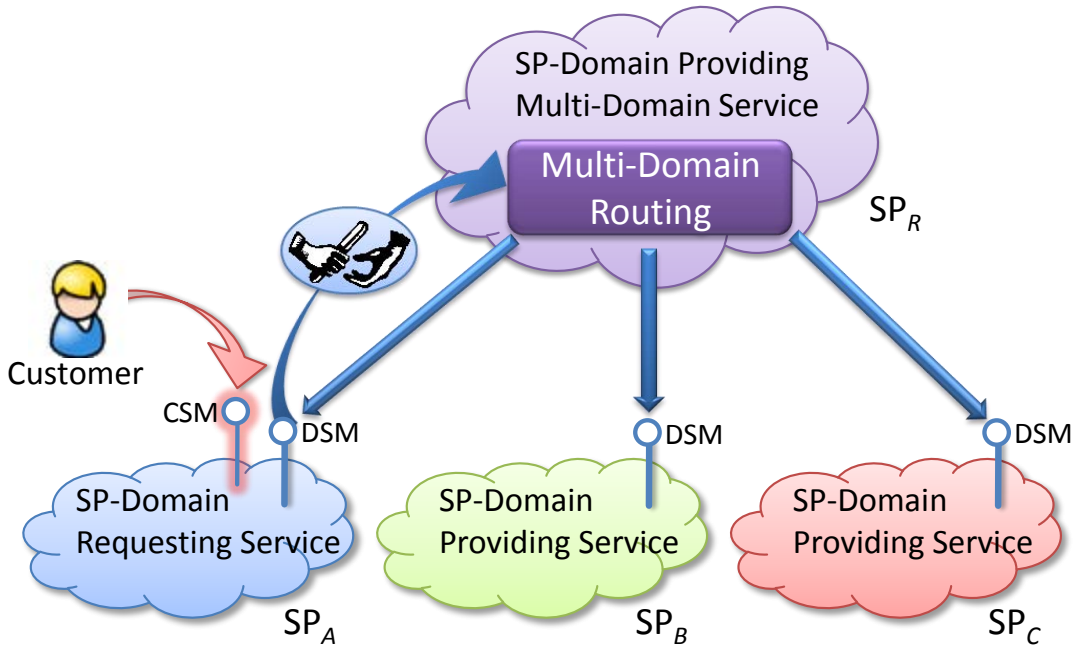


Abbildung 4.43.: Auslagern der Multi-Domain Aufgaben: Routing

Eine ähnliche Vorgehensweise wäre auch bei Verketteten Diensten denkbar. Im Rahmen dieser Arbeit sind vor allem die Delegation der Routing- und Monitoring-Aufgaben interessant, da sie – insbesondere durch deren Optimierung und unterschiedliche Fallunterscheidungen bedingt – sehr komplexe Formen annehmen können, was sich unmittelbar auf deren Betriebs- und Weiterentwicklungskosten auswirken kann.

In der Abbildung 4.43 wird die Delegation der Routingaufgabe dargestellt. In dieser Abbildung ist die Domäne SP_A vom Customer beauftragt, eine E2E-Verbindung aufzubauen. Sollte z.B. SP_A die für das *Multi-Domain Routing* zuständige Komponente nicht haben, kann sie diese Funktionalität bei der SP-Domäne SP_R bestellen. Um die gestellte Aufgabe zu erfüllen, muss SP_R mit der im Abschnitt 4.3 besprochenen Routing-

Strategie vorgehen. Da die Domäne SP_R auch auf Vertrauensprobleme stoßen kann, kann u.U. eine weitere Delegation der Routingaufgabe nötig sein.

Bei der Delegation der Routingaufgabe handelt es sich vor allem um die Auslagerung einer Funktionalität bzw. – technisch präziser ausgedrückt – einer funktionalen Komponente, die ausschließlich innerhalb der Phase "Verhandlung und Inbetriebnahme" des Dienstlebenszyklus aktiv ist. Anders sieht die Situation mit dem Auslagern der Monitoring oder Reporting-Funktionalität aus, die während des gesamten Dienstlebenszyklus einer Dienstinstanz ausgeführt werden müssen. Das bedeutet, dass die für das Routing verantwortliche SP-Domäne bei der Durchführung ihrer Aufgabe Informationen über die "länger lebenden" Multi-Domain Managementfunktionen wissen muss.

Um die Delegation verschiedener Einzelaufgaben (und nicht nur der kompletten Funktionalität) zu ermöglichen, muss folgende Vorgabe erfüllt werden:

Vorgabe (Identifizierung) VI11 - Identifikation der Multi-Domain Funktionalität

Die Multi-Domain Managementfunktionalität, deren Delegation unterstützt werden soll, sowie deren Eigenschaften müssen global eindeutig identifizierbar sein.

Es sind auch Szenarien denkbar, bei denen mehr als eine Managementfunktionalität an i.A. unterschiedliche SP-Domänen delegiert werden kann. Dadurch können vielfältige Konstellationen von SP-Domänen entstehen, die die Teildienste einer Verbindung und/oder Multi-Domain Funktionen anbieten (vergleiche dazu die im Abschnitt 3.7.2 beschriebenen Anordnungsformen zwischen Manager-Objekten und Ressourcen). In der Abbildung 4.44 ist grob der Kommunikationsablauf dargestellt, bei dem die Domäne SP_A, die vom Kunden eine Verbindungsanfrage bekommt, die Routingfunktionalität an die Domäne SP_R und die Überwachungsfunktionalität an die Domäne SP_M delegiert. Wichtig ist, dass zunächst das Einverständnis von SP_M eingeholt wird. Die Kontaktinformationen dieser funktionalen Komponente werden später der Domäne SP_R mitgeteilt. Auch ist wichtig, dass bei der an die SP_M gerichteten Service-Anfrage die Kontaktinformationen aller zu überwachenden SP-Domänen mitgeteilt werden. Das geschieht aus dem Grund, dass bei der ersten Anfrage noch nicht bekannt ist, welche SP-Domänen sich bei der Diensterbringung beteiligen werden. Sollte die Monitoring-Instanz die Überwachungsinformationen einzelner SP-Domänen über Polling abholen, so sind dafür die Adressen der entsprechenden Schnittstellen erforderlich. Sollten die SP-Domänen die Überwachungsdaten (auch) durch einen Push-Mechanismus der Monitoring-Instanz mitteilen, dann kann anhand der Adressen der Kommunikationspartner entschieden werden, ob die Informationen akzeptiert oder als nicht vertrauenswürdig verworfen werden.

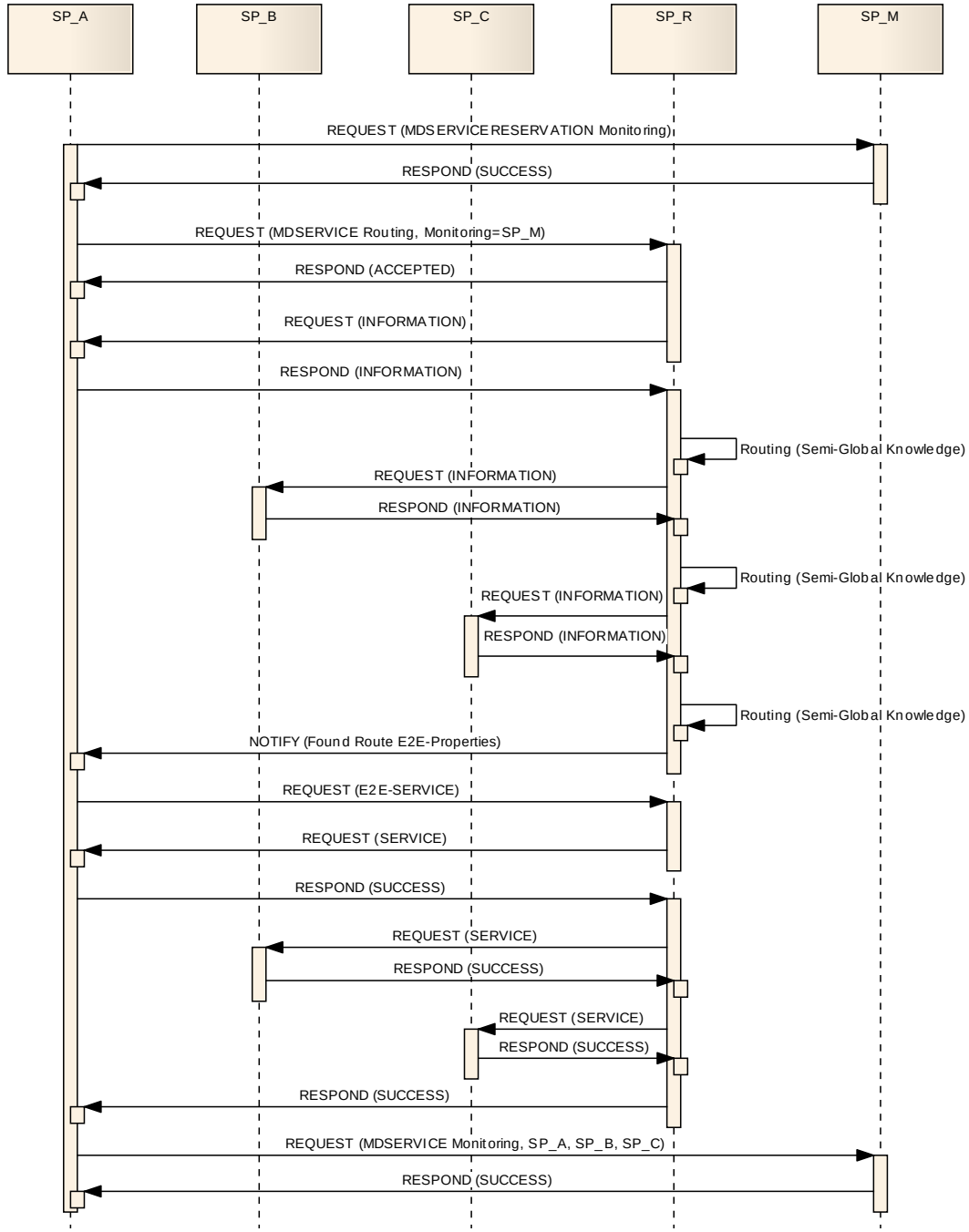


Abbildung 4.44.: Delegation von Monitoring und Routing (Vereinfacht)

Damit die Multi-Domain und die Single-Domain Managementfunktionalitäten miteinander verknüpft werden können, muss die Mitteilung der DSM-Kommunikationsadressen bereits bei den Kommunikationsartefakten vorgesehen werden:

Vorgabe (UML-Modellierung) VM09 - DSM für jede Managementfunktion

Es muss möglich sein, mit jeder Managementfunktionalität eine dafür zuständige DSM-Schnittstelle zu assoziieren.

4.5. SCP und DSM, Bezug zu UNI/NNI

In dieser Arbeit wurden bislang die Konzepte von SCP und DSM unabhängig von UNI/NNI diskutiert und weiterentwickelt (vgl. Abschnitt 3.2). Zur Erinnerung, UNI (*User Network Interface*) und NNI (*Network to Network Interface*) haben sich seit Jahren für die Bezeichnung der Schnittstellen im Netzbereich etabliert. Sie markieren gleichzeitig auch die *demarcation points* der Verantwortungsbereiche von Dienstnutzern bzw. der jeweiligen Service Provider.

	UNI/NNI	SCP
Grenze SP-Domäne	✓	✓
Grenze des Verantwortungsbereiches einer SP-Domäne	✓	✓
Grenze zwischen vollständiger und geteilter Verantwortung	✗	✓
Verbindungspunkte physischer Verbindungen	✓	✓
Verbindungspunkte logischer Verbindungen (VPNs, Trunks usw.)	✓	✓
Repräsentation vorhandener Ressourcen/Verbindungspunkte	✓	✓
Repräsentation potenziell mögliche Verbindungspunkte	✗	✓
Repräsentation eines einzelnen physischen Interfaces	✓	✓
Repräsentation mehrerer physischen Interfacen	✗	✓

✓ – Eigenschaft wird unterstützt

✗ – Eigenschaft wird nicht unterstützt

Tabelle 4.3.: Gegenüberstellung der Eigenschaften: UNI/NNI und SCP

Auf den ersten Blick kann es erscheinen, dass UNI/NNIs in sich beide Aspekte vereinen, für die die getrennten Begriffe SCP und DSM stehen. Bei der genaueren Betrachtung zeichnet sich jedoch eine Reihe von Unterschieden aus, die in den Tabellen 4.3 und 4.4 kurz zusammengefasst werden.

Da UNI/NNI eine Reihe der für SCP und DSM erforderlichen Eigenschaften nicht aufweisen, stellt sich die Frage, in welchen Fällen die entsprechende Erweiterung der UNI/NNI und in welchen die Entwicklung einer zu UNI/NNI parallelen und teilweise darauf aufbauenden Lösung sinnvoll ist. Diese Frage ist vor allem deswegen sehr wichtig, weil die nachträgliche Umstellung auf eine neue Infrastruktur sich als sehr schwierig und langwierig gestalten kann (vergleiche z.B. die Diskussion im Abschnitt 3.9 über Umstellung von IPv4 auf IPv6).

Die Antwort auf diese Frage hängt vor allem vom Umfang der Eigenschaften ab, die für einen Verketteten Dienst von der Providerkooperation unterstützt werden sollen. Sollen z.B. nicht nur bereits vorhandene sondern auch potentielle Dienste und Dienstver-

	UNI/NNI	DSM
Aushandlung verbindungsbezogener Eigenschaften (*Handshaking*)	✓	✗
Aushandlung Dienstgüteeigenschaften einer neuen Dienstinstanz	✗	✓
Aushandlung Managementaspekten einer neuen Dienstinstanz	✗	✓
Berücksichtigung technischer Aspekte	✓	✓
Berücksichtigung organisatorischer Aspekte (z.B. Zeitfenster für Wartung)	✗	✓
Kommunikation mit direkten Nachbarn-Domänen	✓	✓
Direkte Kommunikation mit indirekten Nachbarn	✗	✓
Berücksichtigung der Domain-Policies	✓	✓
Einschränken der Informationen entsprechend den Kundenanforderungen	✗	✓
Austausch von aggregierten Views (unterschiedliche Abstraktionsstufen)	✗	✓

✓ – Eigenschaft wird unterstützt

✗ – Eigenschaft wird nicht unterstützt

Tabelle 4.4.: Gegenüberstellung der Eigenschaften: UNI/NNI und DSM

bindungspunkte unterstützt werden, dann ist die "Zusammenlegung" von SCP/DSM mit UNI/NNI einfach nicht möglich (weil eine Kommunikation mit einer nicht existierenden Schnittstelle nicht möglich ist).

Die Erweiterung von UNI/NNI für die direkte Kommunikation mit nicht direkt angeschlossenen Domänen kann sich bei Diensten, die einen *in-band* Kommunikationskanal nutzen, auch als schwierig erweisen. In diesem Fall kann die Entwicklung einer parallelen Managementinfrastruktur als bevorzugte Lösung angesehen werden, es sei denn, dass ausschließlich QoS mit "einfachen" Aggregatfunktionen unterstützt werden und *Routing by Delegation* ausreicht (vergleiche entsprechende Diskussion im Abschnitt 4.7).

In allen übrigen Fällen stellt die Erweiterung von UNI/NNI mit der benötigten Funktionalität eine angestrebte Lösung dar. Der Grund dafür ist das Vermeiden von nicht-integrierten Lösungen, weil diese erfahrungsgemäß wesentlich anfälliger für Ausfälle sowie schwerer zu betreiben sind. Eine nicht-integrierte Lösung kann dennoch als ein Zwischenschritt zu der integrierten Lösung verwendet werden.

Zu Gunsten der Allgemeinheit der zu entwickelnden Lösung wird an dieser Stelle folgende Entscheidung für die Modellierung getroffen:

Vorgabe (UML-Modellierung) VM10 - Modellierung von SCP und DSM

Bei der Beschreibung der Kommunikationsartefakte müssen DSM-Schnittstellen unabhängig von SCPs beschrieben werden.

4.6. Kommunikationsartefakte und IDs

In den Abschnitten 4.1 bis 4.5 wurde bei der Diskussion unterschiedlicher Routing-Aspekte eine Reihe Vorgaben definiert, denen in diesem Abschnitt durch die Modellierung der Kommunikationsartefakte und durch die Definition von Vorgaben zur Identifizierung einzelner Objekte und Eigenschaften entsprochen werden sollen.

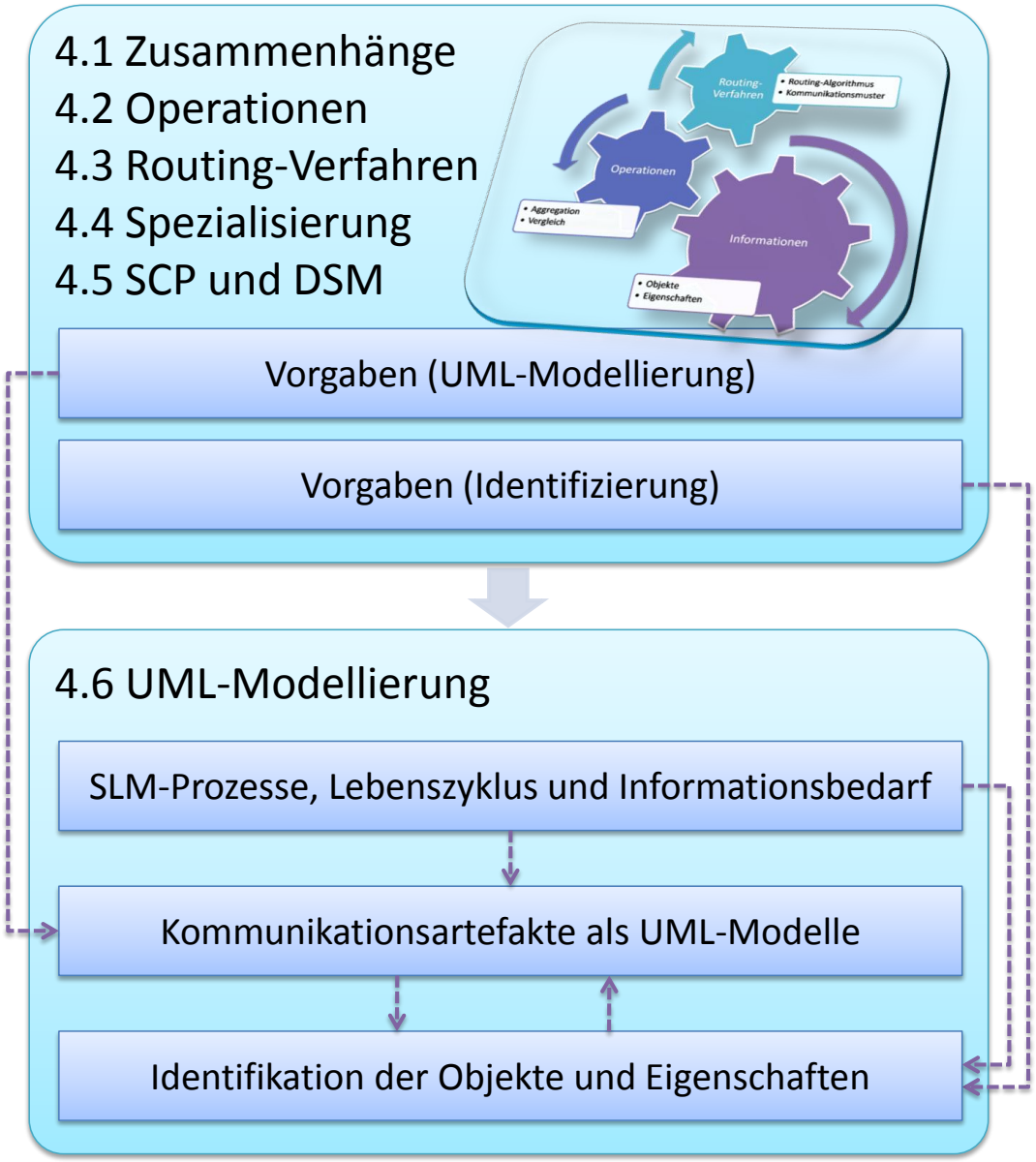


Abbildung 4.45.: Aufbau dieses Abschnittes

Da beim Routing auch die Service-Level-Management-Aspekte berücksichtigt werden sollen, werden in diesem Abschnitt zunächst die SLM-spezifischen Anforderungen in unterschiedlichen Dienstinstanz-Lebenszyklusphasen besprochen. Diese Diskussion liefert einen abschließenden Input für die endgültige Modellierung.

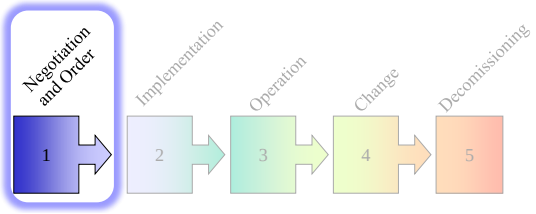
Erst danach werden in Abschnitten 4.6.2 bis 4.6.9 die Kommunikationsartefakte definiert. Anschließend wird im Abschnitt 4.6.10 definiert, welche Identifizierungsmöglichkeiten für die unterschiedlichen Objekte und Eigenschaften verwendet werden sollen.

Der Aufbau des Abschnittes ist graphisch in Abbildung 4.45 dargestellt. Die Abhängigkeiten zwischen unterschiedlichen Teilen dieses Abschnittes sowie der Bezug zu vorherigen Abschnitten sind in dem Bild durch gestrichelte Pfeile angedeutet.

4.6.1. SLM-Prozesse, Lebenszyklusphasen und Informationen

Die Diskussion über spezielle Anforderungen bzgl. der Informationsmodellierung einzelner Multi-Domain SLM-Prozesse wird anhand der Phasen des Dienstinstanz-Lebenszyklus strukturiert. Für eine detaillierte Beschreibung des Kommunikationsprotokolls und der SLM-Prozesse für Verkettete Dienste siehe entsprechend die Kapitel 5 und 6.

4.6.1.1. Lebenszyklusphase: Verhandlung und Dienstanfrage



In der ersten Phase des Dienstlebenszyklus geht es zunächst darum, dass ein Pfad gefunden werden soll, der die E2E-Kundenanforderungen erfüllt. Die qualitativen und die quantitativen QoS-Parameter sowie die Managementfunktionalität sind dabei zu berücksichtigen. Dabei müssen sowohl zeitliche Aspekte für die erwünschte Dienstinstanz als auch der Unsicherheitsfaktor berücksichtigt werden (vergleiche entsprechende Diskussion im Abschnitt 4.1). Der Unsicherheitsfaktor bestimmt, ob die Dienstinstanzen ausschließlich auf der bereits vorhandenen Infrastruktur realisiert werden können oder zumindest teilweise auf eine geplante Infrastruktur angewiesen sind.

Einschränkung auf relevante Informationen

Entsprechend der Definition im Abschnitt 4.1.4 setzt sich die Multi-Domain Sicht auf die verfügbaren Teildienste aus den Teilsichten einzelner SP-Domänen zusammen. Die Einschränkung auf relevante Informationen ist aus mehreren Gründen wichtig: Aus Sicht der SP-Domäne, die das Routing durchführen soll, ist es normalerweise irrelevant, welche Dienste eine andere SP-Domäne erbringen kann. Dazu kann und wird in meisten Fällen auch die vollständige Information über die freie Kapazitäten von einer SP-Domäne als sensitiv betrachtet, weswegen allgemeine Anfragen allein an Policies scheitern werden. Stattdessen ist nur eine Reihe von Diensten interessant, die als Teildienste eines E2E kundenorientierten Verketteten Dienstes fungieren können. Diese Dienste müssen mindestens den E2E-Anforderungen genügen, um bei der Pfadsuche überhaupt betrachtet zu werden. Das entsprechende UML-Diagramm wird im Unterabschnitt 4.6.4 definiert.

Spezifikation der möglichen Teildienste

Im Gegensatz zu den MOs kann eine SP-Domäne selbst entscheiden, welche Dienste sie erbringt. Weiterhin kann eine SP-Domäne aufgrund ihrer internen Policies eine Anfrage für einen technisch unterstützten Dienst einfach zurückweisen, weil z.B. die Vertrauensbeziehung zu der nach Informationen gefragten SP-Domäne nicht gegeben bzw. zu niedrig ist. Falls die SP-Domäne die Anfrage akzeptiert, sendet sie die benötigten Informationen zurück. Jede SP-Domäne darf dabei selbst entscheiden, welchen Umfang die mitgeteilten Informationen haben – ob alle oder nur ein Teil der technisch

möglichen Teildienste bekannt gegeben wird. Die Struktur dieser Informationen wird im Unterabschnitt 4.6.5 festgelegt.

Bei automatisierten Diensten kann dieses Anfrage-Antwort-Zusammenspiel relativ zeitnah geschehen. Solange die Anfrage sich auf die vorhandene Infrastruktur bezieht, kann das relativ leicht realisiert und mit den existierenden Managementtools einer SP-Domäne gekoppelt werden. Anfragen, die sich auch auf nur potentiell mögliche Infrastrukturen beziehen, erfordern normalerweise einen manuellen Eingriff und sind daher zeitaufwendig. Eine Abhilfe kann hier ein Vorgehen wie bei der Anfrage für ein Angebot schaffen (vergleiche Abschnitt 3.5). Außer den bereits besprochenen Randbedingungen muss die Anfrage eine Zeiteinschränkung für das Vorlegen des Angebotes beinhalten. Wird innerhalb dieser Frist kein Angebot vorgelegt, gilt die Anfrage als verfallen.

Damit ein Kommunikationskanal zur Vorlage des Angebots überhaupt aufgebaut werden kann, muss auch die "Rückadresse" (DSM-Schnittstelle) spezifiziert werden. Jede Anfrage ist mit einer eindeutigen[6] ID zu versehen. Mit der Hilfe dieser ID ist es möglich, den Bezug zwischen dem später übermittelten Angebot und der ursprünglichen Anfrage herzustellen. Da ein Angebot aus der Sicht des Service Providers aus finanziellen Gründen nicht beliebig lang aufrecht erhalten werden kann, wird es mit einem Ablaufdatum versehen.

Eigenschaften bei Dienstinstanz-Reservierung oder -Bestellung

Erst nachdem die Informationen über die realisierbaren Dienstinstanzen und deren mögliche Eigenschaftenausprägungen vorliegen, kann die Suche eines zufriedenstellenden Pfades (das eigentliche Routing) durchgeführt werden. Die einzelnen Teildienste des gefundenen Pfades werden zunächst reserviert und dann bestellt (siehe Abschnitt 3.2). Die einzelnen Teildienste können auf unterschiedliche Art und Weise spezifiziert werden. Bei einer Verbindung zwischen zwei SCPs genügt es, zwei Grenzpunkte zusammen mit anderen für diese Dienstinstanz erforderlichen QoS-Parametern und deren erwünschten Werten zu spezifizieren. Besteht zwischen zwei SCPs mehr als eine zufriedenstellende Verbindungsmöglichkeit (mehrere *Component Links*), so kann einer der *Component Links* referenziert werden, was der SP-Domäne eine Abbildung auf die notwendige Infrastruktur erleichtert. Wurde ein Angebot für die Verbindung zwischen zwei SCPs angefordert, so kann das vorgelegte Angebot referenziert werden.

Neben der Spezifikation der topologischen Eigenschaften, die grundsätzlich auf ID-Basis geschehen kann, sollen auch die erforderlichen Eigenschaften exakt beschrieben werden. Die Struktur der letzteren wird im Unterabschnitt 4.6.6 beschrieben

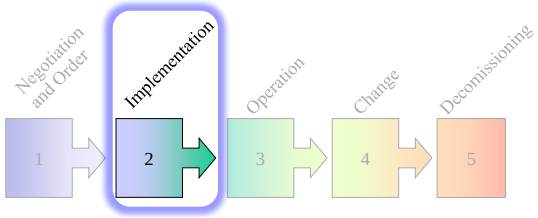
Zugesicherten Eigenschaften

Wenn die Realisierung der angeforderten Dienstinstanz sowohl technisch möglich als auch aus Domain-internen Gründen akzeptabel ist, erfolgt eine Bestätigung. Damit die Kommunikation bzgl. der bestellten Dienstinstanz (z.B. aus Load Balancing Gründen) auch über einen anderen Kommunikationskanal abgewickelt werden kann, kann die

[6] Eindeutigkeit bezieht sich in diesem Fall auf die Requesting Service Domäne und auf das Zeitfenster zwischen Anfrage und der Angebotfrist.

Antwort auch mit der entsprechenden DSM-Adresse versehen werden. Weiterhin sollen dabei die Dienstgüteeigenschaften mitgeteilt werden, die tatsächlich für die reservierte bzw. bestellte Dienstinstanz garantiert werden. Die Definition des entsprechenden Kommunikationsartefaktes wird im Abschnitt 4.6.7 durchgeführt.

4.6.1.2. Lebenszyklusphase: Inbetriebnahme

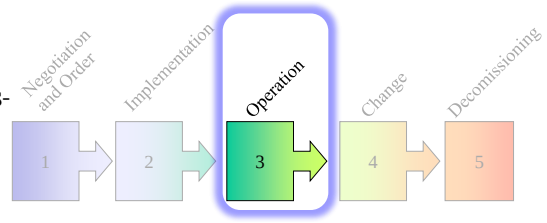


Während bei einigen Diensten, wie z.B. PSTN, die Inbetriebnahme einer Dienstinstanz innerhalb einer Domäne automatisch und zeitnah mit der Anfrage realisierbar ist, sind bei manchen anderen Diensten manuelle Eingriffe bei der Schaltung erforderlich, so z.B. bei E2E Links von Géant2. Es wird daher die Möglichkeit benötigt, den Zustand jeder Teilstrecke einer Dienstinstanz bei der die Teilstrecke erbringenden SP-Domäne abzufragen. Eine Alternative dazu ist eine automatische Benachrichtigung, die die Service Providing SP-Domäne bei der Zustandsveränderung abschicken kann. Im Idealfall signalisiert diese Benachrichtigung, dass die entsprechende Teilstrecke der E2E-Dienstinstanz in Betrieb genommen wurde. Es kann aber auch zu unerwarteten Verzögerungen bei der Inbetriebnahme kommen. Insbesondere kann das Dienstinstanzen betreffen, die auf z.T. während der Bestellung noch nicht vorhandener bzw. noch nicht installierter Infrastruktur realisiert werden. Solche Ereignisse sollten automatisch gemeldet werden.

Bei einer automatischen Benachrichtigung entsteht die Notwendigkeit, die betroffene Dienstinstanz zu identifizieren. Der Grund dafür liegt darin, dass bei Verketteten Diensten i.A. mehrere Service Provider sich an der Erbringung einer Dienstinstanz beteiligen. Während bei einem Anfrage-Antwort Kommunikationsmuster aus demselben Grund die relevante Dienstinstanz bereits bei der Anfrage spezifiziert werden muss, ist die explizite Angabe der Dienstinstanz-ID bei der Antwort nicht erforderlich, solange die Anfrage und die Zugehörige Antwort in Verbindung miteinander gebracht werden können.

In all diesen Fällen sind keine komplexen Datenstrukturen notwendig. Es genügen IDs für die unterstützten Ereignisse. Die Definition des Kommunikationsprotokolls für die automatische Benachrichtigung befindet sich im Abschnitt 5.2.

4.6.1.3. Lebenszyklusphase: Betrieb

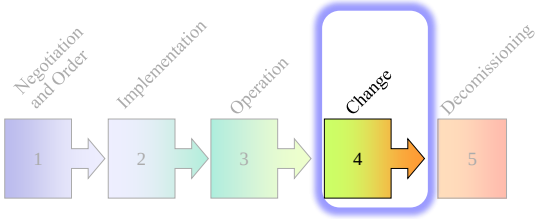


Eine ähnliche Situation gibt es auch im Betrieb, allerdings sind statt des Zustandes der Inbetriebnahme die aktuellen Messwerte der vereinbarten QoS-Parameter interessant. Diese können wiederum entweder durch eine explizite Anfrage (Pull), oder – falls vereinbart – durch eine reguläre Benachrichtigung (Push) zur Verfügung gestellt werden (vergleiche auch Tabelle 2.5 in Abschnitt 2.4.1).

Neben der Identifizierung der Dienstinstanz muss auch die Beschreibung der Messwerte spezifiziert werden. Die Modellierung dieses Kommunikationsartefakts wird im Abschnitt 4.6.9 durchgeführt. Für die Beschreibung des Monitoring-Prozesses siehe Abschnitte 6.6 und 6.7.

Auch im Betrieb kann eine Reihe von Ereignissen auftreten. Relevant sind vor allem Ereignisse, die z.B. zu einer Verletzung der vereinbarten Grenzwerte führen. Da solche Ereignisse asynchron auftreten, können sie zeitnah ausschließlich über den Benachrichtigungsmechanismus gemeldet werden. Die Adresse(n) für solche Benachrichtigungen werden bei der Bestellung einer Dienstinstanz spezifiziert (vgl. Abschnitt 4.6.6). Bei einer solchen Benachrichtigung wird ggf. neben der Dienstinstanz-ID auch eine Ereignis-ID und/oder der aktuelle Monitoring-Zustand mitgeteilt. Der entsprechende Protokollaufruf wird im Abschnitt 5.12 definiert.

4.6.1.4. Lebenszyklusphase: Anpassung



Während des Betriebes kann auch die Notwendigkeit auftreten, die Eigenschaften der Dienstinstanz, wie z.B. die vereinbarten QoS-Grenzwerte, zu verändern. Das kann vor allem dann auftreten, wenn der Kunde seine Anforderungen ändert bzw. ändern möchte.

Es kann aber auch weniger offensichtliche Ursachen dafür geben. Zum Beispiel kann es sein, dass eine der bei der Erbringung eines Verketteten Dienstes beteiligten Domänen einen vereinbarten Parameter aus diversen Gründen nicht einhalten kann. Um das auszugleichen und dem Endkunden weiterhin die vereinbarte E2E-Dienstgüte liefern zu können, können die entsprechenden Parameter bei den anderen beteiligten SP-Domänen angepasst werden.

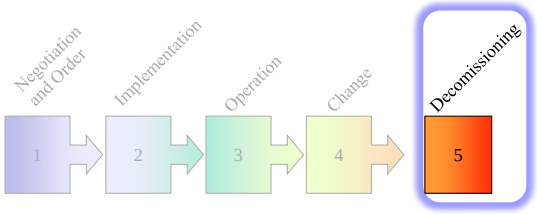
Eine weitere wenig offensichtliche Veränderung stellt die Veränderung der Benachrichtigungsadressen dar. Das kann z.B. zum Erreichen eines besseren Load Balancing nützlich sein.

Die Spezifikation der neuen erforderlichen Eigenschaften ist identisch mit der bei der Bestellung einer neuen Dienstinstanz. Die notwendigen Kommunikationsartefakte können somit entsprechend dem UML-Diagramm aus Abschnitt 4.6.6 beschrieben werden. Die bei einer CHANGE-Anfrage erforderliche Bestätigung der zugesicherten Eigenschaften ist identisch mit dem Fall einer Neubestellung. Die entsprechenden Kommunikationsartefakte können somit wiederum entsprechend dem UML-Diagramm aus dem Abschnitt 4.6.7 beschrieben werden.

Der einzige Unterschied zwischen der Bestellung einer neuen Dienstinstanz und der Veränderung der erforderlichen Eigenschaften bei einer existierenden besteht darin, dass die Angaben sich auf existierende Teildienste bezieht. Dadurch wird es erforderlich, dass jeder bestellte Teildienst bei der Bestätigung mit einer – für die entsprechende SP-Domäne – eindeutigen ID versehen wird (vgl. Abschnitt 4.6.7).

Für die Definition des entsprechenden Protokollaufrufs und des darauf aufbauenden SLM-Prozesses siehe Abschnitte 5.9 und 6.8.

4.6.1.5. Lebenszyklusphase: Dienstauflösung



Für den Abbau einer Dienstinstanz kann es unterschiedliche Gründe geben. Es kann sich z.B. um eine Dienstinstanzen handeln, die nur für eine begrenzte Zeitperiode bestellt wurden. In so einem Fall kann z.B. eine Benachrichtigung über die bevorstehende Beendigung der Dienstinstanz sinnvoll sein. Als Reaktion darauf kann eine Anfrage für die Verlängerung des Dienstes erfolgen. Ein weiterer Grund für solche Benachrichtigung kann sein, dass die SP-Domäne aus diversen internen Gründen (z.B. Infrastrukturausfall oder geplante Wartungsarbeiten) die Dienstinstanz außer Betrieb gestellt hat bzw. in Kürze auflösen wird. Bei so einer Benachrichtigung muss ausschließlich die Dienstinstanz referenziert werden, die in Kürze aufgelöst wird. Die übrigen Angaben wie z.B. Zeit der bevorstehenden Auflösung sind dienstspezifisch und können daher als optional betrachtet werden.

Eine geordnete Möglichkeit, eine Dienstinstanz aufzulösen, besteht in einer entsprechenden Anfrage der SP-Domäne, die die Teildienst(e) ursprünglich angefordert hat. Die Gründe dafür können sowohl Domain-intern als auch eine entsprechende Anfrage vom Endkunden sein. Ob eine solche Anfrage zurückgewiesen werden darf und welche Folgen das hat, hängt einzig und allein von den Kooperationsvereinbarungen

zwischen den beteiligten SP-Domänen ab. Auch in diesem Fall ist ausschließlich die Referenz auf den/die Teildienst(e) erforderlich.

Der entsprechenden Protokollaufruf und der darauf aufbauende SLM-Prozess werden in den Abschnitten 5.14 und 6.9 definiert.

4.6.2. UML-Modell: Properties (Teilmodell)

Gleichzeitig mehrere Eigenschaften

Im Abschnitt 4.1 wurde eine ausführliche Diskussion über die Zusammenhänge zwischen Objekten und deren Eigenschaften geführt. Aus der Sicht der Modellierung besteht eine der wichtigsten Erkenntnisse aus dieser Diskussion darin, dass jeder Verbindungsmöglichkeit (oder genauer gesagt jeder *Component Link*) aus Sicht des Service Providers eine beliebige Anzahl von unterstützten Eigenschaften aufweisen kann. Auf der anderen Seite – diesmal aus der Kundensicht – sind nicht alle diese unterstützten Eigenschaften relevant. Der Kunde kann seinerseits auch beliebig viele Eigenschaften als für ihn relevant angeben und deren erforderlichen Grenzwerte spezifizieren.

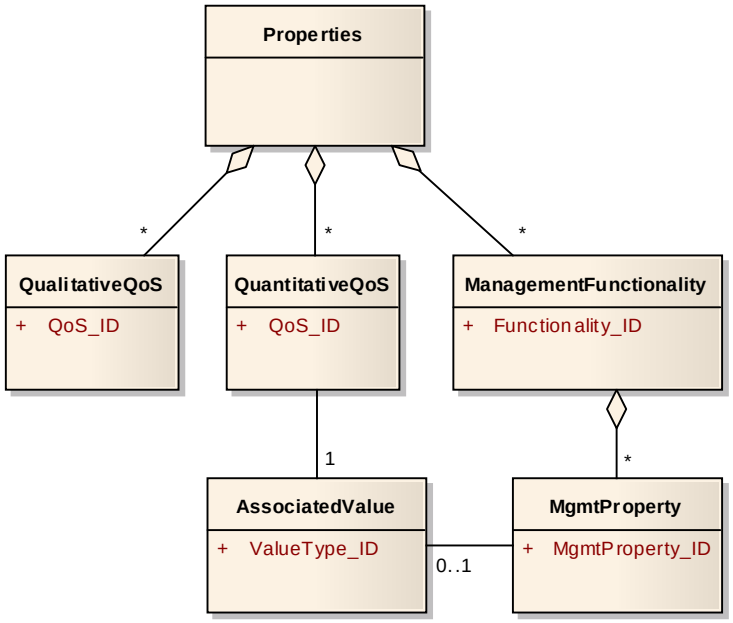


Abbildung 4.46.: Modellierung der Diensteigenschaften

Eigenschaften-Bestandteile

Unter den Eigenschaften eines (Teil-)Dienstes werden in dieser Arbeit sowohl die Dienstgüteeigenschaften (QoS-Parameter) als auch die Managementfunktionalität verstanden. Die QoS-Parameter werden in *qualitative* und *quantitative* unterteilt. Da diese Eigenschaften-Zusammensetzung generell für alle Kommunikationsartefakte gilt, wird das entsprechende Teilmodell in diesem Unterabschnitt definiert und ausführlich beschrieben. Auf die Wiederholung dieser Beschreibung wird bei der Modellierung der tatsächlichen Kommunikationsartefakte verzichtet. Die folgende Beschreibung bezieht sich auf das UML-Modell in Abbildung 4.46.

Qualitative QoS-Parameter

Die qualitativen QoS-Parameter kann man auch als eine Klasse boolescher Parameter bezeichnen. Als Beispiele dazu können "Nummerweiterleitung unterstützt" oder "EU-Richtlinie XY eingehalten" dienen. Bei der Beschreibung eines qualitativen QoS-Parameters reicht somit ein Objekt, das einzig und allein die eindeutige ID dieses

Parameters beinhaltet. Um sowohl eine beliebige Anzahl als auch eine beliebige Kombination gleichzeitig unterstützter qualitativer QoS-Parameter spezifizieren zu können, wird die Klasse QUALITATIVEQOS im UML-Diagramm mit einer "1:n"-Multiplizität versehen.

Quantitative QoS-Parameter

Ein ähnliches Vorgehen kann auch bei den quantitativen QoS-Parametern angewendet werden. Im Gegensatz zu den qualitativen QoS-Parametern müssen bei den QoS-Parametern auch die erlaubten/möglichen Zustände spezifiziert werden. Zu diesem Zweck wird im UML-Diagramm mit der Klasse für quantitative QoS-Parameter die Klasse ASSOCIATEDVALUE assoziiert. Bezogen auf das Beispielnetz aus der Abbildung 4.7 im Abschnitt 4.1.2 würde das bedeuten, dass beide *Component Links* jeweils zwei quantitative QoS-Parameter haben; Delay kann jeweils nur einen festen Wert aufweisen, der Wertebereich der Übertragungsrate kann entweder einfach als eine Liste mit erlaubten Werten oder als eine obere Schranke zusammen mit der Granularität eingegeben werden. Um unterschiedliche Beschreibungen der Wertebereiche zu unterstützen, wird die Klasse ASSOCIATEDVALUE mit der entsprechenden ID für die Beschreibungsart versehen. Anhand dieser ID kann entschieden werden, welche der unterstützten Beschreibungsarten im jeweiligen konkreten Fall zum Einsatz kommt. Durch die Verknüpfung zwischen den Klassen anhand der ID von ASSOCIATEDVALUE ist es möglich, die Erweiterung durch die anderen Strukturierungsmöglichkeiten leicht zu realisieren.

Wie die Klasse ASSOCIATEDVALUE mit den unterschiedlichen Definitionen der Wertebereiche – in Abhängigkeit von VALUESTYPE_ID – assoziiert werden kann, wird im Abschnitt 4.6.3 beschrieben.

Managementfunktionalität

Bei der Managementfunktionalität sieht die Situation um einiges komplizierter aus. Das liegt zu einem daran, dass viele der im Service-Level-Management definierten Aufgaben unterschiedlich strukturiert sind, und zum anderem müssen SLM-Prozesse auch mit anderen Managementprozessen "verknüpft" werden (vergleiche entsprechende Diskussion im Abschnitt 3.4). Bei Verbindung mit anderen Managementprozessen sind globale Multi-Domain und nicht domäneninterne Prozesse gemeint. Bei der Beschreibung der Managementfunktionalität geht es zunächst nicht um die exakten Kommunikationsadressen oder ähnliches, sondern ausschließlich um die Beschreibung der relevanten Funktionalität (vergleiche Diskussion über MIB im Abschnitt 3.7).

Jede Managementfunktionalität kann i.A. mit einer Reihe von funktionsspezifischen Konfigurationsparametern assoziiert werden, die ihrerseits unterschiedliche Werte annehmen können. Beispielsweise kann die Monitoring-Funktionalität der zugrundeliegenden Infrastruktur entweder mit Polling oder basierend auf Traps durchgeführt werden (vergleiche Zusammenfassung in der Tabelle 2.5). Während für Traps – ähnlich wie bei den qualitativen QoS-Parameter – keine weiteren Angaben benötigt werden, ist bei Polling auch sein Intervall wichtig, das analog zur Beschreibung der Wertebereiche quantitativer QoS-Parameter spezifiziert werden kann. Gleichzeitig mit der Überwachungsart kann mit dem Monitoring auch die Benachrichtigungsart assoziiert

werden, wie diese Informationen der daran interessierten Partei zur Verfügung gestellt werden können: durch die automatische Benachrichtigung (*Push*) oder durch explizites Anfragen (*Pull*). Zur Abdeckung der beschriebenen Situationen wird in der Abbildung 4.46 mit der Klasse MANAGEMENTFUNKTIONALITY die Klasse MGMTPROPERTY für jeweils einzelne funktionalitätsspezifische Eigenschaften assoziiert, die wiederum mit ASSOCIATEDVALUE verbunden werden kann, wodurch auch die Beschreibung der sog. "quantitativen Managementparameter", wie z.B. Polling-Intervall, ermöglicht wird.

Objekte, Eigenschaften und IDs

Abschließend soll hier noch folgendes extra betont werden. Durch die Strukturierung der Eigenschaftenbeschreibung anhand einer beliebig großen Menge gleichartiger Objekte einer der drei Kategorien (gemeint sind qualitative und quantitative QoS-Parameter sowie Managementfunktionalität samt den darauf bezogenen Konfigurationsparametern) wird es ermöglicht, alle notwendigen Operationen auf diesen Datenstrukturen zu definieren und die einzelnen Eigenschaften anhand ihrer IDs zu unterscheiden. Für die Definition der Operationen siehe Abschnitt 4.2. Der Einsatz von IDs ermöglicht es weiterhin, auch neue QoS-Parameter zu definieren und zu unterstützen, ohne dass die Struktur der Beschreibung verändern werden muss. Die Diskussion über die Identifizierung unterstützter Eigenschaften wird im Abschnitt 4.6.10 geführt.

4.6.3. UML-Modell: AssociatedValue (Teilmodell)

Generellen Festlegungen

Die Klasse ASSOCIATEDVALUE wird in allen hier zu modellierenden Kommunikationsartefakten gebraucht, um Werte bzw. Wertebereiche mit unterschiedlichen Eigenschaften zu assoziieren. Um die Wertebeschreibung sowohl möglichst flexibel als auch erweiterbar zu gestalten, wird auch hier der Gebrauch von den IDs gemacht. So wird anhand VALUETYPE_ID unterschieden, welche der von ASSOCIATEDVALUE abgeleiteten Klassen verwendet wird (siehe Abbildung 4.47).

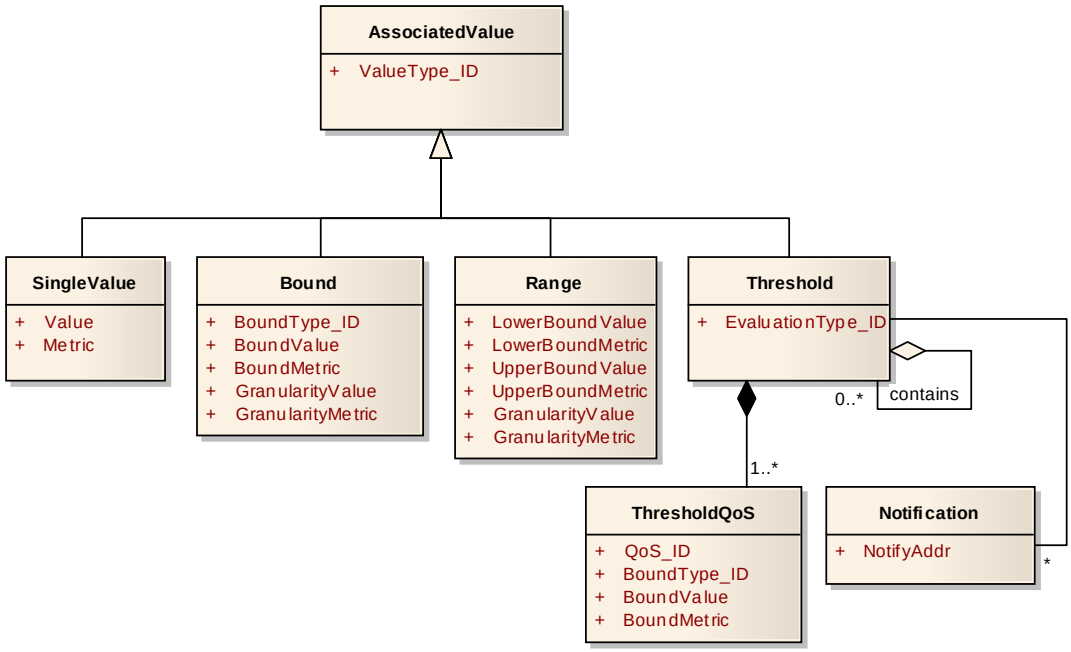


Abbildung 4.47.: Assoziationen der AllowedValues Klasse

Spezifikation der Werte für QoS-Parameter

Neben den selbsterklärenden Klassen SINGLEVALUE und RANGE wird in der Klasse BOUND eine ID benötigt, die bestimmt, ob es sich bei den Werten um einen *Upper-* oder *Lower-Bound* handelt. Jeden Wert extra mit der *Metric* zu versehen ist notwendig, um die Fälle wie aus dem Beispielnetz mit 2Gbps Obergrenze und 100Mbps Granularität abdecken zu können. Die Klasse kann z.B. bei der Bestellung einer Dienstinstanz oder bei der Mitteilung des Monitoring-Zustandes verwendet werden. Die Klassen RANGE und BOUND können dagegen bei den Informationsabfragen bzw. bei den Mitteilungen der realisierbaren Eigenschaften Verwendung finden.

Spezifikation der Werte für Managementfunktionalität

Die Klasse THRESHOLD dagegen wird hier aufgelistet, um die Spezifikation der Parameter für Managementfunktionalität zu illustrieren. So kann es in Abhängigkeit von den Anforderungen an die Überwachung des (Teil-)Dienstes erwünscht sein, eine Benachrichtigung bei einer drohenden SLA-Verletzung zu senden. Üblicherweise werden dafür ein oder mehrere Schwellwerte innerhalb der vereinbarten QoS-Wertebereiche festgelegt (siehe Klasse THRESHOLDQOS). Die Variable EVALUATIONTYPE_ID in der Klasse

THRESHOLD erlaubt es, zusammengesetzte Bedingungen für die Benachrichtigung zu definieren, wenn die Einhaltung von mehreren QoS-Werten überwacht werden soll. Denkbar wären dafür logischen AND- und OR-Verknüpfungen aller in THRESHOLDQOS spezifizierten Schwellwerte. Durch die Aggregation "contains" der Klasse THRESHOLD ist auch der Aufbau von verschachtelten Ereignisdefinitionen möglich, wie z.B. der folgende logische Ausdruck: $(Threshold\_QoS_A \wedge Threshold\_QoS_B) \vee Threshold\_QoS_C$. Durch die Multiplizität der Assoziation-Beziehung zu der Klasse NOTIFICATION wird es auch möglich, für die so definierten zusammengesetzten Schwellwerte auch eine Reihe von Benachrichtigungsadressen zu spezifizieren.

Erweiterbarkeit

Obwohl für viele Fälle die hier aufgelisteten vier Klassen zur Wertebeschreibung genügen werden, kann diese Liste bei weitem nicht als vollständig bezeichnet werden. Stattdessen soll die Beschreibung in diesem Unterabschnitt als eine Vorlage dienen, wie die – in Abhängigkeit von dem Dienst und zu unterstützenden Diensteigenschaften – wirklich benötigten Wertebeschreibungen definiert werden können. Zwischen den einzelnen Wertebeschreibungsarten wird weiterhin anhand VALUETYPE_ID realisiert, wodurch auch die notwendige Erweiterbarkeit garantiert wird. Für für Diskussion darüber, wie diese sowie andere IDs definiert werden sollen, siehe Abschnitt 4.6.10.

4.6.4. UML-Modell: ConstraintTopology und ConstraintProperties

Generell können Einschränkungen der Informationen, wie sie in dieser Arbeit benötigt werden, in zwei Klassen aufgeteilt werden (siehe Abbildung 4.48). Die Klasse CONSTRAINTS baut auf einer optionalen Klasse CONSTRAINTTOPOLOGY und einer obligatorischen Klasse CONSTRAINTPROPERTIES auf. Während die Klasse CONSTRAINTTOPOLOGY ausschließlich bei Verbindungsdiensten genutzt werden kann (siehe insbesondere Diskussion im Abschnitt 4.3.2), kann die Klasse CONSTRAINTPROPERTIES zudem auch bei Informationsabfragen bzgl. Multi-Domain Managementfunktionalität verwendet werden (siehe zusätzlich die Diskussion im Abschnitt 4.4).

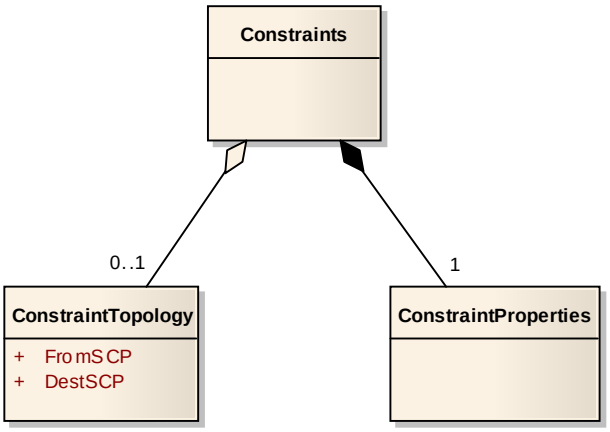


Abbildung 4.48.: Randbedingungen auf Diensteigenschaften

Die Klasse CONSTRAINTTOPOLOGY ist sehr einfach aufgebaut und entspricht direkt der Vorgabe VM07, einen Ausgangs-SCP und einen Ziel-SCP bei der Pfadsuche angeben zu können.

Die Klasse CONSTRAINTPROPERTIES wird verwendet, um die Eigenschaften einzuschränken, die alle Teilstrecken "auf dem Weg zum Ziel" erfüllen sollen (vergleiche auch entsprechende Diskussion im Abschnitt 4.6.1). Die in Abbildung 4.49 dargestellte Klasse CONSTRAINTPROPERTIES lässt sich fast direkt von der Beschreibung der Diensteigenschaften ableiten (vergleiche UML-Diagramme in Abbildungen 4.46). Beim Verzicht auf die Verwendung der Klassen QUALITATIVEQOS und QUANTITATIVEQOS lässt sich diese Klasse, wie bereits angedeutet, zur Einschränkung der erforderlichen Multi-Domain Funktionen und deren Eigenschaften verwenden.

Verglichen mit der Klasse PROPERTIES weist CONSTRAINTPROPERTIES lediglich drei Erweiterungen auf: zwei zusätzliche IDs zur Spezifikation des relevanten Dienstes und des akzeptablen Unsicherheitsfaktors sowie eine assoziierte Klasse TIMEPERIOD, die die erwünschte Dienstinstanz-Laufzeit beschreibt. Für die ausführlichere Diskussion über den Zweck dieser Erweiterungen siehe Abschnitt 4.1.5.

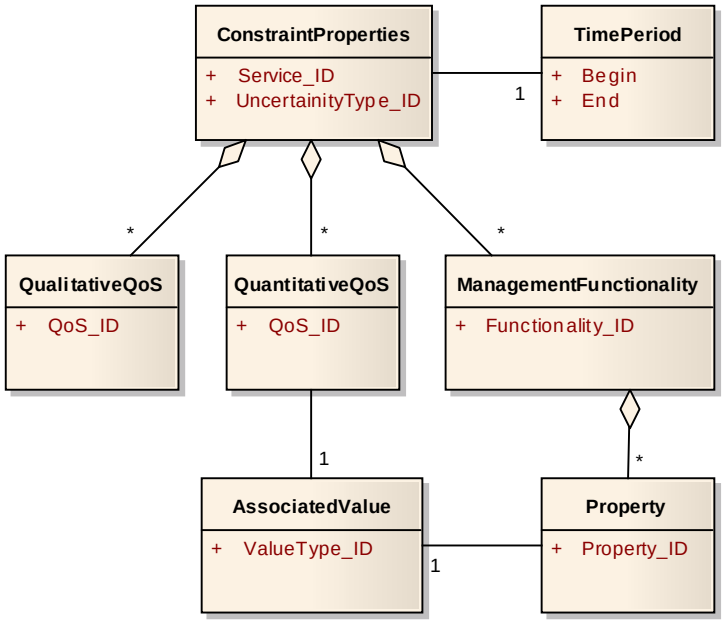


Abbildung 4.49.: Randbedingungen auf Diensteigenschaften

Für die Verwendung dieser Klassen bei der Kommunikation zwischen SP-Domänen siehe Abschnitte 5.2 und 5.3.

4.6.5. UML-Modell: Available Connections/Services

Wie eine Antwort auf eine Informationsanfrage strukturiert werden soll, ist in Abbildung 4.50 dargestellt. Zur Beschreibung der Topologie der Verbindungsdienste werden die Klassen SCP, COMPOUNDLINK, COMPONENTLINK und COMPONENTLINKPART benötigt. Für die Bedeutung der Zusammenhänge zwischen diesen Klassen wird auf die ausführliche Diskussion im Abschnitt 4.1 verwiesen. An dieser Stelle sollen nur noch einige kritische Aspekte extra betont werden. So sind die Klassen SCP und COMPONENTLINK mit der Klasse DOMAIN assoziiert, zu der der *SCP* gehört bzw. die von dem *Compound Link* verbunden werden. Durch die Variable DSM_ADDR in der Klasse DOMAIN wird gewährleistet, dass die DSM-Adressen der zuvor unbekannten SP-Domäne bei Informationsabfragen in Erfahrung gebracht werden. Ein anderer interessanter Aspekt bezieht sich auf die Variable COMPONENTLINKTYPE_ID der Klasse COMPONENTLINK. Durch diese Variable wird zwischen *Domain Links*, *Interdomain Links* und den Teilsichten auf ein und dasselbe *Interdomain Link* unterschieden. Nur im letzteren Fall – der laut Festlegung im Abschnitt 4.1.3 ausschließlich zwischen den benachbarten SP-Domänen auftreten darf – wird auch die Klasse COMPONENTLINKPART gebraucht. Weiterhin setzen sich in diesem Fall auch die Eigenschaften des kompletten *Interdomain Links* aus den zwei Teilsichten darauf zusammen (siehe Assoziation "define" bei LINKPROPERTIES).

Die Beschreibung der mit einem COMPONENTLINK assoziierten Eigenschaften entspricht dem Muster, wie es im Abschnitt 4.6.2 definiert und bei der Eigenschafteneinschränkung im Abschnitt 4.6.4 verwendet wurde. Die UNCERTAINTYTYPE_ID wird benötigt, da unterschiedliche Teildienste einen unterschiedlichen Unsicherheitsfaktor aufweisen können. Dadurch wird dem *Routing-Verantwortlichen* die Möglichkeit gelassen, auch nachträglich eine "sicherere" Route auswählen und beantragen zu können.

Eine weitere Besonderheit des UML-Diagramms in Abbildung 4.50 besteht in der Klasse MULTIDOMAINMANAGEMENTFUNCTIONALITY, die von der Klasse MANAGEMENTFUNCTIONALITY abgeleitet ist. Diese Klasse dient zur Beschreibung der Multi-Domain Managementfunktionalitäten, wie z.B. Multi-Domain Monitoring. Anhand der FUNCTIONALITY_ID können sie von den Managementfunktionalitäten einzelner Teildienste unterschieden werden. Ansonsten werden auch für die Verbindungsdienste typische Eigenschaften der Managementfunktionalität (Klasse PROPERTY) sowie deren Wertebereiche (Klasse ALLOWEDVALUES) benötigt. Ansonsten muss diese Klasse mit TIMEPERIOD assoziiert werden, um die im Abschnitt 4.1.5 angesprochenen zeitlichen Aspekte zu berücksichtigen.

Da eine SP-Domäne sowohl mehrere Verbindungsdienste als auch unterschiedliche Multi-Domain Managementfunktionen nach außen anbieten kann, spiegelt es sich in der Kardinalität der Assoziationen zwischen der Klasse DOMAIN und den Klassen SCP, COMPOUNDLINK sowie MULTIDOMAINMANAGEMENTFUNCTIONALITY wider.

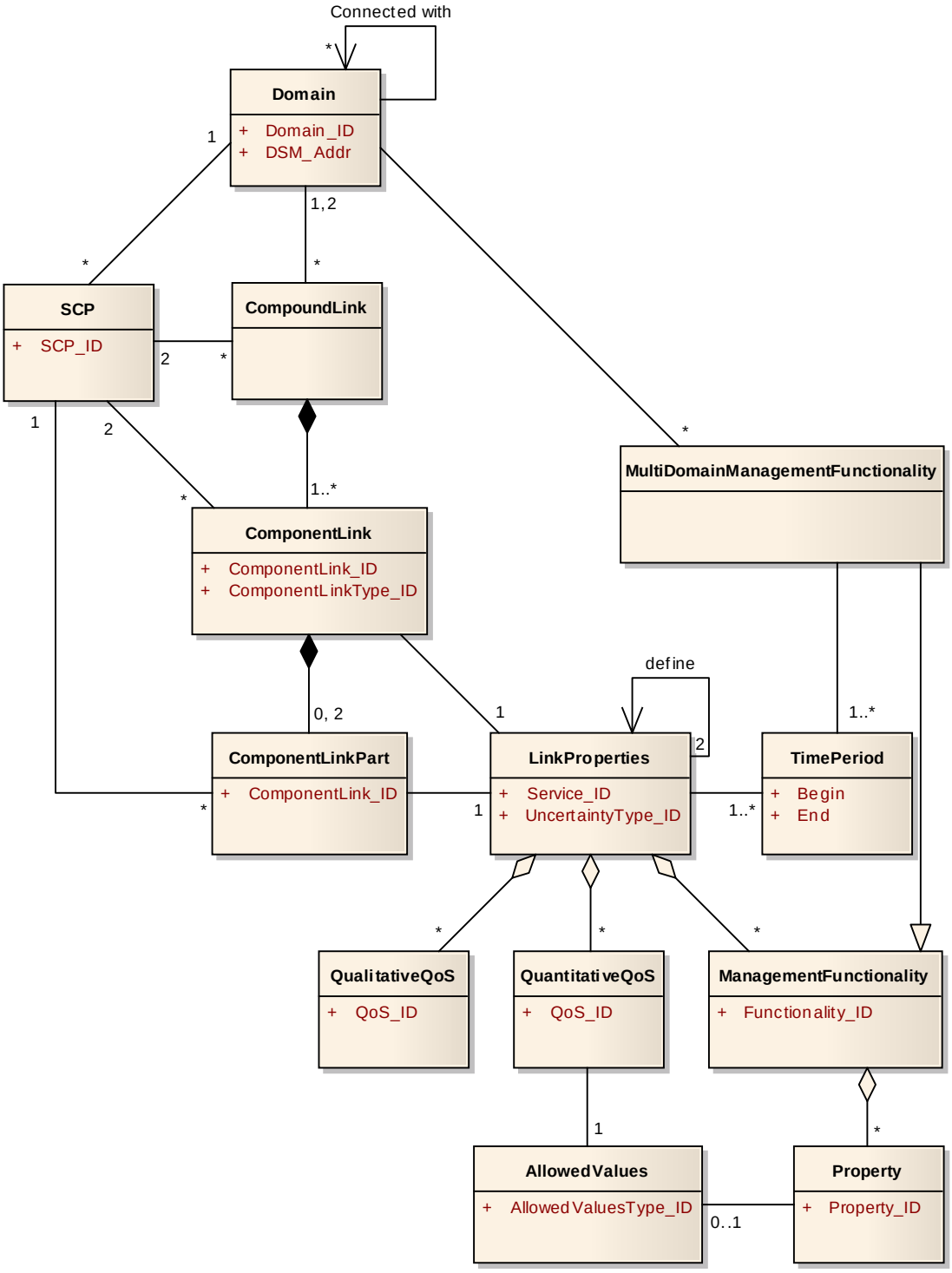


Abbildung 4.50.: Verfügbare (Teil-)Dienste

4.6.6. UML-Modell: RequestedProperties

Die exakte Spezifikation der erforderlichen Diensteigenschaften wird bei Dienst-Reservierung und -Bestellung benötigt (siehe dazu Abschnitt 5.6, 5.8, 5.9 und 5.13).

Verglichen mit den bereits beschriebenen Diagrammen muss bei dem UML-Diagramm in Abbildung 4.51 ausschließlich die Bedeutung der Klasse COMMUNICATIONDSM explizit erklärt werden. Durch diese Klasse wird es möglich, der SP-Domäne zu signalisieren, mit welcher DSM-Kommunikationsschnittstelle die jeweilige von der SP-Domäne zu erbringende Managementfunktionalität kommunizieren soll. Bei dem Monitoring-Dienst wird das die Adresse der Multi-Domain Monitoring-Instanz sein. Erst durch die Spezifikation der DSM-Adresse wird es möglich, die Multi-Domain Funktionalität zu delegieren (vergleiche dazu die Diskussion im Abschnitt 4.4).

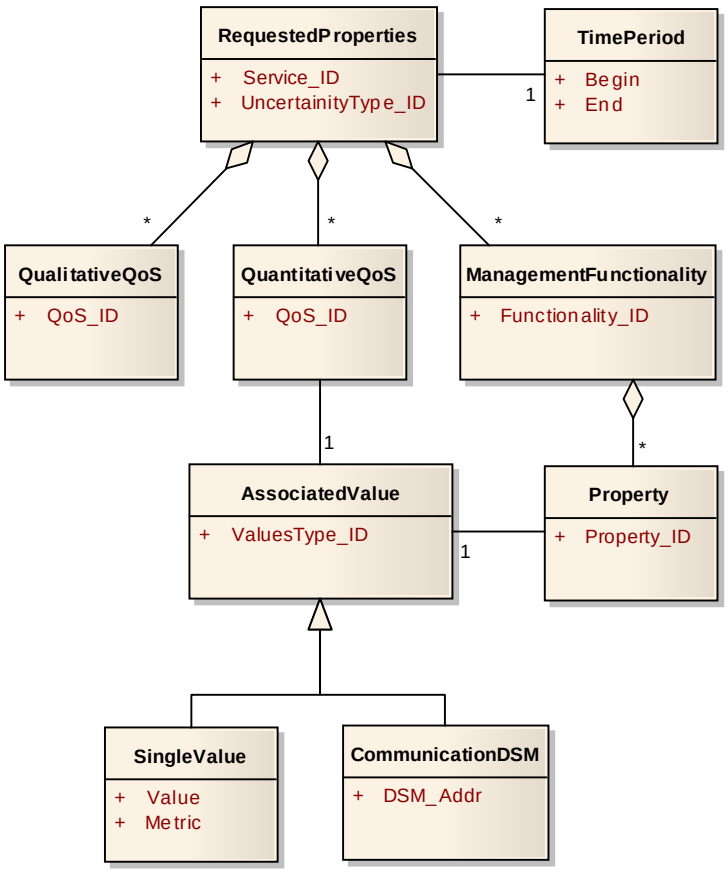


Abbildung 4.51.: Eigenschaftenspezifikation bei einer Dienstinstanzanfrage

4.6.7. UML-Modell: ConfirmedProperties

Das Kommunikationsartefakt für Reservierungs- bzw. Bestellanfrage ist ähnlich zu den bisher beschriebenen. Das UML-Diagramm in Abbildung 4.52 unterscheidet sich zunächst dadurch, dass die Stelle des erwünschten Zeitfensters die Klasse RESERVATIONTIME einnimmt. Diese Klasse wird nur bei der Reservierung gebraucht, was auch ihre Kardinalität bedingt. Um die Problematik mit unterschiedlichen Zeitzonen zu umgehen, wird ausschließlich die Dauer der Reservierung spezifiziert, wodurch die direkte Assoziation mit der Klasse SINGLEVALUE bedingt ist.

Ein anderer wichtiger Unterschied bezieht sich auf die Semantik der Klasse COMMUNICATIONDSM. Im Gegensatz zu den Reservierungs- bzw. Bestellanfragen bezieht sich die DSM-Adresse bei der Bestätigung auf die Managementfunktionalität der SP-Domäne, die die Anfrage bestätigt. Bei dem Monitoring-Service würde das die Adresse bedeuten, die von dem Multi-Domain Monitoring-System beim *Polling* der Teildienste-Zustände kontaktiert werden soll.

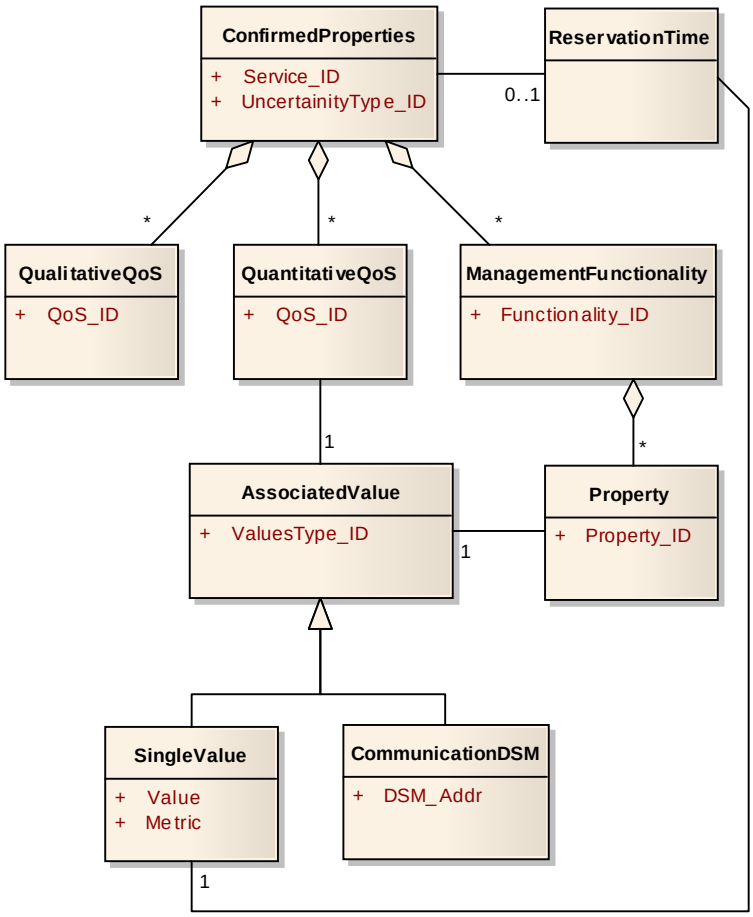


Abbildung 4.52.: Bestätigten Eigenschaften bei einer Dienstinstanzanfrage

4.6.8. UML-Modell: IntermediateProperties

Damit bei der Delegation der Routingaufgabe auch die Zwischenwerte des gefundenen Teilpfades berücksichtigt werden können, muss auch die "Zwischensumme" als ein Kommunikationsartefakt definiert werden (siehe Vorgabe VM08, Abschnitt 4.3). Das UML-Modell für das entsprechedne Kommunikationsartefakt ist in Abbildung 4.53 definiert. Im Gegensatz zu den in Abschnitten 4.6.6 und 4.6.7 definierten UML-Modellen für angefragte und bestätigte Eigenschaften werden bei der Zwischensumme die Zeitangaben nicht benötigt. Dafür muss es aber möglich sein, die Zwischensumme als ein Wertebereich anzugeben. Für die Diskussion über den Umgang mit Wertebereichen wird an dieser Stelle auf den Abschnitt 4.2.4 verwiesen. Die Angabe der Kommunikationsschnittstelle ist notwendig, um die Managementprozesse für den delegierten Anteil der Route mit globalen Managementprozessen zu verknüpfen (siehe dazu auch den Abschnitt 5.13).

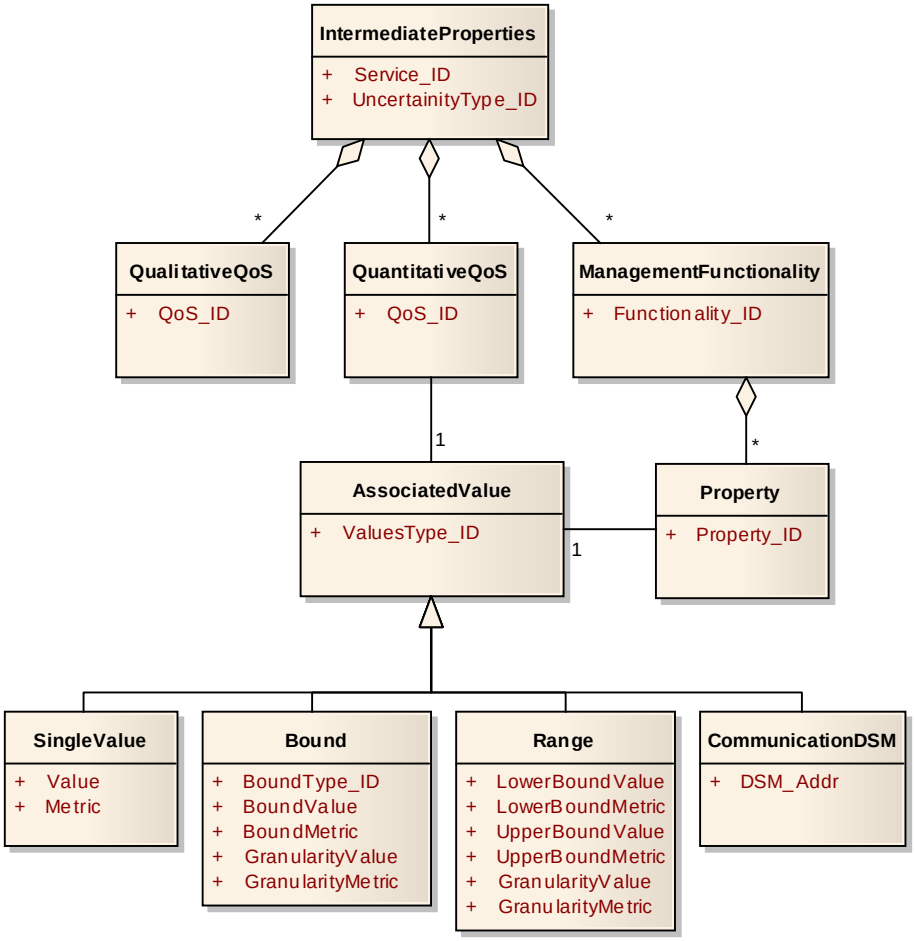


Abbildung 4.53.: Zwischensumme des Pfadgewichtes

4.6.9. UML-Modell: MonitoredState

Wie die Kommunikationsartefakte für die gemessenen Zustände aller vereinbarten QoS-Parameter strukturiert werden können, ist in Abbildung 4.54 dargestellt. Diese Nachrichten werden von den einzelnen SP-Domänen, die ihre Teilstrecken überwachen, an ein Multi-Domain Monitoring-System geschickt (siehe entsprechende Diskussion und Festlegung im Abschnitt 3.6).

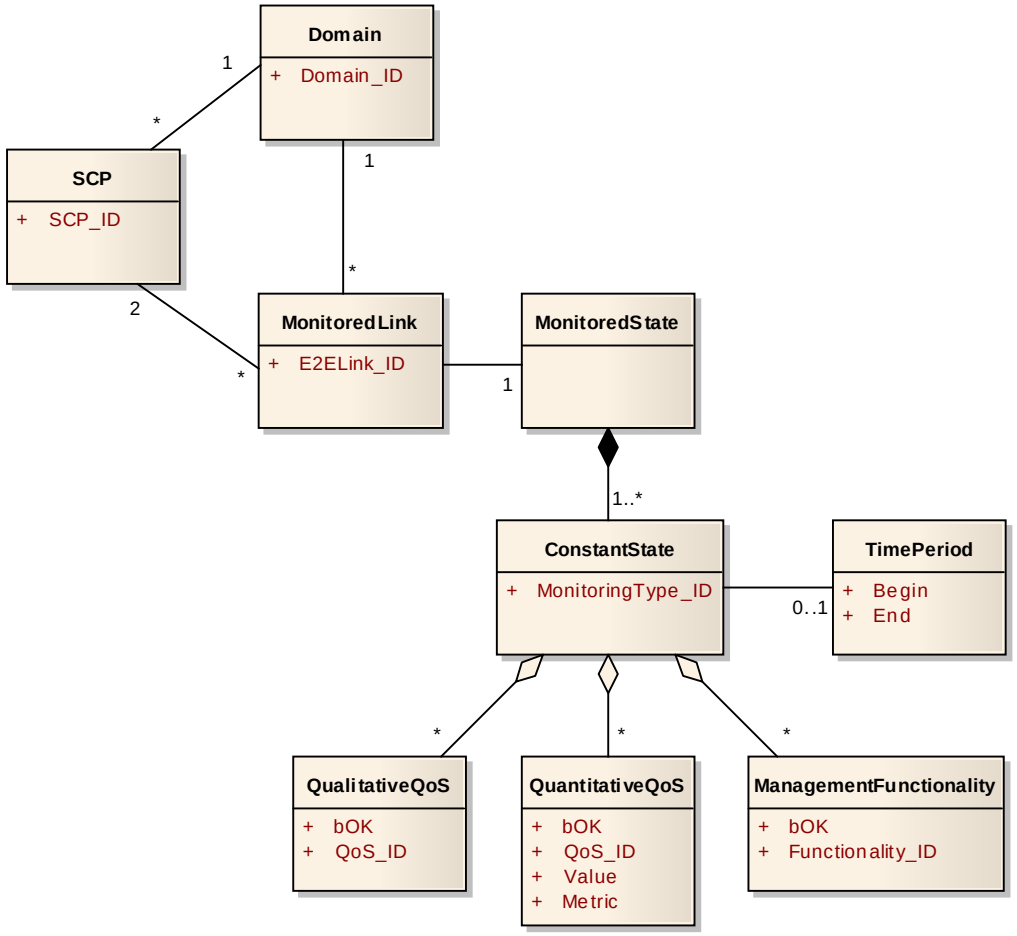


Abbildung 4.54.: Beschreibung eines Monitoringzustandes

Die Struktur der Monitoring-Informationen unterscheidet sich relativ stark von allen bislang definierten Kommunikationsartefakten. Zunächst unterscheidet sich die Beschreibung der Topologie von dem im Abschnitt 4.6.5 definierten UML-Diagramm zur Beschreibung der verfügbaren Verbindungen. An der Stelle von CompoundLink und ComponentLink tritt die Klasse MonitoredLink auf. Diese Klasse repräsentiert die tatsächlich bestellte und überwachte Teilstrecke. Da die SP-Domäne bei der Erbringung mehreren E2E-Dienstinstanzen involviert werden kann, wird die Zugehörigkeit

der Teilstrecke zu einer konkreten Dienstinstanz durch E2ELINK_ID gewährleistet. Innerhalb einer Dienstinstanz wird die Teilstrecke durch zwei SCP_IDs eindeutig identifiziert. Für eine Diskussion über die Zusammensetzung der Monitoring-Informationen anhand der IDs siehe Abschnitt 8.1.

Die Beschreibung der Monitoring-Informationen selbst erfolgt in zwei Verschachtelungsstufen. Die Klasse MONITOREDSTATE umfasst alle Monitoring-Informationen, die sich auf einen MONITOREDLINK beziehen. Diese Klasse umfasst mindestens eine Instanz der CONSTANTSTATE-Klasse, die einen während der in TIMEPERIOD angegebenen Zeitspanne unveränderlichen Zustand erfasst. Dadurch wird auch die Beschreibung der Zustandsschwankungen während der angeforderten Zeitperiode ermöglicht. Sollte ausschließlich der aktuelle Zustand angefragt werden, kann auf TIMEPERIOD verzichtet werden und CONSTANTSTATE muss nur einmal angegeben werden. Die Klasse CONSTANTSTATE beinhaltet eine einzelne Variable, die beschreibt, wie der Monitoring-Zustand erfasst wurde (Polling oder Traps); dadurch wird insbesondere bei kombinierten Überwachungstechniken die Unterscheidung zwischen den jeweiligen Zeitabschnitten möglich.

Die Beschreibung der eigentlichen Monitoring-Daten geschieht zwar strukturell nicht viel anders, es gibt aber einige Unterschiede in den Klassendefinitionen. Jede der Klassen wurde durch eine Variable BOK erweitert, die besagt, ob die *Domain Link* Verbindung in der spezifizierten Zeitspanne die jeweiligen qualitativen QoS-Parameter aufwies, ob die quantitative QoS-Werte gemessen werden konnten und ob die durch FUNCTIONALITY_ID spezifizierte Managementfunktionalität ordnungsgemäß ausgeführt werden konnte. Nur falls diese Variable TRUE ist, sind auch die Werte bei den entsprechenden quantitativen QoS-Parametern valid. Die Variablen für die Beschreibung der Messwerte selbst werden aus der Klasse SINGLEVALUE übernommen.

4.6.10. Identifikation der Objekte und Eigenschaften

Im Laufe dieses Kapitels wurden Anforderungen an die *Identifizierung* unterschiedlicher Objekte aufgestellt, die zur Unterscheidung zwischen gleichartigen Objekten innerhalb einer Domäne sowie in einer Multi-Domain Umgebung verwendet werden soll. Die Klassen aus den Abbildungen 4.46 bis 4.54 können grob in drei Kategorien eingeordnet werden:

- Die Klasse DOMAIN bestimmt einen organisatorischen Rahmen.
- Die Klassen SCP, COMPOUNDLINK, COMPONENTLINK und COMPONENTLINKPART beschreiben die logische Topologie der Verbindungsdienste, die in der SP-Domäne erbracht werden können.
- Die restlichen Klassen beschreiben die Eigenschaften der realisierbaren Teildienste.

Weiter wurden die Anforderungen für die Identifikation einer Reihe weiterer Objekte aufgestellt. Dazu gehören in erster Linie die Schlüsselworte des Kommunikationsprotokolls sowie die IDs für die E2E-Dienstinstanzen und Angebotsanfragen sowie die Adressen für DSM-Schnittstellen (vgl. VI01 im Abschnitt 4.1.1, VI03 im Abschnitt 4.1.2, VI09 im Abschnitt 4.2.6, VI10 im Abschnitt 4.3.5 und VI11 im Abschnitt 4.4).

Für die Wahl der Identifizierungsmöglichkeit ist vor allem entscheidend, ob die ID für die Identifikation eines Objektes (wie z.B. SCP) oder eines semantischen Begriffes verwendet wird, wie es bei den IDs für die QoS-Parameter der Fall ist. Im ersten Fall ist es wichtig, dass ein Objekt mit der ID in dem vorgegebenen Namensraum nur einmal vorkommt, im zweiten steht dagegen eine eindeutige syntaktische Darstellung der Begriffe im Vordergrund, deren Semantik bereits eindeutig definiert wurde. Zwei weitere Faktoren, die allerdings nur bei den Objekt-IDs eine Rolle spielen, sind die Lang- bzw. Kurzlebigkeit dieser IDs, sowie der sog. *Scope*[7] der ID.

Auf der anderen Seite spielen nicht ausschließlich die zu identifizierende Objekte und Eigenschaften selbst bei der Wahl der Identifizierungsmöglichkeiten eine Rolle, sondern auch die Beziehungen und die Dynamik zwischen den beteiligten Service Providern (siehe Abbildung 4.55). So können bei relativ kleinen und stabilen Providerkooperationen (wie z.B. bei Géant2 mit ca. 30 SP-Domänen) Identifizierungsmöglichkeiten ausreichen, die in größeren bzw. hochdynamischen Kooperationen (wie z.B. im Internet) zu Konflikten führen würden.

Um den aus organisatorischer Sicht komplexesten und allgemeingültigsten Fall abzudecken, wird im weiteren Verlauf dieses Abschnittes davon ausgegangen, dass die SP-Domänen einer Kooperation beitreten und sie verlassen können sowie, dass die

[7] Scope wird üblicherweise zur Bezeichnung des Sichtbarkeitsbereichs einer Variablen verwendet. In dem Kontext wird dieser Begriff zur Bezeichnung eines Bereiches verwendet, in dem die Eindeutigkeit einer ID gewährleistet werden soll.

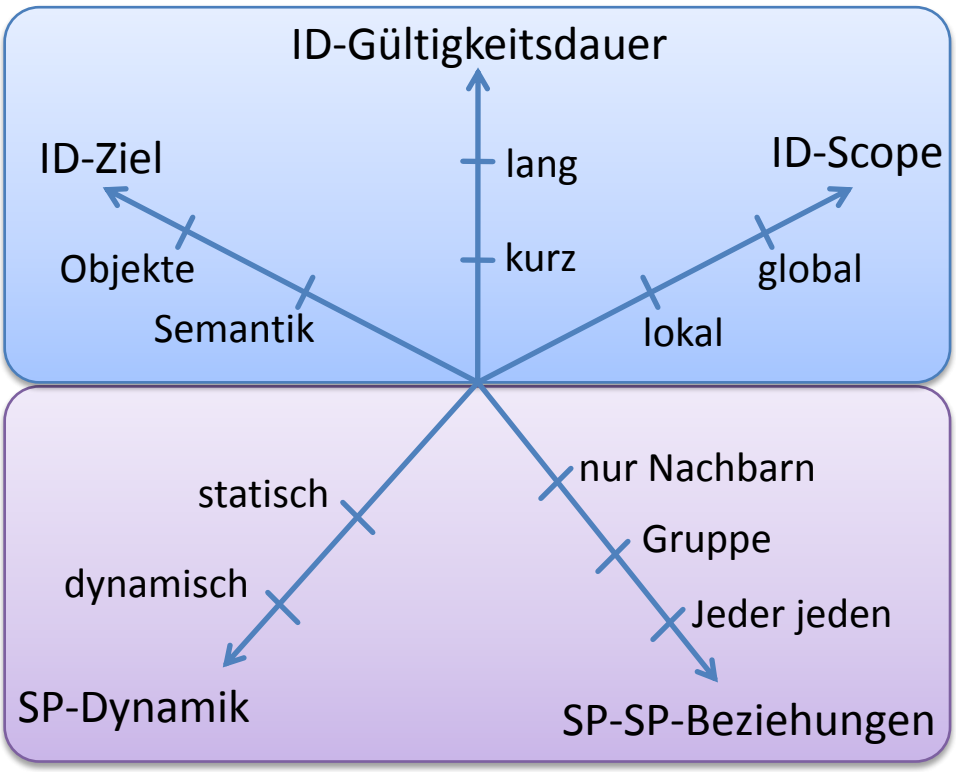


Abbildung 4.55.: Wahl der Identifizierungsmöglichkeiten, Einflussfaktoren

Beziehungen und der Bekanntschaftsgrad einer SP-Domäne beim Betreten der Kooperation sich auf die Nachbardomänen beschränken. Die Besonderheiten fester Service-Provider-Kooperationen und die dabei möglichen Vereinfachungen werden im Abschnitt 4.7 diskutiert.

Die Tabelle 4.5 fasst die in diesem Kapitel angesprochenen Objekte zusammen, die eindeutig identifiziert werden müssen. Die Einordnung des Identifikationsbedarfs im Dimensionsstern der Abbildung 4.55 wird durch die Anfangsbuchstaben der Dimensionswerte in den entsprechenden Spalten dokumentiert.

Grundsätzlich, basierend auf der im Abschnitt 3.9 geführten Diskussion, wurde für die Wahl der Identifizierungsmöglichkeiten folgende Regeln verwendet:

- Für die Gewährleistung der global eindeutigen Semantik sind grundsätzlich Registrierungsbäume am besten geeignet.
- Bei langlebigen Objekten mit globalem Scope ist wiederum eine Identifizierung anhand des Registrierungsbaums empfehlenswert. Die Identifizierung durch URIs ist auch denkbar.

	ID-Ziel	ID-Gültigkeit	ID-Scope	Identifizierung durch…
BoundType_ID	S	l	g	➢ Blatt/Pfad im Registrierungsbaum
ComponentLink_ID	O	k	l	➢ URI (beinhaltet DomainID)
ComponentLinkType_ID	S	l	g	➢ Blatt/Pfad im Registrierungsbaum
Domain_ID	O	l	g	➢ Blatt/Pfad im Registrierungsbaum
DSM_Addr	O	l	g	➢ URL
E2ELink_ID	O	l	g	➢ URI
Eigenschaften-Operationen	S	l	g	➢ Blatt im Registrierungsbaum
Functionality_ID	S	l	g	➢ Blatt/Pfad im Registrierungsbaum
Metric	S	l	g	➢ Blatt/Pfad im Registrierungsbaum
Property_ID	S	l	g	➢ Blatt/Pfad im Registrierungsbaum
Protocol-Keywords	S	l	g	➢ Blatt/Knoten im Registrierungsbaum
QoS_ID	S	l	g	➢ Blatt/Pfad im Registrierungsbaum
ReferenceID	O	k	g	➢ URI (beinhaltet DomainID)
SCP_ID	O	l	g	➢ URI (beinhaltet DomainID)
Service_ID	S	l	g	➢ Blatt/Pfad im Registrierungsbaum
ThresholdType_ID	S	l	g	➢ Blatt/Pfad im Registrierungsbaum
UncertaintyType_ID	S	l	g	➢ Blatt/Pfad im Registrierungsbaum
ValuesType_ID	S	l	g	➢ Blatt/Pfad im Registrierungsbaum
BoundType_ID	S	l	g	➢ Blatt/Pfad im Registrierungsbaum

Tabelle 4.5.: Global eindeutige Identifizierungsmöglichkeiten

- Bei IDs für Objekte mit begrenzter Gültigkeitsdauer und globalem Scope sind grundsätzlich URIs zu verwenden.
- Kurzlebige Objekte mit lokalem Scope sollen bevorzugt mit lokal gültigen IDs versehen werden. Die Verwendung von URIs ist auch denkbar, wenn auch nicht unbedingt notwendig.

Ein Ausschnitt aus einem möglichen Registrierungsbaum ist in Abbildung 4.56 dargestellt. Eine besondere Stellung nehmen dabei die Identifizierung der Schlüsselworte des Kommunikationsprotokolls sowie die Festlegung der Struktur der Kommunikationsartefakte ein. Während zwischen den Versionen diese beide sich ändern bzw. weiterentwickeln können, sollen sie innerhalb einer Version "eingefroren" und unveränderbar sein. Eine ähnliche Stellung nimmt auch die Definition der Eigenschaften ein, mit denen die eigenschaftenbezogenen Funktionen aussoziiert werden (für die entsprechende Diskussion siehe Abschnitt 4.2.6). Diese drei – Kommunikationsprotokoll, Kommunikationsartefakte und Eigenschaften-mit-Operationen – sind die einzigen

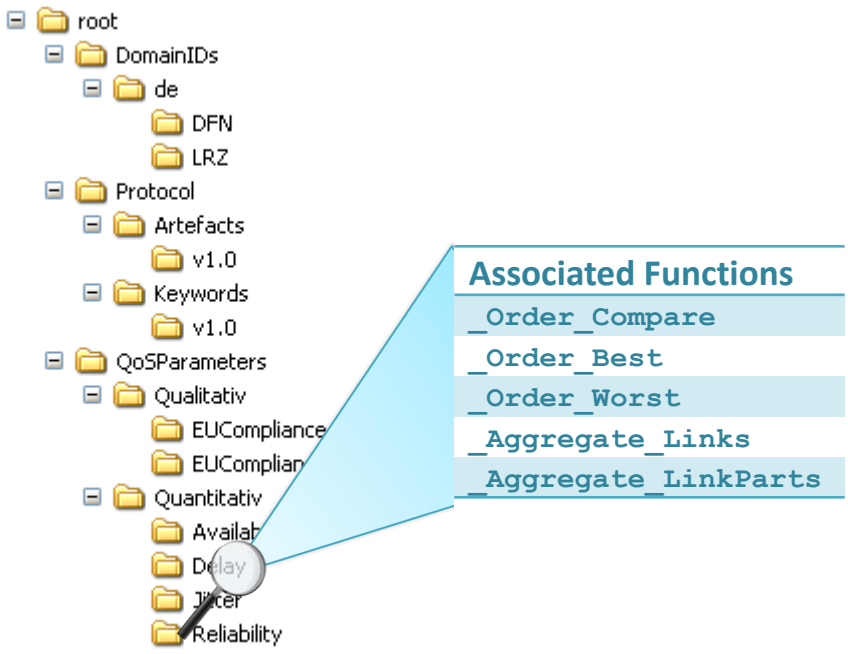


Abbildung 4.56.: Möglicher Registrierungsbaum (Ausschnitt)

komplexen Strukturen, die im Registrierungsbaum festgehalten werden sollen (vergleiche auch die Diskussion im Abschnitt 3.9.4 über die Gefahr einer Inflexibilität bei der Verwendung eines Registrierungsbaumes).

Durch den Einsatz eines Registrierungsbaums sind sowohl die Erweiterungsmöglichkeit als auch die Eindeutigkeit aller zu identifizierenden Objekte gegeben. Da unterschiedliche Providerkooperationen ihre eigene Regestrierungsbäume benutzen können, sind unterschiedliche, an die Randbedingungen der Service-Provider-Kooperationen und den angebotenen Dienst angepasste Strukturierungs- und Benennungsmöglichkeiten denkbar. Der Einsatz von Registrierungsbaum erfordert auch die Definition von einem Verfahren zur Vergabe von IDs für die unterstützten Eigenschaften. Da ein solches Verfahren nur Kooperation spezifisch definiert werden kann, wird an dieser Stelle kein expliziter Vorschlag dafür gemacht. Der Einsatz von URIs bringt einerseits mehr Flexibilität und kurze Zeiten bei der Benennung, garantiert im Gegenzug aber die Einhaltung der Namensgebungsregeln nicht.

4.7. Vereinfachungen bei Sonderfällen

In den Abschnitten 4.3.2 und 4.3.3 wurden allgemeine Fälle von Providerkooperationen diskutiert. Während in den o.g. Abschnitten entsprechend allgemeingültige Routingverfahren präsentiert wurden, sind unterschiedliche Fälle denkbar, die wesentliche Vereinfachungen dieser Verfahren bzw. Kommunikatonsartefakte erlauben würden. Da dadurch sowohl die Steigerung der Effizienz und Reaktionszeiten als auch die Reduktion der Entwicklungs- und Betriebskosten erzielt werden können, werden in diesem Abschnitt einige solche Fälle besprochen.

Verzicht auf Managementfunktionalität

Wie in Abschnitten 3.4 bis 3.7 diskutiert wurde, kann die E2E-Dienstgüte nicht ausschließlich durch die Festlegung der Grenzwerte für QoS-Parameter der einzelnen Verbindungsabschnitte garantiert werden. Um die getroffenen Festlegungen garantieren zu können, müssen die Teildienste im Rahmen von ITSM-Vorgaben erbracht werden. Dabei sind nicht nur das Service-Level-Management selbst, sondern auch weitere relevante Managementprozesse, wie z.B. *Incident&Problem Management*, *Capacity Management* u.a. gemeint.

Am Beispiel von Telefonverbindungen kann man sehen, dass, solange die Verbindungsstrecke ausschließlich über Service Provider geroutet wird, die die erforderliche Dienstgüte der Teilstrecke(n) innerhalb ihrer eigener Domäne garantieren, auch die E2E-Verbindungsqualität entsprechend gut ist. Für solche Situationen – und insbesondere, wenn das Dienstinstanz-Management vom Kunden nicht explizit gefordert wurde – wäre es denkbar, auf die recht aufwendige Kopplung (siehe z.B. Abschnitt 4.4) der domäneninternen Managementprozesse zu einem Multi-Domain-Managementprozess zu verzichten. Bei dieser sog. "*define-and-forget*"-Strategie, wenn ausschließlich die Teilstrecken selbst und deren Dienstgüte definiert werden müssen, entfällt die Notwendigkeit der Multi-Domain-Managementkomponenten, wie z.B. fürs Multi-Domain-Monitoring. Weiterhin wird dabei auch die Menge der auszutauschenden Managementinformationen, deren Komplexität sowie die Kommunikationshäufigkeit dramatisch abnehmen.

QoS mit "einfachen" Aggregatfunktionen

Ein weiterer Sonderfall ist mit den für den Endkunden oder für den angebotenen Dienst relevanten QoS-Parametern verbunden. Wie im Abschnitt 3.2 bei der Beschreibung von ATM-Dienstklassen angesprochen wurde, können in Abhängigkeit vom Anwendungsfall unterschiedliche QoS-Parameter als relevant und die restlichen als irrelevant betrachtet werden. So spielen bei Videokonferenzen und Telefonverbindungen neben der eigentlichen Bandbreite auch Delay und Jitter eine wichtige Rolle, bei reinem Datentransfer dagegen können diese zwei QoS-Parameter schwanken, ohne dass das vom Kunden als negativ empfunden wird.

Im Abschnitt 4.2 wurde zudem formal definiert, wie die E2E-Dienstgüte aus den Dienstgütewerten einzelner Abschnitte mit der Hilfe der QoS-abhängigen Aggregatfunktionen berechnet werden kann. Dabei können die Aggregatfunktionen grob in

zwei Kategorien eingeteilt werden: Aggregatfunktionen, die ausschließlich von den einzelnen zu aggregierenden Werte abhängen, und die, die auch von der Anzahl der Werte (für Teilstrecken) beeinflusst werden. Zur ersten Kategorie gehören u.a. Aggregatfunktionen für alle qualitativen QoS-Parameter (Aggregatfunktion ist als logisches AND definiert); von den quantitativen QoS-Parametern, deren Aggregatfunktionen auch zu dieser Kategorie gehört, kann z.B. die Bandbreite erwähnt werden, deren Funktion als min über alle Teilwerte definiert ist. Delay, Verfügbarkeit, Fehlerrate sowie viele andere häufig verwendeten QoS-Parameter weisen allerdings Aggregatfunktionen auf, die z.B. als ADD oder MULT definiert sind, wodurch auch die Anzahl der zu aggregierenden Werte eine Rolle spielt.

Soll ein Dienst angeboten werden, bei dem ausschließlich QoS-Parameter mit Aggregatfunktionen der ersten Kategorie vorkommen, dann kann beim Routing auf die E2E-Betrachtung verzichtet werden und man kann stattdessen ausschließlich auf lokalen abschnittbezogenen Entscheidungen aufbauen. Das kann insbesondere im Zusammenhang mit dem Verzicht auf Managementfunktionalität interessant sein, weil dadurch *Routing by Delegation* (siehe Abschnitt 4.3.3) angewendet werden kann, wobei ausschließlich die Grenzwerte weitergereicht werden müssen.

Festlegungen bei festen Kooperationen

Eine andere Vereinfachungsmöglichkeit hängt nicht mit den QoS-Parametern oder der Managementfunktionalität, sondern ausschließlich mit der Art der Multi-Domain Providerkooperation zusammen. Implizit wurde in Abschnitten 4.3 und 4.4 von einem allgemeinem Fall ausgegangen, bei dem die SP-Domänen höchstens die Kenntnis von direkten Nachbardomänen haben, mit denen direkte gute Vertrauensbeziehungen verbunden sind. Dieser Fall kann zwar als ein allgemeingültiger und daher auch als ein theoretisch interessanter betrachtet werden, in der Realität kommt er aber nicht allzu häufig vor (mit Ausnahme von z.B. Internet- und Telekommunikationsdienten, in deren Erbringung viele regionale Service Provider involviert sind). In der Praxis kommen oft Fälle vor, bei denen die Service Provider bei der Diensterbringung sehr eng miteinander kooperieren. Dabei können sich Vertrauens- und Vertragsbeziehungen sowohl auf alle Kooperationspartner erstrecken und es können sich strukturierte Domänengruppen bilden. An dieser Stelle wird auf die Géant2 Kooperation von ca. 30 Nationalen Forschungsnetzorganisationen (siehe Abschnitt 2.3.2) sowie auf die internationalen Forschungsprojekte GLIF und DCN (siehe entsprechend Abschnitte 2.3.3 und 2.3.4) verwiesen.

Während bislang von einer dynamischen, Dienstinstanz-spezifischen Festlegung aller Kommunikationswege und der Verteilung der benötigten funktionalen Komponenten ausgegangen wurde, können solche Festlegungen bei engen, langfristigen Kooperationen generell für alle Dienstinstanzen getroffen werden. Insbesondere bei einer relativ geringen Anfragedichte für neue Dienstinstanzen sowie bei einer überschaubar großen Anzahl zu überwachender Dienste kann es sinnvoll sein, diese Aufgaben statisch – und nicht dynamisch, wie es im Abschnitt 4.4 beschrieben wurde – an darauf spezialisierende SP-Domänen zu delegieren. Die qualitative Bezeichnungen "gering" und

"überschaubar" sind dabei im Verhältnis mit der Bearbeitungskapazität der jeweiligen Komponenten zu beurteilen.

Eine weitere Anpassung bezieht sich auf die im Abschnitt 4.1.3 getroffene Festlegung, dass im allgemeinen Fall jede SP-Domäne als Proxy für die *Interdomain Links* zu ihrer Nachbardomänen agieren soll. Dadurch entstehen allerdings ein erhöhter Managementaufwand bei allen SP-Domänen sowie eine zusätzliche Kommunikationsstufe, wodurch die Reaktionszeit bei allen Managementprozessen beeinträchtigt wird. Durch die bei festen Kooperationen gegebenen Vertrauensbeziehungen können alle Managementoperationen, die sich auf die *Interdomain Links* beziehen, nicht wie im o.g. Abschnitt spezifiziert über eine Proxy-SP, sondern durch direkte Kommunikation mit beiden aneinander angeschlossenen Domänen realisiert werden. Zusätzlich zu den bereits angesprochenen Verbesserungen bzgl. Laufzeit der Managementoperationen und der Robustheit befreit dieses Vorgehen auch die jeweiligen SP-Domänen von der Notwendigkeit, eine Proxy-Funktionalität zu implementieren und zu betreiben.

Zusätzlich kann bei geschlossenen und eher statischen Kooperationen die Identifizierung der verwendeten Objekte vereinfacht werden (vergleiche Abschnitt 4.6.10). So können bei solchen Kooperationen statt richtiger URIs einfache, aus zwei Teilen (Domain-Akronyme, LocalID) zusammengesetzte IDs verwendet werden. Als richtig vorteilhaft kann bei diesem Vorgehen nur verbesserte manuelle Lesbarkeit der verwendeten IDs betrachtet werden. Dadurch steigt steigt allerdings die Kollisionsgefahr: so können unterschiedliche Organisationen dieselbe Akronyme und somit die bevorzugten DomainIDs haben. Deswegen soll diese Vereinfachungsmöglichkeit eher mit Bedacht verwendet werden.

4.8. Softwarearchitektur einer SP-Domäne

Skizze einer Softwarearchitektur in einer Domäne

Der bislang nur am Rande angesprochene Aspekt bezieht sich auf die Realisierung der Funktionalität innerhalb einer SP-Domäne, die für die in diesem Kapitel erarbeitete Lösung benötigt wird. Obwohl der Fokus dieser Arbeit bei den Multi-Domain Aspekten liegt, hängt die Anwendbarkeit der entwickelten Lösung in der Praxis davon ab, wie die einzelnen Single-Domain Teile realisiert werden können. Aus diesem Grund wird hier eine mögliche Softwarearchitektur innerhalb einer SP-Domäne vorgeschlagen. Eine grobe Skizze dafür ist in der Abbildung 4.57 dargestellt.

Die durch die DSM-Schnittstelle kommenden Anfragen müssen zunächst interpretiert werden. Erst dann kann mit Einbezug verschiedener Kriterien (im Bild sind dafür Domain-Policies sowie die Identity und Trust Management Komponenten abgebildet) entschieden werden, ob die Anfrage bearbeitet oder zurückgewiesen werden soll.

Sollte eine Anfrage zurückgewiesen werden, kann das gleich der anfragenden SP-Domäne mitgeteilt werden. Architekturbausteine, die durch eine Anfrage direkt oder indirekt angesprochen werden, werden in der Abbildung in drei Kategorien unterteilt:

Connection steht stellvertretend für die *Domain-* und *Interdomain Links*, die von dieser Domäne erbracht werden können oder erbracht werden.

Single-Domain referenziert alle Managementaufgaben, die sich auf Objekte und Daten dieser einen Domäne beziehen. Dazu gehören z.B. das Monitoring eigener Abschnitte sowie Benachrichtigungen bei Threshold-Überschreitungen.

Multi-Domain referenzieren analog alle Managementaufgaben, die i.A. Ojekte und Daten aus mehreren Domänen einbeziehen. Dazu gehören z.B. das Routing selbst, oder auch Multi-Domain Monitoring, bei dem Überwachungsinformationen aus mehreren Domänen abgefragt und aggregiert werden.

Die allgemeinen Zusammenhänge zwischen einzelnen für die *Verketteten Dienste* relevanten Services sowie zwischen deren Eigenschaften sind in Abbildung 4.58 dargestellt.

Da die nach außen sichtbaren Dienste eine Abstraktion der in der Domäne verwendeten Ressourcen darstellen, muss bei der Durchführung der angefragten Aufgaben eine Abbildung der Außensicht auf die Innensicht und bei der Benachrichtigungen über Ergebnisse umgekehrt von der Innensicht auf die Außensicht durchgeführt werden. Dazu ist die "Mapping"-Komponente zuständig, die bei ihrer Arbeit eng mit der "ID-Management"-Komponente interagieren muss, damit die Informationen und Managementanfragen eindeutig abgebildet werden.

Die von den "Supported Services" nach außen gemeldeten Informationen müssen den Vorgaben der Domain-Policies entsprechen. Im Bild ist das durch den Einfluss der

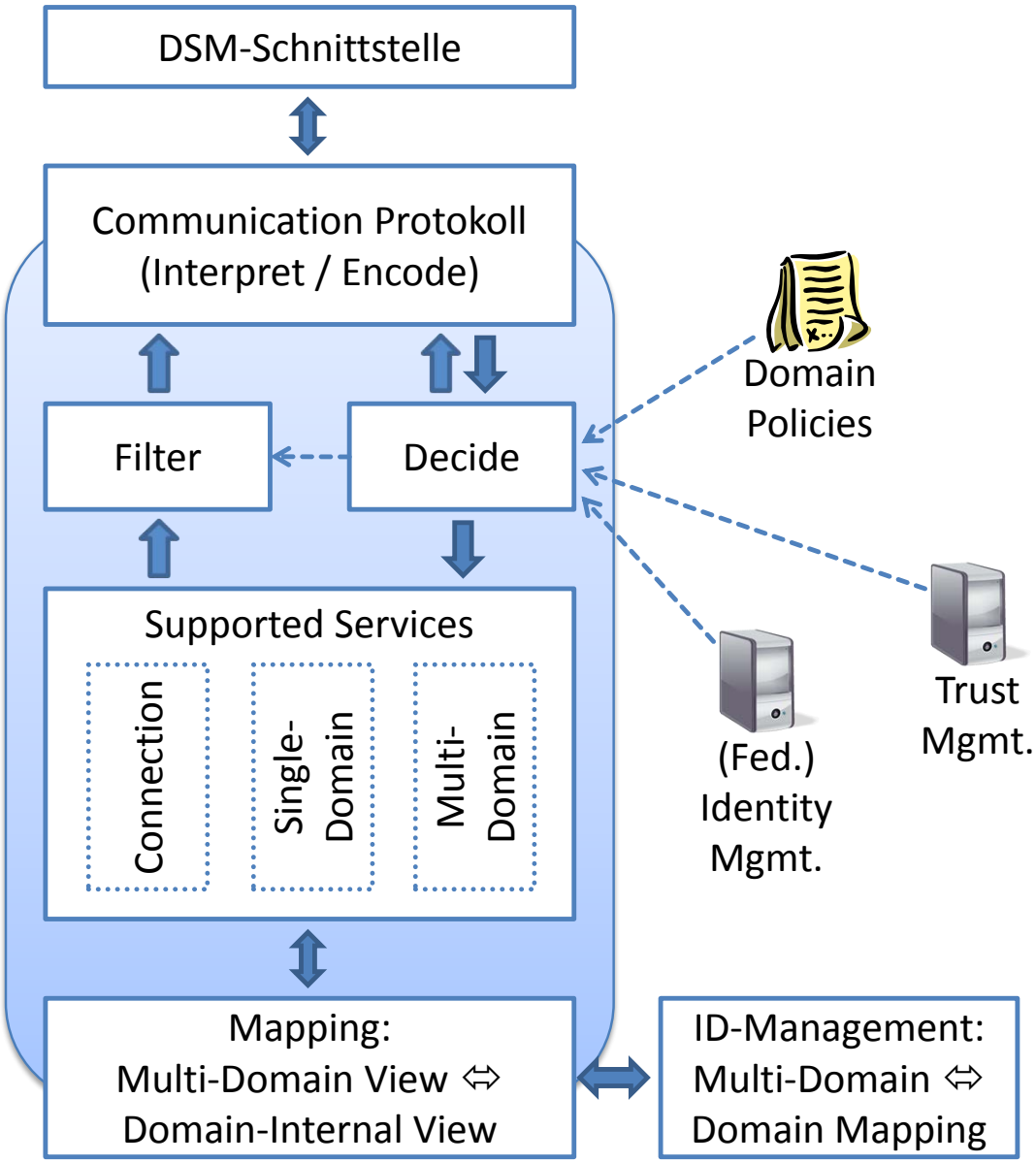


Abbildung 4.57.: Bausteine einer Softwarearchitektur fürs Management Verketteter Dienste innerhalb einer Domäne

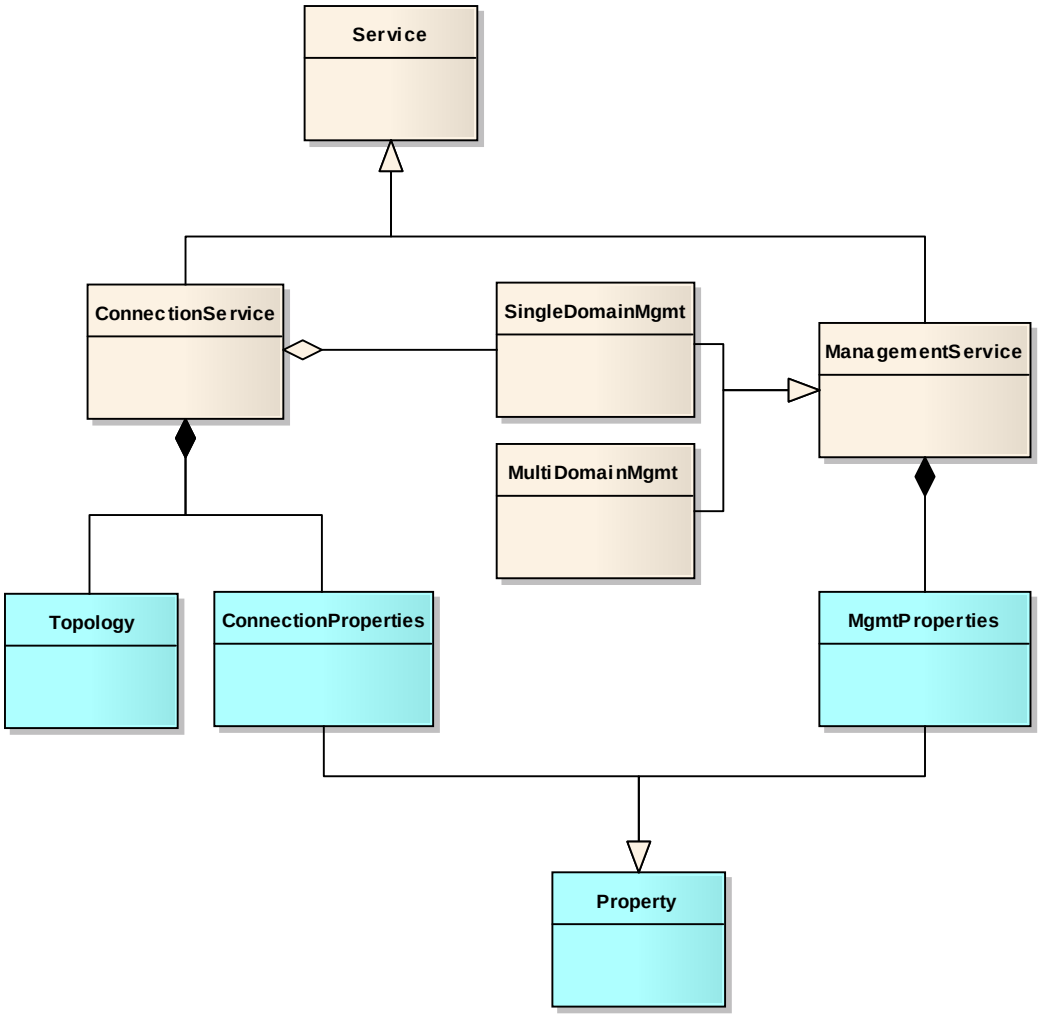


Abbildung 4.58.: Unterstützte Dienste, Zusammenhänge

"Decide"-Komponente auf "Filter" angedeutet. Eine andere, nicht weniger wichtige Aufgabe von "Filter" ist die Reduktion der Informationsmenge auf die, von der anfragenden SP-Domäne spezifizierten Informationen.

Die so spezifizierten Benachrichtigungen nach Außen müssen ihrerseits von der domaininternen Repräsentation auf die im Rahmen des Kommunikationsprotokolls spezifizierte abgebildet und über die DSM-Schnittstelle dem jeweiligen Kommunikationspartner mitgeteilt werden.

Relevanten Arbeiten

Für die gegenseitige Identifikation der SP-Domänen wird an dieser Stelle auf die Arbeit von HOMMEL [Hom07] verwiesen, die sich mit dieser Problematik in föderierten Multi-Domain Umgebungen auseinandersetzt und dafür ein in sich abgeschlossenes Konzept präsentiert. Da die Identifizierung allein noch nicht über die Vertrauenswürdigkeit des Kommunikationspartners aussagt, wird an dieser Stelle empfohlen, föderiertes Identity-Management mit Trust-Management zu kombinieren. Für diese Aufgabe wird auf die Arbeit von BOURSAS [Bou09] verwiesen, die sich mit nicht-direkten Vertrauensbeziehungen in föderierten Multi-Domain Umgebungen befasst.

5

Kommunikationsprotokoll und Basisprozesse

Dieses Kapitel beschreibt die Verknüpfung zwischen der im Kapitel 4 definierten Routingarchitektur und den Managementprozessen, die im Kapitel 6 beschrieben werden. Der Fokus dieses Kapitels liegt sowohl in der Definition des Kommunikationsprotokolls, das als ein Teil der Routingarchitektur angesehen werden kann, als auch in der Verbindung des Protokolls mit den Basisprozessen, die ihrerseits als die Grundbausteine der Multi-Domain Managementprozesse verwendet werden.

Zuerst werden im Abschnitt 5.1 die Struktur des Protokolls sowie eine Reihe von grundlegenden Konzepten festgelegt. Diese Konzepte behalten ihre Gültigkeit bei der Definition aller Basisprozesse in Abschnitten 5.2 bis 5.14. Bei der Definition von Basisprozessen wird auf die Konventionen und die Beschreibungsstruktur von *ITSMCooP* [Ham09] zurückgegriffen. Das Kapitel endet mit einem kurzen Überblick über das definierte Protokoll, der im Abschnitt 5.15 in tabellarischer Form gemacht wird.

5.1. Generelle Zusammenhänge und Festlegungen

Kommunikationsmuster und Rollen

Um ein Protokoll sowohl möglichst flexibel als auch erweiterbar und an die Domäneninteressen anpassbar zu machen, wird die ganze Kommunikation zwischen einer Domäne und der Außenwelt in bereits bei OSI- und Internet-Managementarchitekturen bewährter Weise in drei Nachrichtenkategorien – Anfrage, Antwort und Benachrichtigung – unterteilt (siehe Abbildung 5.1).

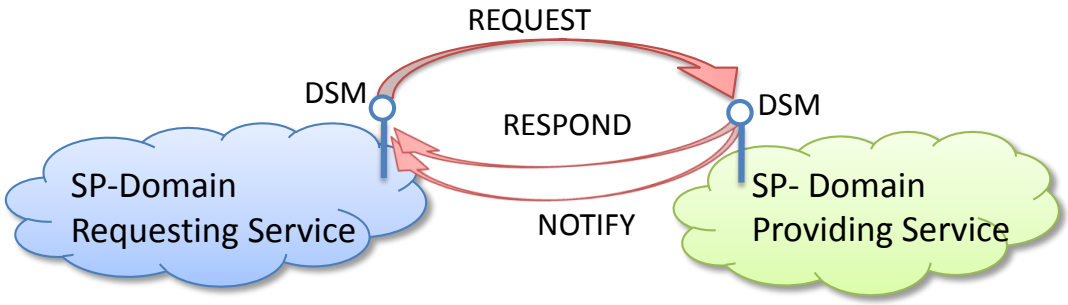


Abbildung 5.1.: Communication Protocoll

Die Erweiterungsmöglichkeit wird dadurch gewährleistet, dass alle drei – `REQUEST`, `RESPOND` und `NOTIFY` – erst durch *Specifier* ihre genaue Bedeutung erlangen. Der Specifier bestimmt weiterhin die Anzahl und die Bedeutung der zugehörigen Parameter (siehe Tabelle 5.1).

REQUEST	<RequestSpecifier>	[<RequestParameters>]
RESPOND	<RespondSpecifier>	[<RespondParameters>]
NOTIFY	<NotificationSpecifier>	[<NotificationParameters>]

Tabelle 5.1.: Verfeinerung des Kommunikationsmusters

Eine SP-Domäne, die eine Anfrage an eine andere Domäne schickt, wird als "*Requesting Service*" referenziert. Die SP-Domäne, die auf eine Anfrage antwortet und i.A. auch einen angeforderten Dienst erbringt, wird als SP-Domäne "*Providing Service*" bezeichnet. Der Nachrichtenaustausch zwischen zwei SP-Domänen findet immer über eine DSM (*Domain Service Management*) Schnittstelle statt. Die Verantwortlichkeit der Rollen ist kurz in Tabelle 5.2 zusammengefasst.

Zustände, Zustandsübergänge und Protocol-Keywords

Drei Einflussfaktoren spielen bei der Definition des Kommunikationsprotokolls eine entscheidende Rolle: das Routingverfahren und die Architekturfestlegungen, damit alle notwendigen Operationen abgedeckt werden können, der Dienstaufbau, damit alle Bestandteile eines Dienstes einzeln referenziert werden können, und die Dienstinstanz-Zustände, damit die erforderlichen Zustandsübergänge angefordert werden können. Für die Strukturierung der REQUEST-Anfragen wird in dieser Arbeit der letzte der genannten Einflussfaktoren verwendet. Die in Abbildung 5.2 dargestellten

Rolle	Bezeichnung	Rollendefinition	
R_1	SP-DOMAIN REQUESTING SERVICE	*Verantwortlichkeiten*	• Auswahl der SP-DOMAIN PROVIDING SERVICE • Bestimmung der benötigten Funktionalität • Abschicken einer Anfrage • Reaktion auf die Antwort
		Fokus	ConcatenatedService
		Kardinalität	1
		Art der Partizipation	statisch
		Vergabeverfahren	–
		Kandidatenmenge	–
R_2	SP-DOMAIN PROVIDING SERVICE	*Verantwortlichkeiten*	• Entscheidung, ob Anfrage akzeptiert oder abgelehnt wird • Bearbeitung der Anfrage • Mitteilung der Ergebnisses der SP-DOMAIN REQUESTING SERVICE
		Fokus	PartialService, u.U. auch ConcatenatedService
		Kardinalität	1, n
		Art der Partizipation	dynamisch
		Vergabeverfahren	Auswahl durch SP-DOMAIN REQUESTING SERVICE
		Kandidatenmenge	alle SP-Domänen

Tabelle 5.2.: Rollen in Basisprozssen

Zustandsübergänge werden mit den Schlüsselworten beschrieben, die an der Stelle von <REQUESTSPECIFIER> auftreten dürfen. Dieses Bild wird auch bei der weiteren Beschreibung der Basisprozesse wiederverwendet, um graphisch darzustellen, zwischen welchen Zuständen die Dienstinstanz bei dem jeweiligen Basisprozess wechselt.

Der Dienstaufbau bildet einen weiteren Strukturierungsfaktor des Protokolls. Entsprechend den Festlegungen im Kapitel 4 kann ein Verketteter Dienst aus einem oder mehreren Verbindungsdiensten sowie einer Reihe von Multi-Domain Managementdiensten und höchstens einem weiteren Verketteten Dienst bestehen (siehe insbesondere Abschnitte 4.3.4 und 4.8). In Abbildung 5.3 sind die Klassenassoziationen mit den Schlüsselworten beschriftet, die für das Referenzieren der jeweiligen Dienstkomponenten verwendet werden.

Der Einfluss des Routingverfahrens und der Architekturfestlegungen kommt am deutlichsten bei automatischen Benachrichtigungen zum Vorschein. Beim Routing werden Informationen über verfügbare Interdomain-Verbindungen und deren realisierbare Eigenschaften jeweils von einer SP-Domäne abgefragt, die stellvertretend auch für die mit dem *Interdomain Link* verbundene Nachbardomäne "spricht". Zwar reichen dafür auch on-demand Informationsabfragen aus, im Abschnitt 4.1.2 wurde eine u.U.

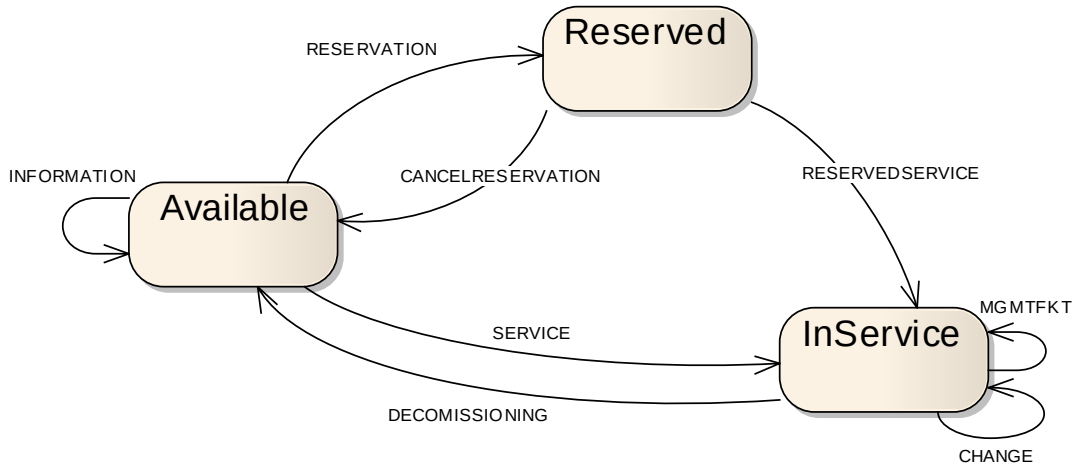


Abbildung 5.2.: Zustandsautomat und REQUEST-Optionen

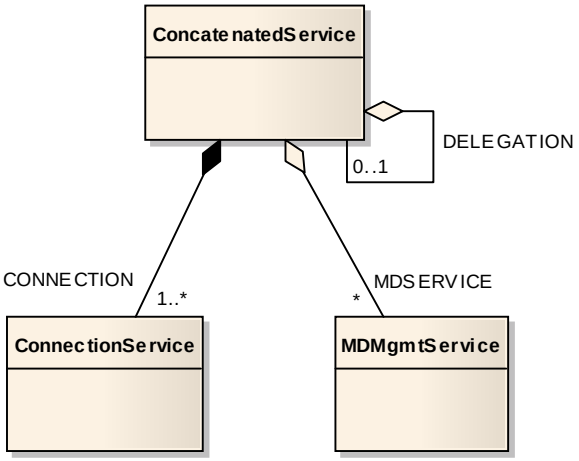


Abbildung 5.3.: Concatenated Service, Zusammensetzung

bevorzugte Variante mit automatischen Benachrichtigungen vorgestellt. Dafür müssen jedoch die entsprechenden Informationen abonnierbar sein. In Abbildung 5.4 werden die Zustandsübergänge mit den entsprechenden Protokollaufrufen beschriftet.

Eine weitere Möglichkeit, die automatische Benachrichtigung zu abonnieren, ist implizit in der Bestellung eines Verbindungsdienstes verborgen. Diese Benachrichtigungen beziehen sich somit auf eine Dienstinstanz (im Gegensatz zu INFORMATION-Benachrichtigungen, die sich auf die allgemein verfügbaren Kapazitäten beziehen). Bei einer Dienstinstanz ist – in Bezug auf das Service-Level-Management – vor allem ihr aktueller Zustand interessant, um die kontinuierliche Überwachung (engl.: *Monitoring*) und die Berichterstattung (engl.: *Reporting*) zu ermöglichen. Weiterhin ist oft

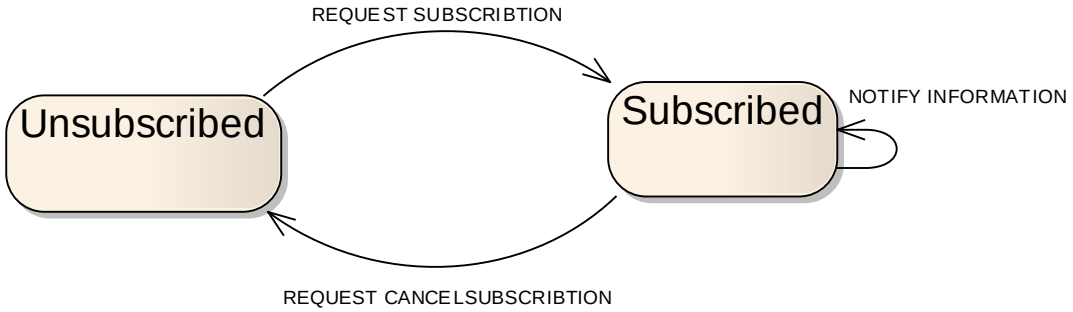


Abbildung 5.4.: Abonnieren einer automatischen Benachrichtigung

das Eintreffen der vordefinierten Ereignisse interessant, wie z.B. das Verletzung einer vordefinierten Zustandsgrenze (engl.: *Threshold*), um die Einflüsse auf SLA festzustellen. Diese zwei Benachrichtigungsarten werden weiter in dem Kapitel als INSTANCE-STATE und EVENT Schlüsselworte für <NOTIFICATIONSPECIFIER> referenziert und in den entsprechenden Basisprozessen beschrieben.

Verhandlungsmuster: Rechte und Pflichten der Rolle SP-Domain Providing Service

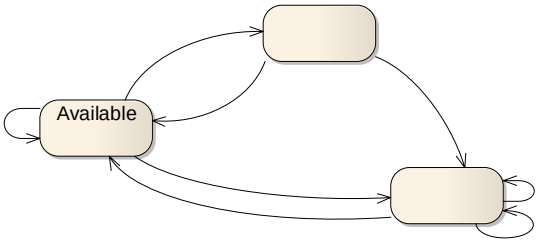
Essentiell ist auch die Festlegung der Rechte und Pflichte von *SP-Domain Providing Service* bei allen Arten der Protokollanfragen. Wegen der herrschenden Heterarchie der Service Provider muss jedem *SP-Domain Providing Service* der Recht eingeräumt werden, jede Informations- oder Dienstanfrage abzulehnen.

Weiterhin soll zwischen Reservierungs- und Bestellanfragen unterschieden werden. Hier wird auf die Ergebnisse der im Abschnitt 3.2 geführten Diskussion über Verhandlungsmuster zurückgegriffen. Entsprechend der dort getroffenen Entscheidungen soll dem *SP-Domain Providing Service* bei der Reservierungsanfrage das Recht eingeräumt werden, mit einem schlechteren Angebot als die angefragten Eigenschaften zu antworten. Bei Bestellanfragen darf der *SP-Domain Providing Service* dagegen die angefragten Eigenschaften ausschließlich verbessern. Falls die Erfüllung der bei der Dienstbestellung angefragten Eigenschaften unmöglich ist, muss der *SP-Domain Providing Service* mit einer Fehlermeldung antworten.

Sollte der *SP-Domain Providing Service* die Bestellanfrage für eine neue Dienstinstanz (bzw. Teildienst) akzeptieren, dann sind die bestätigten Eigenschaften für den *SP-Domain Providing Service* verpflichtend. Diese Bedingung ist notwendig, damit die E2E-Eigenschaften garantiert werden können.

5.2. REQUEST INFORMATION

5.2.1. Einführung



Bei der Suche nach einem Pfad, der die E2E-Anforderungen erfüllt, werden Informationen über die verfügbaren Kapazitäten benötigt. Diese können mit dem Protokollaufruf `REQUEST INFORMATION` abgefragt werden. Die Informationsmenge wird durch die Angab der benötigten Eigenschaften sowie der Ausgangs- und Zielpunkte (SCPs) eingeschränkt. Die Antwort verpflichtet die angefragte SP-Domäne nicht, die Ressourcen zu reservieren, sondern entspricht lediglich einer Momentaufnahme.

Die Informationsanfrage kann zwischen völlig automatisierten und teil-automatisierten Diensten unterscheiden. Insbesondere kann das in Verbindung mit Anfragen relevant sein, die noch nicht vorhandene Infrastruktur berücksichtigen sollen. Um beide Fälle abdecken zu können, werden in diesem Abschnitt zwei entsprechende Prozessalternativen definiert.

5.2.2. Aktivitäten

Tabelle 5.3 beschreibt alle Aktivitäten, die bei Informationsabfrage benötigt werden. Die Aktivität A_5 wird ausschließlich bei asynchroner Benachrichtigung bei den teil-automatisierten Prozessen verwendet. Die Aufgabe der restlichen Aktivitäten stimmt in beiden Fällen überein (vgl. Abschnitt 5.2.4).

5.2.3. Prozessartefakte

Für das im Abschnitt 4.3.4 definierte Routingverfahren kann der Protokollaufruf zur Informationsabfrage wie folgt spezifiziert werden:

```
REQUEST INFORMATION <ConstraintTopology> <ConstraintProperties>
```

Dabei handelt es sich bei <CONSTRAINTTOPOLOGY> um die Angaben der zwei SCPs – einem Ausgangspunkt für weiteres Routing und einem Endpunkt, in dessen Richtung ein Weg gesucht wird. Die Beschreibung der Einschränkungen wurde im Abschnitt 4.6.4 als UML-Diagramme 4.48 und 4.49 definiert. Im Falle einer positiven Antwort sollen die zurückgeschickten Informationen entsprechend dem UML-Diagramm aus der Abbildung 4.50 strukturiert werden (für die zugehörige Beschreibung siehe Abschnitt 4.6.5).

Aktivität	Bezeichnung	Beschreibung	
A_1	REQUEST INFORMATION	*Input*	
		Tätigkeiten	• Start des Prozesses • Definition der Einschränkungen der benötigten Informationen • Abschicken der vorbereiteten Anfrage an die SP-Domain Providing Service
		Output	CONSTRAINTS
A_2	WAIT FOR RESPOND	*Input*	AVAILABLESERVICES
		Tätigkeiten	• Warten auf die Antwort der SP-Domain Providing Service • Abbruch bei Zeitüberschreitung
		Output	
A_3	CHECK CREDENTIALS OF SP REQUESTING SERVICE	*Input*	
		Tätigkeiten	• Überprüfen, ob die SP-Domain Requesting Service nach Domain-Policies zugelassen werden darf • Überprüfen, ob die Anfrage unterstützt wird • Treffen der Entscheidung
		Output	
A_4	PREPARE INFORMATION REGARDING CONSTRAINTS	*Input*	• CONSTRAINTS • DOMAIN DATA (SP-DOMAIN PROVIDING SERVICE)
		Tätigkeiten	Zusammenstellen der angefragten Informationen
		Output	REQUESTED INFORMATION
		Zeitvorgabe	Werden von SP-DOMAIN REQUESTING SERVICE spezifiziert
A_5	WAIT FOR NOTIFICATION	*Input*	• REFERENCEID • AVAILABLESERVICES
		Tätigkeiten	• Warten auf die Benachrichtigung von SP-Domain Providing Service • Abbruch bei Zeitüberschreitung
		Output	

Tabelle 5.3.: REQUEST INFORMATION – Aktivitäten

5.2.4. Globales Prozessmodell

Beide Versionen des Prozessablaufes sind in Abbildungen 5.5 und 5.6 dargestellt. Zunächst wird in diesem Abschnitt die synchrone Version für automatisierte Prozesse beschrieben und anschließend werden die Abweichungen davon bei dem entsprechenden asynchronen Prozess erläutert.

In beiden Fällen wird der Prozess von R_1 (*SP-Domain Requesting Service*) gestartet. Nachdem in Aktivität A_1 eine Informationsanfrage mit den entsprechenden Einschränkungen an R_2 (*SP-Domain Providing Service*) samt aller relevanten Einschränkungen geschickt wurde, wird in Aktion A_2 auf die zugehörige Antwort gewartet. Bei Zeitüber-

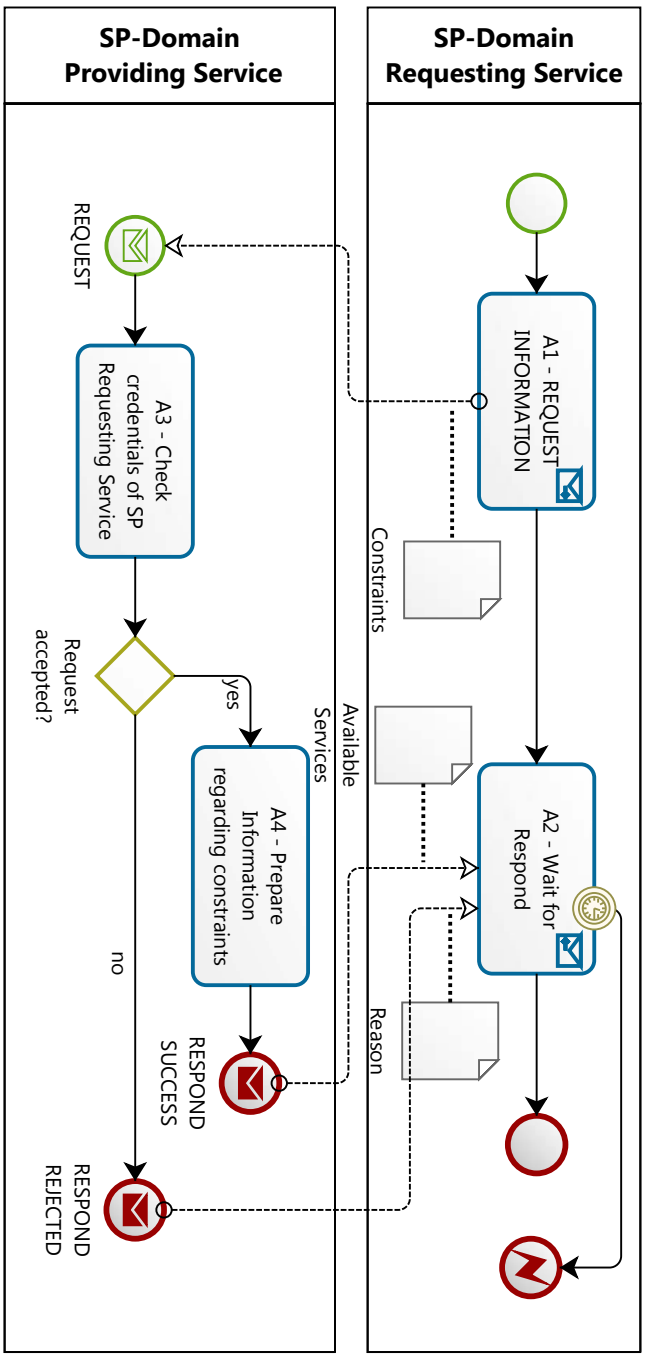


Abbildung 5.5.: REQUEST INFORMATION

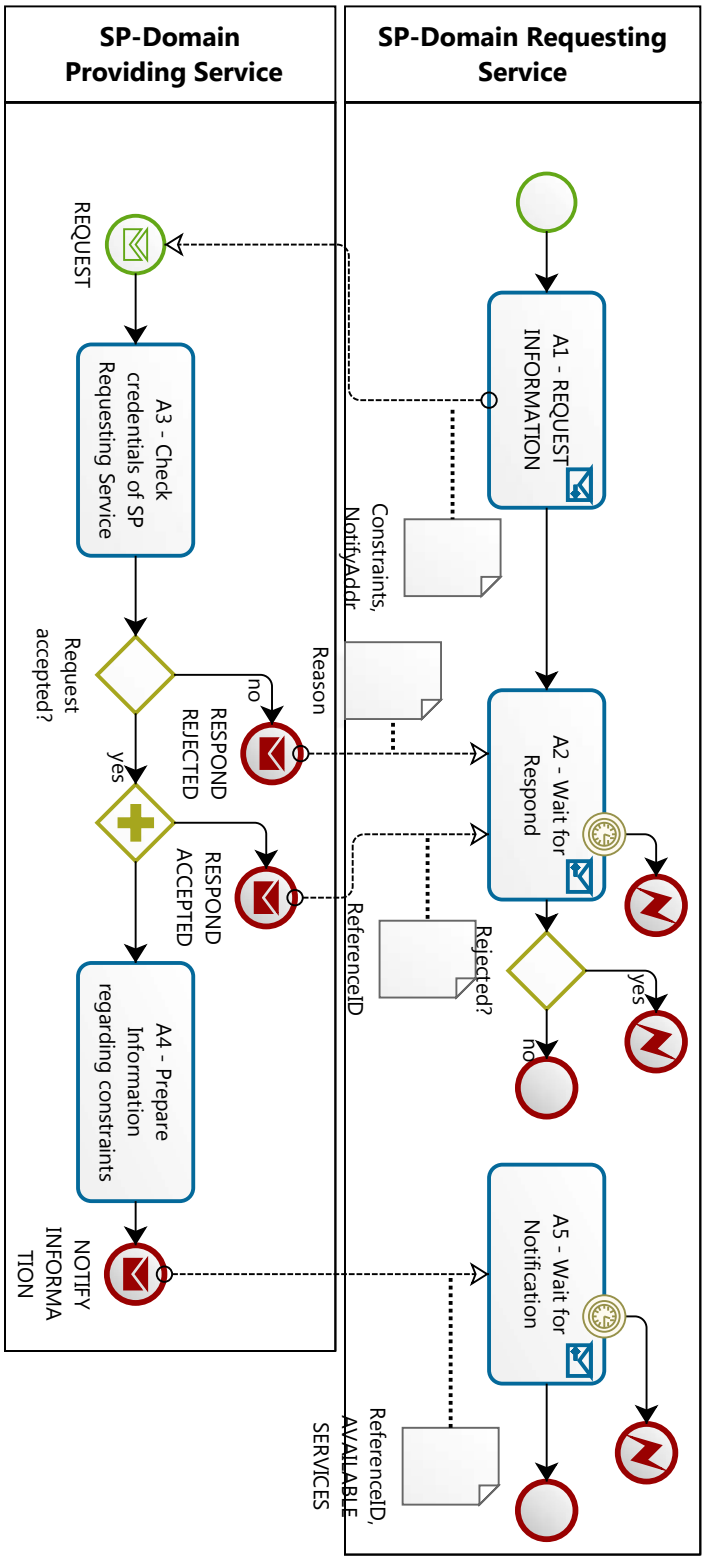


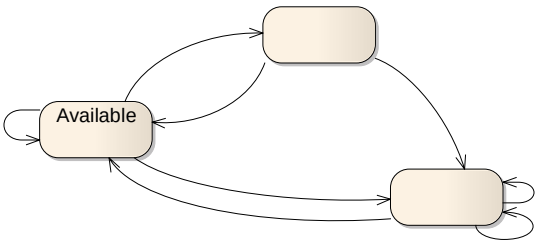
Abbildung 5.6.: REQUEST INFORMATION (Asynchron)

schreitung wird das Warten abgebrochen. Währenddessen wird von R_2 in der Aktion A_3 entschieden, ob die Anfrage akzeptiert oder zurückgewiesen werden soll. Sollte die Anfrage zurückgewiesen werden, wird das R_1 durch `RESPOND REJECTED` mitgeteilt. Ansonsten werden in A_4 die erforderlichen Informationen vorbereitet und mit `RESPOND SUCCESS` zurückgeschickt.

Bei der asynchronen Variante der Informationsabfrage (siehe Abbildung 5.6) werden die ersten drei Aktivitäten identisch ausgeführt. Sollte nach A_3 die Anfrage akzeptiert werden, dann wird zunächst eine Bestätigung `RESPOND ACCEPTED` zurückgeschickt. Diese Bestätigung wird mit einer REFERENCEID versehen, um die Benachrichtigungen zu unterschiedlichen Anfragen auseinanderhalten zu können. Danach wird in R_2 die Aktion A_4 ausgeführt und es werden die erforderlichen Informationen diesmal mit der Benachrichtigung (`NOTIFY INFORMATION`) an R_1 zurückgeschickt. Bei R_1 wird nach A_2 zunächst die Antwort ausgewertet. Soll die Anfrage zurückgewiesen werden, dann wird der Prozess gestoppt. Ansonsten wird in A_5 auf die Benachrichtigung mit den erforderlichen Informationen gewartet.

5.3. REQUEST SUBSCRIPTION

5.3.1. Einführung



Im Abschnitt 4.1.3 wurde diskutiert, dass u.U. eine automatische Benachrichtigung über die Veränderung der verfügbaren Kapazitäten sinnvoll sein kann. Diese Möglichkeit wird ausschließlich für direkt aneinander angeschlossene SP-Domänen eingeräumt, damit die Anzahl der Informationsanfragen reduziert wird. Ähnlich wie bei `REQUEST INFORMATION` können beim Abonnieren automatischer Benachrichtigungen verschiedene Einschränkungen der Informationen spezifiziert werden. Die Unterstützung der aktiven Benachrichtigung ist optional, da die benötigten Informationen auch mit `REQUEST INFORMATION` abgefragt werden können.

5.3.2. Aktivitäten

Tabelle 5.4 beschreibt alle Aktivitäten, die bei der Informationsabfrage benötigt werden.

5.3.3. Prozessartefakte

Genauso wie bei `REQUEST INFORMATION` erfolgt die Angabe der Eigenschafteneinschränkungen das UML-Diagramme gemäß der Spezifikation der UML-Diagramme in den Abbildungen 4.48 und 4.49 verwendet. Zusätzlich wird eine Adresse NotifyAddr spezifiziert, an die die abonnierten automatischen Benachrichtigungen mit `NOTIFY INFORMATION` (siehe Abschnitt 5.4) geschickt werden. Weitere Angaben sind nicht nötig, da durch die Akteure, die die Rollen *SP-Domain Requesting Service* und *SP-Domain Providing Service* einnehmen, implizit auch die relevanten Interdomain Verbindungen spezifiziert werden. Eine "Verfeinerung" anhand von SCP-IDs wird in dieser Arbeit absichtlich vermieden, da diese relativ geringfügige Informationseinschränkung einen wesentlich höhereren Managementaufwand erfordern würde.

Bei erfolgreichem Prozessablauf wird der SP-Domäne Requesting Service eine REFERENCEID mitgeteilt, die sowohl bei den abonnierten Benachrichtigungen als auch bei deren Abbestellung verwendet wird (siehe Abschnitte 5.4 und 5.5).

Aktivität	Bezeichnung	Beschreibung	
A_1	REQUEST SUBSCRIPTION	*Input*	
		Tätigkeiten	• Start des Prozesses • Definition der Einschränkungen auf die benötigte Informationen • Abschicken der vorbereiteten Anfrage an die SP-Domain Providing Service
		Output	
A_2	WAIT FOR RESPOND	*Input*	
		Tätigkeiten	• Warten auf die Antwort der SP-Domain Providing Service • Abbruch bei Zeitüberschreitung
		Output	
A_3	CHECK CREDENTIALS OF SP REQUESTING SERVICE	*Input*	
		Tätigkeiten	• Überprüfen, ob die SP-Domain Requesting Service nach Domain-Policies zugelassen werden darf • Überprüfen, ob die Anfrage unterstützt wird • Treffen Entscheidung
		Output	
A_4	UPDATE SUBSCRIBER LIST	*Input*	• CONSTRAINTS • NOTIFYADDR
		Tätigkeiten	• Aktualisieren der Benachrichtigung-Liste • Verbinden einer neuen ReferenceID mit dem Abonnement
		Output	REFERENCEID

Tabelle 5.4.: REQUEST SUBSCRIPTION – Aktivitäten

5.3.4. Globales Prozessmodell

Bei dem Prozessablauf sind die Aktivitäten A_1 bis A_3 identisch mit den entsprechenden Aktivitäten beim `REQUEST INFORMATION` (siehe Abschnitt 5.2.4). Nach A_3 wird allerdings eine zusätzliche Fallunterscheidung durchgeführt: falls die automatische Benachrichtigung vom *SP-Domain Providing Service* nicht unterstützt wird, wird das der anfragenden SP-Domäne durch `RESPOND FAILED` mitgeteilt. Ansonsten wird die Subscriber-Liste aktualisiert und die Bestätigung samt REFERENCEID mit `RESPOND SUCCESS` mitgeteilt.

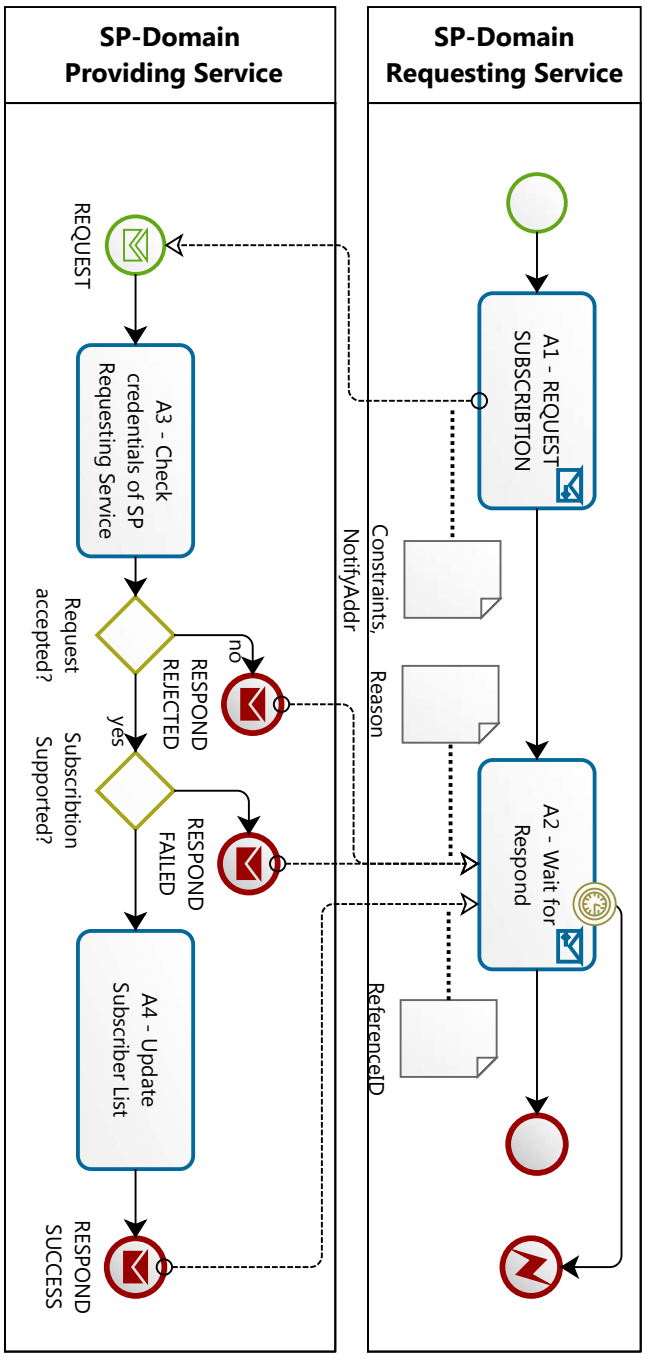
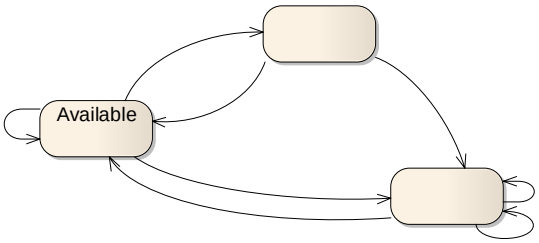


Abbildung 5.7.: REQUEST SUBSCRIPTION

5.4. NOTIFY INFORMATION

5.4.1. Einführung

Wenn die automatische Benachrichtigung abonniert wurde, können Veränderungen der freien Kapazitäten automatisch mitgeteilt werden. Die abonnierten Benachrichtigungen werden an die DSM-Adresse geschickt, die beim `REQUEST SUBSCRIPTION` als NotifyAddr spezifizierte wurde (siehe Abschnitt 5.3).



5.4.2. Aktivitäten

In Tabelle 5.5 sind alle für den Prozess relevanten Aktivitäten zusammengefasst.

Aktivität	Bezeichnung	Beschreibung	
A_1	CHECK SUBSCRIBTION LIST	*Input*	–
		Tätigkeiten	Überprüfe, ob die Veränderung der verfügbaren Kapazitäten einen oder mehrere Benachrichtigungsempfänger betrifft
		Output	
A_2	NOTIFY AFFECTED SUBSCRIBER	*Input*	–
		Tätigkeiten	Mitteilung an den Subscriber die relevanten Informationen
		Output	AVAILABLE COMPONENT LINK(S) INFORMATION
A_3	CORRELATE INFORMATION WITH OWN VIEW	*Input*	• AVAILABLE COMPONENT LINK(S) INFORMATION • DOMAIN DATA (SP-DOMAIN REQUESTING SERVICE)
		Tätigkeiten	Korrelieren der mitgeteilten und eigenen Teilsichten an die InterDomain Links
		Output	
A_4	STORE INFORMATION ABOUT IDLS	*Input*	
		Tätigkeiten	Abspeichern korrelierter Informationen
		Output	–

Tabelle 5.5.: NOTIFY INFORMATION – Aktivitäten

5.4.3. Prozessartefakte

Die automatisch mitgeteilten Informationen sollen, ähnlich wie bei `REQUEST INFORMATION` (siehe Abschnitt 5.2), entsprechend dem UML-Diagramm in Abbildung 4.50 strukturiert werden.

5.4.4. Globales Prozessmodell

Der Prozess für die automatische Benachrichtigung ist in Abbildung 5.8 dargestellt. Er wird gestartet, sobald bei einem oder mehreren *Interdomain Links* andere Verbindungseigenschaften erbracht werden können. Das kann z.B. der Fall sein, wenn eine neue Infrastruktur installiert wird oder nach der Auflösung einer existierenden Dienstinstanz neue Kapazitäten freigegeben wurden. Nach dem Eintreten des Ereignisses wird die Gesamtsituation in A_1 analysiert, ob dadurch ein oder mehrere Subscriber betroffen sind. Sollte das der Fall sein, werden in A_2 entsprechende Benachrichtigungen an die betroffenen Subscriber geschickt. Es können i.A. mehrere gleichzeitig gültige Abonnements existieren, die wiederum gleichzeitig betroffen sein können. Deswegen kann A_2 u.U. nicht nur eine, sondern eine Reihe von Benachrichtigungen versenden.

Die *SP-Domain Requesting Service* korreliert in A_3 die mitgeteilten Informationen mit der eigenen Sicht auf die Interdomain-Verbindungen (siehe dazu auch die entsprechenden Diskussion im Abschnitten 4.1.3 und 4.2.2). Die aggregierte Sicht kann anschließend in A_4 abgespeichert werden, sodass bei Informationsanfragen diese Information im Voraus vorhanden ist.

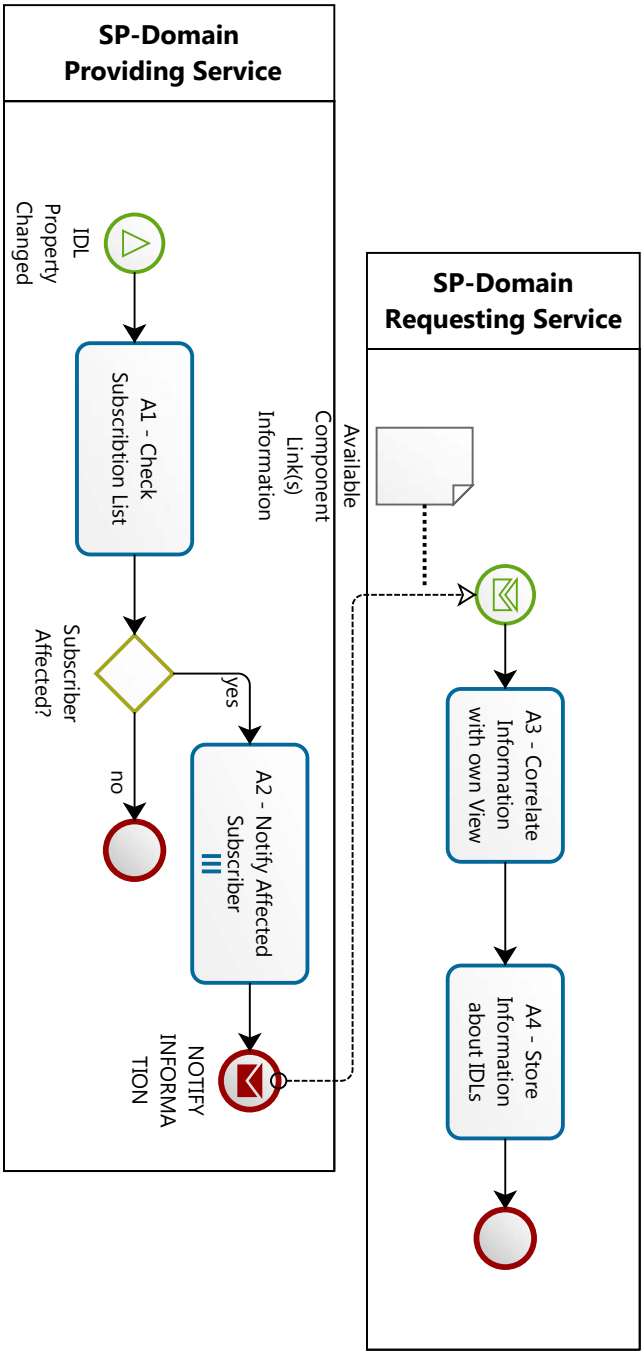
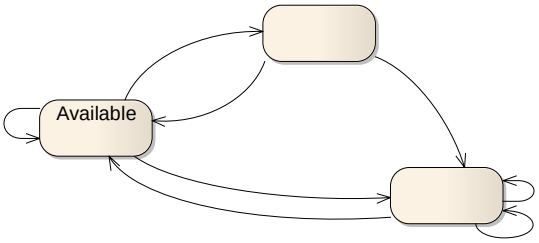


Abbildung 5.8.: NOTIFY INFORMATION

5.5. REQUEST CANCELSUBSCRIPTION

5.5.1. Einführung



Für den Fall, dass die automatische Benachrichtigung nicht mehr benötigt wird, muss auch eine entsprechende Signalisierungsmöglichkeit vorgesehen werden. Da eine SP-Domäne mehrere Benachrichtigungen abonnieren kann, die sich lediglich durch die spezifizierten Einschränkungen voneinander unterscheiden, wird beim Abbestellen auf die REFERENCEID der Bezug genommen.

5.5.2. Aktivitäten

In Tabelle 5.6 sind alle für den Prozess relevanten Aktivitäten zusammengefasst.

Aktivität	Bezeichnung	Beschreibung	
A_1	REQUEST CANCELSUBSCRIPTION	*Input*	
		Tätigkeiten	Abschicken der Anfrage für Subscription-Auflösung
		Output	
A_2	WAIT FOR RESPOND	*Input*	
		Tätigkeiten	• Warten auf die Antwort von SP-Domain Providing Service • Abbruch bei Zeitüberschreitung
		Output	
A_3	CHECK CREDENTIALS OF SP REQUESTING SERVICE	*Input*	• REFERENCEID • Subscription List (SP-Domain Providing Service)
		Tätigkeiten	• Überprüfen, ob die SP-Domain Requesting Service entsprechend den Domain-Policies zugelassen werden darf • Überprüfen, ob die ReferenceID-bezogene Anfrage der SP-Domain Requesting Service zulässig ist • Treffen einer Entscheidung
		Output	
A_4	CANCEL SUBSCRIPTION (USE REFERENCEID)	*Input*	REFERENCEID
		Tätigkeiten	Entfernen des Eintrags mit ReferenceID aus der Benachrichtigung-Liste
		Output	

Tabelle 5.6.: REQUEST CANCELSUBSCRIPTION – Aktivitäten

5.5.3. Prozessartefakte

Als Prozessartefakt wird bei diesem Prozess ausschließlich die REFERENCEID benötigt, die bei der korrespondierenden `REQUEST SUBSCRIPTION` Anfrage zurückgeliefert wurde (siehe Abschnitt 5.3).

5.5.4. Globales Prozessmodell

Beim Prozessablauf (siehe Abbildung 5.9) gibt es bei den ersten drei Aktivitäten lediglich eine kleine Abweichung von bereits beschriebenen Prozessen. In A_2 wird nicht nur die Berechtigung der *SP-Domain Requesting Service* überprüft, die Anfrage grundsätzlich zu stellen, sondern auch die Berechtigung, diese Anfrage in Bezug auf die spezifizierte REFERENCEID zu stellen. Erst wenn das der Fall ist, wird A_4 ausgeführt und die Subscriber-Liste aktualisiert.

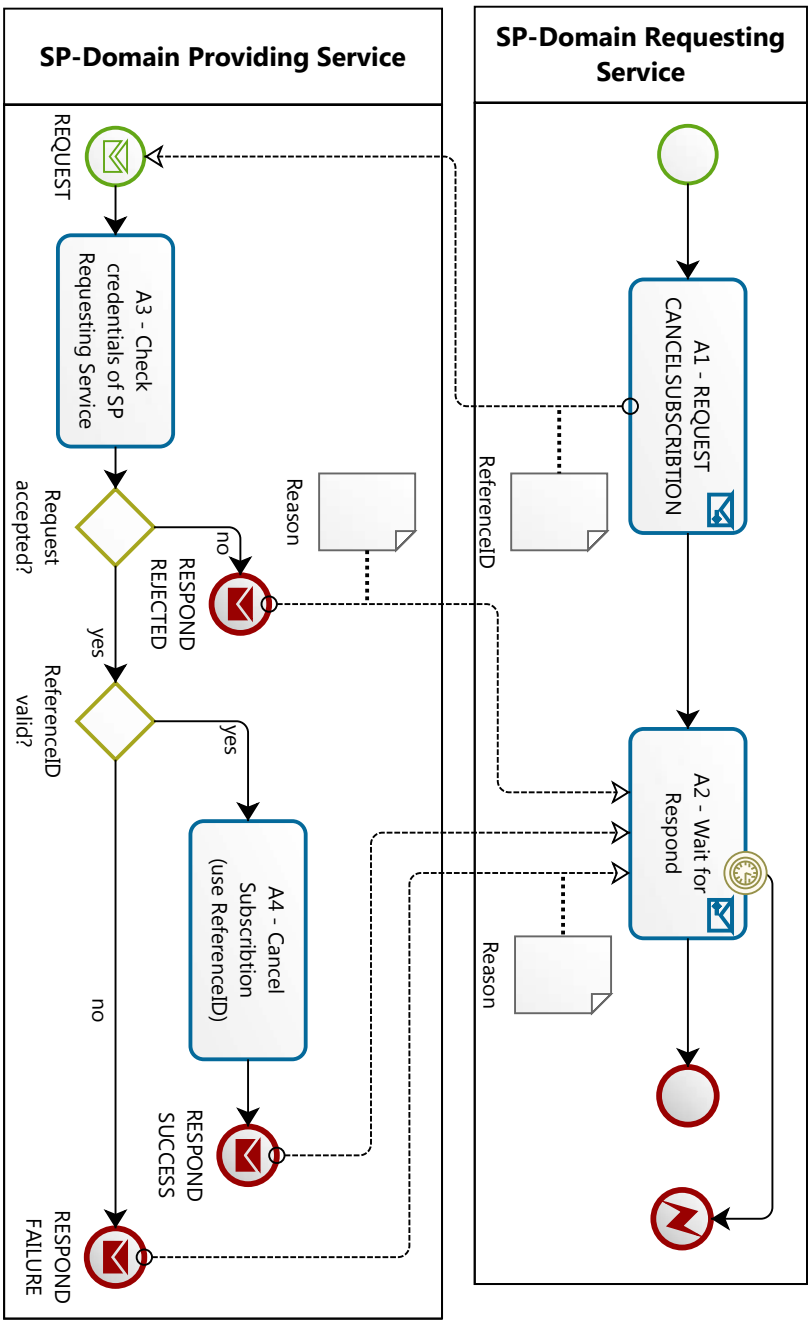
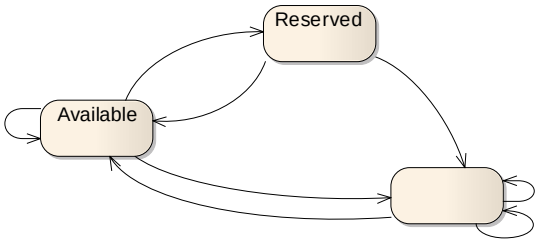


Abbildung 5.9.: REQUEST CANCELSUBSCRIPTION

5.6. REQUEST RESERVATION

5.6.1. Einführung

Bei einer Reservierung von Diensten handelt es sich um eine zeitlich begrenzte Reservierung der Ressourcen, die für die Diensterbringung mit den spezifizierten Eigenschaften erforderlich sind. Die Reservierung kann sich sowohl auf die Verbindungsdienste als auch auf die Multi-Domain Managementfunktionalität beziehen.



5.6.2. Aktivitäten

Alle für den Prozess relevanten Aktivitäten sind in den Tabellen 5.7 und 5.8 zusammengefasst.

Aktivität	Bezeichnung	Beschreibung	
A_1	REQUEST RESERVATION	*Input*	
		Tätigkeiten	• Start des Prozesses • Spezifikation der Einschränkungen, die die reservierten Dienste aufweisen sollen • Abschicken der vorbereiteten Anfrage an die SP-Domain Providing Service
		Output	
A_2	WAIT FOR RESPOND	*Input*	
		Tätigkeiten	• Warten auf die Antwort der SP-Domain Providing Service • Abbruch bei Zeitüberschreitung
		Output	
A_3	CHECK CREDENTIALS OF SP REQUESTING SERVICE REQUEST INFORMATION	*Input*	
		Tätigkeiten	• Überprüfen, ob die SP-Domain Requesting Service entsprechend der Domain-Policies zugelassen werden darf • Überprüfen, ob die Anfrage unterstützt wird • Treffen einer Entscheidung
		Input	

Tabelle 5.7.: REQUEST RESERVATION – Aktivitäten (1/2)

Aktivität	Bezeichnung	Beschreibung	
A_4	TEMPORARY RESERVE INFRASTRUCTURE REQUIRED FOR CONNECTION SERVICE	*Input*	• E2ELINKID • TOPOLOGYSPECIFIER • REQUESTEDPROPERTIES • DOMAIN DATA (SP-DOMAIN PROVIDING SERVICE)
		Tätigkeiten	• Reservierung von Ressourcen, die für die Erbringung des Verbindungsdienstes mit den angefragten Eigenschaften benötigt werden. Die Erfüllung der Einschränkungen ist nicht obligatorisch • Generierung einer neuen eindeutigen REFERENCEID • Assoziation der reservierten Ressourcen mit E2ELINKID und ReferenceID
		Output	• REFERENCEID • CONFIRMEDPROPERTIES (inklusive RESERVATIONTIME)
A_5	TEMPORARY RESERVE INFRASTRUCTURE REQUIRED FOR MD-MGMT. SERVICE	*Input*	• E2ELINKID • REQUESTEDPROPERTIES • DOMAIN DATA (SP-DOMAIN PROVIDING SERVICE)
		Tätigkeiten	• Reservierung der Ressourcen, die für die Erbringung des Multi-Domain Managementdienstes mit den angefragten Eigenschaften benötigt werden. Die Erfüllung der Einschränkungen ist nicht obligatorisch • Generierung einer neuen eindeutigen REFERENCEID Assoziation der reservierten Ressourcen mit E2ELINKID und ReferenceID
		Output	• REFERENCEID • CONFIRMEDPROPERTIES (inklusive RESERVATIONTIME)
A_6	NOTIFY: REQUESTED SERVICE NOT SUPPORTED	*Input*	
		Tätigkeiten	Benachrichtige SP-DOMAIN REQUESTING SERVICE, dass der angefragte Dienst nicht unterstützt wird
		Output	
A_7	START RESERVATION TIMER	*Input*	
		Tätigkeiten	Starte Timer, nach dessen Ablauf die reservierten Ressourcen freigegeben werden
		Output	
A_8	FREE RESERVED RESSOURCES	*Input*	
		Tätigkeiten	Aufheben der Ressourcenreservierung nach Ablauf der definierten Zeit
		Input	

Tabelle 5.8.: REQUEST RESERVATION – Aktivitäten (2/2)

5.6.3. Prozessartefakte

Bei der Anfrage für die Reservierung werden zunächst E2ELINKID und SERVICETYPEID spezifiziert. Die E2ELINKID wird benötigt, um den Bezug zu einer Dienstinstanz herstellen zu können, sie wird auch für die Verbindung einzelner Teildienste derselben Dienstinstanz benötigt. Die SERVICETYPEID signalisiert die benötigte Dienstart sowie bestimmt weitere Qualifizierungsparameter der Reservierungsanfrage.

Die Reservierung wird für den Verbindungsdienst (SERVICETYPEID nimmt in diesem Fall den Wert CONNECTION ein) und den Multi-Domain Managementdienst (SERVICETYPEID nimmt den Wert MDSERVICE ein) unterstützt. Im ersten Fall – bei CONNECTION-Service – werden zwei SCPs der erwünschten Verbindung sowie die Spezifikation der erwünschten Verbindungseigenschaften angegeben. Alternativ dazu kann eine ID des erwünschten *Component Links* angegeben werden, der diese zwei SCPs verbindet. Diese ID kann der Antwort auf die Informationsanfrage entnommen werden (siehe dazu auch Abschnitt 5.4). Die Angabe der Verbindungseigenschaften wird entsprechend dem UML-Diagramm aus der Abbildung 4.51 durchgeführt, wodurch sowohl die Dienstgüteeigenschaften als auch die mit der Verbindung assoziierte Single-Domain Managementfunktionalität spezifiziert werden kann. Bei MDSERVICE-Anfrage können die relevanten Eigenschaften wiederum entsprechend dem UML-Diagramm aus der Abbildung 4.51 durchgeführt werden.

Bei einer erfolgreichen Ressourcenreservierung werden die REFERENCEID und die RESERVEDPROPERTIES zurückgeliefert. Die REFERENCEID ist nötig, um zwischen unterschiedlichen Teildiensten ein und desselben E2ELinks (z.B. *Domain-* und *Interdomain Links*) zu unterscheiden. Diese können bei `REQUEST CANCELRESERVATION` (siehe Abschnitt 5.7) und `REQUEST RESERVEDSERVICE` (siehe Abschnitt 5.8) angesprochen werden. Die Mitteilung der reservierten Diensteigenschaften wird entsprechend dem UML-Diagramm aus der Abbildung 4.52 durchgeführt werden. Bei der Reservierung wird dabei auch die Reservierungsdauer (siehe Klasse RESERVATIONTIME in Abbildung 4.52) mitgeteilt. Die Reservierungszeit bestimmt, für wie lange die Reservierung erhalten bleibt.

Die Mitteilung von ReservedProperties ist notwendig, weil die *SP-Domain Providing Service* bei der Reservierung schlechtere Eigenschaften als die angefragten zusichern darf (vergleiche entsprechende Diskussionen und Festlegungen in Abschnitten 3.2 und 5.1).

5.6.4. Globales Prozessmodell

Der mit `REQUEST RESERVATION` verbundene globale Prozess ist in Abbildung 5.10 dargestellt. Der Ablauf der ersten drei Aktivitäten folgt dem üblichen Muster. Nachdem

die Anfrage zugelassen wurde, wird anhand der SERVICETYPEID entschieden, welche der Aktivitäten A_4, A_5 oder A_6 ausgeführt werden muss. Die Aktivität A_6 dient ausschließlich zur Benachrichtigung, dass SERVICETYPEID ungültig ist. Bei A_4 und A_5 wird nach Abarbeitung zunächst überprüft, ob die durchgeführte Reservierungsaktion erfolgreich war oder nicht. Falls nicht, wird das der *SP-Domain Requesting Service* durch `RESPOND FAILED` mitgeteilt. Ansonsten wird vor der `RESPOND SUCCESS` Benachrichtigung in der Aktion A_7 der Reservierung-Timer gestartet. Sollte vor dem Ablauf des Timers weder eine explizite Freigabe reservierter Ressourcen (siehe Abschnitt 5.7) noch deren Bestellung für die Dienstinstanz (siehe Abschnitt 5.8) erfolgen, werden diese Ressourcen in der Aktion A_8 ohne weitere Benachrichtigung freigegeben.

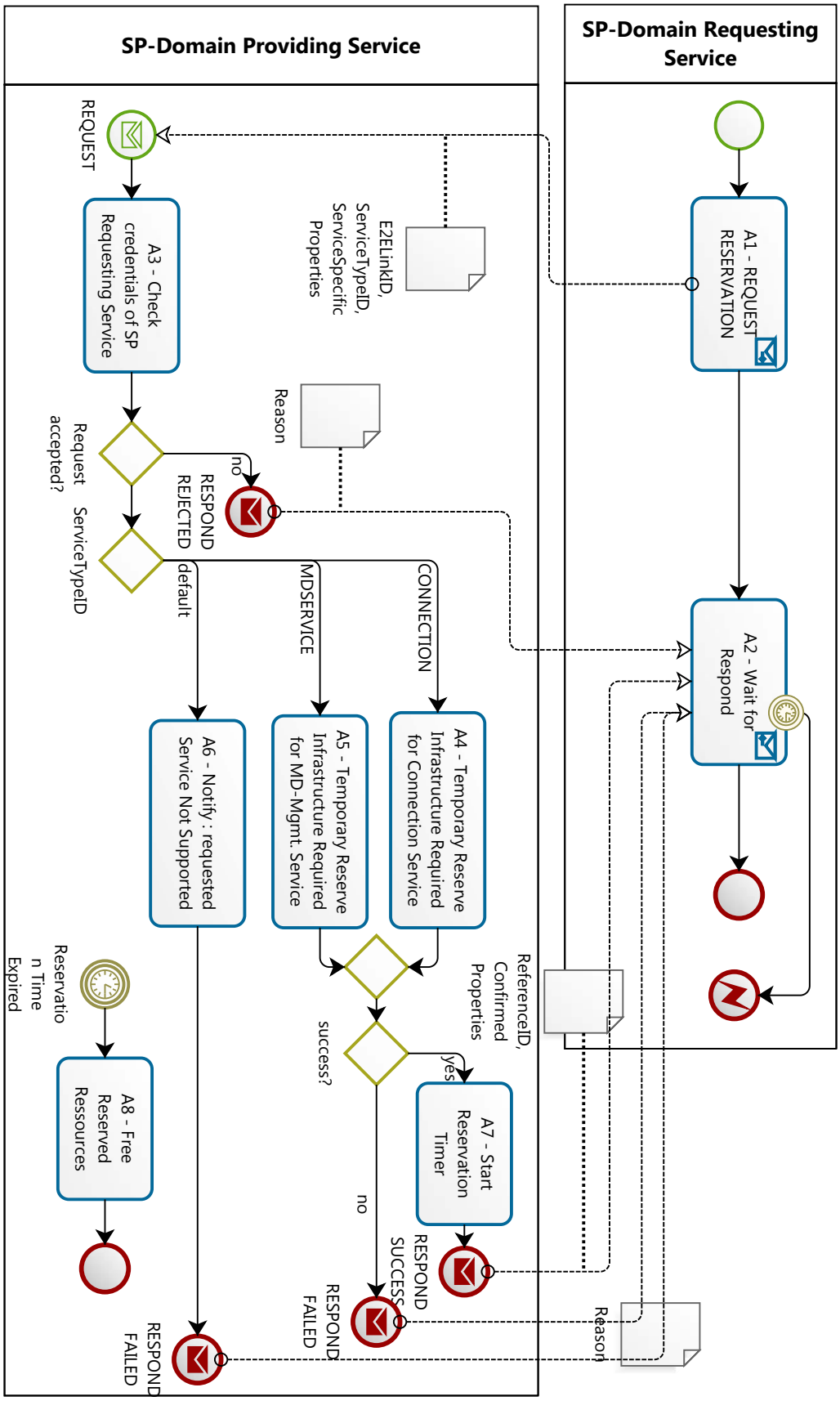
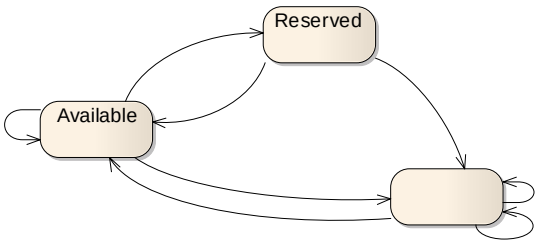


Abbildung 5.10.: REQUEST RESERVATION

5.7. REQUEST CANCELRESERVATION

5.7.1. Einführung



Insbesondere beim Routing können Situationen entstehen, dass bereits reservierte Teildienste nicht mehr benötigt werden. Obwohl bei der Reservierung (siehe Abschnitt 5.6) eine implizite Freigabe der Ressourcen nach dem Zeitablauf vorgesehen wurde, kann das u.U. Störeinflüsse und gegenseitige Behinderungen zwischen den nebenläufigen Multi-Domain Prozessen verursachen. Um die Störeinflüsse zu minimieren, wird hier die Möglichkeit einer expliziten Freigabe definiert.

5.7.2. Aktivitäten

Alle prozessrelevanten Aktivitäten sind in der der Tabelle 5.9 zusammengefasst.

Aktivität	Bezeichnung	Beschreibung	
A_1	REQUEST CANCELRESERVATION	*Input*	
		Tätigkeiten	Abschicken der expliziten Anfrage für die Freigabe von reservierten Ressourcen
		Output	
A_2	WAIT FOR RESPOND	*Input*	
		Tätigkeiten	• Warten auf die Antwort der SP-Domain Providing Service • Abbruch bei Zeitüberschreitung
		Output	
A_3	CHECK CREDENTIALS OF SP REQUESTING SERVICE	*Input*	• REFERENCEID • RESERVIERUNGSINFORMATIONEN (SP-DOMAIN PROVIDING SERVICE)
		Tätigkeiten	• Überprüfen, ob die SP-Domain Requesting Service entsprechend der Domain-Policies zugelassen werden darf • Überprüfen, ob die ReferenceID-bezogene Anfrage der SP-Domain Requesting Service zulässig ist • Treffen einer Entscheidung
		Output	
A_4	CANCEL RESERVATION (USE REFERENCEID)	*Input*	REFERENCEID
		Tätigkeiten	Freigabe der Ressourcen, die mit ReferenceID assoziiert wurden
		Output	

Tabelle 5.9.: REQUEST CANCELRESERVATION – Aktivitäten

5.7.3. Prozessartefakte

Als Prozessartefakt wird bei diesem Prozess ausschließlich die REFERENCEID benötigt, die bei der korrespondierenden `REQUEST RESERVATION` Anfrage zurückgeliefert wurde (siehe Abschnitt 5.6).

5.7.4. Globales Prozessmodell

Der Prozess in Abbildung 5.11 läuft ähnlich wie bei `REQUEST CANCELSUBSCRIPTION` ab (vergleiche Abschnitt 5.5). Lediglich wird bei Aktivität A_2 statt der Liste der abonnierten Benachrichtigungen die Liste der reservierten Ressourcen aktualisiert.

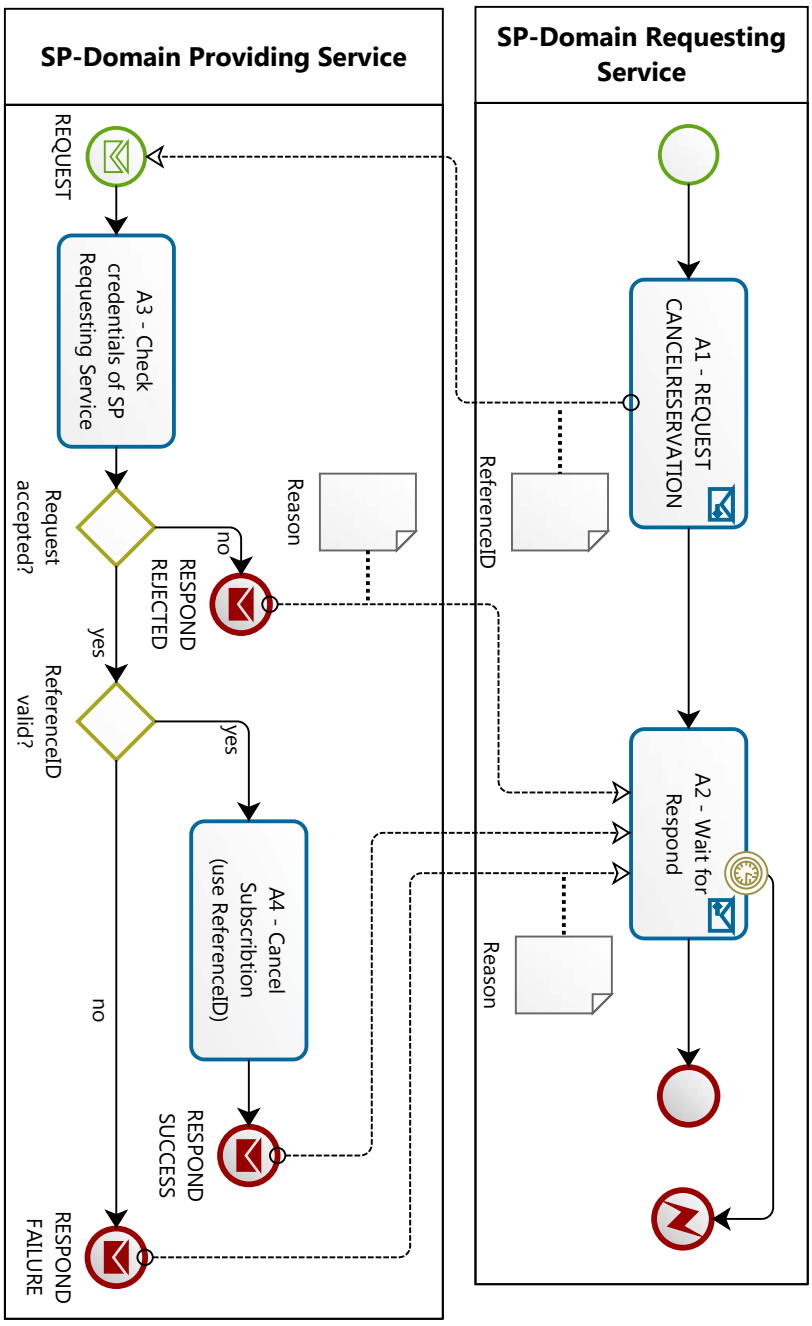
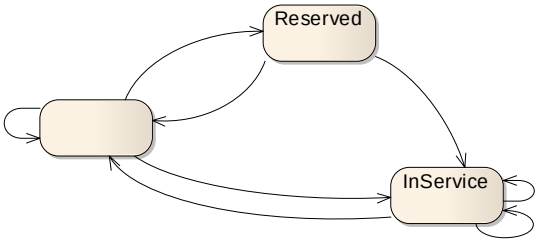


Abbildung 5.11.: REQUEST CANCELRESERVATION

5.8. REQUEST RESERVEDSERVICE

5.8.1. Einführung



Solange die Reservierungszeit nicht abgelaufen ist, können reservierte Teildienste endgültig bestellt werden. Die bei der Reservierung (siehe Abschnitt 5.6) zugesicherten Eigenschaften können dabei als garantiert betrachtet werden. Der SP-Domain Requesting Service wird die Möglichkeit eingeräumt, bei der Bestellung die endgültigen Anforderungen an die Teildienste zu korrigieren.

5.8.2. Aktivitäten

In Tabelle 5.10 sind alle für den Prozess relevanten Aktivitäten zusammengefasst.

5.8.3. Prozessartefakte

Die Anfrage für die Bestellung des zuvor reservierten Dienstes bezieht sich auf die REFERENCEID, die zuvor bei der korrespondierenden `REQUEST RESERVATION` Anfrage zurückgeliefert wurde (siehe Abschnitt 5.6). Dem *SP-Domain Requesting Service* wird die Möglichkeit eingeräumt, die bei der Reservierung zugesicherten Werte noch mal "nach unten" zu korrigieren. Die endgültigen Anforderungen werden genauso wie bei der Reservierung entsprechend dem UML-Diagramm aus der Abbildung 4.51 strukturiert. Die Einhaltung der endgültigen REQUESTEDPROPERTIES ist für den *SP-Domain Providing Service* verpflichtend und darf lediglich verbessert werden (vergleiche entsprechende Diskussionen und Festlegungen in den Abschnitten 3.2 und 5.1).

Sollte die Bestellung eines reservierten Dienstes erfolgreich durchgeführt werden, erfolgt eine Bestätigung mit dem `RESPOND SUCCESS`. Dabei wird der *SP-Domain Requesting Service* eine REFERENCEID sowie die endgültig zugesicherten Eigenschaften mitgeteilt. Um die interne Verwaltung der *SP-Domain Providing Service* zu vereinfachen, kann sich die REFERENCEID eines bestellten Dienstes i.A. von der REFERENCEID eines reservierten Dienstes unterscheiden. Die Einhaltung der endgültig zugesagten Diensteigenschaften CONFIRMEDPROPERTIES ist für die SP-Domain Providing Properties verpflichtend. Die Eigenschaften sollen – ähnlich wie bei `REQUEST RESERVATION` – entsprechend dem UML-Diagramm aus der Abbildung 4.52 spezifiziert werden.

Aktivität	Bezeichnung	Beschreibung	
A_1	REQUEST RESERVEDSERVICE	*Input*	
		Tätigkeiten	Abschicken der Anfrage für die Bestellung des reservierten Dienstes
		Output	
A_2	WAIT FOR RESPOND	*Input*	
		Tätigkeiten	• Warten auf die Antwort der SP-Domain Providing Service • Abbruch bei Zeitüberschreitung
		Output	
A_3	CHECK CREDENTIALS OF SP REQUESTING SERVICE	*Input*	• REFERENCEID • RESERVATION LIST (SP-DOMAIN PROVIDING SERVICE)
		Tätigkeiten	• Überprüfen, ob die SP-Domain Requesting Service entsprechend der Domain-Policies zugelassen werden darf • Überprüfen, ob die ReferenceID-bezogene Anfrage der SP-Domain Requesting Service zulässig ist • Treffen einer Entscheidung
		Input	
A_4	CANCEL TEMPORARY RESSOURCE RESERVATION TIMER	*Input*	REFERENCEID
		Tätigkeiten	Einstellen des Freigabetimers für die reservierten Ressourcen
		Output	–
A_5	RESERVE REQUIRED INFRASTRUCTURE FOR SERVICE-TIME	*Input*	• REFERENCEID • REQUESTEDPROPERTIES
		Tätigkeiten	• Reservieren der Ressourcen für die Dienstinstanz • Verbinden (zusammenschalten) einzelner aneinander angeschlossenen Teildienste derselben E2E-Dienstinstanz
		Output	• REFERENCEID • CONFIRMEDPROPERTIES

Tabelle 5.10.: REQUEST RESERVEDSERVICE – Aktivitäten

5.8.4. Globales Prozessmodell

Der Prozessablauf der ersten drei Aktivitäten folgt dem üblichen Muster. Nachdem die Anfrage und REFERENCEID validiert wurden, wird in A_4 der Timer gestoppt und in der darauffolgenden Aktivität A_5 die für die Diensterbringung benötigte Infrastruktur der Dienstinstanz zugewiesen und in Betrieb genommen. Sollte es sich um einen Verbindungsdienst handeln, dann werden die aneinander angeschlossenen Teildienste einer Dienstinstanz zusammengeschaltet. Bei erfolgreicher Durchführung werden die endgültig zugesicherten Diensteigenschaften an die *SP-Domain Requesting Service* mit `RESPOND SUCCESS` gemeldet, ansonsten wird mit `RESPOND FAILED` die Ursache für das Fehlschlagen mitgeteilt.

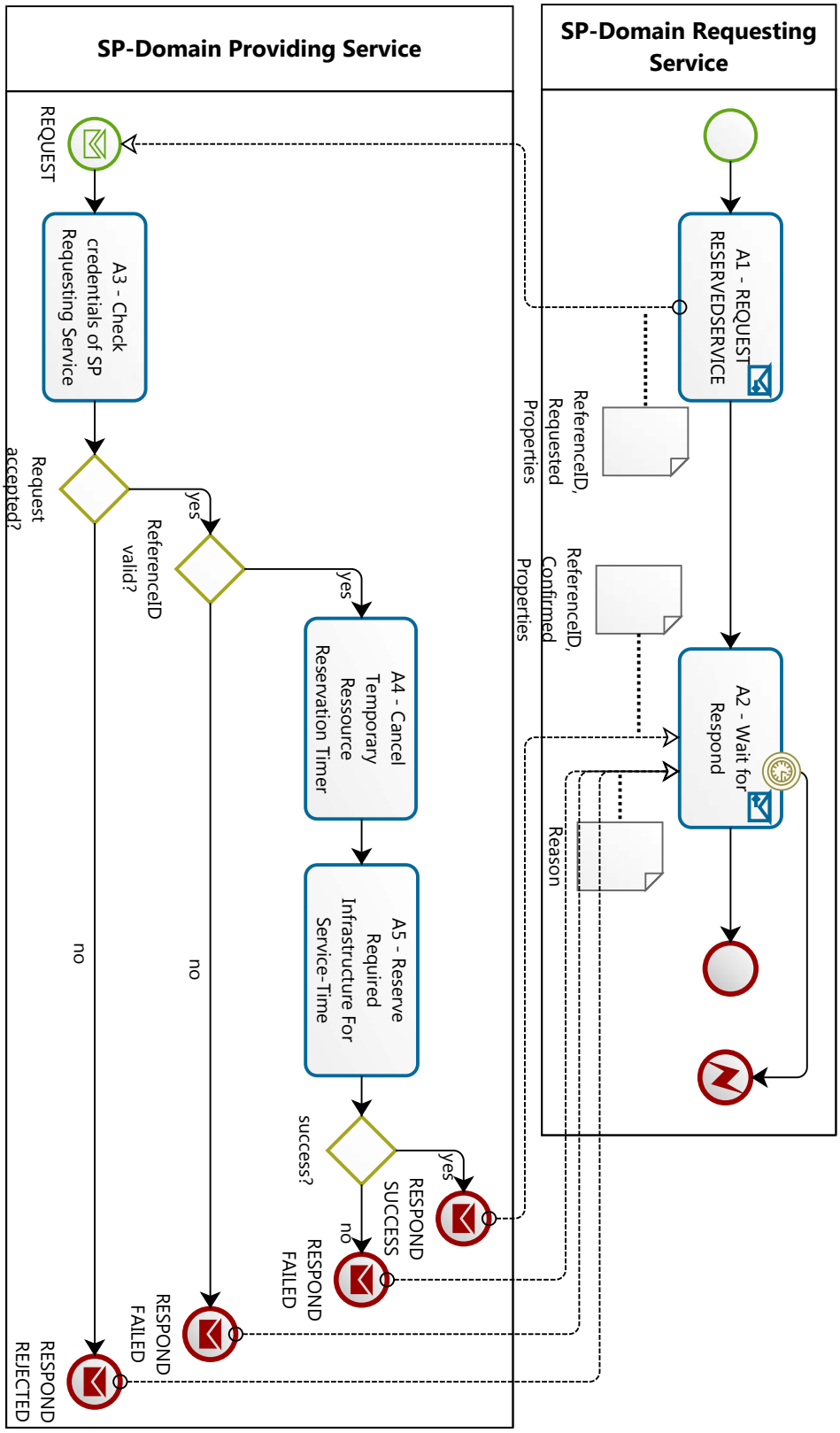
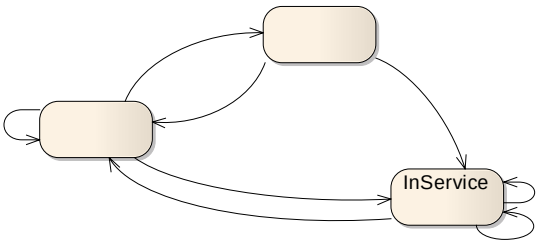


Abbildung 5.12.: REQUEST RESERVEDSERVICE

5.9. REQUEST CHANGE

5.9.1. Einführung



Es gibt grundsätzlich zwei Möglichkeiten, im Betrieb die Diensteigenschaften zu verändern. Es können ein oder mehrere Teildienste einer Dienstinstanz durch neue Teildienste mit den entsprechend den Anforderungen angepassten Eigenschaften ersetzt werden, oder es können die Eigenschaften bereits existierender Teildienste verändert werden. Die erste Variante erfordert zwar komplexere Multi-Domain Managementprozesse, ist allerdings so gut wie immer möglich, da sie ausschließlich die der Dienstbestellung und -Abbestellung beruht. Bei der zweiten Variante wird die Komplexität in den *SP-Domain Providing Service* verlagert. Diese Variante kann allerdings nicht von allen SPs unterstützt werden, weswegen die Anfrage auch zurückgewiesen werden darf.

5.9.2. Aktivitäten

In Tabelle 5.11 sind alle für den Prozess relevanten Aktivitäten zusammengefasst.

5.9.3. Prozessartefakte

Die Change-Anfrage bezieht sich immer auf den Dienst mit der REFERENCEID, die bei den Anfragen `REQUEST RESERVEDSERVICE` (siehe Abschnitt 5.8) oder `REQUEST SERVICE` (siehe Abschnitt 5.13) zurückgeschickt wurde. Die Angabe neuer Anforderungen geschieht ähnlich wie bei den o.g. Dienstanfragen nach dem UML-Diagramm aus der Abbildung 4.51. Der Parameter TIMELIMIT schränkt die maximale Ausführungszeit der angefragten Operation ein.

Die erfolgreiche Veränderung der Diensteigenschaften wird mit `RESPOND SUCCESS` signalisiert. Dabei werden auch i.A. eine neue REFERENCEID sowie die zugesicherten Eigenschaften ConfirmedProperties zurückgeschickt. Die letzteren werden wiederum entsprechend dem UML-Diagramm 4.52 strukturiert.

Aktivität	Bezeichnung	Beschreibung	
A_1	REQUEST CHANGE	*Input*	
		Tätigkeiten	Abschicken der Anfrage für die Veränderung der Diensteigenschaften im Betrieb
		Output	
A_2	WAIT FOR RESPOND	*Input*	
		Tätigkeiten	• Warten auf die Antwort der SP-Domain Providing Service • Abbruch bei Zeitüberschreitung
		Output	
A_3	CHECK CREDENTIALS OF SP REQUESTING SERVICE	*Input*	• REFERENCEID • DOMAIN DATA (SP-DOMAIN PROVIDING SERVICE)
		Tätigkeiten	• Überprüfen, ob die SP-Domain Requesting Service nach Domain-Policies zugelassen werden darf • Überprüfen, ob die ReferenceID-bezogene Anfrage der SP-Domain Requesting Service zulässig ist • Treffen einer Entscheidung
		Input	
A_4	PERFORM REQUESTED CHANGES	*Input*	• REFERENCEID • REQUESTEDPROPERTIES • DOMAIN DATA (SP-DOMAIN PROVIDING SERVICE)
		Tätigkeiten	• Verändern der Diensteigenschaften in eigener Domäne • Aktualisieren der relevanten DOMAIN DATA
		Output	• REFERENCEID • CONFIRMEDPROPERTIES
A_5	CALCULATE NEW PROPERTIES FOR SERVICEPARTS	*Input*	• REFERENCEID • REQUESTEDPROPERTIES • DOMAIN DATA (SP-DOMAIN PROVIDING SERVICE)
		Tätigkeiten	Berechnen der neuen erforderlichen Eigenschaften für alle Teildienste, für die die Verantwortung an die SP-Domain Providing Service delegiert wurde
		Output	REQUESTEDPROPERTIES (PRO INVOLVED SERVICE-PART)
A_6	REQUEST CHANGE (TO FURTHER SPS PROVIDING SERVICE)	*Input*	• REFERENCEID (SERVICE-PART SPECIFIC) • REQUESTEDPROPERTIES (SERVICE-PART SPECIFIC)
		Tätigkeiten	• Senden REQUEST CHANGE Anfrage an alle beteiligten SP-Domains • Warten auf die Antwort
		Output	• CONFIRMEDPROPERTIES (PRO INVOLVED SERVICE-PART)
A_7	REQUEST CHANGE (TO PROXY-SP)	*Input*	• REFERENCEID (PROXY-SP SPECIFIC) • REQUESTEDPROPERTIES (PROXY-SP SPECIFIC)
		Tätigkeiten	• Rausschicken REQUEST CHANGE Anfrage an Proxy-SP • Warten auf die Antwort
		Output	• CONFIRMEDPROPERTIES (PROXY-SP SPECIFIC)
A_8	CALCULATE OVERALL CONFIRMED PROPERTIES	*Input*	REQUESTEDPROPERTIES (ONE PRO EVERY SERVICE-PART)
		Tätigkeiten	Berechne Zusicherung für eigenen Verantwortungsbereich
		Output	REQUESTEDPROPERTIES (AGGREGATED FOR ALL PARTS)

Tabelle 5.11.: REQUEST CHANGE – Aktivitäten

5.9.4. Globales Prozessmodell

Der Prozessablauf ist in Abbildung 5.13 dargestellt. Der Ablauf bei den ersten drei Aktivitäten wird leicht verändert, da die Unterstützung der Dienstanpassung im Betrieb nicht obligatorisch ist. Sollte die *SP-Domain Providing Service* diese Funktionalität nicht unterstützen, wird das mit `RESPOND FAILED` der anfragenden Domäne mitgeteilt.

Wenn die Funktionalität unterstützt und die Anfrage in A_3 akzeptiert wurde, wird unterschieden, ob die *SP-Domain Providing Service* als ein Diensterbringer oder als ein Proxy fungiert (siehe ausführliche Diskussionen über Delegation im Abschnitt 4.3 sowie die Delegationsanfrage in Abschnitt 5.13). Wenn die *SP-Domain Providing Service* als Diensterbringer agiert, wird in A_4 die erforderliche Anpassung des eigenen Teildienstes durchgeführt. Ansonsten werden zunächst in A_5 die in REQUESTEDPROPERTIES mitgeteilten neuen Anforderungen auf die Teildienste der anderen Service Provider abgebildet. Danach wird eine `REQUEST CHANGE` Anfrage in A_6 und A_7 an alle Provider dieser Teildienste geleitet, wodurch eine Rekursion des Prozessablaufes entsteht. Zwischen diesen zwei Aktivitäten wird lediglich aus semantischen Gründen unterschieden, um zu betonen, dass in einem Fall mit dem Erbringer der Teildienste und in anderem mit der Proxy-SP kommuniziert wird. Nach dem Eingang der Antworten von SPs aller Teildienste kann in A_8 ein Zusage-Wert für den Verantwortungsbereich berechnet werden. Wenn bei allen Teildiensten die Veränderung erfolgreich durchgeführt wurde, wird CommittedProperty zusammen mit einer i.A. neuen REFERENCEID als Teile der `RESPOND SUCCESS` Antwort zurückgeschickt. Ansonsten wird das Fehlschlagen mit `RESPOND FAILED` mitgeteilt.

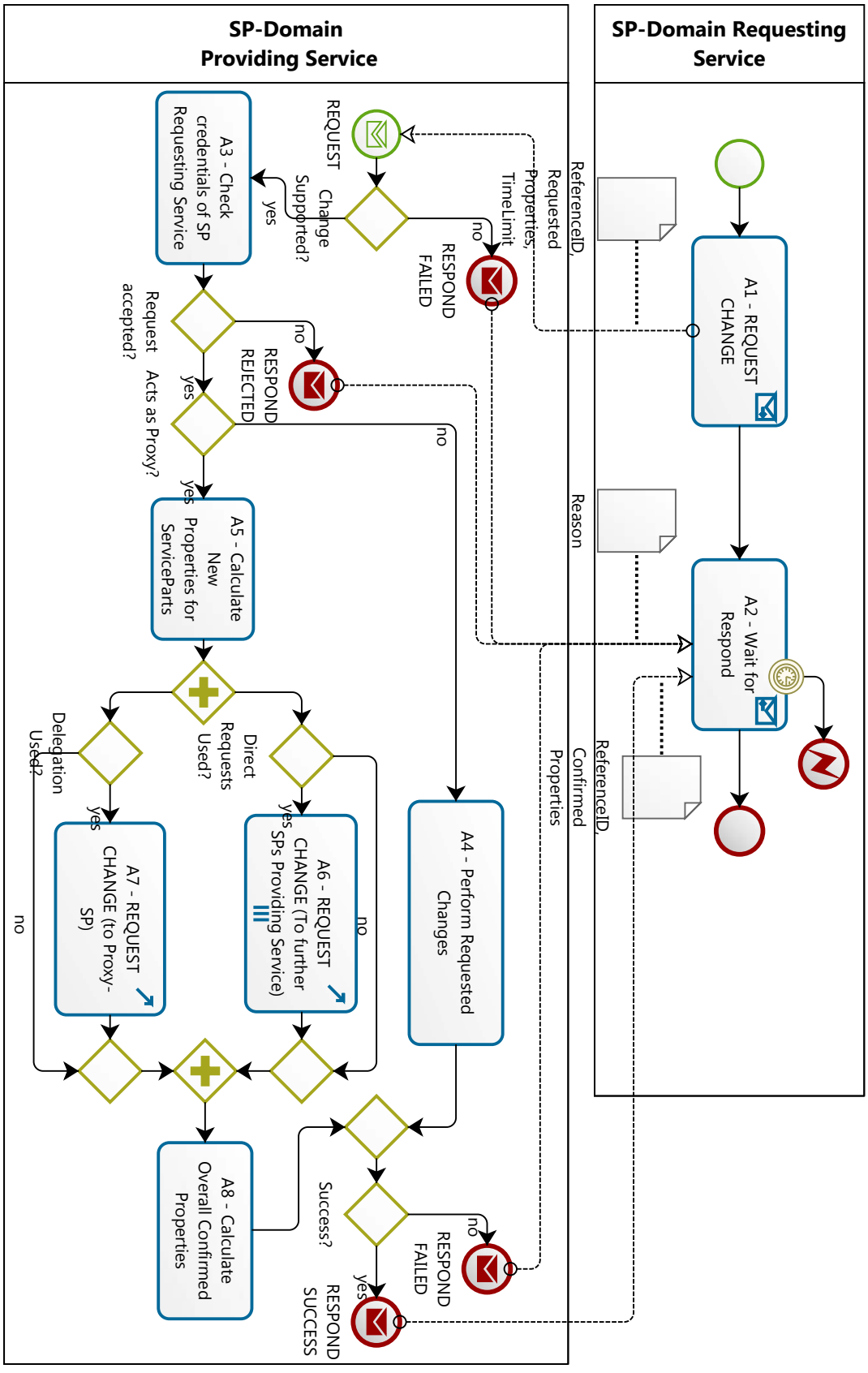
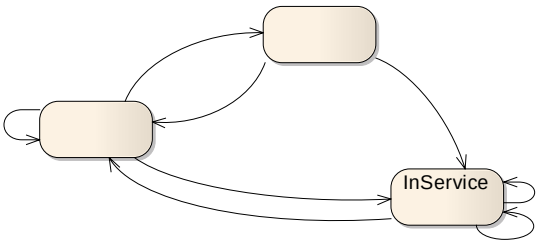


Abbildung 5.13.: REQUEST CHANGE

5.10. REQUEST MGMTFCT

5.10.1. Einführung



Während `REQUEST CHANGE` die vereinbarten Parameter eines Dienstes verändert, wird mit Hilfe der Anfrage `REQUEST MGMTFCT` auf die Managementfunktionalität eines Dienstes innerhalb vereinbarter Parameter zugegriffen. Bei einem Verbindungsdienst handelt es sich zumeist um die Abfrage von Monitoring-Informationen, bei einem Multi-Domain Managementdienst wie z.B. ROUTING-Dienst kann dabei auf unterschiedliche Funktionen wie "Route Finden", "Route Reservieren" und "Route Bestellen" zugegriffen werden (mehr dazu siehe im Kapitel 6). Der in diesem Abschnitt beschriebene Prozess kann als ein Template angesehen werden, der für die unterschiedlichen Managementfunktionen weiter verfeinert wird.

5.10.2. Aktivitäten

In Tabelle 5.12 sind alle für den Prozess relevanten Aktivitäten zusammengefasst.

5.10.3. Prozessartefakte

Bei dem Aufruf werden drei Kommunikationsartefakte benötigt. Die ersten zwei, REFERENCEID und MGMTFCTID, bestimmen den (Teil-)Dienst sowie die Managementfunktionalität, die ausgeführt werden muss. Der dritte Parameter sowie der Rückgabewert hängen von dem Parameter MGMTFCTID ab. Die Verfeinerungen für unterschiedlichen Managementfunktionen werden in Kapitel 6 definiert. Der letzte Parameter TIMELIMIT schränkt die maximale Ausführungszeit der angefragten Funktion ein.

5.10.4. Globales Prozessmodell

Bei den ersten drei Aktionen folgt der Prozessfluss (siehe Abbildung 5.14) dem üblichen Ablauf. Sollte die Anfrage akzeptiert werden, wird ähnlich wie bei REQUEST CHANGE (siehe Abschnitt 5.9) danach unterschieden, ob die *SP-Domain Providing Service* als ein Diensterbringer oder als Proxy-SP agiert. Im ersten Fall wird die angefragte Managementfunktionalität in Aktion A_4 ausgeführt. Ansonsten wird zunächst in A_5 und A_6 die Anfrage an die Sub-Provider weitergeleitet und anschließend in A_7 deren

Aktivität	Bezeichnung	Beschreibung	
A_1	REQUEST MGMTFCT	*Input*	
		Tätigkeiten	Abschicken der Anfrage nach Managementfunktionalität eines bereits bestellten (Teil-)Dienstes
		Output	
A_2	WAIT FOR RESPOND	*Input*	
		Tätigkeiten	• Warten auf die Antwort der SP-Domain Providing Service • Abbruch bei Zeitüberschreitung
		Output	
A_3	CHECK CREDENTIALS OF SP REQUESTING SERVICE	*Input*	• REFERENCEID • DOMAIN DATA (SP-DOMAIN PROVIDING SERVICE)
		Tätigkeiten	• Überprüfen, ob die SP-Domain Requesting Service nach Domain-Policies zugelassen werden darf • Überprüfen, ob die ReferenceID-bezogene Anfrage der SP-Domain Requesting Service zulässig ist • Treffen einer Entscheidung
		Input	
A_4	PERFORM REQUESTED MANAGEMENT FUNCTIONALITY	*Input*	• REFERENCEID • MGMTFCTID • RELATEDPARAMETERS • DOMAIN DATA (SP-DOMAIN PROVIDING SERVICE)
		Tätigkeiten	Durchführen der durch MGMTFCTID identifizierten Managementfunktionalität entsprechend RELATEDPARAMETERS
		Output	• REQUESTSPECIFICRESULT
A_5	REQUEST MGMTFCT (TO FURTHER SPS PROVIDING SERVICE)	*Input*	• REFERENCEID (SERVICE-PART SPECIFIC) • MGMTFCTID • RELATEDPARAMETERS
		Tätigkeiten	• Senden einer REQUEST MGMTFCT Anfrage an alle beteiligten SP-Domains • Warten auf die Antwort
		Output	• REQUESTSPECIFICRESULT (PRO INVOLVED SERVICE-PART)
A_6	REQUEST MGMTFCT (TO PROXY-SP)	*Input*	• REFERENCEID (PROXY-SP SPECIFIC) • MGMTFCTID • RELATEDPARAMETERS
		Tätigkeiten	• Senden einer REQUEST MGMTFCT Anfrage an den Proxy-SP • Warten auf die Antwort
		Output	• REQUESTSPECIFICRESULT (PROXY-SP SPECIFIC)
A_7	CALCULATE OVERALL RESULT	*Input*	REQUESTSPECIFICRESULT (ONE PRO EVERY SERVICE-PART)
		Tätigkeiten	Berechne Zusicherungswert für eigenen Verantwortungsbereich
		Output	REQUESTSPECIFICRESULT (AGGREGATED FOR ALL PARTS)

Tabelle 5.12.: REQUEST MGMTFCT – Aktivitäten

Ergebnisse zu einem Gesamtwert aggregiert. Dabei ist das für die Teildiensteigenschafte definierte Verfahren zu befolgen (siehe Abschnitte 4.2 und 4.6.10). In beiden Fällen wird der Erfolg mit `RESPOND SUCCESS` zusammen mit dem MGMTFCTID-spezifischen Ergebnis an die *SP-Domain Requesting Service* mitgeteilt. Falls bei mindestens einem Teildienst die Funktionsdurchführung fehlschlug, wird das mit `RESPOND FAILED` gemeldet.

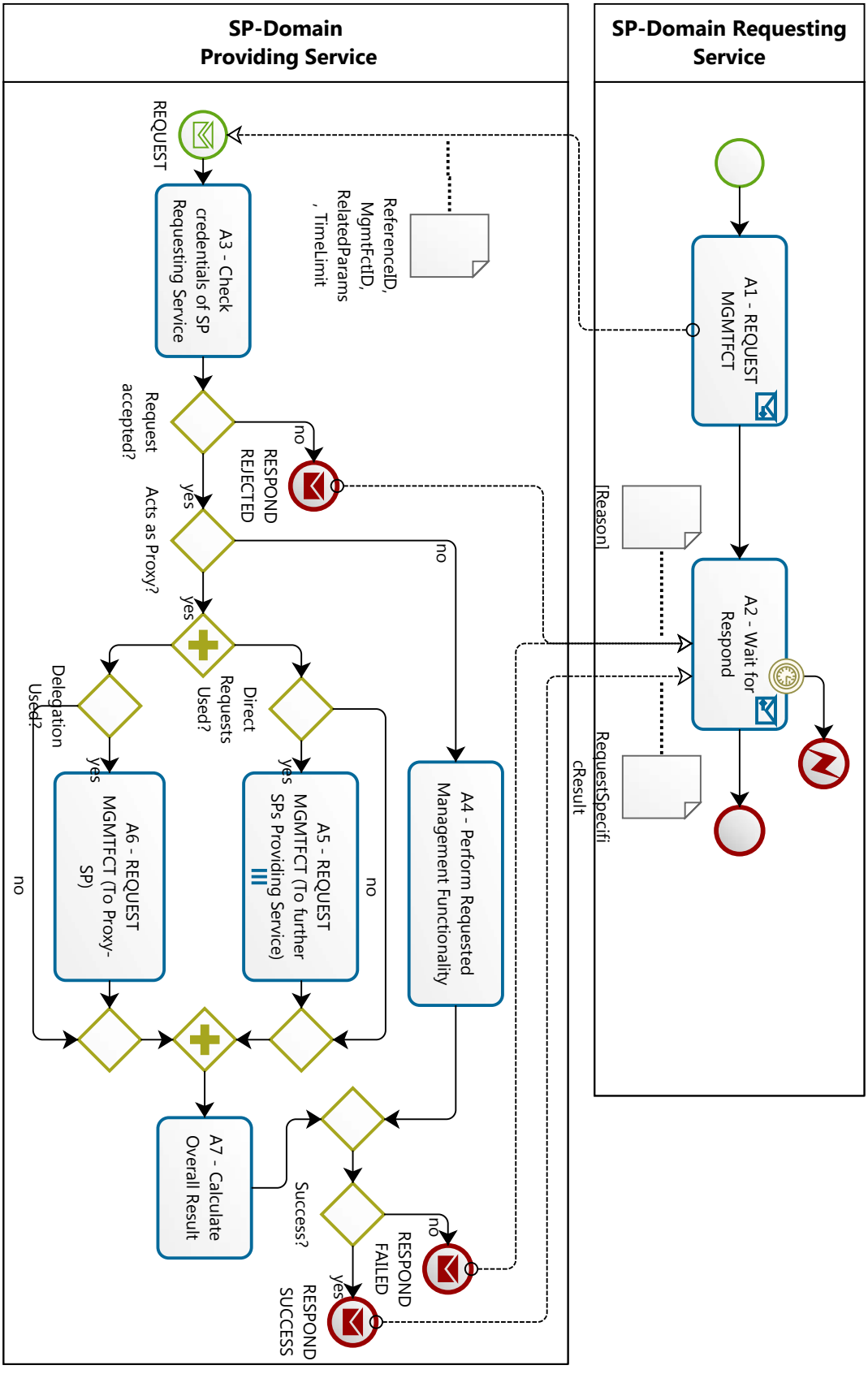
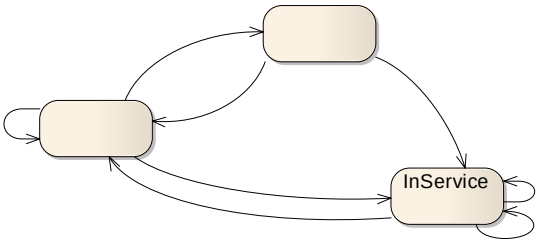


Abbildung 5.14.: REQUEST MGMTFCT

5.11. NOTIFY INSTANCESTATE

5.11.1. Einführung

Sollte bei der Bestellung eines Dienstes (siehe Abschnitte 5.8 und 5.13) eine automatische Benachrichtigung mitbestellt werden, können die Veränderungen des Dienstinstanzzustandes bzw. regelmäßige Monitoring-Informationen via Protokollaufruf `NOTIFY INSTANCESTATE` der *SP-Domain Requesting Service* mitgeteilt werden.



5.11.2. Aktivitäten

In Tabelle 5.13 sind alle für den Prozess relevanten Aktivitäten zusammengefasst.

5.11.3. Prozessartefakte

Da zwischen der *SP-Domain Providing Service* und der *SP-Domain Requesting Service* mehr als eine einzige Beziehung (z.B. wegen mehreren für unterschiedlichen Dienstinstanzen bestellten Teildienste) bestehen kann, werden mit Hilfe der E2ELINKID die Dienstinstanz und mit REFERENCEID der Teildienst innerhalb dieser Dienstinstanz identifiziert. Die Informationen über den Dienstzustand werden entsprechend dem UML-Diagramm aus der Abbildung 4.54 strukturiert.

5.11.4. Globales Prozessmodell

Der Prozess wird gestartet, wenn eine Veränderung des Dienstinstanzzustandes erkannt wird. Daraufhin wird in Aktivität A_1 überprüft, ob eine automatische Benachrichtigung dafür an den *SP-Domain Requesting Service* geschickt werden soll. Sollte das der Fall sein, werden in A_2 die notwendigen Informationen vorbereitet und an den *SP-Domain Requesting Service* geschickt.

Der *SP-Domain Requesting Service* korreliert zunächst in A_3 die Benachrichtigungsinformationen mit den bereits vorhandenen Informationen über andere Teildienste. Dabei ist das für die Teildiensteigenschafte definierte Verfahren zu befolgen (siehe Abschnitte 4.2 und 4.6.10). Das Ergebnis wird in A_4 für die spätere Wiederverwendung abgespeichert.

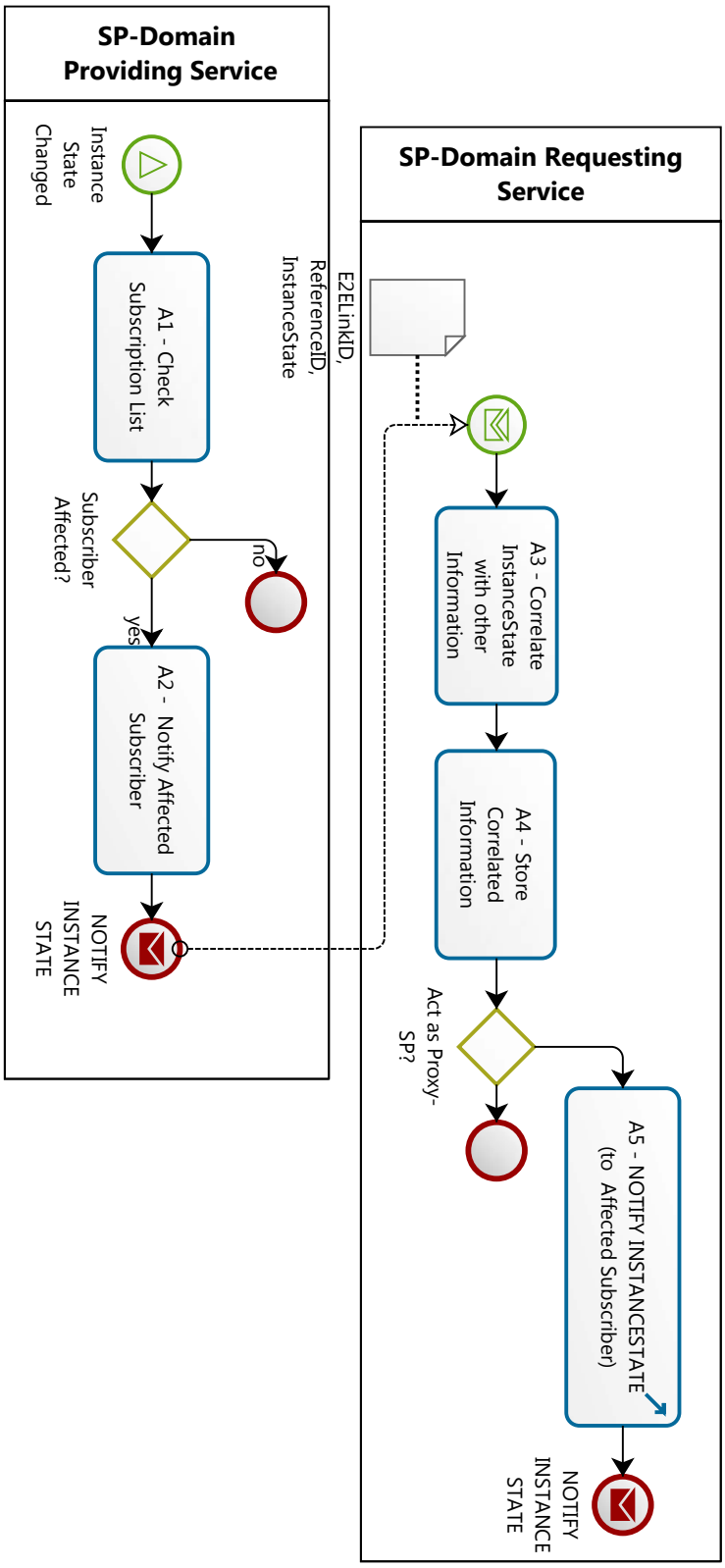


Abbildung 5.15.: NOTIFY INSTANCESTATE

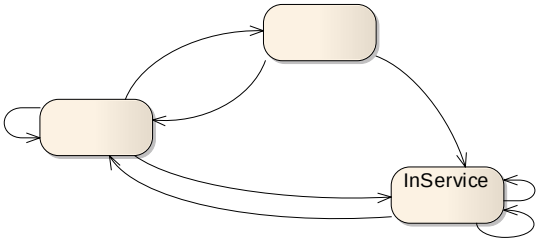
Aktivität	Bezeichnung	Beschreibung	
A_1	CHECK SUBSCRIPTION LIST	*Input*	
		Tätigkeiten	Überprüfen ob und wer die automatische Benachrichtigung über die Veränderung der Dienstinstanz abonniert hat
		Output	
A_2	NOTIFY AFFECTED SUBSCRIBER	*Input*	
		Tätigkeiten	• Vorbereiten der abonnierten Informationen • Schicken relevanter Informationen an den Subscriber
		Output	• E2ELINKID • REFERENCEID • INSTANCESTATE
A_3	CORRELATE INSTANCESTATE WITH OTHER INFORMATION	*Input*	• E2ELINKID • INSTANCESTATE • E2E LINK DATA (STATES OF OTHER RELEVANT E2E LINK PARTS)
		Tätigkeiten	Berechnen eines aggregierten Instanz-Zustands basierend auf der neuen Information
		Output	CORRELATEDINFORMATION
A_4	STORE CORRELATED INFORMATION	*Input*	CORRELATEDINFORMATION
		Tätigkeiten	Abspeichern der korrelierten Informationen, so dass sie später abgeholt bzw. wiederverwendet werden können
		Output	
A_5	NOTIFY INSTANCESTATE (TO AFFECTED SUBSCRIBER)	*Input*	
		Tätigkeiten	• Überprüfen, ob die Benachrichtigung für den korrelierten Zustand weiter geschickt werden soll • Abschicken der Benachrichtigung falls nötig
		Output	CORRELATEDINFORMATION

Tabelle 5.13.: NOTIFY INSTANCESTATE – Aktivitäten

Sollte der *SP-Domain Requesting Service* als ein Proxy-SP agieren, wird in Aktivität A_5 der Prozessvorgang rekursiv ausgeführt.

5.12. NOTIFY EVENT

5.12.1. Einführung



In vielen Fällen ist der aktuelle Zustand der Dienstinstanz weniger interessant als der Fakt, ob eine der vordefinierten Grenzwerte gebrochen wurde. Sollte dies bei der Dienstbestellung (siehe Abschnitte 5.8 und 5.13) vereinbart werden, kann die Tatsache einer Grenzwertverletzung dem *SP-Domain Requesting Service* mit `NOTIFY EVENT` automatisch mitgeteilt werden.

5.12.2. Aktivitäten

In Tabelle 5.14 sind alle für den Prozess relevanten Aktivitäten zusammengefasst.

5.12.3. Prozessartefakte

Analog wie bei `NOTIFY INSTANCESTATE` (siehe Abschnitt 5.11) sollen auch bei den Ereignisbenachrichtigungen die Parameter E2ELINKID und REFERENCEID vorhanden sein, um den Bezug zu dem Teildienst einer Dienstinstanz herzustellen. Das Ereignis selbst wird durch EVENTTYPEID identifiziert. Zusätzlich soll auch der aktuelle Zustand des Teildienstes mitgeteilt werden, der entsprechend dem UML-Diagramm in Abbildung 4.54 strukturiert werden soll. Dies soll insbesondere den Fall abdecken, wenn keine oder nur eine mangelhafte kontinuierliche Überwachung stattfindet.

5.12.4. Globales Prozessmodell

Der Prozess wird gestartet, wenn eine Veränderung des Dienstinstanzzustandes erkannt wird. Zunächst wird überprüft, ob einer der vereinbarten Grenzwerte gebrochen wurde, und erst dann wird fortgefahren. In Aktivität A_1 wird überprüft, ob eine automatische Benachrichtigung dafür an den *SP-Domain Requesting Service* geschickt werden soll. Sollte das der Fall sein, werden in A_2 die notwendigen Informationen vorbereitet und an den *SP-Domain Requesting Service* geschickt.

Der *SP-Domain Requesting Service* korreliert zunächst in A_3 die Benachrichtigungsinformationen mit den bereits vorhandenen Informationen über andere Teildienste. Dabei ist das für die Teildiensteigenschafte definierte Verfahren zu befolgen (siehe Abschnitte 4.2 und 4.6.10). Das Ergebnis wird in A_4 für die spätere Wiederverwendung abgespeichert.

Aktivität	Bezeichnung	Beschreibung	
A_1	CHECK SUBSCRIPTION LIST	*Input*	
		Tätigkeiten	Überprüfen ob ein Threshold gebrochen wurde und falls ja, ob die automatische Benachrichtigung darüber abonniert wurde
		Output	
A_2	NOTIFY AFFECTED SUBSCRIBER	*Input*	
		Tätigkeiten	• Vorbereiten der abonnierten Informationen • Schicken relevanter Informationen an den Subscriber
		Output	• E2ELINKID • REFERENCEID INSTANCESTATE
A_3	CORRELATE INSTANCESTATE WITH OTHER INFORMATION	*Input*	• E2ELINKID • INSTANCESTATE • E2E LINK DATA (STATES OF OTHER RELEVANT E2E LINK PARTS)
		Tätigkeiten	• Berechnen der aggregierten Instanz-Zustand basierend auf der neuen Information
		Input	CORRELATEDINFORMATION
A_4	STORE CORRELATED INFORMATION		CORRELATEDINFORMATION
			Abspeichern der korrelierten Informationen, so dass sie später abgeholt bzw. wiederverwendet werden können
A_5	NOTIFY EVENT (TO AFFECTED SUBSCRIBER)		
			• Überprüfen, ob der korrelierte Zustand einen Threshold bricht und falls ja, ob die Benachrichtigung für dieses Ereignis weiter geschickt werden soll • Abschicken der Benachrichtigung falls nötig
			• CORRELATEDINFORMATION

Tabelle 5.14.: NOTIFY EVENT – Aktivitäten

Sollte der *SP-Domain Requesting Service* als ein Proxy-SP agieren, wird in Aktivität A_5 der Prozessvorgang rekursiv ausgeführt.

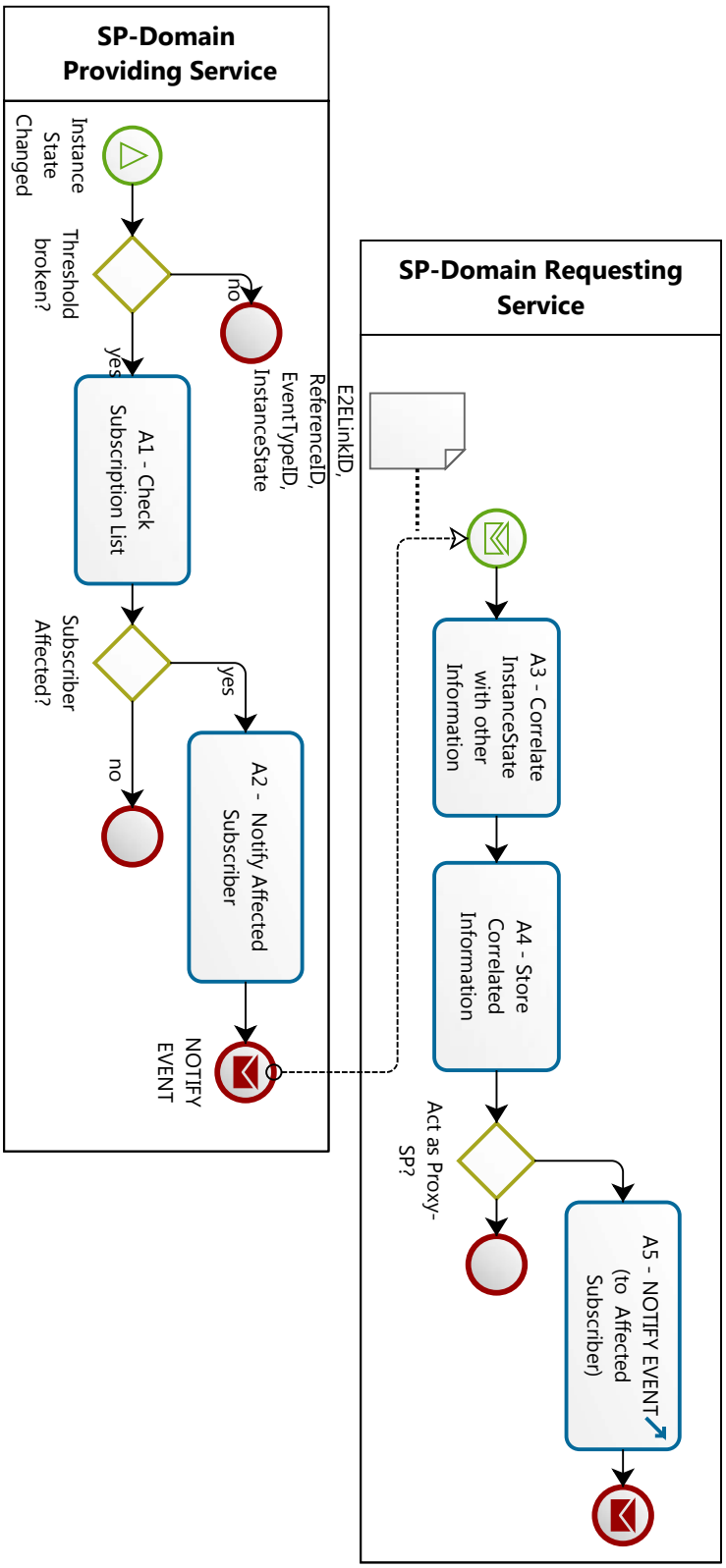
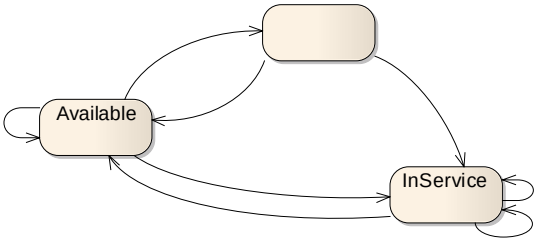


Abbildung 5.16.: NOTIFY EVENT

5.13. REQUEST SERVICE

5.13.1. Einführung



Auch wenn die meisten Dienste ausschließlich mittels "Umweg" über den Reservierungszustand bestellt werden dürfen (siehe Abschnitte 5.6 und 5.8), muss bei Delegation der Dienst gleich in Anspruch genommen werden, allein um Informationsanfragen durchführen zu können. Ähnliches gilt auch für den Multi-Domain Managementdienst ROUTING, denn erst von diesem Dienst können die zu reservierenden Teilstrecken bestimmt werden.

5.13.2. Aktivitäten

In Tabelle 5.15 sind alle für den Prozess relevanten Aktivitäten zusammengefasst.

5.13.3. Prozessartefakte

Die Kommunikationsartefakte bei der direkten Dienstanfrage unterteilen sich, ähnlich wie bei `REQUEST RESERVATION` (siehe entsprechend Abschnitt 5.6), in drei Teile. Die ersten zwei Parameter stellen den Bezug zu der E2E-Dienstinstanz (E2ELINKID) her und bestimmen den angefragten Dienst (SERVICETYPEID). Der dritte Parameter (SERVICEPARAMS) unterteilt sich in weitere Teile, die für die zwei einzigen unterstützten Dienste (`DELEGATION` und `MDSERVICE ROUTING`) identisch sind:

```
ServiceParams ::= <ConstraintTopology>
                  <ConstraintProperties>
                  <IntermediateProperties>
                  <DelegationTypeID>
```

Die Identität der Parameter ist dadurch bedingt, dass bei der Delegation die *SP-Domain Providing Service* auf jeden Fall das Routing für den eigenen Verantwortungsbereich übernehmen soll. Das bedeutet, dass in beiden Fällen die Start- und End-SCPs (<CONSTRAINTTOPOLOGY>, strukturiert entsprechend dem UML-Diagramm in Abbildung 4.48) sowie die E2E-Einschränkungen (<CONSTRAINTPROPERTIES>, strukturiert entsprechend dem UML-Diagramm in Abbildung 4.49) und die Zwischensumme (<INTERMEDIATEPROPERTIES>, strukturiert entsprechend dem UML-Diagramm in Abbildung 4.53) der *SP-Domain Providing Service* mitgeteilt werden müssen. Während des Routings soll die Managementfunktionalität einzelner Teildienste in den globalen

Aktivität	Bezeichnung	Beschreibung	
A_1	REQUEST SERVICE	*Input*	
		Tätigkeiten	Abschicken der Anfrage für die Bestellung und Inbetriebnahme einer neuen Dienstinstanz
		Output	
A_2	WAIT FOR RESPOND	*Input*	
		Tätigkeiten	• Warten auf die Antwort von SP-Domain Providing Service • Abbruch bei Zeitüberschreitung
		Output	
A_3	CHECK CREDENTIALS OF SP REQUESTING SERVICE	*Input*	• E2ELINKID • SERVICETYPEID
		Tätigkeiten	• Überprüfen, ob SP-Domain Requesting Service nach Domain-Policies zugelassen werden darf • Überprüfen, ob die Anfrage unterstützt wird • Treffen Entscheidung
		Input	
A_4	ALLOCATE PROXY-RESSOURCES	*Input*	• E2ELINKID • SERVICEPARAMS
		Tätigkeiten	Allokieren der für die Tätigkeit als Proxyy-SP notwendigen Ressourcen
		Output	REFERENCEID
A_5	REQUEST SERVICE MDSERVICE ROUTING	*Input*	E2ELINKID
		Tätigkeiten	• Bestimmen SP-Domain Providing Service für ROUTING Multi-Domain Service • Abschicken einer Anfrage an den ausgewählte SP • Warten auf die Antwort
		Output	
A_6	REQUEST RESERVATION REQUIRED MD-SERVICES	*Input*	• E2ELINKID • SERVICEPARAMS
		Tätigkeiten	• Bestimmen, welche Multi-Domain Dienste bei der Erbringung neuer Dienstinstanz notwendig sind • Bestimmen SP-Domänen für die Erbringung dieser Dienste • Abschicken einer Anfrage an den ausgewählte SP • Warten auf die Antwort
		Output	
A_7	ALLOCATE RESSOURCES FOR ROUTING SERVICE	*Input*	• E2ELINKID
		Tätigkeiten	Allokieren der für die Durchführung der Routingoperationen notwendigen Ressourcen
		Output	
A_8	NOTIFY: REQUESTED SERVICE NOT SUPPORTED	*Input*	
		Tätigkeiten	Benachrichtige SP-DOMAIN REQUESTING SERVICE, dass der angefragte Dienst nicht unterstützt wird
		Output	

Tabelle 5.15.: REQUEST SERVICE - Aktivitäten

Managementprozess integriert werden. Die Angaben der globalen Managementprozesse werden durch COMMUNICATIONDSM bei der Zwischensumme mitgeteilt (siehe auch entsprechende Diskussion im Abschnitt 4.6.8). Dies ändert sich auch dann nicht, wenn bei der Delegation entsprechend DELEGATIONTYPEID die Verschattung des internen Dienstaufbaus erwünscht wird (zu unterschiedlichen Delegationsformen siehe die entsprechende Diskussion im Abschnitt 4.3).

Da in beiden Fällen ausschließlich Ressourcen für den angefragten Dienst allokiert werden und keine Suchaktion ausgeführt wird, wird ausschließlich der Identifikator des bestellten Dienstes REFERENCEID zurückgeschickt.

5.13.4. Globales Prozessmodell

Der Prozessablauf ist in Abbildung 5.17 dargestellt. Der Ablauf der ersten drei Aktivitäten entspricht dem üblichen Muster, bei dem auch die Unterstützung des angefragten Dienstes überprüft wird. Nachdem die Anfrage akzeptiert wurde, wird anhand der SERVICETYPEID unterschieden, welche Aktionen ausgeführt werden müssen. Wird weder Delegation noch Routing angefragt, dann wird in A_8 der *SP-Domain Requesting Service* mitgeteilt, dass der angefragte Dienst (bei der direkten Bestellung) nicht unterstützt wird. Bei der Anfrage nach dem Routingdienst werden in A_7 die dafür notwendigen Ressourcen allokiert und mit E2ELINKID assoziiert. Der Prozessablauf bei der Delegation ist um einiges komplexer. Unabhängig davon, welche Delegationsart erwünscht wird, werden in A_4 die für Proxy-SP notwendigen Ressourcen allokiert sowie in A_5 der Routingdienst bestellt. Parallel dazu werden, falls eine komplette Verschattung des Dienstaufbaus signalisiert wurde, in A_6 die Anfragen für Reservierung der benötigten Multi-Domain Dienste an weitere SP-Domänen geschickt.

Die Routingaufgabe (Aktion A_5) sowie weitere Multi-Domain Managementaufgaben (Aktion A_6) müssen nicht unbedingt an weitere SP-Domänen delegiert werden und können i.A. auch von der *SP-Domain Providing Service* in Eigenregie übernommen werden. Zu Gunsten der besseren Lesbarkeit des Ablaufdiagramms wird die entsprechende triviale Fallunterscheidung nicht explizit dargestellt.

Falls alle relevanten Aktionen erfolgreich abgeschlossen wurden, wird das mit der Antwort `RESPOND SUCCESS` zusammen mit REFERENCEID der Dienst-anfragenden SP-Domäne mitgeteilt. Ansonsten wird mit `RESPOND FAILED` das Fehlschlagen des Aufrufs signalisiert.

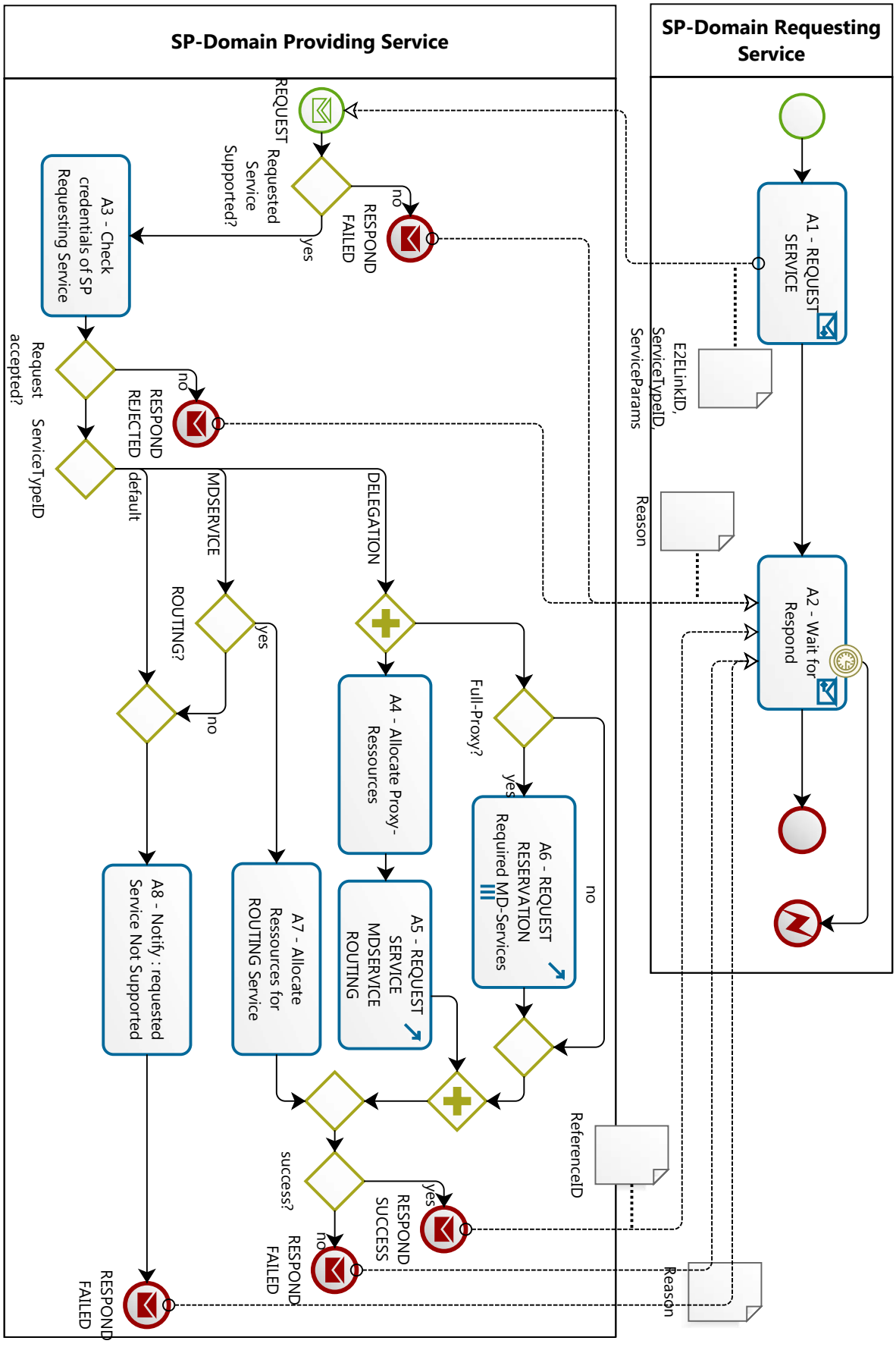
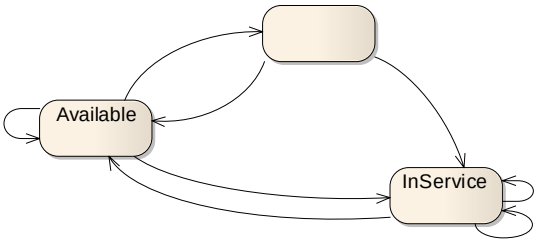


Abbildung 5.17.: REQUEST SERVICE

5.14. REQUEST DECOMISSIONING

5.14.1. Einführung



Unabhängig davon, ob eine Dienstinstanz für eine Zeitspanne oder "open end" bestellt wurde, kann sie i.A. jederzeit durch den Kunden abgestellt werden. Das erfordert eine Möglichkeit, alle bei der Erbringung dieser Dienstinstanz beteiligten SP-Domänen zu benachrichtigen, sodass sie die für diese Instanz verwendeten Ressourcen freigeben können.

5.14.2. Aktivitäten

In Tabelle 5.16 sind alle für den Prozess relevanten Aktivitäten zusammengefasst.

5.14.3. Prozessartefakte

Als Prozessartefakt wird beim Prozess ausschließlich die REFERENCEID benötigt, die bei einer erfolgreichen `REQUEST RESERVEDSRVICE` oder `REQUEST SERVICE` Anfrage zurück geliefert wurde (siehe Abschnitte 5.8 und 5.13).

5.14.4. Globales Prozessmodell

Der Prozessablauf ist in Abbildung 5.18 dargestellt. Der Ablauf der ersten drei Aktionen entspricht dem üblichen Muster. Sollte die Anfrage akzeptiert werden, wird danach unterschieden, ob die *SP-Domain Providing Service* direkt einen Teildienst erbringt oder als eine Proxy-SP agiert. Im ersten Fall werden in A_4 die verwendeten Ressourcen freigegeben. Ansonsten wird zunächst in A_5 und A_6 die Dienstauflösungsanfrage an alle weiteren SP-Domainen geschickt, die von der Proxy-SP mit der Teildiensterbringung beauftragt wurden. Anschließend werden in A_7 die Ressourcen freigegeben, die für die Verwaltung der Proxy-Aufgaben verwendet wurden.

Aktivität	Bezeichnung	Beschreibung	
A_1	REQUEST DECOMISSIONING	*Input*	
		Tätigkeiten	Abschicken der Anfrage für die Abbestellung des Teildienstes
		Output	
A_2	WAIT FOR RESPOND	*Input*	
		Tätigkeiten	• Warten auf die Antwort von SP-Domain Providing Service • Abbruch bei Zeitüberschreitung
		Output	
A_3	CHECK CREDENTIALS OF SP REQUESTING SERVICE	*Input*	• REFERENCEID • DOMAIN DATA (SP-DOMAIN PROVIDING SERVICE)
		Tätigkeiten	• Überprüfen, ob die SP-Domain Requesting Service entsprechend der Domain-Policies zugelassen werden darf • Überprüfen, ob die ReferenceID-bezogene Anfrage der SP-Domain Requesting Service zulässig ist • Treffen einer Entscheidung
		Input	
A_4	RELEASE USED INFRASTRUCTURE	*Input*	REFERENCEID
		Tätigkeiten	Freigeben der Ressourcen, die für die Diensterbringung verwendetet wurden
		Output	
A_5	FORWARD REQUEST TO FURTHER SP-DOMAINS PROVIDING SERVICE	*Input*	REFERENCEID
		Tätigkeiten	• Bestimmen aller Subprovider-SPs anhand der REFERENCEID, deren Kommunikationsadressen und deren Teildienstspezifischen REFERENCEIDS • Abschicken einer Dienstbeendigung-Anfrage an alle Subprovider-SPs • Warten auf die Antworten
		Output	
A_6	FORWARD REQUEST TO PROXY-SP	*Input*	REFERENCEID
		Tätigkeiten	• Bestimmen der Proxy-SP anhand der REFERENCEID, ihre Kommunikationsadresse und deren Teildienstspezifischen REFERENCEIDS • Abschicken einer Dienstbeendigung-Anfrage an die Proxy-SPs • Warten auf die Antworten
		Output	
A_7	FREE PROXY-RESSOURCES	*Input*	REFERENCEID
		Tätigkeiten	Freigeben der Ressourcen, die für die Verwaltung der Proxy-Aufgaben verwendet wurden
		Output	

Tabelle 5.16.: REQUEST DECOMISSIONING – Aktivitäten

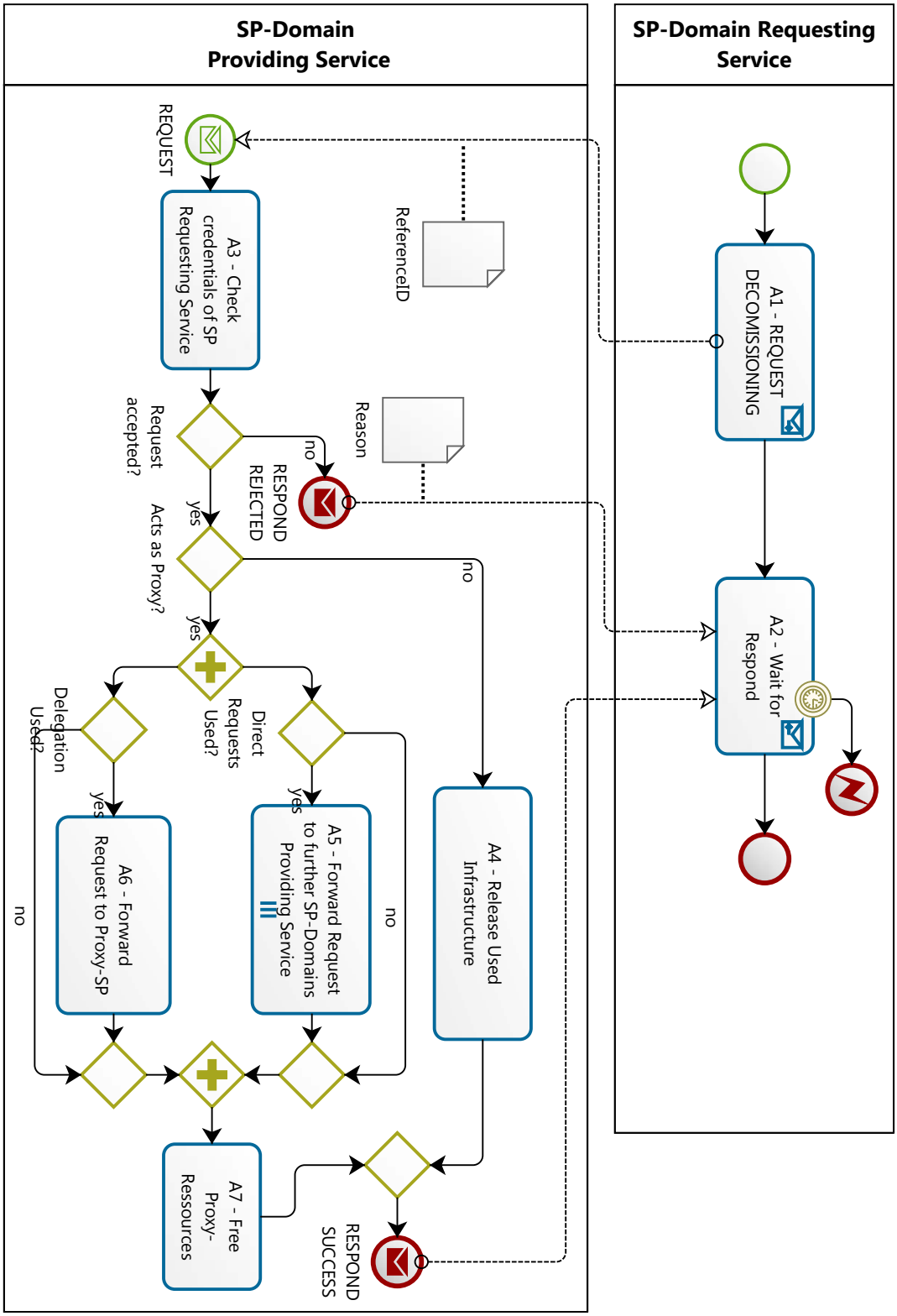


Abbildung 5.18.: REQUEST DECOMISSIONING

5.15. Protokoll: Zusammenfassung

Alle in diesem Abschnitt definierten Protokoll-Schlüsselworte sind in Tabelle 5.17 mit einer kurzen Beschreibung zusammengefasst.

REQUEST	**Verwendung und Ziel**	
	Initiiert die Multi-Domain Kommunikation und ermöglicht der SP-Domäne *Requesting Service* Anfragen für Dienste und/oder Informationen an die SP-Domäne *Providing Service* zu schicken. Diese Anfrage bestimmt auch die Rollenverteilung.	
	SpecifierID	Beschreibung
	INFORMATION	Eine *on-demand* Abfrage der für die Pfadsuche benötigten Informationen.
	SUBSCRIPTION	Anfrage für regelmäßige Updates zu spezifizierten Informationen. Diese Option ist für den Austausch der Teilsichten auf die InterDomain Links zwischen den benachbarten SP-Domänen gedacht.
	CANCELSUBSCRIBTION	Explizite Rücknahme der automatischen Benachrichtigung.
	RESERVATION	Anfrage für Reservierung eines Dienstes.
	CANCELRESERVATION	Explizite Rücknahme der Reservierung.
	RESERVEDSERVICE	Anfrage für einen bereits reservierten Dienst
	MGMTFCT	Anfrage nach einer Managementfunktion. Weitere Verfeinerung ist benötigt.
	CHANGE	Anfrage für Änderung der Dienstinstanzeigenschaften
	SERVICE	Anfrage für einen (nicht reservierten) Dienst
	DECOMISSIONING	Anfrage für Dienstauflösung
RESPOND	**Verwendung und Ziel**	
	Eine unmittelbare Antwort auf jede definierte REQUEST-Anfrage	
	SpecifierID	Beschreibung
	INFORMATION	Liefert die angefragten Informationen zurück
	REJECTED	Die Anfrage wurde (z.B. aus Sicherheitsgründen) zurückgewiesen
	ACCEPTED	Die Anfrage, deren Ausübung längere Zeit in Anspruch nehmen kann, wurde akzeptiert. Die Benachrichtigung über Ergebnisse wird der *Requesting Service* SP-Domäne mit NOTIFY mitgeteilt.
	SUCCESS	Angefragte Aktion wurde erfolgreich ausgeführt. Weitere anfragespezifische Informationen werden zurückgeschickt.
	FAILED	Die Anfrage wurde zwar akzeptiert, deren Durchführung ist aber fehlgeschlagen
NOTIFY	**Verwendung und Ziel**	
	Asynchrone Benachrichtigungen.	
	SpecifierID	Beschreibung
	INFORMATION	Bei akzeptierter REQUEST SUBSCRIBTION – eine proaktive Mitteilung der Änderungen der vorhandenen Kapazitäten. Verwendung: Austausch von Informationen über InterDomain Links zwischen Nachbar-SPs
	INSTANCESTATE	Eine proaktive Mitteilung der Veränderung des Instanzzustandes
	EVENT	Eine proaktive Mitteilung eines Ereignisses, wie z.B. Verletzung eines Threshholds

Tabelle 5.17.: Protocol-Keywords, Überblick

6

Referenzprozesse für SLM bei Verketteten Diensten

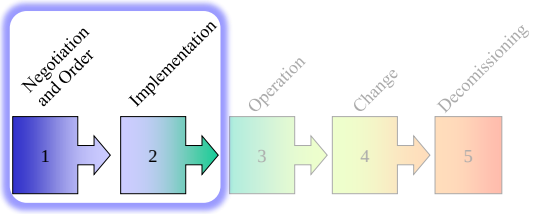
Aufbauend auf den Basisprozessen werden in diesem Kapitel die Service-Level-Management-Prozesse für Verkettete Dienste definiert. Obwohl die Multi-Domain Managementfunktionalität sowohl von jedem Service Provider in Eigenregie erbracht werden kann als auch von einem anderen darauf spezialisierten Service Provider bestellt werden kann, kann diese Fallunterscheidung die Beschreibung der SLM-Prozesse unnötig verkomplizieren. Aus diesem Grund wird bei der Definition aller SLM-Prozesse stets die zweite Alternative verwendet, was einer allgemeineren Darstellung entspricht. Wie die Unterscheidung zwischen der lokal und der global erbrachten Managementfunktionalität modelliert und in die Prozessdefinition integriert werden kann, wird im Abschnitt 6.2 erläutert.

Bei der Modellierung der SLM-Prozesse werden oft Funktionen benötigt, die im Kapitel 5 nur ansatzweise angedeutet wurden. In solchen Fällen werden entsprechende Aktivitäten der Basisfunktionen aufgabenbezogen verfeinert. Die Definition der Verfeinerungen der Basisprozesse folgt der Definition der Managementprozesse, sodass deren Einbettung und Kontext klar definiert sind.

Die einzelnen Prozesse sind entsprechend den Dienstlebenszyklusphasen angeordnet, in denen sie auftreten. Für die bessere Referenzierbarkeit ist die entsprechende Phase am Anfang jedes Abschnittes graphisch dargestellt.

6.1. SLM-Prozess: Bestellung und Inbetriebnahme

6.1.1. Einführung



Klassischerweise werden am Anfang des Dienstinstanzlebenszyklus drei Aufgaben – Verhandlung, Bestellung und Inbetriebnahme – unterschieden, die oft auch als Phasen oder Prozesse aufgefasst werden. Die Übergänge zwischen diesen Phasen sind fließend und können zwischen unterschiedlichen Diensten stark variieren. In diesem Abschnitt werden daher alle drei Prozesse in einem zusammengefasst, was dem Vorgehen bei automatisierten Diensten wie z.B. Telefonverbindungen entspricht. Das Standardvorgehen wird lediglich um die Option erweitert, eine Kundenbestätigung einzuholen.

Im Prozessdiagramm wird zu Gunsten der besseren Lesbarkeit keine Fallunterscheidung zwischen lokal und extern erbrachten Multi-Domain Managementdiensten gemacht. Aus demselben Grund werden auch weder die Überprüfung der Ergebnisse der unterschiedlichen Operationen, wie z.B. Reservierung, noch das Freigeben der verwendeten Ressourcen bei fehlgeschlagenen Aktionen explizit dargestellt. Bei der Realisierung muss deswegen dieses Diagramm um entsprechende Fallunterscheidungen und Aktionen erweitert werden.

6.1.2. Rollen

Die für den Ordering-Prozess relevanten Rollen sowie deren Verantwortlichkeiten sind in Tabelle 6.1 zusammengefast.

6.1.3. Aktivitäten

Alle für den Ordering-Prozess relevanten Aktivitäten sind in den Tabellen 6.2 und 6.3 zusammengefasst.

6.1.4. Prozessartefakte

Die Kommunikationsartefakte zwischen *End Site* und dem *Connection-SP*, der die Rolle des *Concatenated Service Providers* ausübt, lassen sich unterschiedlich gestalten. Das hängt vor allem davon ab, wie der Dienst von dem jeweiligen Service Provider den Kunden angeboten wird. Sie können von e-Mail Kommunikation, wie z.B. bei

Rolle	Bezeichnung	Rollendefinition	
R_1	END SITE	*Verantwortlichkeiten*	• Repräsentant auf Kundenseite • Hier: Bestellung einer neuen E2E Dienstinstanz
		Fokus	–
		Kardinalität	1
		Art der Partizipation	statisch
		Vergabeverfahren	–
		Kandidatenmenge	potentielle Kunden, die an den angeschlossen CONNECTION-SP sind
R_2	CONNECTION-SP	*Verantwortlichkeiten*	• Lokaler Provider der END SITE • Hier: Anschluss der END SITE und Angebot unterstützter Dienste
		Fokus	–
		Kardinalität	1
		Art der Partizipation	statisch
		Vergabeverfahren	die End-Site wendet sich an ihren lokalen Provider
		Kandidatenmenge	alle Provider
R_3	CONCATENATED SERVICE PROVIDER	*Verantwortlichkeiten*	Vermittlung zwischen END SITE und CONCATENATED SERVICE MANAGER während des Ordering-Prozesses und Erstellung eines Angebots
		Fokus	ConcatenatedService
		Kardinalität	1
		Art der Partizipation	statisch
		Vergabeverfahren	Wird von CONNECTION-SP eingenommen
		Kandidatenmenge	–
R_4	CONCATENATED SERVICE MANAGER	*Verantwortlichkeiten*	• Rollenzuweisung für den Ordering- sowie weitere Prozesse • Koordination aller Multi-Domain Aktivitäten während des Ordering-Prozesses
		Fokus	ConcatenatedService
		Kardinalität	1
		Art der Partizipation	statisch
		Vergabeverfahren	Wird von CONNECTION-SP eingenommen
		Kandidatenmenge	–

Tabelle 6.1.: SLM-Processes Ordering – Rollen

Aktivität	Bezeichnung	Beschreibung	
A_1	DETERMINE E2E-REQUIREMENTS	*Input*	
		Tätigkeiten	Festlegen der Anforderungen an die E2E-Dienstgüte und an die E2E-Managementfunktionalität neuer Dienstinstanzen
		Output	
A_2	REQUEST NEW E2E LNSTANCE	*Input*	
		Tätigkeiten	Schicken einer Anfrage für eine neue Dienstinstanz an CONNECTION-SP
		Output	• END-POINTS • E2E-REQUIREMENTS
A_3	CHECK CUSTOMER CREDENTIALS	*Input*	
		Tätigkeiten	• Überprüfen, ob der End-User eine neue Dienstinstanz bestellen darf • Treffen Entscheidung
		Output	
A_4	ALLOCATE RESSOURCES FOR ORDER MANAGEMENT	*Input*	
		Tätigkeiten	• Allokieren der für die Verwaltung eines neuen Orders notwendigen Ressourcen • Bestimmen einer neuen eindeutigen E2ELINKID
		Output	E2ELINKID
A_5	DETERMINE REQUIRED MGMT. FUNCTIONALITY	*Input*	CUSTOMER-REQUIREMENTS
		Tätigkeiten	Bestimmen, welche Multi-Domain Dienste bei der Erbringung der neuen Dienstinstanz notwendig sind, um die Kundenanforderungen garantieren zu können
		Output	
A_6	REQUEST SERVICE MDSERVICE ROUTING	*Input*	
		Tätigkeiten	• Bestimmen der SP-Domänen für die Erbringung des Multi-Domain Routing-Dienstes • Abschicken einer Anfrage an den ausgewählten SP • Warten auf die Antwort
		Output	ROUTING MANAGER
A_7	REQUEST RESERVATION MDSERVICE MDMGMTFCTID	*Input*	
		Tätigkeiten	• Bestimmen der SP-Domänen für die Erbringung der Multi-Domain Dienste • Abschicken von Reservierungsanfragen an die SPs • Warten auf die Bestätigungen
		Output	REFERENCEID (pro MDMGMTFCT erbringenden SP)
A_8	REQUEST MGMTFCT FINDROUTE	*Input*	• ENDPOINTS • E2ERESTRICTIONS • INTERMEDIATEPROPERTIES (INCLUDING MDMGMTFCT-DSMS)
		Tätigkeiten	• Abschicken einer Anfrage an den Routing-SP zur Findung einer Route über mehrere SP-Domänen, die den E2E-Kundenanforderungen genügt • Warten auf die Antwort
		Output	• REFERENCEID (FOUND ROUTE) • FOUND ROUTE PROPERTIES

Tabelle 6.2.: SLM-Processes Ordering - Aktivitäten (1/2)

Aktivität	Bezeichnung	Beschreibung	
A_9	REQUEST MGMTFCT RESERVEROUTE	*Input*	• REFERENCEID (FOUND ROUTE) • INTERMEDIATEPROPERTIES
		Tätigkeiten	• Abschicken einer Anfrage an den Routing-SP für das Reservieren der gefundenen Route • Warten auf die Antwort
		Output	• REFERENCEID (RESERVED ROUTE) • FOUND ROUTE PROPERTIES
A_{10}	CHECK OFFER AND DECIDE	*Input*	OFFERED E2E LINK PROPERTIES
		Tätigkeiten	• Validieren des Angebots und treffen einer Entscheidung • Getroffene Entscheidung dem CONCATENATED SERVICE PROVIDER mitteilen
		Output	DECISION
A_{11}	WAIT FOR ORDER CONFIRMATION	*Input*	DECISION
		Tätigkeiten	• Warten auf die Entscheidung der END SITE • Abbruch bei Zeitüberschreitung
		Input	
A_{12}	REQUEST MGMTFCT ORDERROUTE	*Input*	REFERENCEID (RESERVED ROUTE)
		Tätigkeiten	• Abschicken einer Anfrage an den Routing-SP für die Bestellung der reservierten Route • Warten auf die Antwort
		Output	• REFERENCEID (PRO SECTION) • DSM (PRO SECTION)
A_{13}	REQUEST RESERVEDSERVICE REFERENCEID (MDMGMTFCT)	*Input*	REFERENCEID (pro MDMGMTFCT erbringenden SP)
		Tätigkeiten	• Abschicken einer Service-Anfrage an die SP-Domänen, die Multi-Domain Dienste erbringen sollen • Warten auf die Antwort
		Output	REFERENCEID (pro MDMGMTFCT erbringenden SP)
A_{14}	SAVE ROUTE INFORMATION	*Input*	• REFERENCEDI (PRO SECTION AND PRO MDMGMTFCT) • DSM (PRO SECTION AND PRO MDMGMTFCT)
		Tätigkeiten	Abspeichern der Kontaktinformationen für alle Teildienste
		Output	
A_{15}	REQUEST MGMTFCT RELEASEROUTE	*Input*	REFERENCEID (PRO SECTION)
		Tätigkeiten	• Abschicken einer Anfrage für Dienstauflösung • Warten auf die Antwort
		Output	
A_{16}	REQUEST DECOMISSIONING REFERENCEID (MDMGMTFCT)	*Input*	REFERENCEID (PRO MDMGMTFCT)
		Tätigkeiten	• Abschicken einer Anfrage für Dienstauflösung • Warten auf die Antwort
		Output	
A_{17}	FREE RESSOURCES ALLOCATE FOR ORDER MANAGEMENT	*Input*	E2ELINKID
		Tätigkeiten	Freigeben Ressourcen, die für die Verwaltung des Orders allokiert wurden (Gegenpart zu A_4)
		Output	

Tabelle 6.3.: SLM-Processes Ordering – Aktivitäten (2/2)

im Abschnitt 2.3.2 Géant2 E2E Link Dienst, bis hin zum standardisierten Signalisierungsprotokoll, wie z.B. bei Telefondienst, variieren. Bei den automatisierten Diensten bietet sich an, das UML-Diagramm aus der Abbildung 4.51 für die Strukturierung der E2E-Anforderungen und des Angebotes zu verwenden.

6.1.5. Globales Prozessmodell

Nachdem der Endkunde in A_1 die E2E-Anforderungen festgelegt und in A_2 an seinen Anschluss-SP mitgeteilt hat, wird in A_3 überprüft, ob die Anfrage zulässig ist oder nicht. Sollte die Anfrage akzeptiert werden, können in A_4 alle für die Verwaltung einer neuen Bestellung notwendigen Ressourcen allokiert werden. Anschließend wird die Kontrolle an die Rolle *Concatenated Service Manager* übergeben, die von demselben Anschluss-SP ausgeübt wird.

Als erstes bestimmt der *Concatenated Service Manager* in A_5, welche Managementfunktionalität benötigt wird, um die E2E-Kundenanforderungen erfüllen zu können. Da die E2E-Dienstinstanz i.A. aus mehreren Teilstrecken besteht, wird in A_6 für die Teilstreckenbestimmung der ROUTING-Dienst bestellt (entsprechender Basisprozess ist im Abschnitt 5.13 beschrieben). Der Erbringer des ROUTING-Dienstes nimmt dabei die Rolle *Routing Manager* ein. Parallel dazu werden in A_7 alle weiteren benötigten Multi-Domain Managementdienste reserviert (entsprechender Basisprozess ist im Abschnitt 5.6 beschrieben).

Bemerkung: Auch wenn im Prozessdiagramm nicht explizit dargestellt, sollte bei der Implementierung an der Stelle überprüft werden, ob alle Managementdienste bestellt werden konnten und nur beim Erfolg weiter dem dargestellten Prozessablauf gefolgt werden. Beim Fehlschlagen sollen alle reservierten Ressourcen freigegeben und das Fehlschlagen dem Kunden mitgeteilt werden.

Nachdem die Managementdienste reserviert und der Routingdienst bestellt wurden, wird der *Routing Manager* in A_8 beauftragt, eine Route entsprechend den E2E-Anforderungen zu finden und anschließend in A_9 sie zu reservieren (die entsprechende Hilfsprozesse sowie Rolle sind in Abschnitten 6.2 und 6.3 beschrieben). Genauso wie bei der Bestellung bzw. Reservierung soll das Ergebnis dieser Aktionen überprüft werden und evtl. die weitere Prozessausführung abgebrochen werden (vergleiche Bemerkung zu A_6 und A_7).

Nachdem die gefundene Route reserviert wurde, wird unterschieden, ob eine zusätzliche Kundenbestätigung erforderlich ist oder nicht. Sollte das der Fall sein, wird dem Kunden ein entsprechendes Angebot geschickt, anhand dessen in A_{10} die endgültige Entscheidung getroffen wird. Diese Entscheidung wird in A_{11} vom *Concatenated Service Provider* empfangen.

Sollte das Angebot akzeptiert bzw. eine Bestätigung nicht benötigt werden, wird weiter parallel mit A_{12} und A_{13} vorgegangen. Bei A_{12} handelt es sich wiederum um einen

Hilfsprozess (siehe Abschnitt 6.4), um die reservierte Route zu bestellen. Die Aktion A_{13} baut dagegen gleich auf dem im Abschnitt 5.8 definierten Basisprozess auf. Bei Erfolg werden alle für das Dienstinstanz-Management benötigten Informationen in A_{14} abgespeichert und die entsprechende Mitteilung an die *End Site* geschickt, so dass die Dienstinstanz genutzt werden kann.

Bei Fehlschlagen der Bestellung mindestens eines Teildienstes werden in A_{15} (der Hilfsprozess ist im Abschnitt 6.5 beschrieben) und A_{16} (der Basisprozess ist im Abschnitt 5.14 definiert) alle erfolgreich bestellten Teildienste abbestellt. Der Grund für die explizite Abbestellung liegt darin, dass – im Gegensatz zur Reservierung – die bestellten Teildienste i.A. nicht automatisch nach einer kurzen Zeitspanne freigegeben werden. Abschließend können in A_{17} die in A_4 für die Order-Verwaltung allokierten Ressourcen freigegeben werden und eine Mitteilung über das Fehlschlagen der Bestellung an die *End Site* geschickt werden.

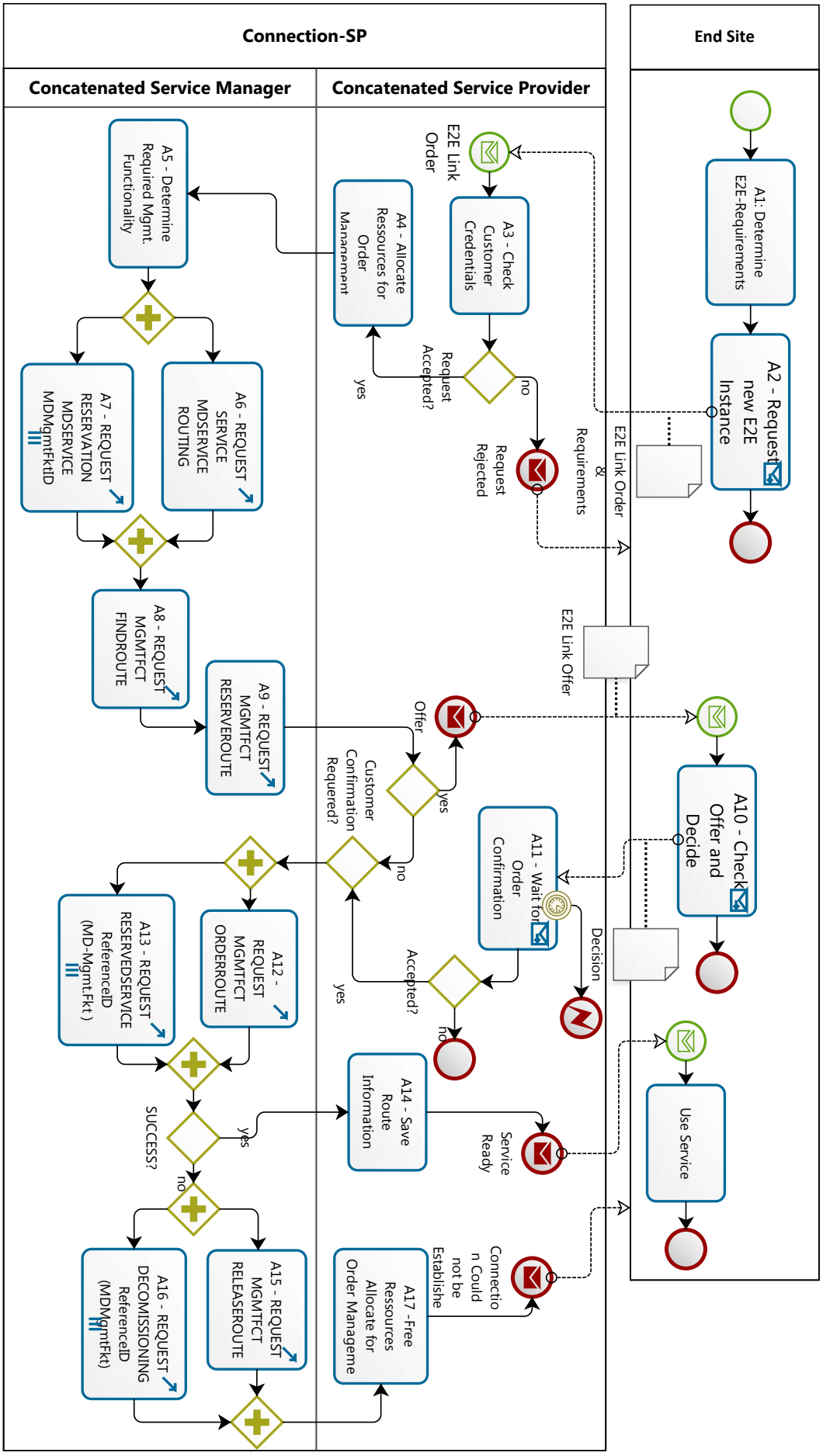
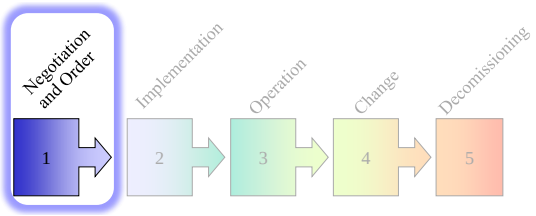


Abbildung 6.1.: Ordering

6.2. Hilfsprozess: Find Route

6.2.1. Einführung



Das Suchen und Finden einer Route wird in dieser Arbeit als eine Managementfunktion des ROUTING-Dienstes definiert und stellt somit die Verfeinerung der Aktivität A_4 in Abbildung 5.14 dar (für die genaue Beschreibung siehe Abschnitt 5.10). Die Suche einer Route selbst folgt dem im Kapitel 4 entwickelten *Source Routing mit semi-globalem Wissen und on-demand Delegation* Algorithmus.

6.2.2. Rollen

Die für den Ordering-Prozess relevanten Rollen sowie deren Verantwortlichkeiten sind in Tabelle 6.4 zusammengefasst.

6.2.3. Aktivitäten

Alle für den Hilfsprozess relevanten Aktivitäten sind in Tabelle 6.5 zusammengefasst.

6.2.4. Prozessartefakte

Wie bereits bei der Beschreibung dieses Hilfsprozesses als Teil der Bestellung erwähnt wurde (siehe insbesondere Beschreibung der Aktivität A_8 in Tabelle 6.2), werden für die Durchführung der Pfadsuche Informationen über die zwei End-Punkte, E2E-Anforderungen, Zwischensumme der Pfadsuche sowie die Informationen über Multi-Domain Managementdienste benötigt. Die Zwischensumme wird benötigt, um die Suche auch mittels Delegation dieser Aufgabe für den Rest der Strecke durchführen zu können. Die Angabe der Multi-Domain Managementdienste erlaubt bereits bei der Pfadsuche die Service Provider auszuschließen, die die Zusammenarbeit mit den angegebenen Providern der Managementdienste z.B. aus Policy-Gründen zurückweisen.

Rolle	Bezeichnung	Rollendefinition	
R_1	CONNECTION-SP	*Verantwortlichkeiten*	• Lokaler Provider der END SITE • Hier: Anschluss der END SITE und Anbieten unterstützter Dienste
		Fokus	–
		Kardinalität	1
		Art der Partizipation	statisch
		Vergabeverfahren	die End-Site wendet sich an ihren lokalen Provider
		Kandidatenmenge	alle Provider
R_2	CONCATENATED SERVICE MANAGER	*Verantwortlichkeiten*	• Bestimmung von ROUTING MANAGER • Kommunikation mit ROUTING MANAGER
		Fokus	ConcatenatedService
		Kardinalität	1
		Art der Partizipation	statisch
		Vergabeverfahren	Wird von CONNECTION-SP eingenommen
		Kandidatenmenge	–
R_3	ROUTING MANAGER	*Verantwortlichkeiten*	• Finden einer Route, die die spezifizierten Anforderungen erfüllt • Speichern der Informationen über die Route für die späteren Reservierungs- und Bestellungsanfragen
		Fokus	ConcatenatedService
		Kardinalität	1
		Art der Partizipation	dynamisch
		Vergabeverfahren	Wird von CONCATENATED SERVICE MANAGER gewählt
		Kandidatenmenge	alle Provider, die Routing-Dienst anbieten

Tabelle 6.4.: Hilfsprozess: *Find Route* – Rollen

6.2.5. Globales Prozessmodell

Der Suchalgorithmus (siehe Abbildung 6.2) beginnt mit der Wahl des nächsten SCP. Initial ist es einer der Endpunkte bzw. bei der Delegation der Routing-Aufgabe ist es der letzte SCP, bis zu dem eine Route gefunden wurde. Die Aktion A_1 markiert somit die "äußere Schleife" der Iteration über alle SCPs. Sollte kein SCP gefunden werden, wird die Suche erfolglos abgebrochen. Ansonsten wird überprüft, ob die Informationen über vorhandene Kapazitäten ausgehend vom ausgewählten SCP_{cur} weiter in die Richtung des End-Punktes vorhanden sind. Das kann z.B. dann der Fall sein, wenn durch die Schleifen ein und derselbe SCP über unterschiedlichen Wege erreicht werden kann. Da bei Verketteten Diensten i.A. mehr als eine Diensteigenschaft berücksichtigt werden soll, wird das Optimalitätsprinzip von Bellmann nicht eingehalten

Aktivität	Bezeichnung	Beschreibung	
A_1	DETERMINE NEXT SCP	*Input*	
		Tätigkeiten	Bestimmen des SCP_{cur} ausgehend von dem in die Richtung von SCP_{dest} gesucht wird.
		Output	
A_2	REQUEST INFORMATION (FROM SCPCUR TO SCPEND)	*Input*	• CONSTRAINTSTOPOLOGY (SCPCUR, SCPDEST) • CONSTRAINTSPROPERTIES (QOS, MGMTFCT)
		Tätigkeiten	• Abschicken einer Informationsanfrage an den SP, von dem der SCP_{cur} betrieben wird • Warten auf die Antwort
		Output	POSSIBLESECTIONS (INCLUDING PROPERTIES)
A_3	DETERMINE NEXT SECTION	*Input*	POSSIBLESECTIONS
		Tätigkeiten	Bestimmen welche Teilstrecke nach dem SCP_{cur} als nächste untersucht werden soll
		Input	• SECTIONPROPERTIES • SCPNEXT
A_4	CALCULATE AGGREGATED VALUE	*Input*	• INTERMEDIATEPROPERTIES (UP TO SCPCUR) • SECTIONPROPERTIES
		Tätigkeiten	Berechnen eines neuen Pfadgewichts aus den Eigenschaften des Weges bis SCP_{cur} und der ausgewählten Teilstrecke
		Output	• INTERMEDIATEPROPERTIES (UP TO SCPNEXT)
A_5	SAVE ROUTE INFORMATION	*Input*	• SECTIONDSM (PRO SECTION IN FOUND ROUTE) • SECTIONPROPERTIES (PRO SECTION IN FOUND ROUTE)
		Tätigkeiten	Abspeichern der Informationen über die gefundenen Route, so dass sie später reserviert und bestellt werden kann
		Output	
A_6	REQUEST SERVICE DELEGATION	*Input*	• E2ELINKID • SERVICEPARAMS
		Tätigkeiten	• Bestimmen des Proxy-SP, an den die Verantwortung für den Weg zwischen SCP_{cur} und SCP_{dest} delegiert werden soll • Abschicken einer Anfrage an den ausgewählten SP • Warten auf die Antwort
		Output	REFERENCEID (PROXY-SERVICE)
A_7	REQUEST MGMTFCT FINDROUTE (AN PROXY-SP)	*Input*	• REFERENCEID (PROXY-SERVICE) • SEARCHPARAMS (SCPCUR, SCPDEST, INTERMEDIATEPROPERTIES, E2E-CONSTRAINTS)
		Tätigkeiten	• Abschicken einer Anfrage für die Route-Suche an den Proxy-SP • Warten auf die Bestätigung
		Output	• REFERENCEID (REFERENCE TO FOUND ROUTE) • ROUTEPROPERTIES
A_8	REQUEST DECOMISSIONING REFERENCEID (PROXY-SP)	*Input*	REFERENCEID (PROXY-SERVICE)
		Tätigkeiten	• Abschicken der Anfrage über das Abbestellen des Proxy-Dienstes • Warten auf die Antwort
		Output	

Tabelle 6.5.: Hilfsprozess: *Find Route* – Aktivitäten

und der neue Weg muss untersucht werden (für eine ausführliche Diskussion zum Thema siehe Abschnitt 3.3).

Wenn die benötigte Information fehlt, wird sie in A_2 direkt bei der zuständigen SP-Domäne abgefragt (für die Beschreibung dieses Basisprozesses siehe Abschnitt 5.2). Sollte die direkte Informationsabfrage z.B. aus Policy-Gründen zurückgewiesen werden, wird in A_6 (siehe Abschnitt 5.13) und A_7 (siehe Abschnitt 5.10) versucht, die Information über den Rest der Route mit Hilfe der Aufgabendelegation abzufragen. Sollte auch das nicht gelingen, wird mit der Auswahl des nächsten SCPs in der Aktion A_1 fortgefahren.

Wenn die benötigte Information vorhanden ist oder *on-demand* abgefragt werden konnte, wird in der Aktion A_3 eine der aus dem SCP_{cur} ausgehende Strecke ausgewählt. Diese Aktion markiert die "innere Schleife", die über alle von SCP_{cur} ausgehenden Teilstrecken durch iteriert, die von der zuständigen SP-Domäne vorgeschlagen wurden. Erst wenn alle Teilstrecken erfolglos untersucht wurden, wird mit der Auswahl des nächsten SCPs in A_1 fortgefahren. Ansonsten wird in A_4 ein Aggregat-Wert aus den Eigenschaften des bereits untersuchten Weges und der neuen Teilstrecke berechnet. Sollte der neue Weg sowohl die E2E-Anforderungen erfüllen als auch mit der neuen Strecke den End-Punkt erreichen, dann wird in A_5 die Information über den Routen-Aufbau abgespeichert und der Suchprozess erfolgreich beendet.

Falls der neue Weg den End-Point noch nicht erreicht, aber die E2E-Anforderungen weiterhin erfüllt, dann wird weiter mit A_1 fortgefahren, um ausgehend von dem letzten SCP weiter suchen zu können. Falls jedoch bereits bei der Aggregation die E2E-Anforderungen gebrochen wurden, dann muss in A_3 eine alternative Teilstrecke ausgewählt werden. Zuerst muss aber der Fall berücksichtigt werden, dass die Informationen über den Rest des Weges durch die Delegation ermittelt wurde. In diesem Fall wird der entsprechende Dienst in A_8 freigegeben (für die Beschreibung dieses Basisprozesses siehe Abschnitt 5.14).

Der Prozess in Abbildung 6.2 verfeinert Aktivität A_4 des `REQUEST MGMTFCT` Prozesses (siehe Abschnitt 5.10) und stellt die Lösung des MCP-Problems (siehe Abschnitt 3.3) dar. Je nach Dienstart kann eine andere Strategie verfolgt werden bzw. es können unterschiedliche Suchverfahren parametrisiert angesprochen werden. Dies wird jedoch nicht weiter beschrieben.

Ein weiterer bereits angesprochener Aspekt hängt damit zusammen, dass in diesem Kapitel alle Multi-Domain Managementfunktionen als extern betrachtet werden. Bei der Implementierung des Verfahrens können viele dieser Funktionen i.A. von dem Service Provider übernommen werden, der auch die Rolle *Concatenated Service Provider* einnimmt. In Abbildung 6.3 wird die entsprechende Fallunterscheidung "Is functionality locally available?" zu Illustrationszwecken dargestellt. Auf eine gesonderte Beschreibung dieses Prozesses wird an dieser Stelle verzichtet.

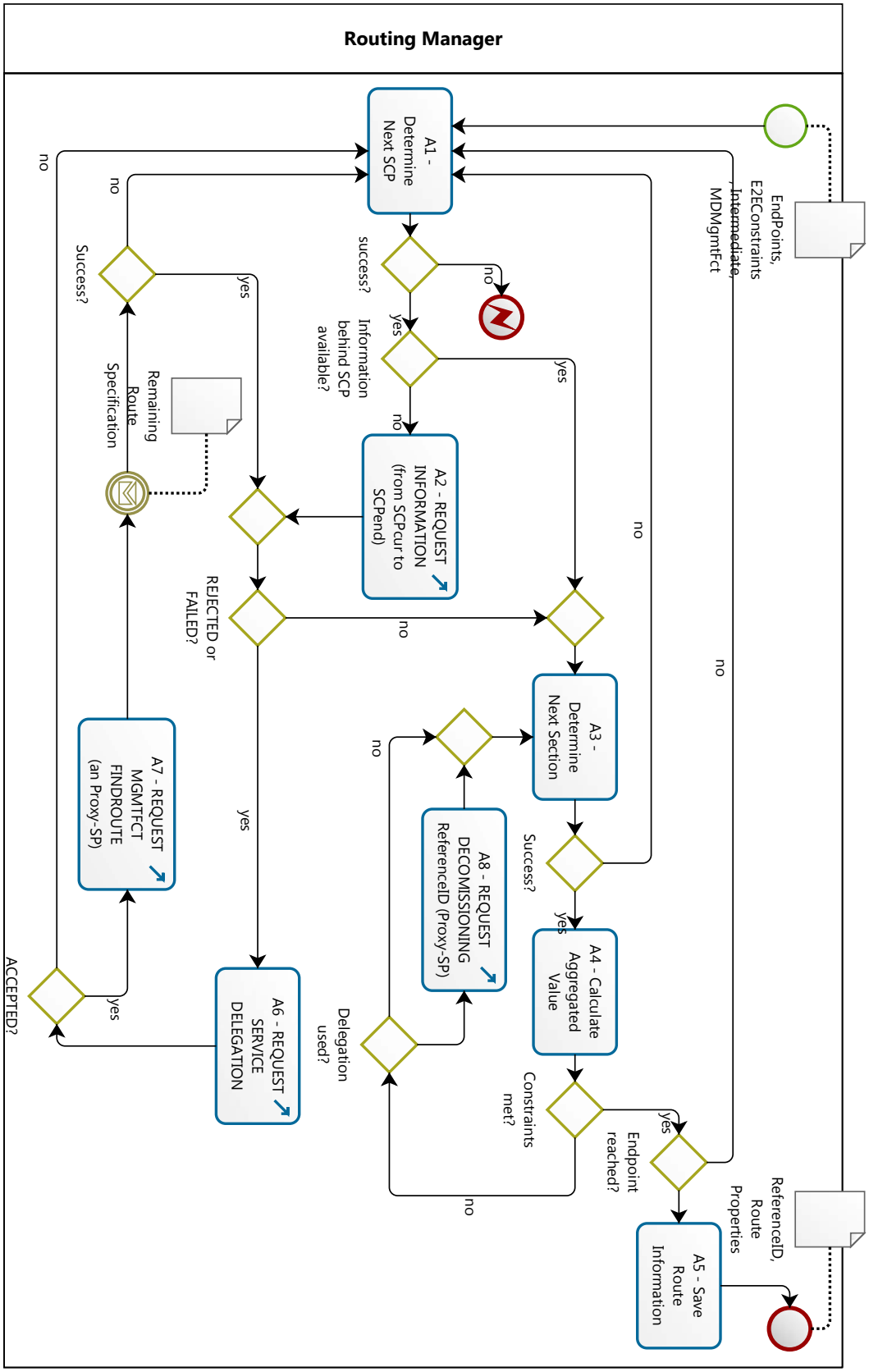


Abbildung 6.2.: Hilfsprozess: Find Route

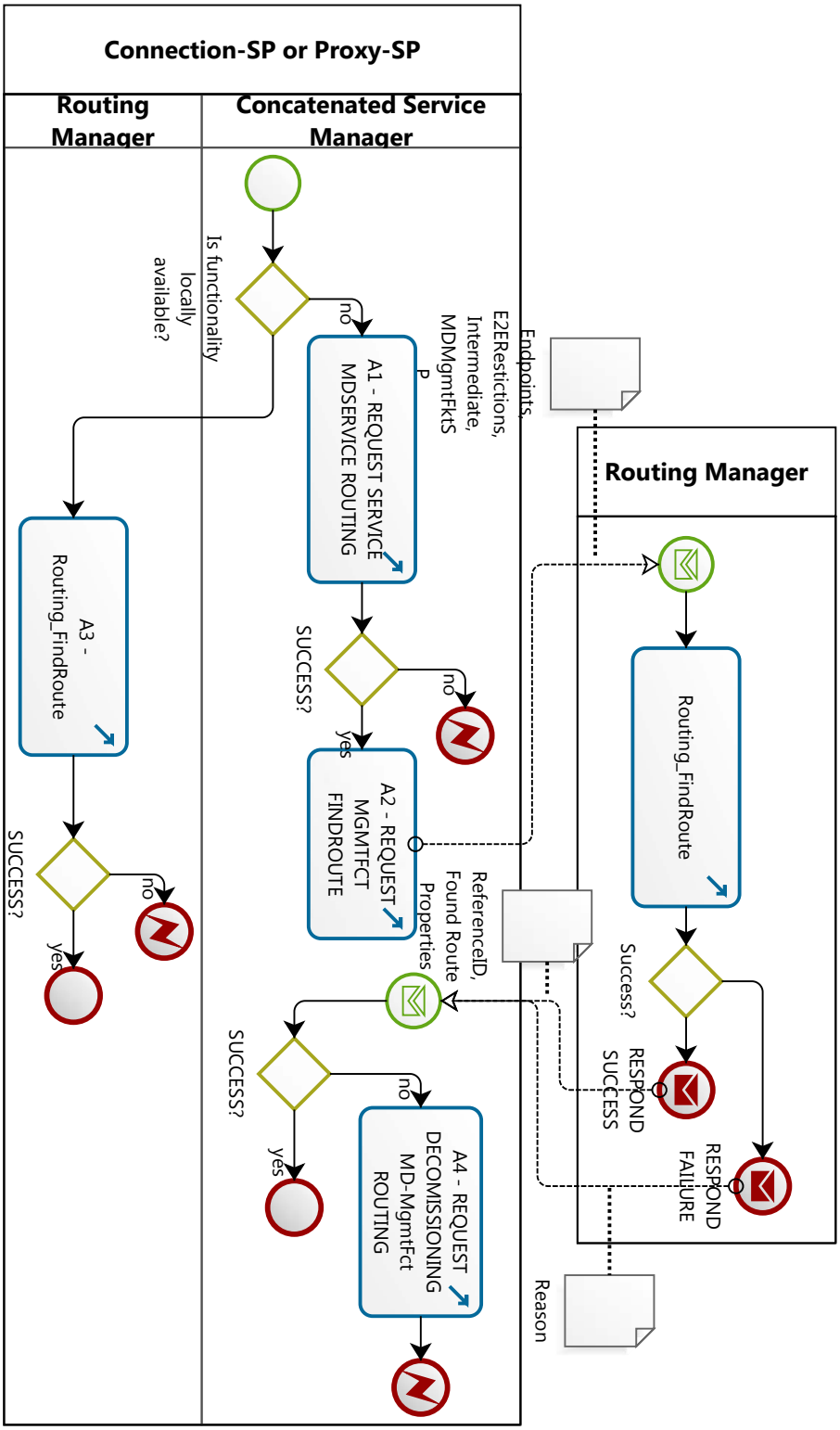
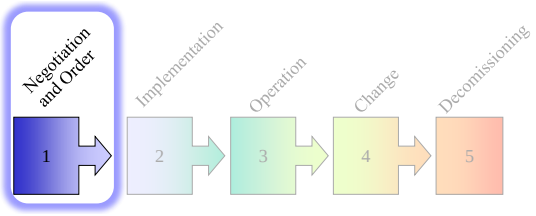


Abbildung 6.3.: Wrapper: Find Route

6.3. Hilfsprozess: Reserve Route

6.3.1. Einführung



Das Reservieren der gefundenen Route wird – ähnlich wie der Hilfsprozess *Find Route* (siehe Abschnitt 6.2) – als eine Managementfunktion des ROUTING-Dienstes definiert. Der Prozess stellt somit eine weitere Verfeinerung der Aktivität A_4 in Abbildung 5.14 dar (für die genaue Beschreibung siehe Abschnitt 5.10).

Da bei der Reservierung der einzelnen Teildienste dei Provider schlechtere Eigenschaften zusichern dürfen (siehe entsprechende Diskussionen und Festlegungen in Abschnitten 3.2 und 5.1), wird u.U. ein Re-Routing benötigt. Um das zu ermöglichen, werden die Reservierungsanfrage für die Teilstrecken nicht gleichzeitig, sondern sequentiell entlang der gefundenen Route versendet.

6.3.2. Rollen

Die für den Ordering-Prozess relevanten Rollen sowie deren Verantwortlichkeiten sind in Tabelle 6.6 zusammengefasst.

Rolle	Bezeichnung	Rollendefinition	
R_1	ROUTING MANAGER	*Verantwortlichkeiten*	• Reservierung der zuvor gefundenen Route für die spätere Bestellungsanfrage
		Fokus	ConcatenatedService
		Kardinalität	1
		Art der Partizipation	dynamisch
		Vergabeverfahren	Wird von CONCATENATED SERVICE MANAGER gewählt
		Kandidatenmenge	alle Provider, die Routing-Dienst anbieten

Tabelle 6.6.: Hilfsprozess: *Reserve Route* – Rollen

6.3.3. Aktivitäten

Alle für den Hilfsprozess relevanten Aktivitäten sind in Tabelle 6.7 zusammengefasst.

Aktivität	Bezeichnung	Beschreibung	
A_1	CALCULATE PER-SECTION REQUIREMENTS	*Input*	• SECTIONPROPERTIES (PROPERTY-RANGE, PER SECTION) • E2ERESTRICTIONS
		Tätigkeiten	Ausgehend von den Informationen über die möglichen Wertebereiche Berechnen der Anforderungen an jede Teilstrecke entlang der gefundenen Route
		Output	• REQUESTEDREQUIREMENTS (PROPERTY-VALUE, PER SECTION)
A_2	CHOOSE NEXT SECTION FOR RESERVATION	*Input*	FOUND ROUTE
		Tätigkeiten	Bestimmen der nächsten zu reservierenden Teilstrecke
		Output	
A_3	REQUEST RESERVATION CONNECTION	*Input*	REQUESTEDREQUIREMENTS (PROPERTY-VALUE)
		Tätigkeiten	• Abschicken einer Reservierungsanfrage an den Teilstreckenprovider • Warten auf die Antwort
		Input	RESERVEDPROPERTIES
A_4	REQUEST MGMTFCT RESERVEROUTE (AN PROXY-SP)	*Input*	INTERMEDIATEPROPERTIES (UP TO SCPCUR)
		Tätigkeiten	• Abschicken der Reservierungsanfrage für den Rest der Route an den Proxy-SP • Warten auf die Antwort
		Output	RESERVEDPROPERTIES
A_5	REQUEST DECOMISSIONING REFERENCEID (PROXY-SP)	*Input*	REFERENCEID (PROXY-SERVICE)
		Tätigkeiten	• Abschicken der Anfrage für das Abbestellen des Proxy-Dienstes • Warten auf die Antwort
		Output	
A_6	FIND ROUTE (FOR REMAINING PART)	*Input*	SEARCHPARAMS (SCPCUR, SCPDEST, INTERMEDIATEPROPERTIES, E2E-CONSTRAINTS)
		Tätigkeiten	Finden eines neuen Wegs zwischen SCP_{cur} und SCP_{dest} sodass die E2E-Anforderungen erfüllt werden können
		Output	
A_7	REQUEST CANCELRESERVATION (RESERVED SECTIONS)	*Input*	REFERENCEID (PER RESERVED SECTION)
		Tätigkeiten	• Abschicken der Anfrage für die Beendigung der Teilstreckenreservierung • Warten auf die Antwort
		Output	

Tabelle 6.7.: Hilfsprozess: *Reserve Route* – Aktivitäten

6.3.4. Prozessartefakte

Für die Reservierung wird vor allem die REFERENCEID gebraucht, um den Bezug zu der bereits gefundenen Route herzustellen. Um die Delegation zu unterstützen, muss weiterhin die Zwischensumme INTERMEDIATE beim Prozessaufruf übergeben werden, so dass der Proxy-SP in seinem Verantwortungsbereich die Anforderungen an die Teildienste entsprechend berechnen kann. Die Zwischensumme soll entsprechend dem UML-Diagramm aus Abbildung 4.53 strukturiert werden, wobei keine Wertebereiche, sondern ausschließlich feste Werte vorkommen dürfen.

Im Erfolgsfall entspricht das Ergebnis des Prozesses den zugesicherten Eigenschaften für den eigenen Verantwortungsbereich. Wird die Verantwortung für eine Teilstrecke an einen Proxy-SP delegiert, so werden dessen Zusicherungen dabei auch mitberücksichtigt. Die zugesicherten Eigenschaftenwerte sollen nach dem UML-Diagramm aus der Abbildung 4.52 strukturiert werden.

6.3.5. Globales Prozessmodell

Die "äußere Schleife" des Route-Reservierungsprozesses (siehe Abbildung 6.4) wird durch die Aktion A_1 markiert, in der für alle noch zu reservierenden Teilstrecken ein Soll-Wert für deren Eigenschaften bestimmt wird. Sollte das unter der Berücksichtigung der E2E-Anforderungen möglich sein, wird in A_2 die nächste zu reservierende Strecke ausgewählt. Die Reservierung der ausgewählten Teilstrecke wird entweder in A_3 direkt, oder – falls deren tatsächlicher Aufbau von Proxy-SP verschattet wird – in A_4 indirekt angefordert (die entsprechende Basisprozesse siehe in Abschnitten 5.6 und 5.10).

Nach einer erfolgreichen Reservierung wird zunächst überprüft, ob der Ziel-End-Point bereits erreicht wurde oder nicht. Sollte das der Fall sein, wird der Reservierungsprozess beendet. Falls der End-Point noch nicht erreicht wurde, entscheidet sich das weitere Vorgehen anhand der zugesicherten Teilstreckeneigenschaften: entsprechen die zugesicherten Werte den geforderten, dann wird mit der Aktion A_2 weitergefahren, ansonsten wird die Aktion A_1 als nächste ausgeführt.

Sollte die Reservierung der Teilstrecke fehlschlagen, dann wird in der Aktion A_6 auf die *Find Route* Hilfsfunktion zurückgegriffen (siehe Abschnitt 6.2). Dabei wird versucht, ausgehend vom letzten SCP einen neuen Weg zum Ziel-SCP zu finden, der die E2E-Anforderungen erfüllt. Zuvor soll allerdings – falls vorhanden – der Proxy-Dienst abbestellt werden, was in der Aktion A_5 geschieht (siehe Abschnitt 5.14). Diese Freigabe soll unabhängig davon erfolgen, ob A_3 oder A_4 fehlschlug, denn die neue Route kann u.U. einen komplett anderen Verlauf nehmen.

Falls das Re-Routing erfolgreich durchgeführt werden konnte, wird weiter mit A_1 fortgefahren. Ansonsten werden in A_7 alle reservierten Teilstrecken freigegeben (siehe Abschnitt 5.7) und der Algorithmus wird abgebrochen.

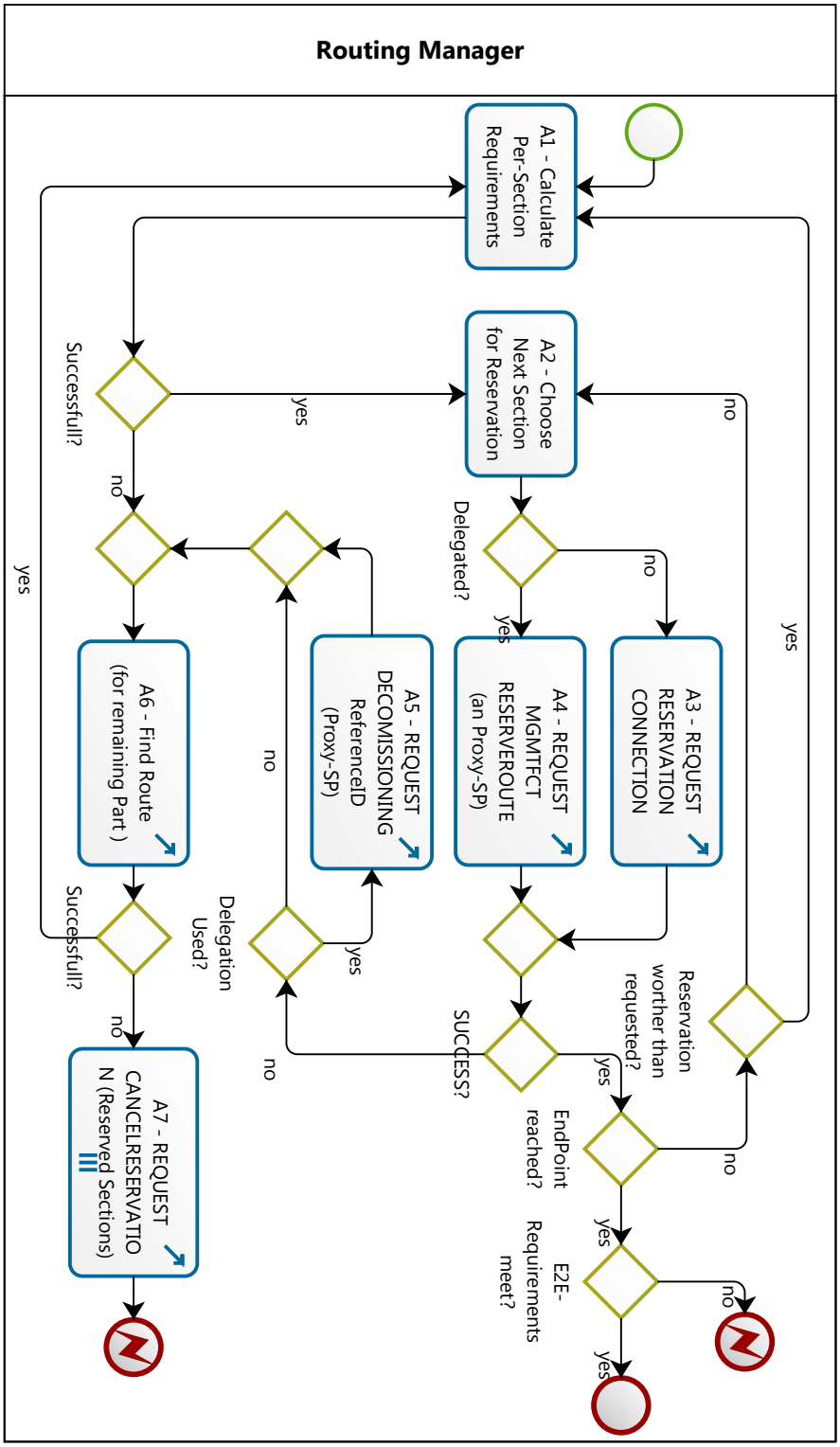
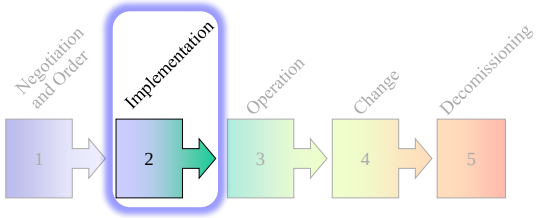


Abbildung 6.4.: Routing: Reservieren der Teildienste entlang einer Route

6.4. Hilfsprozess: Order Route

6.4.1. Einführung



Die Bestellung der bereits reservierten Teildienste entlang der Route stellt eine weitere Verfeinerung der Aktivität A_4 in Abbildung 5.14 dar (für die genaue Beschreibung des Basisprozesses siehe Abschnitt 5.10). Da bei der Bestellung der reservierten Teildienste ihre Provider nicht schlechtere Eigenschaften als gefordert zusichern dürfen (siehe entsprechende Diskussionen und Festlegungen in Abschnitten 3.2 und 5.1), kann die Reservierungsanfrage für alle reservierten Teilstrecken einer neuen Dienstinstanz gleichzeitig an die jeweilige SPs geschickt werden.

6.4.2. Rollen

Die für den Ordering-Prozess relevanten Rollen sowie deren Verantwortlichkeiten sind in Tabelle 6.8 zusammengefasst.

Rolle	Bezeichnung	Rollendefinition	
R_1	ROUTING MANAGER	*Verantwortlichkeiten*	Bestellung der zuvor reservierten Route
		Fokus	ConcatenatedService
		Kardinalität	1
		Art der Partizipation	dynamisch
		Vergabeverfahren	Wird von CONCATENATED SERVICE MANAGER gewählt
		Kandidatenmenge	alle Provider, die Routing-Dienst anbieten

Tabelle 6.8.: Hilfsprozess: *Order Route* – Rollen

6.4.3. Aktivitäten

Alle für den Hilfsprozess relevanten Aktivitäten sind in Tabelle 6.9 zusammengefasst.

Aktivität	Bezeichnung	Beschreibung	
A_1	REQUEST MGMTFCT ORDERROUTE (AN PROXY-SP)	*Input*	REFERENCEID (PROXY-SERVICE)
		Tätigkeiten	• Abschicken an den Proxy-SP der Anfrage für die Bestellung aller Teildienste in seinem Verantwortungsbereich • Warten auf die Antwort
		Output	
A_2	REQUEST RESERVEDSERVICE (RESERVED SECTIONS)	*Input*	REFERENCEID (PER RESERVED SECTION)
		Tätigkeiten	• Abschicken der Bestellanfragen an alle Provider der reservierten Teildienste • Warten auf die Antwort
		Output	

Tabelle 6.9.: Hilfsprozess: *Order Route* – Aktivitäten

6.4.4. Prozessartefakte

Für das Ordering wird ausschließlich die REFERENCEID benötigt, um den Bezug zu der bereits reservierten Route herzustellen. Weitere für die Bestellung relevanten Informationen sollten von dem *Routing Manager* SP bereits nach der erfolgreichen Reservierung abgespeichert werden.

6.4.5. Globales Prozessmodell

Die Aktionen A_1 und A_2 werden parallel ausgeführt. Die Aktion A_1 wird erst dann ausgeführt, wenn ein Proxy-SP verwendet wird. In A_1 wird an den Proxy-SP eine Anfrage für die Bestellung aller Teilstrecken in deren Verantwortungsbereich geschickt (siehe auch Abschnitt 5.10). Die Aktion A_2 wird analog erst dann ausgeführt, wenn es direkt reservierte Teilstrecken gibt. In A_2 wird die Bestellungsanfrage (siehe Abschnitt 5.8) gleichzeitig an alle Teilstrecken-Provider geschickt. Das Ergebnis dieses Prozesses wird dadurch bestimmt, ob alle Teilstrecken erfolgreich bestellt werden konnten oder nicht.

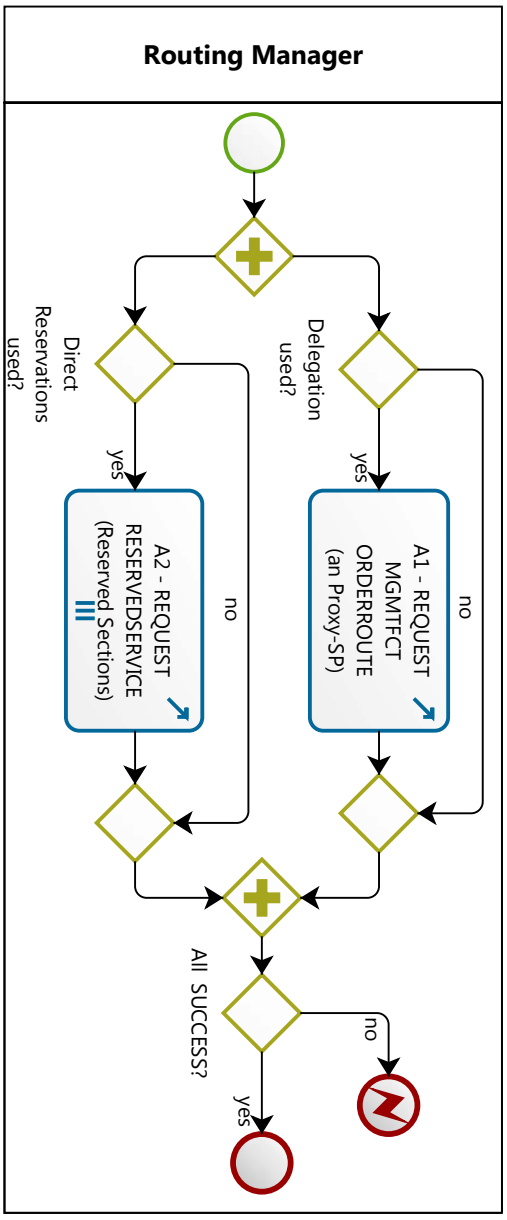
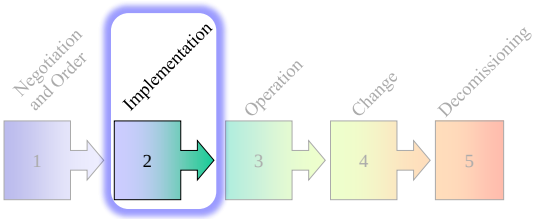


Abbildung 6.5.: Routing: Bestellen der Teildienste entlang einer Route

6.5. Hilfsprozess: Release Route

6.5.1. Einführung



Falls beim Hilfsprozess *Order Route* (siehe Abschnitt 6.4) mindestens ein Teildienst nicht bestellt werden konnte, kann die Verbindung nicht geschaltet werden. Da die bestellten Teildienste i.A. nicht automatisch freigegeben werden, müssen alle erfolgreich bestellten Teilstrecken explizit freigegeben werden. Da dies auch dann durchgeführt werden muss, wenn die Bestellung der Multi-Domain Managementfunktionalität fehlgeschlagen ist (siehe SLM-Prozess *Ordering* im Abschnitt 6.1), wird die Freigabe der bestellten Teilstrecken als ein separater Hilfsprozess aufgefasst. Die Anfrage für die Dienstinstanz-Abbestellung wird gleichzeitig an alle Teilstreckenerbringer geschickt, um ein unnötiges Blockieren der Ressourcen möglichst zu vermeiden.

6.5.2. Rollen

Die für den Ordering-Prozess relevanten Rollen sowie deren Verantwortlichkeiten sind in Tabelle 6.10 zusammengefasst.

Rolle	Bezeichnung	Rollendefinition	
R_1	ROUTING MANAGER	*Verantwortlichkeiten*	Freigabe der zuvor reservierten Route
		Fokus	ConcatenatedService
		Kardinalität	1
		Art der Partizipation	dynamisch
		Vergabeverfahren	Wird von CONCATENATED SERVICE MANAGER gewählt
		Kandidatenmenge	alle Provider, die Routing-Dienst anbieten

Tabelle 6.10.: Hilfsprozess: *Release Route* – Rollen

6.5.3. Aktivitäten

Alle für den Hilfsprozess relevanten Aktivitäten sind in Tabelle 6.11 zusammengefasst.

Aktivität	Bezeichnung	Beschreibung	
A_1	REQUEST DECOMISSIONING (ORDERED SECTIONS)	*Input*	REFERENCEID (PER RESERVED SECTION)
		Tätigkeiten	• Abschicken der Abbestellungsanfragen an alle Provider, bei denen Teilstrecken erfolgreich bestellt wurden • Warten auf die Antwort
A_2	REQUEST MGMTFCT RELEASEROUTE (TO PROXY-SP)	*Input*	REFERENCEID (PROXY-SERVICE)
		Tätigkeiten	• Abschicken an den Proxy-SP der Anfrage für die Abbestellung aller Teildienste in dessen Verantwortungsbereich • Warten auf die Antwort
		Output	
A_3	REQUEST DECOMISSIONING (PROXY-SP)	*Input*	REFERENCEID (PROXY-SERVICE)
		Tätigkeiten	• Abschicken der Anfrage für das Abbestellen des Proxy-Dienstes • Warten auf die Antwort
		Output	

Tabelle 6.11.: Hilfsprozess: *Release Route* – Aktivitäten

6.5.4. Prozessartefakte

Für das Abbestellen der Teilstrecken wird ausschließlich die REFERENCEID benötigt, um den Bezug zu den Routeninformationen herzustellen. Die REFERENCEIDs der jeweiligen Teilstrecken sowie die DSM-Kommunikationsschnittstellen der entsprechenden SP-Domäne sind ein Teil dieser Informationen.

6.5.5. Globales Prozessmodell

Der Prozess zur Freigabe der bestellten Teilstrecken ist in Abbildung 6.6 dargestellt. Die Aktionen A_1 und A_2, in denen die Abbestellung der Teildienste an die jeweiligen Provider bzw. an den Proxy-SP signalisiert wird, können gleichzeitig ausgeführt werden (für die Beschreibung dieser Basisfunktionen siehe entsprechend die Abschnitte 5.10 und 5.14). Nachdem die Ausführung von A_2 abgeschlossen wurde, wird in A_3 der Proxy-Dienst selbst abbestellt. Der Prozess endet, nachdem alle Teilstrecken und die – u.U. mehrere "verschachtelten" – Proxy-SPs abbestellt wurden.

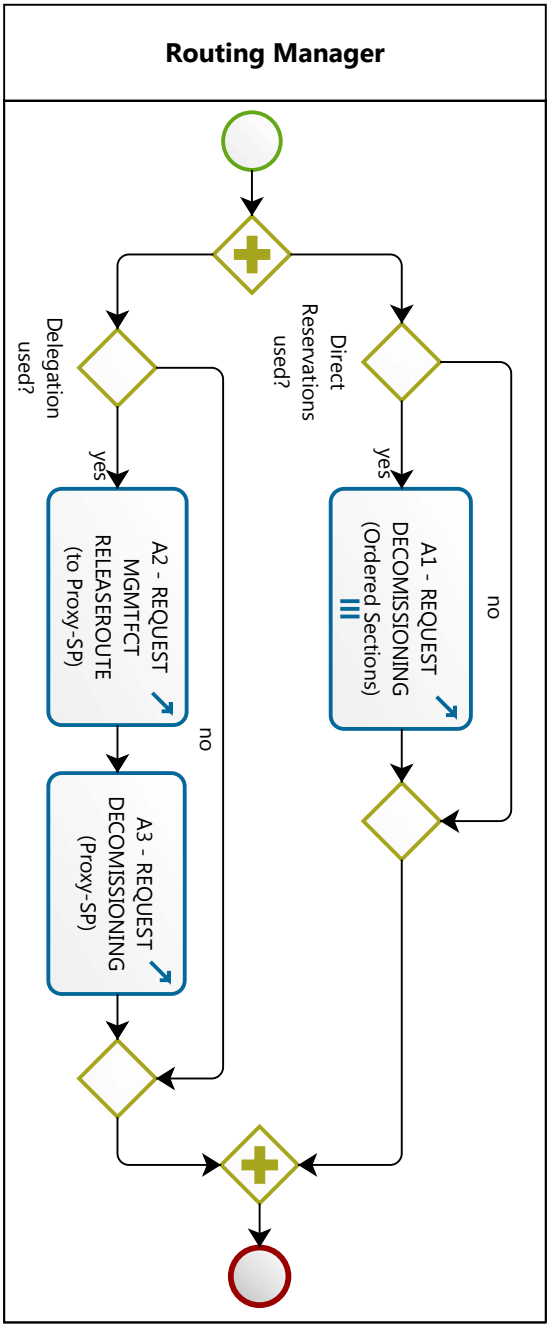
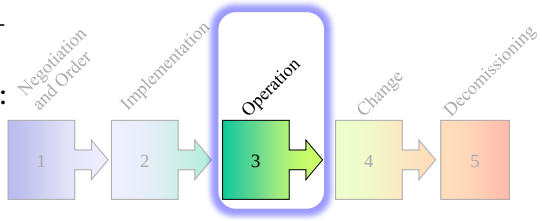


Abbildung 6.6.: Freigeben bestellter Teildienste entlang der Route

6.6. SLM-Prozess: Monitoring, Reporting und Anbindung an Incident & Problem Management

6.6.1. Einführung



Im Betrieb gehört die kontinuierliche Überwachung der Dienstinstanz-QoS (engl.: *Monitoring*) sowie die Berichterstattung (engl.: *Reporting*) an den Customer in den vereinbarten Zeitabständen zu den Aufgaben des Service-Level-Managements (vergleiche auch Abschnitte 3.4, 3.5 und 3.6).
Das Ziel der Überwachung besteht nicht nur darin, die Zustandsinformationen für Berichte zu sammeln, sondern vor allem darin, die Verletzung der vereinbarten Dienstgüte zu erkennen und die Ausführung der Fehlerbehebungsprozesse (nach ITIL-Nomenklatur *Incident & Problem Management*) anzustoßen. Da diese Aufgaben sehr stark miteinander verflochten sind, werden sie in diesem Abschnitt in einem gemeinsamen Prozess definiert.

6.6.2. Rollen

Die für den Ordering-Prozess relevanten Rollen sowie deren Verantwortlichkeiten sind in Tabelle 6.12 zusammengefasst.

6.6.3. Aktivitäten

Alle für der Prozess relevanten Aktivitäten sind in Tabelle 6.13 zusammengefasst.

6.6.4. Prozessartefakte

Für die Kommunikation mit der *End Site* werden hier, ähnlich wie bei Bestellung und Inbetriebnahme (siehe Abschnitt 6.1) keine festen Vorgaben gemacht. Für die Kopplung automatischer Überwachungssysteme bietet es sich an, sowohl die Monitoring-Informationen als auch die Berichte entsprechend dem UML-Diagramm in Abbildung 4.50 zu strukturieren. Diese Strukturierungsart soll auf jeden Fall für die Antwort der Informationsabfrage verwendet werden (siehe A_1 in Abbildung 6.7 oder auch die Definition des entsprechenden Basisprozesses im Abschnitt 5.10). Dasselbe gilt auch für die Benachrichtigung des *Incident & Problem Managers*.

Rolle	Bezeichnung	Rollendefinition	
R_1	END SITE	*Verantwortlichkeiten*	• Repräsentant auf Kundenseite • Hier: Nimmt die Überwachungsinformationen und Berichte entgegen
		Fokus	–
		Kardinalität	1
		Art der Partizipation	statisch
		Vergabeverfahren	wird bei der Bestellung bestimmt
		Kandidatenmenge	–
R_2	CONNECTION-SP	*Verantwortlichkeiten*	• Lokaler Provider der END SITE • Hier: Anschluss der END SITE und Anbieten unterstützter Dienste
		Fokus	–
		Kardinalität	1
		Art der Partizipation	statisch
		Vergabeverfahren	die End-Site wendet sich an ihren lokalen Provider
		Kandidatenmenge	alle Provider
R_3	CONCATENATED SERVICE PROVIDER	*Verantwortlichkeiten*	Stellt der End Site die Monitoring-Informationen und Überwachungsberichte zur Verfügung
		Fokus	ConcatenatedService
		Kardinalität	1
		Art der Partizipation	statisch
		Vergabeverfahren	Wird von CONNECTION-SP eingenommen
		Kandidatenmenge	–
R_4	CONCATENATED SERVICE MANAGER	*Verantwortlichkeiten*	• Abholen der Monitoring-Informationen • Update der Überwachungsberichte • Benachrichtigung von INCIDENT & PROBLEM MANAGER in Problemfällen
		Fokus	ConcatenatedService
		Kardinalität	1
		Art der Partizipation	statisch
		Vergabeverfahren	Wird von CONNECTION-SP eingenommen
		Kandidatenmenge	–
R_5	INCIDENT & PROBLEM MANAGER	*Verantwortlichkeiten*	Behandlung der aufgetretenen Probleme
		Fokus	ConcatenatedService
		Kardinalität	1
		Art der Partizipation	statisch
		Vergabeverfahren	–
		Kandidatenmenge	alle Provider, die diesen Managementdient anbieten

Tabelle 6.12.: SLM-Processes Monitoring und Reporting – Rollen

Aktivität	Bezeichnung	Beschreibung	
A_1	REQUEST MGMTFCT GETMONSTATE (to MONITORING MANAGER)	*Input*	E2ELINKID
		Tätigkeiten	• Schicken einer Anfrage an den MONITORING MANAGER, um die Monitoring-Informationen abzuholen • Warten auf die Antwort
		Output	MONITORINGSTATE
A_2	PROVIDE MONITORING DATA TO CUSTOMER	*Input*	MONITORINGSTATE
		Tätigkeiten	• Vorbereiten der Monitoring-Informationen entsprechend der END SITE Anforderungen • Stellen die Monitoring-Informationen der END SITE zur Verfügung
		Output	
A_3	NOTIFY INCIDENT&PROBLEM MANAGER	*Input*	• E2ELINKID • MONITORINGSTATE
		Tätigkeiten	Benachrichtigen des für die Dienstinstanz zuständigen INCIDENT&PROBLEM MANAGERS über die Verletzung eines Thresholds, sodass der Fehlerbehebungsprozess gestartet werden kann
		Output	
A_4	UPDATE REPORT INFORMATION	*Input*	• E2ELINKID • REPORTINFORMETION • MONITORINGSTATE
		Tätigkeiten	Update des Reports mit den Monitoring-Informationen
		Output	REPORTINFORMATION
A_5	PROVIDE REPORT TO CUSTOMER	*Input*	• E2ELINKID • REPORTINFORMATION
		Tätigkeiten	Übermitteln des Berichts an die END SIZE
		Output	

Tabelle 6.13.: Monitoring und Reporting – Aktivitäten

6.6.5. Globales Prozessmodell

Der Prozess (siehe Abbildung 6.7) wird von einem regelmäßigen Timer-Event angestoßen. In der Aktion A_1 wird eine Informationsanfrage an die für das Monitoring verantwortliche Rolle geschickt (für die Beschreibung der entsprechenden Basisfunktion siehe Abschnitt 5.10). Nach dem Erhalt der Antwort unterteilt sich die Prozessausführung in zwei Flows, die parallel vom *Concatenated Service Provider* und vom *Concatenated Service Manager* ausgeführt werden. Falls die *End Site* die Monitoring-Informationen erhalten darf, werden sie in A_2 zunächst entsprechend der Vereinbarung aufbereitet und dann der *End Site* zur Verfügung gestellt. Parallel dazu wird vom *Concatenated Service Manager* überprüft, ob der aktuelle Dienstinstanz-Zustand einen der vereinbarten Grenzwerte (engl.: *Threshold*) nicht einhalten konnte. Sollte

das der Fall sein, wird in A_3 eine entsprechende Benachrichtigung an den *Incident & Problem Manager* geschickt. Der Bericht in A_4 aktualisiert. Der Bericht selbst wird der *End Site* in A_5 zur Verfügung gestellt; diese Aktivität wird von einem separaten Timer angestoßen, der für die Einhaltung der vereinbarten Berichtintervalle zuständig ist.

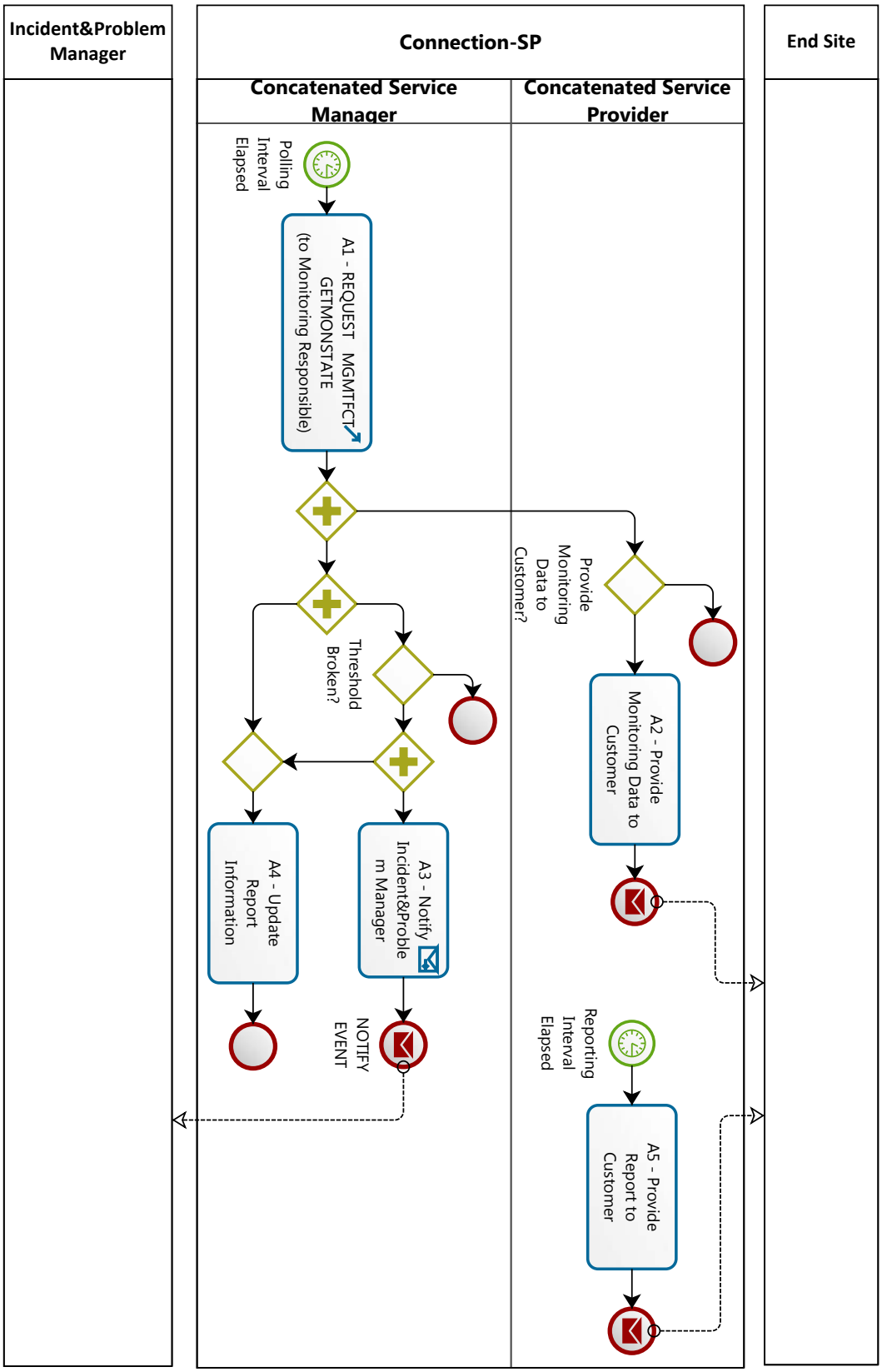
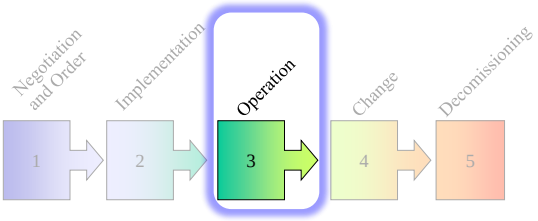


Abbildung 6.7.: Monitoring, Reporting

6.7. Hilfsprozess: Monitor Concatenated Service

6.7.1. Einführung



Der SLM-Prozess für die Dienstinstanzüberwachung (siehe Abschnitt 6.6) stützt sich auf die Informationen, die ihm von dem Monitoring-Verantwortlichen zur Verfügung gestellt werden. Das Monitoring ist ein kontinuierliches Prozess und ist i.A. vom Aktualisierungsintervall dieser Informationen unabhängig. Die Aktualität der Zustandsinformationen einzelner Teildienste kann sowohl durch ein aktives Polling seitens des *Monitoring Manager* als auch durch ein Push-Modell seitens des *Partial Service Providers* garantiert werden.

6.7.2. Rollen

Die für den Ordering-Prozess relevanten Rollen sowie deren Verantwortlichkeiten sind in Tabelle 6.14 zusammengefasst.

6.7.3. Aktivitäten

Alle für den Hilfsprozess relevanten Aktivitäten sind in Tabelle 6.15 zusammengefasst.

6.7.4. Prozessartefakte

Die Informationsabfrage sowie die Zugehörigkeit der Monitoring-Informationen zu einer Dienstinstanz werden anhand der E2ELINKID sichergestellt. Die Zustandsinformationen sind entsprechend dem UML-Diagramm aus der Abbildung 4.54 zu strukturieren.

Rolle	Bezeichnung	Rollendefinition	
R_1	MONITORING MANAGER	*Verantwortlichkeiten*	• Koordiniert das Abholen der Informationen aus allen in Teildienst-Monitoring involvierten SP-Domänen • Korreliert Informationen mehrerer SP-Domänen
		Fokus	ConcatenatedService
		Kardinalität	1
		Art der Partizipation	dynamisch
		Vergabeverfahren	Wird vom CONCATENATED SERVICE MANAGER während der Ordering-Prozesses gewählt
		Kandidatenmenge	alle Provider, die diesen Managementdient anbieten
R_2	PARTIAL SERVICE PROVIDER (SUPPORT INFO PULL)	*Verantwortlichkeiten*	• Überwachen eigener Teilstrecken • Warten auf Anfrage bzgl. Überwachungsdaten • Weitergabe der Monitoring-Informationen an den MONITORING MANAGER
		Fokus	MonitoredLink
		Kardinalität	n
		Art der Partizipation	dynamisch
		Vergabeverfahren	Wird von ROUTING MANAGER während des Routings bestimmt
		Kandidatenmenge	alle Provider, die Verbindungsdienste anbieten
R_3	PARTIAL SERVICE PROVIDER (SUPPORT INFO PUSH)	*Verantwortlichkeiten*	• Überwachen der eigenen Teilstrecken • Benachrichtigung des MONITORING MANAGER über den Monitoring-Zustand
		Fokus	MonitoredLink
		Kardinalität	n
		Art der Partizipation	dynamisch
		Vergabeverfahren	Wird vom ROUTING MANAGER während des Routings bestimmt
		Kandidatenmenge	alle Provider, die Verbindungsdienste anbieten

Tabelle 6.14.: Hilfsprozess: *Monitoring* – Rollen

6.7.5. Globales Prozessmodell

Der Monitoring-Prozess bei automatisch geschalteten Diensten soll zeitnah mit der Bestellung einer neuen Dienstinstanz (siehe Aktivität A_{13} in Abbildung 6.1) starten. Bei manuell geschalteten Diensten können Abweichungen von dieser Regel auftreten, in Abhängigkeit davon, ob die Teilstrecken der noch nicht in Betrieb genommenen Dienstinstanz überwacht werden sollen (z.B. zum Zwecke der Statusverfolgung) oder erst nachdem alle Teilstrecken in Betrieb genommen und zusammen geschaltet wurden.

Aktivität	Bezeichnung	Beschreibung	
A_1	START POLLING TIMER	*Input*	
		Tätigkeiten	• Bestimmen der Häufigkeit, mit der die Monitoring-Informationen von den einzelnen SP-Domänen abgefragt werden sollen • Timer starten
		Output	
A_2	REQUEST MGMTFCT GETMONSTATE	*Input*	E2ELINKID
		Tätigkeiten	• Abfragen des Monitoring-Zustands aller Verbindungsdienste, die von der SP-Domäne als Teil der Dienstinstanz mit E2ELINKID erbracht werden • Warten auf die Antwort
		Output	PARTIALSERVICESTATE
A_3	RETRIEVE MONITORING STATE	*Input*	E2ELINKID
		Tätigkeiten	• Abholen der Monitoring-Daten für die in Eigenregie erbrachten Teildienste eines E2E Links • Aufbereiten der Daten, sodass nur die bei Dienstbestellung Informationen vorkommen
		Output	PARTIALSERVICESTATE
A_4	WAIT FOR ANSWER	*Input*	
		Tätigkeiten	• Warten auf die Antwort des PARTIAL SERVICE PROVIDERS • Abbruch bei Zeitüberschreitung
		Output	
A_5	UPDATE MONITORING INFORMATION	*Input*	• E2EINSTANCESTATE • PARTIALSERVICESTATE
		Tätigkeiten	Aktualisieren des E2E-Instanzzustands, basierend auf dem Zustand deren Teildienste
		Input	E2EINSTANCESTATE
A_6	WAIT FOR NOTIFICATION	*Input*	
		Tätigkeiten	• Warten auf automatische Benachrichtigungen von den PARTIAL SERVICE PROVIDER, die das Push-Modell unterstützen • Abbruch bei Zeitüberschreitung (Optional, hängt mit der Monitoring-Strategie zusammen)
		Output	PARTIALSERVICESTATE

Tabelle 6.15.: Hilfsprozess: *Monitor Concatenated Service* – Aktivitäten

In Abhängigkeit davon, ob Teildienste involviert sind, deren Monitoring-Zustand durch Polling abgefragt wird, wird in der Aktivität A_1 der entsprechende Timer gestartet. Analog dazu, falls die Provider mancher Teildienste das Push-Modell unterstützen, wird die Schleife aus den Aktivitäten A_6 und A_5 gestartet, die erst mit der Abbestellung des Monitoring-Dienstes beendet wird.

Das aktive Polling wird von dem in A_1 gestarteten Timer angestoßen und in der Aktivität A_2 ausgeführt, die gleichzeitig mehrere *Partial Service Provider* kontaktiert und auf ihre Antworte wartet (für die Beschreibung des Basisprozesses siehe Abschnitt 5.10). Die Monitoring-Informationen werden vom *Partial Service Provider* in A_3 vorbereitet und zurück an A_4 geschickt. Das Warten auf eine Antwort in A_4 kann mit einer zeitlichen Begrenzung gestaltet werden, so dass sowohl eine gültige Antwort als auch der Abbruch wegen Zeitüberschreitung bei der Berechnung des Gesamtzustandes in A_5 berücksichtigt werden können.

Bei den *Partial Service Provider*, die ein Pushing der Monitoring-Informationen unterstützen, ist das Verhalten nur geringfügig abweichend. Das Abfragen der Dienstgüte eigener Teilstrecke(n) kann entweder Timer- oder Ereignis-gesteuert gestaltet werden. Nachdem die Monitoring-Informationen in A_3 vorbereitet wurden, können sie via `NOTIFY INSTANCESTATE` (siehe Abschnitt 5.11) an den *Monitoring Manager* geschickt werden. Zudem kann der *Partial Service Provider* auch in Eigenregie die Einhaltung der Grenzwerte überprüfen und, falls deren Verletzung stattgefunden hat, ein `NOTIFY EVENT` (siehe Abschnitt 5.12) an den *Monitoring Manager* schicken. Das Warten auf eine Benachrichtigung in A_6 kann zeitlich begrenzt gestaltet werden, so dass auch das Fehlen der Benachrichtigung in A_5 bei der Berechnung des Gesamtzustandes berücksichtigt werden kann.

Insbesondere bei der Unterstützung verschiedener Überwachungsarten durch verschiedene Teilstrecken müssen beiden Arten der Informationsabfragen gleichzeitig ausgeführt werden. Eine Kombination aus Push- und Pull-Verfahren für dieselben Teilstrecken ist auch denkbar.

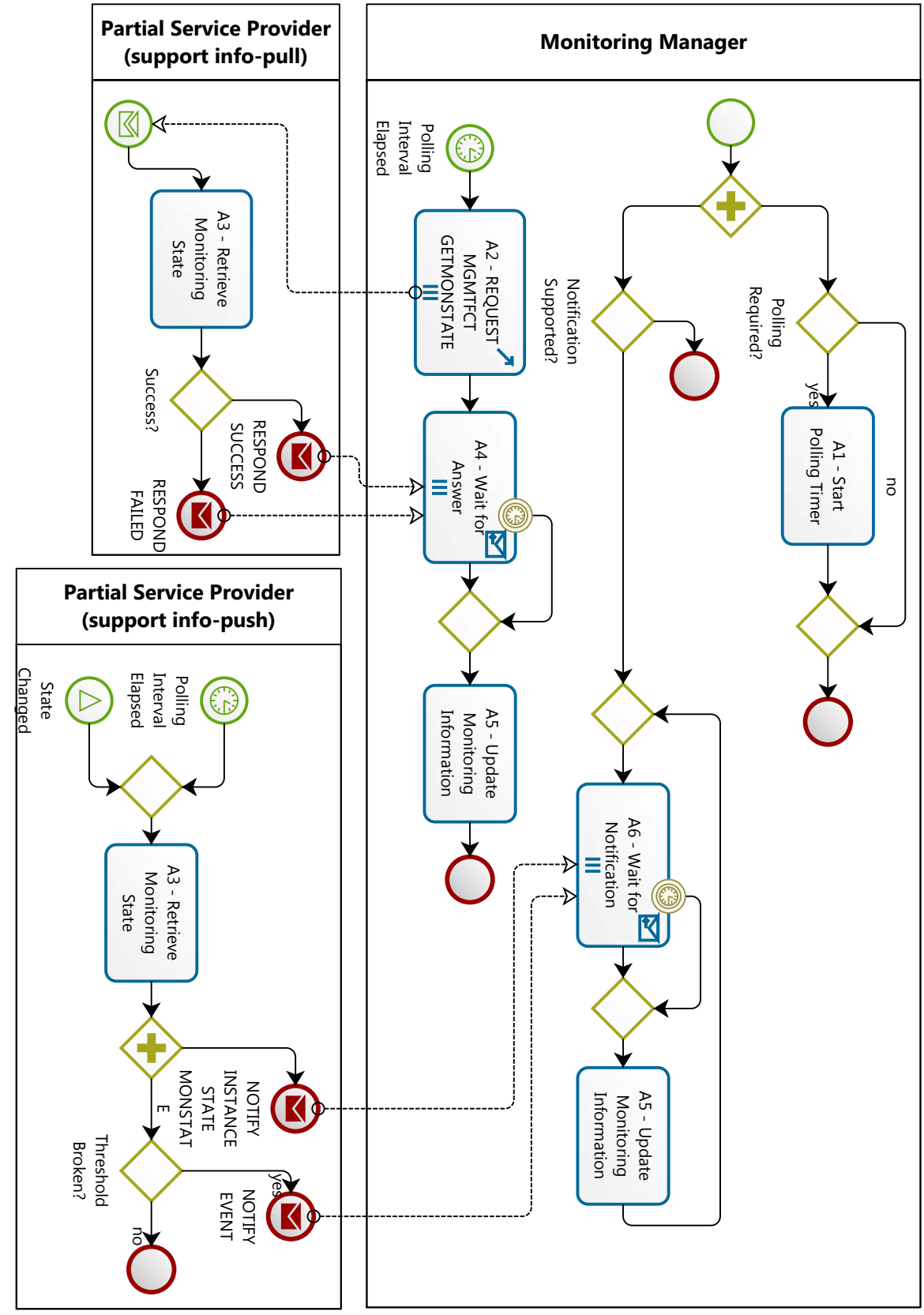
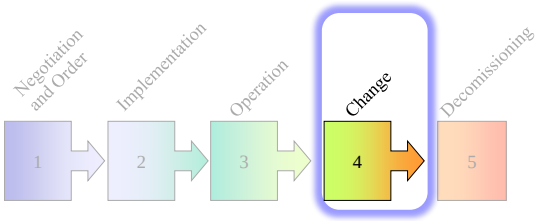


Abbildung 6.8.: Überwachen

6.8. SLM-Prozess: Change

6.8.1. Einführung

Für eine Änderung im Betrieb kann es unterschiedlichen Gründe geben. In diesem Abschnitt wird die Situation beschrieben, wenn der Customer einer Dienstinstanz die E2E-Anforderungen ändern möchte.



Alternativ dazu kann die Anfrage für eine Änderung auch intern auftreten. So kann z.B. der *Concatenated Service Manager* basierend auf der Überwachung der Dienstinstanz feststellen, dass eine der Teilstrecken die erforderlichen Grenzwerte nicht einhält. Um das bei der E2E-Instanz auszugleichen, können die Soll-Werte bei einer Reihe anderen Teilstrecken verschärft werden. Der entsprechende Prozess wird wegen seiner Ähnlichkeit zu dem hier vorgestellten Prozess nicht explizit beschrieben.

6.8.2. Rollen

Die für den Ordering-Prozess relevanten Rollen sowie deren Verantwortlichkeiten sind in Tabelle 6.16 zusammengefasst.

6.8.3. Aktivitäten

Alle für den Prozess relevanten Aktivitäten sind in Tabelle 6.17 zusammengefasst.

6.8.4. Prozessartefakte

Bei der Anfrage nach einer Änderung der Soll-Eigenschaften sind die E2ELINKID der Dienstinstanz sowie die erwünschten neuen Eigenschaften erforderlich. Nach der erfolgreichen Prozessdurchführung werden die aktuell zugesicherten Eigenschaften zurück an die *End Site* geschickt. Die Dienstinstanzeigenschaften werden, ähnlich wie bei den Dienstreservierungsanfragen (siehe Abschnitt 5.6), entsprechend dem UML-Diagramm aus der Abbildung 4.51 strukturiert.

Rolle	Bezeichnung	Rollendefinition	
R_1	END SITE	*Verantwortlichkeiten*	• Repräsentant auf Kundenseite • Hier: Beantragen der Änderung der Eigenschaften einer bereits bestellten E2E Dienstinstanz
		Fokus	–
		Kardinalität	1
		Art der Partizipation	statisch
		Vergabeverfahren	–
		Kandidatenmenge	potentielle Kunden, die an den CONNECTION-SP angeschlossen sind
R_2	CONNECTION-SP	*Verantwortlichkeiten*	• Lokaler Provider der END SITE • Hier: Anschluss der END SITE und Anbieten unterstützter Managementfunktionalität für bestellte Dienste
		Fokus	–
		Kardinalität	1
		Art der Partizipation	statisch
		Vergabeverfahren	die End-Site wendet sich an ihren lokalen Provider
		Kandidatenmenge	alle Provider
R_3	CONCATENATED SERVICE PROVIDER	*Verantwortlichkeiten*	• Entgegennehmen der Anfrage und der Spezifikationen neuer Anforderungen • Benachrichtigung über das Ergebnis der Anfrage
		Fokus	ConcatenatedService
		Kardinalität	1
		Art der Partizipation	statisch
		Vergabeverfahren	Wird vom CONNECTION-SP eingenommen
		Kandidatenmenge	–
R_4	CONCATENATED SERVICE MANAGER	*Verantwortlichkeiten*	• Abbilden der neuen Eigenschaften auf die Teildienste der relevanten Dienstinstanz • Weiterleiten der neuen Anforderungen an die beteiligten SP-Domänen • Korrelation der Ergebnisse dieser Anfragen
		Fokus	ConcatenatedService
		Kardinalität	1
		Art der Partizipation	statisch
		Vergabeverfahren	Wird von CONNECTION-SP eingenommen
		Kandidatenmenge	–

Tabelle 6.16.: SLM-Processes Change – Rollen

Aktivität	Bezeichnung	Beschreibung	
A_1	REQUEST CHANGE OF E2E INSTANCE PROPERTIES	*Input*	
		Tätigkeiten	• Festlegen neuer E2E-Anforderungen an die Dienstinstanz • Schicken der entsprechenden Anfrage an den CONCATENATED SERVICE PROVIDER
		Output	• E2ELINKID • NEWPROPERTIES (E2E-INSTANCE)
A_2	WAIT FOR CONFIRMATION	*Input*	CONFIRMEDPROPERTIES
		Tätigkeiten	Warten auf die Bestätigung der Anpassung
		Output	
A_3	CHECK CUSTOMER CREDENTIALS	*Input*	
		Tätigkeiten	• Überprüfen, ob die END SITE die Änderung der vereinbarten Dienstinstanzeigenschaften beantragen darf • Treffen einer Entscheidung
		Output	
A_4	CALCULATE NEW PROPERTIES FOR SERVICEPARTS	*Input*	• NEWPROPERTIES • ROUTEINFORMATION
		Tätigkeiten	• Berechnen der neuen erforderlichen Eigenschaften für alle Teildienste der E2E Verbindung mit E2ELINKID
		Output	NEWPROPERTIES (PRO INVOLVED SERVICE-PART)
A_5	REQUEST CHANGE (SERVICEPARTS)	*Input*	• REFERENCEID (PRO INVOLVED SERVICE-PART) • DOMAINDSM (PRO INVOLVED SERVICE-PART) • NEWPROPERTIES (PRO INVOLVED SERVICE-PART)
		Tätigkeiten	• Schicken Anfragen an die involvierten Provider der einzelnen Teildienste • Warten auf die Antwort (von allen involvierten SPs)
		Output	
A_6	CALCULATE OVERALL COMMITTED PROPERTIES	*Input*	NEWPROPERTIES (PRO INVOLVED SERVICE-PART)
		Tätigkeiten	Berechne Zusicherungswert für die E2E-Instanz
		Output	COMMITTEDPROPERTIES (aggregiert für alle PARTS)
A_7	NOTE CHANGES	*Input*	
		Tätigkeiten	Update Dienstinstanz-Informationen
		Output	

Tabelle 6.17.: Change – Aktivitäten

6.8.5. Globales Prozessmodell

Der Prozess (siehe Abbildung 6.9) startet, indem der Kunde in der Aktion A_1 dem *Concatenated Service Provider* die Anfrage für die Änderung schickt und die neuen erwünschten Dienstinstanzeigenschaften mitteilt. Danach wartet der Kunde in A_1 auf das Ergebnis seiner Anfrage.

Die Aufgabe des *Concatenated Service Providers* beschränkt sich zunächst auf die in A_3 durchgeführte Überprüfung, ob die Anfrage zugelassen oder zurückgewiesen werden soll. Falls die Anfrage zugelassen wird, wird die Kontrolle über die Prozessausführung an den *Concatenated Service Manager* übergeben. Der berechnet zunächst in A_4, wie die veränderten Dienstgüteeigenschaften sich auf alle beteiligten Teildienste verteilen sollen. Die Anfragen für die beschlossenen Veränderungen werden dann im nächsten Schritt in A_5 an die entsprechenden *Partial Service Provider* geschickt (für den Basisprozess siehe Abschnitt 5.9). Nachdem die Antworten von allen *Partial Service Provider* gekommen sind, können in A_6 die für die E2E-Dienstinstanz bestätigten Dienstgüteeigenschaften berechnet werden. Danach wird die Kontrolle zurück an den *Concatenated Service Provider* zurückgegeben. Dieser überprüft, ob diebestätigten Eigenschaften die Anfrage erfüllen oder nicht und schickt anschließend eine entsprechende Mitteilung an die *End Site*. Im Erfolgsfall werden zuvor in A_7 die Dienstinstanzinformationen aktualisiert.

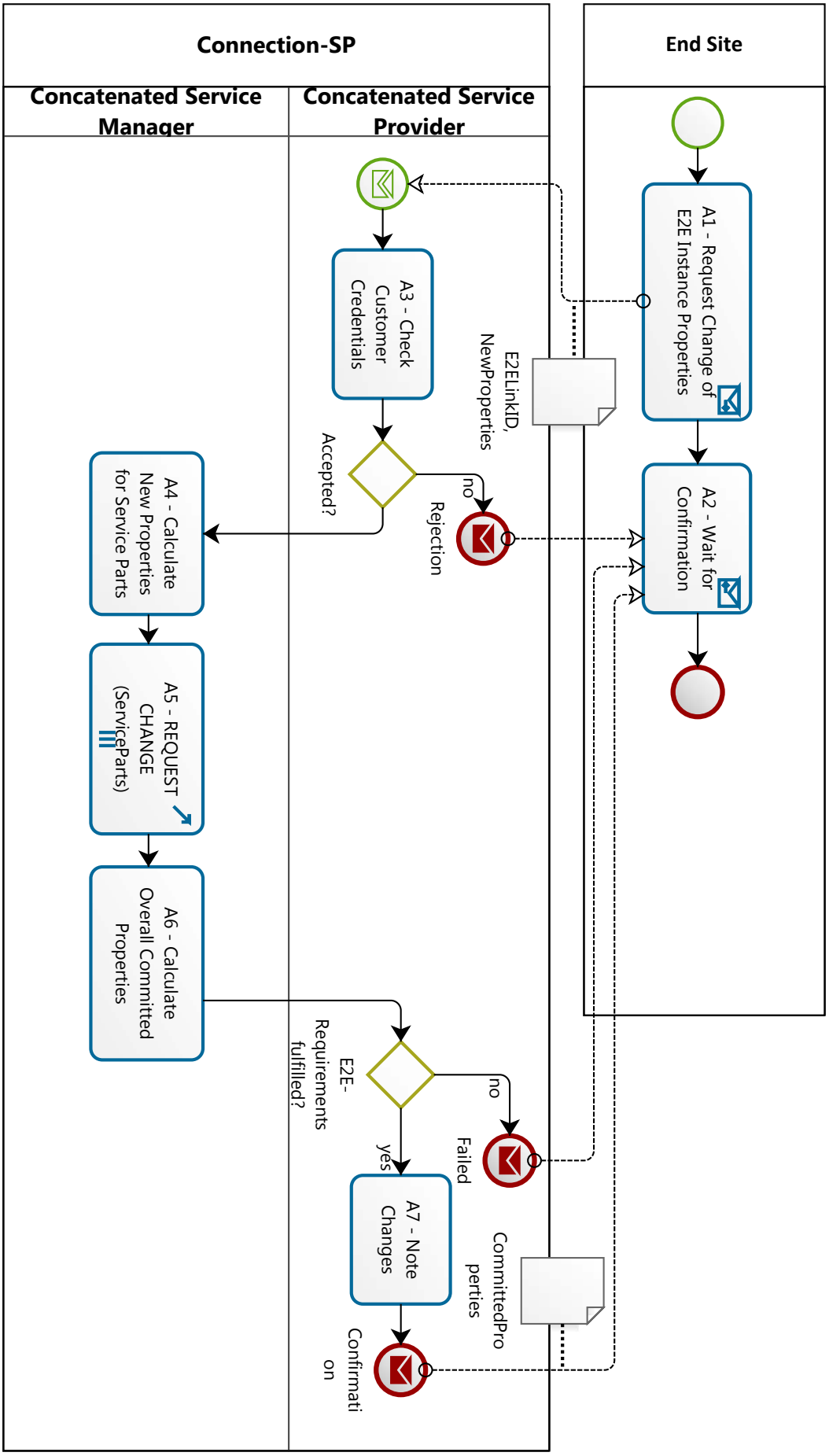
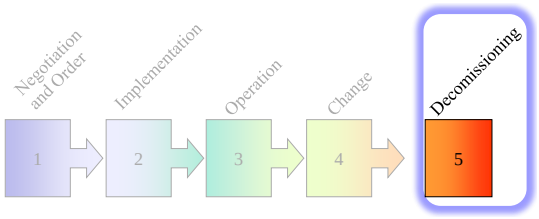


Abbildung 6.9.: Change

6.9. SLM-Prozess: Decomissioning

6.9.1. Einführung

In diesem Abschnitt wird das Abbestellen einer Dienstinstanz des Verketteten Dienstes beschrieben, das vom Endkunden initiiert wird. Diese stützt sich auf den im Abschnitt 5.14 beschriebenen Basisprozess zum Abbestellen einzelner Teildienste einer Dienstinstanz.



6.9.2. Rollen

Die für den Ordering-Prozess relevanten Rollen sowie deren Verantwortlichkeiten sind in Tabelle 6.18 zusammengefasst.

6.9.3. Aktivitäten

Alle für den Prozess relevanten Aktivitäten sind in Tabelle 6.19 zusammengefasst.

6.9.4. Prozessartefakte

Bei der Anfrage muss von der *End Site* ausschließlich die E2ELINKID angegeben werden. Es ist kein Datenaustausch in die Rückrichtung erforderlich, kann aber – in Abhängigkeit vom Dienst – auch mit Informationen wie z.B. einem Bericht für die ganze Periode oder auch abschließenden Abrechnungsdaten versehen werden.

6.9.5. Globales Prozessmodell

Der Prozess (siehe Abbildung 6.10) wird vom Customer initiiert, indem er in der Aktion A_1 eine Anfrage über das Abbestellen der Dienstinstanz mit E2ELINKID beantragt. Der Customer wartet danach in A_2 auf eine Bestätigung seitens des *Concatenated Service Providers*.

Der *Concatenated Service Provider* untersucht zunächst in A_3, ob die *End Site* diese Anfrage für die spezifizierte Dienstinstanz stellen darf oder nicht. Wenn das der Fall ist, notiert der *Concatenated Service Provider* in A_4 die Zeit der Instanz-Abbestellung und schickt eine Bestätigung an die *End Site*.

Rolle	Bezeichnung	Rollendefinition	
R_1	END SITE	*Verantwortlichkeiten*	• Repräsentant auf Kundenseite • Hier: Beantragen der Abbestellung einer E2E Dienstinstanz
		Fokus	–
		Kardinalität	1
		Art der Partizipation	statisch
		Vergabeverfahren	–
		Kandidatenmenge	potentielle Kunden, die an den CONNECTION-SP angeschlossen sind
R_2	CONNECTION-SP	*Verantwortlichkeiten*	• Lokaler Provider der END SITE • Hier: Anschluss der END SITE und Anbieten unterstützter Managementfunktionalität für bestellte Dienste
		Fokus	–
		Kardinalität	1
		Art der Partizipation	statisch
		Vergabeverfahren	die End-Site wendet sich an ihren lokalen Provider
		Kandidatenmenge	alle Provider
R_3	CONCATENATED SERVICE PROVIDER	*Verantwortlichkeiten*	• Entgegennehmen der Anfrage • Bestätigung der Abbestellung der Dienstinstanz
		Fokus	ConcatenatedService
		Kardinalität	1
		Art der Partizipation	statisch
		Vergabeverfahren	Wird vom CONNECTION-SP eingenommen
		Kandidatenmenge	–
R_4	CONCATENATED SERVICE MANAGER	*Verantwortlichkeiten*	Weiterleiten der Abbestellungsanfrage an alle involvierten SP-Domänen
		Fokus	ConcatenatedService
		Kardinalität	1
		Art der Partizipation	statisch
		Vergabeverfahren	Wird von CONNECTION-SP eingenommen
		Kandidatenmenge	–

Tabelle 6.18.: SLM-Processes Decomissioning – Rollen

Aktivität	Bezeichnung	Beschreibung	
A_1	REQUEST DECOMISSIONING OF E2E INSTANCE	*Input*	
		Tätigkeiten	Schicken einer Anfrage für das Abbestellen einer Dienstinstanz an CONNECTION-SP
		Output	E2ELINKID
A_2	WAIT FOR CONFIRMATION	*Input*	
		Tätigkeiten	Warten auf die Bestätigung
		Output	
A_3	CHECK CUSTOMER CREDENTIALS	*Input*	
		Tätigkeiten	• Überprüfen, ob die END SITE die spezifizierte Dienstinstanz abbestellen darf • Treffen Entscheidung
		Output	
A_4	NOTE INSTANCE ENDTIME	*Input*	
		Tätigkeiten	Update der Instanz-Verwaltungsinformationen (z.B. für Accounting)
		Output	
A_5	RELEASE ROUTE	*Input*	REFERENCEID (PRO SECTION)
		Tätigkeiten	• Abschicken einer Anfrage für Dienstauflösung an alle beteiligten Provider der Teildienste • Warten auf die Antwort
		Output	
A_6	REQUEST DECOMISSIONING (MDMGMTFCT)	*Input*	REFERENCEID (PRO MDMGMTFCT)
		Tätigkeiten	• Abschicken einer Anfrage für Dienstauflösung an alle beteiligten Provider der Multi-Domain Managementdienste • Warten auf die Antwort
		Output	
A_7	FREE RESSOURCES USED FOR SP-FACED MANAGEMENT	*Input*	E2ELINKID
		Tätigkeiten	Freigeben aller Ressourcen, die für die Verwaltung des an die SPs PROVIDING SERVICE ausgerichteten Managements der abbestellten Dienstinstanz verwendet wurden
		Output	
A_8	FREE RESSOURCES USED FOR CUSTOMER-FACED MANAGEMNT	*Input*	E2ELINKID
		Tätigkeiten	Freigeben aller Ressourcen, die für die Verwaltung des an END SITE ausgerichteten Managements der abbestellten Dienstinstanz verwendet wurden
		Output	

Tabelle 6.19.: Decomissioning – Aktivitäten

Parallel zu A_4 wird die Kontrolle auch an den *Concatenated Service Manager* übergeben, der für die Abbestellung einzelner Teildienste der spezifizierten Dienstinstanz zuständig ist. Das geschieht in parallel ausgeführten Aktivitäten A_5 und A_6, in denen entsprechend die Teilstrecken und die Multi-Domain Managementfunktionalität abbestellt werden (für die entsprechenden Hilfs- bzw. Basisprozesse siehe Abschnitte 6.5 bzw. 5.14). Erst nachdem alle in der Dienstinstanz involvierten Teildienste anderer Provider abbestellt wurden, können in A_7 die für die Verwaltung der Dienstinstanz-Teildienste verwendeten Ressourcen freigegeben werden. Anschließend können in A_8 auch die Ressourcen freigegeben werden, die für die kundenbezogene Verwaltung verwendet wurden.

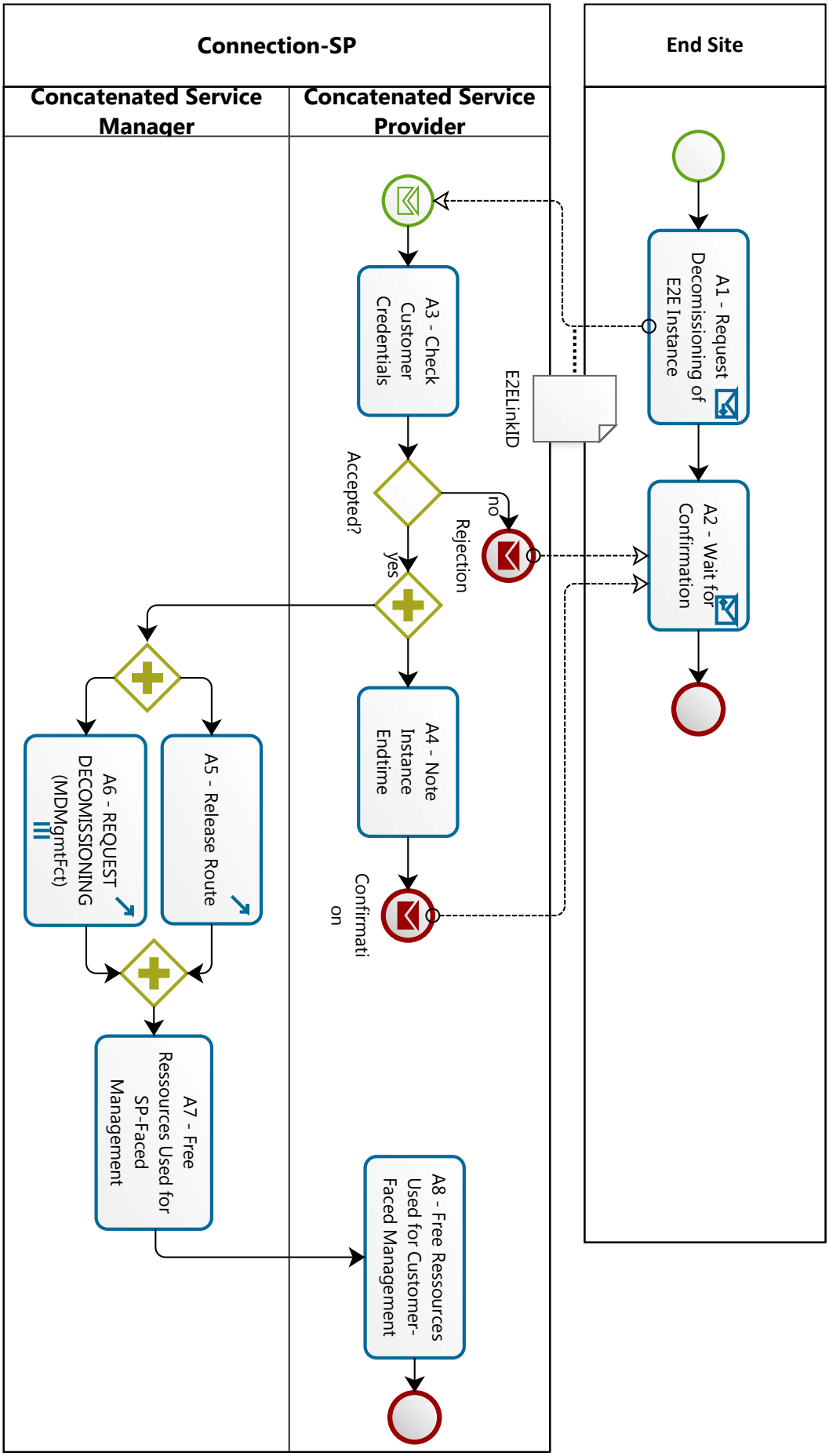


Abbildung 6.10.: Decomissioning

Teil III.

Evaluation, Bewertung und Ausblick

7 Konkretisierung und Evaluation am Beispiel

Die in den Kapiteln 4 bis 6 entwickelte Lösung umfasst viele, oft aufeinander aufbauende Lösungsteile. Da das Zusammenspiel dieser Teile an manchen Stellen nicht ganz trivial ist, wird in diesem Kapitel verdeutlicht, wie die entwickelten Konzepte umgesetzt und als Teile einer Gesamtlösung eingesetzt werden können. Zur Veranschaulichung wird ein Beispiel verwendet, an dem die Prozessdurchführung durchgespielt und die kritischsten Aspekte verdeutlicht werden können. Insbesondere wird darauf geachtet, wie die "Verschachtelung" einzelner Prozesse zu interpretieren ist.

Für die Kommunikation zwischen den SP-Domänen werden *Web Services* gewählt, die sich in den letzten Jahren als sehr effektiv bei der Kopplung lose angebundener Dienste bewährt haben, was auch bei der entwickelten Lösung der Fall ist. Die XML-Nachrichten, die bei der Prozessausführung zwischen SPs ausgetauscht werden müssen, werden von den zuvor definierten UML-Diagrammen abgeleitet. Bei der Beschreibung der jeweiligen XML-Nachrichten wird insbesondere die Umsetzung der kritischen Aspekte betont. Dazu gehören u.a. die Bestimmung der Management-Funktionalität und die Kopplung einzelner Teildienste bereits bei der Durchführung des Routingprozesses.

Das Kapitel ist wie folgt strukturiert: Im Abschnitt 7.1 wird kurz die Multi-Domain Umgebung skizziert, in der das Beispiel durchgespielt wird. Im Abschnitt 7.2 wird die Umsetzung der entwickelten Lösung anhand des Bestellprozesses sowie aller dabei benötigten Hilfs- und Basisprozesse illustriert. Da die Umsetzung aller anderen SLM-Prozesse und der Kommunikationsartefakte auf denselben Prinzipien beruht, wird hier auf deren explizite Beschreibung verzichtet. Besonders ausführlich wird dabei der Routing-Prozess beschrieben, da er den Kern der entwickelten Lösung darstellt. Die am Beispiel erkennbaren charakteristischen Eigenschaften der entwickelten Lösung werden anschließend im Abschnitt 7.3 kurz zusammengefasst und bewertet.

7.1. Ausgangssituation

Für die Illustration der Vorgänge wird das im Kapitel 4 bereits verwendetes Multi-Domain Szenario wiederverwendet und entsprechend erweitert. In Abbildung 7.1 ist eine Reihe von Service Provider dargestellt, die unterschiedliche Dienste anbieten. So können die Provider SP_1 bis SP_5 Verbindungsdienste erbringen, die Provider SP_R und SP_M sind ausschließlich auf die Multi-Domain Managementdienste *Routing* bzw. *Monitoring* und *Reporting* spezialisiert, die Domänen SP_4 und SP_5 können zusätzlich zu den Verbindungsdiensten auch Multi-Domain Managementdienste *Routing* und *Monitoring* erbringen. Die in der Abbildung dargestellten Verbindungsmöglichkeiten und Multi-Domain Managementdienste stellen die Gesamtheit aller Dienste dar, die im Beispiel gegeben sind.

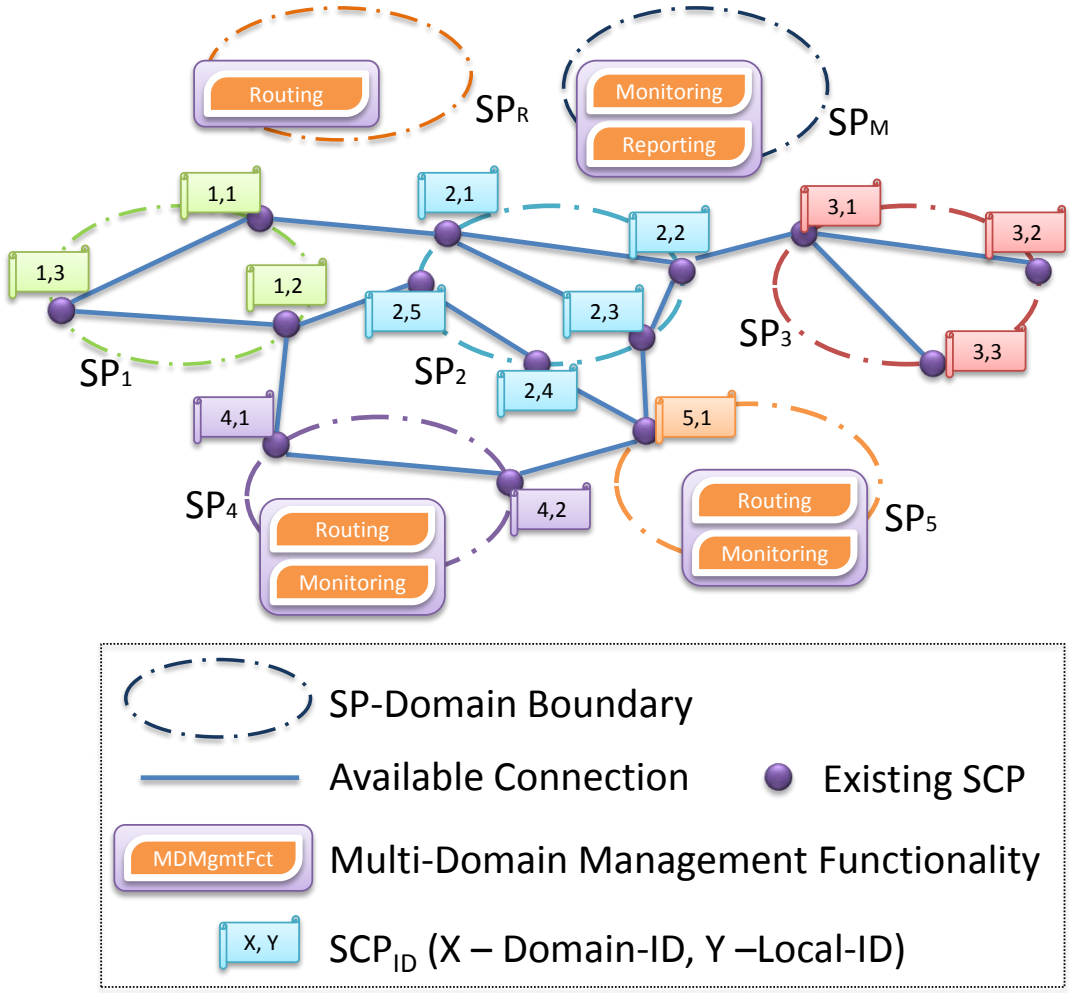
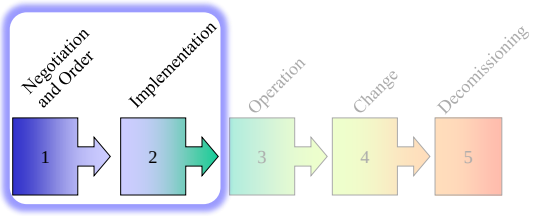


Abbildung 7.1.: Beispielszenario

Für die bessere Referenzierbarkeit werden alle SCPs mit einer numerischen "X,Y"-ID beschriftet, die sich aus der SP-Kennnummer und internen laufenden Nummern zusammensetzt. Die einzelnen Teilstrecken werden im Laufe des Beispiels stets durch die IDs verbundener SCPs identifiziert. Diese Identifizierungsart wurde für die bessere Lesbarkeit des Beispiels gewählt.

In Abbildung sind ausschließlich die Verbindungsmöglichkeiten dargestellt, die die E2E-Kundenanforderungen auf die neue Dienstinstanz erfüllen und daher vom Suchalgorithmus u.U. abgefragt und betrachtet werden müssen. Um das Beispiel möglichst einfach zu halten, wird in allen Fällen immer von einem einzigen *Component Link* in dem entsprechenden *Compound Link* ausgegangen (die Beschreibungsart der Teilstrecken ist im Abschnitt 4.1 festgelegt). Einzige Ausnahme ist die Verbindung zwischen $SCP_{2,1}$ und $SCP_{2,2}$, um den Umgang mit mehreren *Component Links* zu illustrieren.

7.2. Bestellung und Inbetriebnahme am Beispiel



Der Prozess für die Bestellung und die Inbetriebnahme einer neuen Instanz des Verketteten Dienstes wurde im Abschnitt 6.1 definiert. Am Anfang des Prozesses formuliert der Kunde seine E2E-Anforderungen an die neue Dienstinstanz und teilt diese seinem Anschluss-SP mit.

Im Beispiel wird davon ausgegangen, dass der Kunde eine Dienstinstanz zwischen $SCP_{1,3}$ und $SCP_{3,2}$ bestellt, die die in Tabelle 7.1 zusammengefassten E2E-Anforderungen erfüllen soll. Um das Beispiel möglichst allgemein zu gestalten, umfassen diese Anforderungen mehrere Eigenschaften, die sich sowohl auf die QoS-Anforderungen der Verbindung (Bandbreite und Delay) als auch auf die erforderliche Single- bzw. Multi-Domain Managementfunktionalität (Wartung und Monitoring) erstrecken.

Eigenschaft	Wert
Bandbreite	min 1 Gbps
Delay	max 20 ms
Maintenance Window	06:00-10:00 MET
Max. Maintenance Duration	max 1 hr
E2E-Monitoring	required

Tabelle 7.1.: E2E-Kundenanforderungen an neue Dienstinstanz

Ausgehend von den Anforderungen wird für die Dienstinstanz die Multi-Domain Managementfunktionalität *Monitoring* benötigt. Da SP_1 diese Multi-Domain Managementfunktionalität nicht in der Eigenregie erbringen kann, wird die in Abbildung 7.2 dargestellte Reservierungsanfrage an die SP-Domäne SP_M geschickt (siehe auch die Beschreibung der Aktion A_7 im Abschnitt 6.1 und die Definition des Basisprozesses im Abschnitt 5.6). Die Reservierungsanfrage des Monitoring-Dienstes ist relativ einfach, da zu diesem Zeitpunkt noch keine Informationen über die zu überwachende Route vorhanden sind. In der Anfrage müssen lediglich der erwünschte Dienst (Monitoring) sowie die zu überwachenden Eigenschaften spezifiziert werden. Weiterhin wird auch die ID der neuen Dienstinstanz angegeben, um später im Betrieb die Zusammengehörigkeit einzelner Teildienst-Informationen zu derselben Dienstinstanz bestimmen zu können.

Eine Bestätigung dieser Anfrage ist in Abbildung 7.3 dargestellt. Für die spätere Kommunikation beinhaltet die Antwort die Kommunikationsadresse, sowie die REFERENCEID, um den Monitoring-Dienst für die E2E-Dienstinstanz referenzieren zu können. Da es sich um die Reservierung handelt, wird auch die Reservierungsdauer fest-

```
<REQUEST>
    <RESERVATION>

        <E2ELinkID>
            URI:http://namespaceSP1.com/E2ELinkID/SCP13-SCP32-12/
        </E2ELinkID>
        <ConcatenatedServiceProvider>...

        <MDSERVICE>
            <MONITORING>
                <OperationalState>
                    <Bandwidth/>
                    <Delay/>
                </OperationalState>
                <AdministrativeState>
                    <Maintenance/>
                </AdministrativeState>
            </MONITORING>
        </MDSERVICE>

    </RESERVATION>
</REQUEST>
```

Abbildung 7.2.: Reservierungsanfrage für den Monitoring-Dienst

gelegt, nach der die Ressourcen freigegeben und die angegebenen REFERENCEID sowie die Kommunikationsadresse nicht mehr gültig sein werden.

Da SP_1 auch das Routing nicht selber durchführen kann, wird diese Managementfunktionalität bei einem externen Service Provider – diesmal bei SP_R – bestellt. Die Anfrage entspricht der Aktivität A_6 in Abbildung 6.1 (der entsprechende Basisprozess ist im Abschnitt 5.13 definiert). Die Anfrage für den Routing-Dienst ist wesentlich komplexer und ist deswegen separat in Abbildung 7.4 dargestellt. Wegen der Größe der Nachricht werden einige ihrer Abschnitte ausgeblendet, um einen Gesamtüberblick über die Nachrichteninhalte zu geben. Die zusammengefassten Teile der Nachricht werden in Abbildung 7.5 wieder expandiert, damit auch die Details sichtbar werden.

Die Komplexität der Nachricht wird dadurch verursacht, dass bei der Bestellung des Routing-Dienstes eine Reihe von Parametern übergeben wird, die während aller Operationen gültig bleiben. Das ist eine Optimierungsmaßnahme, die zur Reduktion des Kommunikationsverkehrs sowie zur besseren Nachrichtenbearbeitungszeit beiträgt. Von allen übergebenen Parametern ist die Kommunikationsadresse für den Monitoring-Dienst besonders interessant. Diese wird verwendet, um bereits bei der Pfadsuche die Verknüpfung zwischen der Managementfunktionalität einzelner Teildienste herzustellen.

Die Antwort des Routing-Providers SP_R unterscheidet sich nur unwesentlich von der Antwort auf die Reservierungsanfrage des Monitoring-Dienstes. Da dabei die Dienstinstanz-spezifische REFERENCEID sowie die Kommunikationsschnittstelle mitgeteilt werden, wird diese Antwort in Abbildung 7.6 explizit dargestellt. Um die Unabhängigkeit

```
<RESPOND>
    <SUCCESS>

        <ReferenceID>
            URI:http://namespaceSPm.com/ReferenceID/Mon/id239/
        </ReferenceID>

        <CommunicationDSM>
            http://dsm.domainSPm.com/mon/Mon_239/
        </CommunicationDSM>

        <ReservationTime>
            <SingleValue>
                <Value>1</Value>
                <Metric>hr</Metric>
            </SingleValue>
        </ReservationTime>

    </SUCCESS>
</RESPOND>
```

Abbildung 7.3.: Bestätigung der Reservierungsanfrage für den Monitoring-Dienst

der Service Provider zu betonen, werden sowohl die REFERENCEID als auch Kommunikationsadresse in einer leicht abweichenden Form dargestellt. Da es sich diesmal auch um die Bestellung eines Dienstes handelt, fällt bei der Antwort die Angabe der Reservierungszeit weg.

Nach der Reservierung bzw. Bestellung der notwendigen Multi-Domain Dienste schickt SP_1, der die Rolle des *Concatenated Service Managers* wahrnimmt, die "Find Route"-Anfrage an SP_R (siehe Aktion A_8 in Abbildung 6.1). Die XML-Repräsentation dieser Anfrage ist in Abbildung 7.7 dargestellt. Diese Anfrage wird an die zuvor mitgeteilte Kommunikationsadresse geschickt. Um den Bezug zu dem zuvor bestellten Dienst herzustellen, wird die in der Antwort mitgeteilte REFERENCEID verwendet. Da alle erforderlichen "Eckdaten" bereits bei der Dienstbestellung mitgeteilt wurden, ist ausschließlich die Angabe der notwendigen Operation erforderlich.

Ab da geht die Kontrolle zu SP_R über und es wird der im Abschnitt 6.2 beschriebene Hilfsprozess ausgeführt. Für das *Routing* werden Informationen über die derzeit vorhandenen Kapazitäten und bevorzugte Suchrichtungen benötigt. Deswegen wird zunächst eine entsprechende Anfrage an SP_1 geschickt, genauer gesagt an die in Zeile 25 in Abbildung 7.4 spezifizierte Kommunikationsadresse. Dieses Verhalten ist notwendig, da SP_R noch keine Informationen über die in SP_1 vorhandenen Kapazitäten besitzt. Technisch ist es zwar möglich, diese Information bereits bei der Anfrage des Routing-Dienstes zu übergeben, von dieser Möglichkeit wird hier aber Abstand genommen, um eine abweichende Logik für die Anfangsdomäne zu vermeiden.

Die Informationsabfrage ist im Wesentlichen mit der Anfrage für den Routing-Dienst identisch, wird aber vollständigkeitshalber explizit in Abbildung 7.8 dargestellt: die

```
<REQUEST>
    <SERVICE>

        <E2ELinkID>
            URI:http://namespaceSP1.com/E2ELinkID/SCP13-SCP32-12/
        </E2ELinkID>
        <ConcatenatedServiceProvider>
            <Domain_ID>
                URI://http://ConcatenatedServiceNamespace.com/Domains/SP1/
            </Domain_ID>
            <CommunicationDSM>
                http://dsm.domainSP1.com/E2ELinkDSM/SCP13-SCP32-12/
            </CommunicationDSM>
        </ConcatenatedServiceProvider>

        <MDSERVICE>
            <ROUTING>

                <ConstraintTopology>
                    <FromSCP>
                        <SCP_ID>
                            URI:http://namespaceSP1.com/SCP_ID/SCP_1_3/
                        </SCP_ID>
                        <CommunicationDSM>
                            http://dsm.domainSP1.com/SCP_1_3/
                        </CommunicationDSM>
                    </FromSCP>
                    <DestSCP>
                        <SCP_ID>
                            URI:http://namespaceSP3.com/SCP_ID/SCP_3_2/
                        </SCP_ID>
                    </DestSCP>
                </ConstraintTopology>

                <ConstraintProperties>
                    <Service_ID>CONNECTION</Service_ID>
                    <Uncertainity>FALSE</Uncertainity>

                    <TimePeriod>...

                    <QuantitativeQoS>...

                    <QuantitativeQoS>...

                    <ManagementFunctionality>...

                    <ManagementFunctionality>...

                </ConstraintProperties>

                <DelegationTypeID>TransparentProxy</DelegationTypeID>

                <MDServices>
                    <MONITORING>
                        <CommunicationDSM>
                            http://dsm.domainSPm.com/mon/Mon_239/
                        </CommunicationDSM>
                    </MONITORING>
                </MDServices>

            </ROUTING>
        </MDSERVICE>
    </SERVICE>
</REQUEST>
```

Abbildung 7.4.: Bestellanfrage für den Routing-Dienst (Überblick)

```
44                      <QuantitativeQoS>
45                          <QoS_ID>Bandwith</QoS_ID>
46                          <AssociatedValue>
47                              <SingleValue>
48                                  <Value>1</Value>
49                                  <Metric>Gbps</Metric>
50                              </SingleValue>
51                          </AssociatedValue>
52                      </QuantitativeQoS>
53
54                      <QuantitativeQoS>
55                          <QoS_ID>Delay</QoS_ID>
56                          <AssociatedValue>
57                              <SingleValue>
58                                  <Value>20</Value>
59                                  <Metric>ms</Metric>
60                              </SingleValue>
61                          </AssociatedValue>
62                      </QuantitativeQoS>
63
64                      <ManagementFunctionality>
65                          <Functionality_ID>
66                              MAINTENANCE
67                          </Functionality_ID>
68                          <Property>
69                              <Property_ID>
70                                  MAINTENANCE_WINDOW
71                              </Property_ID>
72                              <AssociatedValue>
73                                  <TimeRange>
74                                      <Begin>06:00</Begin>
75                                      <End>10:00</End>
76                                      <TimeZone>MET</TimeZone>
77                                  </TimeRange>
78                              </AssociatedValue>
79                          </Property>
80                          <Property>
81                              <Property_ID>
82                                  MAINTENANCE_DURATION
83                              </Property_ID>
84                              <AssociatedValue>
85                                  <SingleValue>
86                                      <Value>1</Value>
87                                      <Metric>hr</Metric>
88                                  </SingleValue>
89                              </AssociatedValue>
90                          </Property>
91                      </ManagementFunctionality>
92
93                      <ManagementFunctionality>
94                          <MONITORING>
95                              <OperationalState>
96                                  <Bandwidth/>
97                                  <Delay/>
98                              </OperationalState>
99                              <AdministrativeState>...
102                         </MONITORING>
103                     </ManagementFunctionality>
```

Abbildung 7.5.: Bestellanfrage für den Routing-Dienst (Expandierter Ausschnitt)

```
<RESPOND>
    <SUCCESS>

        <ReferenceID>
            URI:http://namespaceSPr.com/ReferenceID/Routing/srv93/
        </ReferenceID>

        <CommunicationDSM>
            http://dsm.domainSPr.com/SrvDSM/srv93/
        </CommunicationDSM>

    </SUCCESS>
</RESPOND>
```

Abbildung 7.6.: Bestätigung der Anfrage für den Routing-Dienst

```
<REQUEST>
    <MGMTFCT>

        <ReferenceID>
            URI:http://namespaceSPr.com/ReferenceID/Routing/srv93/
        </ReferenceID>

        <FINDROUTE/>

    </MGMTFCT>
</REQUEST>
```

Abbildung 7.7.: Anfrage der "FINDROUTE"-Managementfunktionalität

<CONSTRAINTTOPOLOGY>- und <CONSTRAINTPROPERTIES>-Blöcke werden nun in einen <INFORMATION>-Block eingebettet; die Angabe der DSM-Schnittstelle für $SP_{1,3}$ wird jetzt überflüssig; die Informationen über Multi-Domain Dienste (in diesem Fall nur Monitoring) werden weiterhin spezifiziert. Bei den späteren Informationsanfragen, die im Laufe des Route-Finding-Prozesses von SP_R an unterschiedliche DSMs geschickt werden, wird sich ausschließlich das Attribut <FROMSCP> ändern (siehe Zeile 19 in Abbildung 7.8). Diese Art der Informationsanfrage gibt zwar die E2E-Kundenanforderungen an jeden SP entlang der gesuchten Route preis, ermöglicht allerdings, auf eine ständige Umrechnung der Randbedingungen für einen konkreten Service Provider zu verzichten und – was für die Vorbeugung des Missbrauchs viel wichtiger ist – zwingt die SPs die unterstützten Wertebereiche anzugeben, aus denen die Auswahl für die Route getroffen werden kann.

Wie im Abschnitt 5.2 definiert wurde, ist die Antwort auf die Informationsanfrage entsprechend dem UML-Diagramm aus Abbildung 4.50 strukturiert. Eine entsprechende XML-Repräsentation der Antwort von SP_1 ist in Abbildung 7.9 dargestellt.

Hier sind vor allem die <COMMUNICATIONDSM>-Blöcke interessant, die mit den SCPs assoziiert sind (siehe Zeilen 15 und 101 in Abbildung 7.9). Diese stellen "Entry Points" für die späteren Anfragen bzgl. der vorhandenen Verbindungen, die von den entsprechenden SCPs ausgehen. In dem Beispiel wird von SP_1 für beide SCPs eine identische

```
<REQUEST>
    <INFORMATION>

        <E2ELinkID>
            URI:http://namespaceSP1.com/E2ELinkID/SCP13-SCP32-12/
        </E2ELinkID>
        <ConcatenatedServiceProvider>
            <Domain_ID>
                URI://http://ConcatenatedServiceNamespace.com/Domains/SP1/
            </Domain_ID>
            <CommunicationDSM>
                http://dsm.domainSP1.com/E2ELinkDSM/SCP13-SCP32-12/
            </CommunicationDSM>
        </ConcatenatedServiceProvider>

        <ConstraintTopology>
            <FromSCP>
                <SCP_ID>
                    URI:http://namespaceSP1/SCP_ID/SCP_1_3/
                </SCP_ID>
            </FromSCP>
            <DestSCP>
                <SCP_ID>
                    URI:http://namespaceSP3/SCP_ID/SCP_3_2/
                </SCP_ID>
            </DestSCP>
        </ConstraintTopology>

        <ConstraintProperties>
            <Service_ID>CONNECTION</Service_ID>
            <Uncertainity>FALSE</Uncertainity>

            <TimePeriod>...

            <QuantitativeQoS>...

            <QuantitativeQoS>...

            <ManagementFunctionality>...

            <ManagementFunctionality>...

        </ConstraintProperties>

        <MDServices>
            <MONITORING>
                <CommunicationDSM>
                    http://dsm.domainSPm.com/mon/Mon_239/
                </CommunicationDSM>
            </MONITORING>
        </MDServices>

    </INFORMATION>
</REQUEST>
```

Abbildung 7.8.: Informationsabfrage während des Route-Finding-Prozesses

```
<RESPOND>
    <SUCCESS>
        <RequestedInformation>
            <CompoundLink>
                <FromSCP>
                    <SCP_ID>
                        URI:http://namespaceSP1/SCP_ID/SCP_1_3/
                    </SCP_ID>
                </FromSCP>
                <ToSCP>
                    <SCP_ID>
                        URI:http://namespaceSP1/SCP_ID/SCP_1_1/
                    </SCP_ID>
                    <CommunicationDSM>
                        http://dsm.domainSP1.com/SCP_DSM_InforRequests/
                    </CommunicationDSM>
                </ToSCP>

                <ComponentLink>
                    <LinkProperties>

                        <QuantitativeQoS>...

                        <QuantitativeQoS>...

                        <ManagementFunctionality>...

                        <ManagementFunctionality>
                            <MONITORING>
                                <OperationalState>...
                                <AdministrativeState>...
                                <MonitoringInforAccess>
                                    PULL
                                </MonitoringInforAccess>
                            </MONITORING>
                        </ManagementFunctionality>

                    </LinkProperties>
                </ComponentLink>
            </CompoundLink>

            <CompoundLink>
                <FromSCP>
                    <SCP_ID>
                        URI:http://namespaceSP1/SCP_ID/SCP_1_3/
                    </SCP_ID>
                </FromSCP>
                <ToSCP>
                    <SCP_ID>
                        URI:http://namespaceSP1/SCP_ID/SCP_1_2/
                    </SCP_ID>
                    <CommunicationDSM>
                        http://dsm.domainSP1.com/SCP_DSM_InforRequests/
                    </CommunicationDSM>
                </ToSCP>

                <ComponentLink>
                    <LinkProperties>...
                </ComponentLink>
            </CompoundLink>
        </RequestedInformation>
    </SUCCESS>
</RESPOND>
```

Abbildung 7.9.: Bestätigung zusammen mit den angefragten Informationen

DSM-Adresse angegeben. Es ist i.A. eine domäneninterne Entscheidung, ob und wie viele Kommunikationsschnittstellen und für welche Zwecke sie definiert werden. Eine zweckbezogene "Zuteilung" der Kommunikationsschnittstellen hat z.B. den Vorteil, dass die Software für die entsprechenden Anfragen optimiert (und nicht allgemein) geschrieben werden kann.

In Abbildung sind zwei Verbindungsmöglichkeiten spezifiziert: <COMPOUNDLINK>s zu $SCP_{1,1}$ und $SCP_{1,2}$. Beide beinhalten jeweils einen <COMPONENTLINK>, i.A. können es aber mehrere Alternativen sein, die sich durch die unterstützten Eigenschaften voneinander unterscheiden (für die ausführliche Diskussion darüber siehe Abschnitt 4.1.2). Bei mehreren Verbindungsmöglichkeiten ist vor allem die Reihenfolge (in diesem Fall in der XML-Nachricht) und nicht das lokale Eigenschaften-Optimum oder gar lexikographische Ordnung der Endpunkte wichtig. Laut der Definition des Routing-Verfahrens im Abschnitt 4.3.4 kann der Service Provider durch diese Reihenfolge den bevorzugten Route-Verlauf signalisieren. Diese Wahl kann z.B. auf Hintergrundwissen über den Rest der Route bzw. auf finanziellen Aspekten beruhen. Im Beispiel wird signalisiert, dass zunächst die Verbindung über $SCP_{1,1}$ gesucht werden soll und erst, wenn das nicht geht, auf die Alternativroute über $SCP_{1,2}$ ausgewichen werden soll.

Zu den weiteren interessanten Aspekten in Abbildung zählt die Angabe der Methode, wie die Monitoring-Informationen abgefragt werden können (siehe Zeile 81 in Abbildung 7.9). Es wird noch keine Kommunikationsadresse dafür angegeben, da diese u.U. erst bei der Bestellung der Teilstrecke festgelegt wird.

Auch soll bemerkt werden, dass die in Abbildung 7.9 dargestellte Antwort keine REFERENCEID aufweist. Das liegt auf der Unverbindlichkeit der Informationen, die sich – im Gegensatz zu den Informationen bei Reservierungs- oder Bestellungsanfragen – ohne weiteres ändern dürfen.

Nun folgt im "Find Route" Prozess (siehe Abschnitt 6.2) eine Reihe sich wiederholender Aktionen, die aus der Informationsabfragen, Aggregation mit dem Zwischenwert und der Entscheidung über den weiteren Suchverlauf bestehen. Diese werden an dieser Stelle übersprungen, da sie nichts Neues in Bezug auf die Inter-Domain-Kommunikation aufweisen. Um weitere Aspekte zu illustrieren, wird nun ein Zwischenstand der Routensuche betrachtet, der grafisch in Abbildung 7.10 dargestellt ist. Die Abbildung repräsentiert den Stand gleich nach der Informationsabfrage von $SCP_{2,2}$ in die Richtung zu $SCP_{3,2}$.

Die zur Illustration des Szenarios definierten Eigenschafteninformationen sind in Tabelle 7.2 zusammengefasst. Um das Beispiel möglichst einfach zu halten, sind in der Tabelle die Bandbreite und die maximale Dauer der Wartungsarbeiten entsprechend auf "1 Gbps" und "1 hr" fixiert. Die Veränderungen finden nur bei *Delay* und *Maintenance Window* statt, was die Nachverfolgung der Beschreibung erleichtern soll. In der Realität können u.U. mehr als die o.g. vier Eigenschaften berücksichtigt werden, die zudem sich frei verändern können.

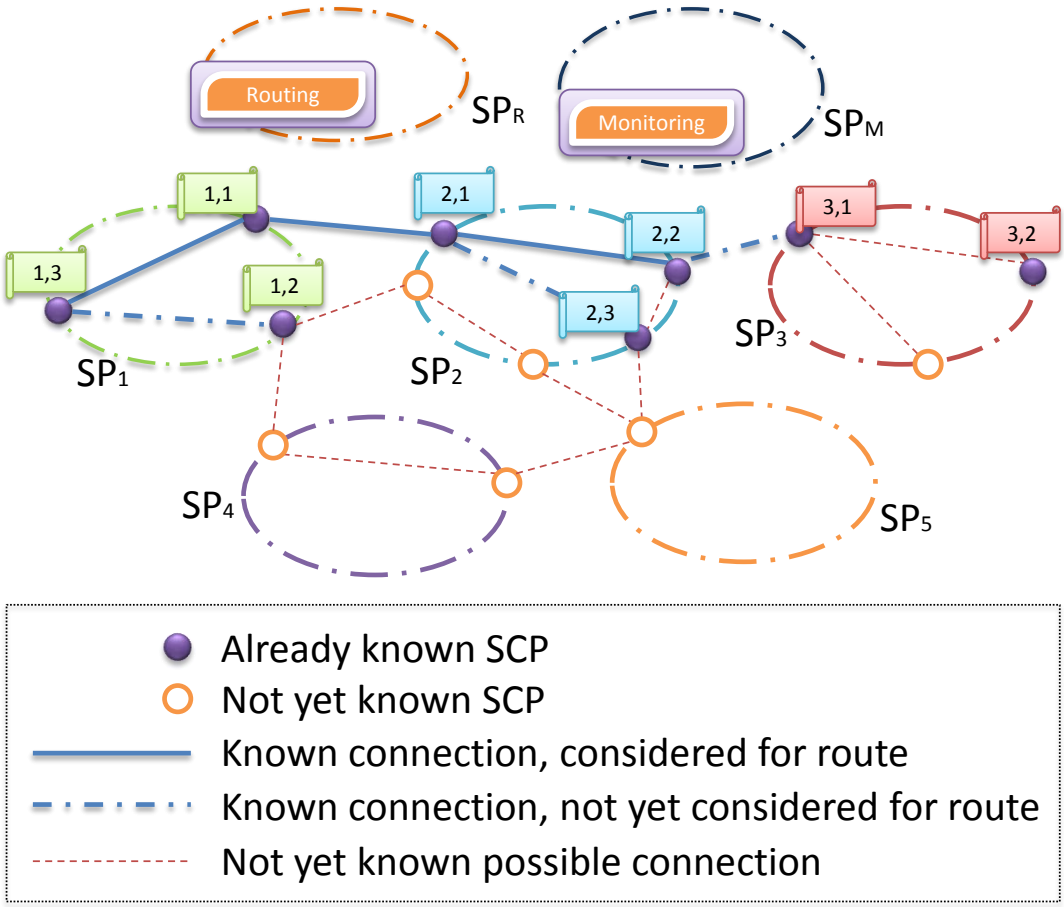


Abbildung 7.10.: Zwischenzustand der Routensuchen

Im präsentierten Beispiel beläuft sich der Aggregatwert für Delay zwischen $SCP_{1,3}$ und $SCP_{2,2}$ auf 17 ms, ein gemeinsames Fenster für die Wartungsarbeiten ist nur zwischen 06:00 und 08:00 MET möglich. Wenn man die Werte für die Verbindung zwischen $SCP_{2,2}$ und $SCP_{3,1}$ mit der Zwischensumme aggregiert, übersteigt der Delay-Wert (21 ms) die aufgestellten E2E-Anforderungen (20ms, siehe Tabelle 7.1). Auch wenn alle anderen Eigenschaften die E2E-Anforderungen erfüllen, wird dadurch die Suche nach einer Alternativroute erforderlich.

Laut Informationen in Tabelle 7.2 hat der Provider SP_2 für die Verbindung zwischen $SCP_{2,1}$ und $SCP_{2,2}$ zwei *Component Links* mit unterschiedlichen Eigenschaften gemeldet. Untersucht man die Route basierend auf der zweiten Alternative, wird der aggregierte Delay-Wert zwar die E2E-Anforderungen erfüllen, es wird dafür unmöglich, ein gemeinsames Fenster für die Wartungsarbeiten zu definieren. Dieses Beispiel soll noch einmal betonen, dass bei einer Pfadsuche mit mehreren zu berücksichtigenden E2E-Anforderungen das Optimalitätsprinzip von BELLMAN nicht mehr

From	To	Route-Part?	Property	Value
$SCP_{1,3}$	$SCP_{1,1}$	✓	Bandwidth	1 Gbps
			Delay	6 ms
			Maintenance Window	06:00-10:00 MET
			Maintenance Duration	1 hr
$SCP_{1,3}$	$SCP_{1,2}$	-	Bandwidth	1 Gbps
			Delay	5 ms
			Maintenance Window	06:00-10:00 MET
			Maintenance Duration	1 hr
$SCP_{1,2}$	$SCP_{2,1}$	✓	Bandwidth	1 Gbps
			Delay	3 ms
			Maintenance Window	06:00-08:00 MET
			Maintenance Duration	1 hr
$SCP_{2,1}$	$SCP_{2,2}$	✓	Bandwidth	1 Gbps
			Delay	8 ms
			Maintenance Window	06:00-10:00 MET
			Maintenance Duration	1 hr
$SCP_{2,1}$	$SCP_{2,2}$	-	Bandwidth	1 Gbps
			Delay	6 ms
			Maintenance Window	09:00-10:00 MET
			Maintenance Duration	1 hr
$SCP_{2,1}$	$SCP_{2,3}$	-	Bandwidth	1 Gbps
			Delay	12 ms
			Maintenance Window	06:00-10:00 MET
			Maintenance Duration	1 hr
$SCP_{2,2}$	$SCP_{3,1}$	-	Bandwidth	1 Gbps
			Delay	4 ms
			Maintenance Window	06:00-10:00 MET
			Maintenance Duration	1 hr

Tabelle 7.2.: Wissenstand im Zwischenzustand

angewandt werden kann (für eine ausführliche Diskussion darüber siehe Abschnitt 3.3.2).

Die Werte in Tabelle 7.2 sind absichtlich so gewählt, dass bei der Suche nach einer alternativen Route ein Weg über $SCP_{1,2}$ betrachtet wird. Nehmen wir an, dass SP_1 für diesen Fall den Routenverlauf über SP_4 bevorzugt, was in dem Beispiel zwangsläufig zu dem Verlauf über SP_5 führt (siehe Abbildung 7.11). Um die Delegation illustrieren zu können, gehen wir jetzt davon aus, dass die SP-Domäne SP_5 die Informationsabfrage von SP_R wegen eines zu niedrigen Vertrauensniveaus zurückweist (eine entspre-

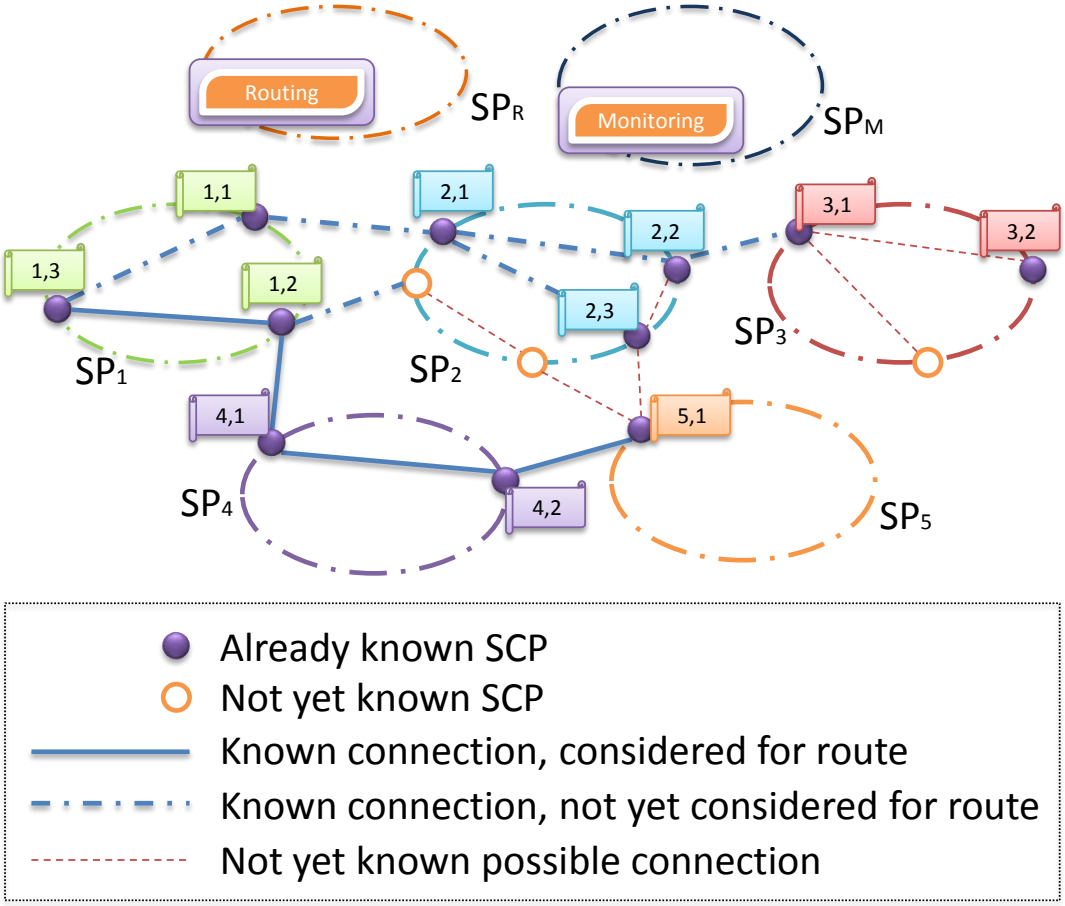


Abbildung 7.11.: Zwischenzustand der Routensuchen (Alternativroute)

chende XML-Nachricht ist in Abbildung 7.12 dargestellt). Laut der Prozessdefinition im Abschnitt 6.2 wird danach die Aufgabendelegation bei der vorherigen SP-Domäne – in diesem Fall bei SP_4 – beantragt. Die entsprechende XML-Nachricht ist in Abbildung 7.13 dargestellt.

In der XML-Nachricht für eine Delegationsanfrage sind vor allem zwei Aspekte wichtig – die <ConcatenatedServiceProvider> und die <Intermediate> Sektionen. Bei der ersten Sektion (siehe Zeilen 7 bis 14 in Abbildung 7.13) handelt es sich um die Angaben des Service Providers, dem gegenüber die für die Delegation gefragte Domäne für ihren Verantwortungsbereich Zusicherungen machen wird. Sollte in unserem Beispiel SP_4 die Proxy-Rolle übernehmen, wird bei den weiteren Informations- bzw. Bestellungs-Anfragen diese Sektion mit den Daten von SP_4 gefüllt. Der angefragte Verantwortungsbereich umfasst alle Teilstrecken zwischen $SCP_{5,1}$ und $SCP_{3,2}$ (siehe Zeilen 17 bis 28 in Abbildung 7.13). Die Delegation des Monitorings an SP_M ist durch die Spezifikation der Delegationsart bestimmt (siehe Zeile 166 in Abbildung 7.13). Eine weitere Delegation des Verantwortungsbereiches ist auch möglich, die Einhaltung der

```
1 <RESPOND>
2     <REJECTED>
3         <Reason>
4             INSUFFICIENT_TRUST_LEVEL
5         </Reason>
6     </REJECTED>
7 </RESPOND>
```

Abbildung 7.12.: Zurückweisung einer Informationsanfrage

Delegationsart ist in diesem Fall zwingend (siehe ausführliche Diskussion darüber im Abschnitt 4.4).

Die Angabe der <INTERMEDIATE> Sektion (siehe Zeilen 102 bis 164 in Abbildung 7.13) erlaubt die Mitberücksichtigung der möglichen Werte des bereits gefundenen Teilpfades bei der weiteren Suche, sodass die Erfüllung der E2E-Anforderungen auch bei der Verschattung des Dienstaufbaus garantiert werden kann (siehe Diskussionen darüber in Abschnitten 4.3 und 4.4).

Die Bestätigung der Delegationsanfrage ist identisch mit der Bestätigung für den Routing-Dienst strukturiert (siehe Abbildung 7.6). Die Abweichungen entstehen lediglich durch andere REFERENCEID- und COMMUNICATIONDSM-Werte, weswegen die entsprechende Antwort nicht extra dargestellt wird. Nach der Bestätigung kann der für das Routing verantwortliche SP_R eine `REQUEST MGMTFCT FINDROUTE` Anfrage an SP_4 schicken (siehe Aktivität A7 in Abbildung 6.2). Mit der Ausnahme von REFERENCEID ist die entsprechende XML-Nachricht mit der in Abbildung 7.7 identisch, weswegen auch sie nicht extra dargestellt wird.

Von diesem Zeitpunkt übernimmt SP_4 die Routing-Aufgabe für den Rest des Weges. Da SP_4 die Routing-Funktionalität in Eigenregie erbringen kann (siehe die Definition der Ausgangssituation im Abschnitt 7.1), muss diese Funktionalität bei der Delegationsanfrage nicht extra bestellt werden. Nach der FINDROUTE-Anfrage führt SP_4 den Prozess in Abbildung 6.2 selbst aus.

Um das Beispiel weiter zu führen, nehmen wir an, dass SP_4 eine Route über $SCP_{2,3}$, $SCP_{2,2}$ und $SCP_{3,1}$ nach $SCP_{3,2}$ gefunden hat. Die entsprechende Erfolgsmeldung ist in Abbildung 7.14 dargestellt. In der XML-Nachricht sind die REFERENCEID und COMMUNICATIONDSM angegeben, um die gemeldete gefundene Route direkt referenzieren zu können. Die Angabe der COMMUNICATIONDSM ist optional und ersetzt die vorherige Kommunikationsadresse mit SP_4, so dass auch zwischen den Operationen ein *Load Balancing* bzw. Spezialisierung auf dedizierter Aufgabe möglich ist. In der Sektion <ROUTEPROPERTIES> (siehe Zeilen 12 bis 81 in Abbildung 7.14) werden die Eigenschaften für die Teilstrecke zwischen $SCP_{5,1}$ und $SCP_{3,2}$ angegeben. Das ermöglicht beim Prozessablauf sowohl bei direkt abgefragten Teilstrecken eines einzelnen Providers als auch bei den über Proxy-SP erhaltene Informationen eine identische Berechnungslogik auch über u.U. zusammengesetzte Teilstrecken anzuwenden.

```
<REQUEST>
    <SERVICE>

        <E2ELinkID>
            URI:http://namespaceSP1.com/E2ELinkID/SCP13-SCP32-12/
        </E2ELinkID>
        <ConcatenatedServiceProvider>
            <Domain_ID>
                URI://http://ConcatenatedServiceNamespace.com/Domains/SP1/
            </Domain_ID>
            <CommunicationDSM>
                http://dsm.domainSP1.com/E2ELinkDSM/SCP13-SCP32-12/
            </CommunicationDSM>
        </ConcatenatedServiceProvider>

        <DELEGATION>
            <ConstraintTopology>
                <FromSCP>
                    <SCP_ID>
                        URI:http://namespaceSP5.com/SCP_ID/SCP_5_1/
                    </SCP_ID>
                </FromSCP>
                <DestSCP>
                    <SCP_ID>
                        URI:http://namespaceSP3.com/SCP_ID/SCP_3_2/
                    </SCP_ID>
                </DestSCP>
            </ConstraintTopology>

            <ConstraintProperties>...

            <Intermediate>
                <QuantitativeQoS>
                    <QoS_ID>Bandwith</QoS_ID>
                    <AssociatedValue>...
                </QuantitativeQoS>

                <QuantitativeQoS>
                    <QoS_ID>Delay</QoS_ID>
                    <AssociatedValue>...
                </QuantitativeQoS>

                <ManagementFunctionality>...

                <ManagementFunctionality>...

            </Intermediate>

            <DelegationTypeID>TransparentProxy</DelegationTypeID>

            <MDServices>
                <MONITORING>
                    <CommunicationDSM>
                        http://dsm.domainSPm.com/mon/Mon_239/
                    </CommunicationDSM>
                </MONITORING>
            </MDServices>

        </DELEGATION>
    </SERVICE>
</REQUEST>
```

Abbildung 7.13.: Anfrage für Delegation des Verantwortungsbereiches

```
<REQUEST>
    <SUCCESS>

        <ReferenceID>
            URI:http://namespaceSP4.com/ReferenceID/ProxySrv/id74/
        </ReferenceID>

        <CommunicationDSM>
            http://dsm.domainSP4.com/SrvDSM/ProxySrv/id74/
        </CommunicationDSM>

        <RouteProperties>
            <Service_ID>CONNECTION</Service_ID>
            <Uncertainity>FALSE</Uncertainity>

            <TimePeriod>...

            <QuantitativeQoS>...

            <QuantitativeQoS>...

            <ManagementFunctionality>...

            <ManagementFunctionality>...
        </RouteProperties>

    </SUCCESS>
</REQUEST>
```

Abbildung 7.14.: Rückmeldung über gefundene Route bei Delegation

Sobald SP_R eine SUCCESS-Antwort bekommt, wird die delegierte Teilstrecke als nächste Sektion anerkannt, anschließend wird der aggregierte Wert für den gefundenen Weg zwischen $SCP_{1,3}$ und $SCP_{3,2}$ berechnet und eine Erfolgsmeldung mit dem Gesamtwert an SP_1 geschickt. Strukturell ist diese XML-Nachricht mit der Bestätigung von Proxy-SP identisch (siehe Abbildung 7.14) und wird deswegen hier nicht explizit dargestellt.

Reservierung der gefundenen Route

Darüber hinaus schickt SP_1 an SP_R eine `REQUEST MGMTFCT` Anfrage (siehe Aktivität A9 in Abbildung 6.1). Durch diese wird der im Abschnitt 6.3 beschriebene *Reserve Route* Prozess angestoßen. In diesem Prozess werden in Bezug auf die Inter-Domain Kommunikation vor allem die Aktivitäten A_3 und A_4 wichtig, bei denen Reservierungsanfragen entweder direkt an den Provider einer Teilstrecke oder indirekt an den Proxy-SP geschickt werden. Entsprechende XML-Nachrichten sind in den Abbildungen 7.15 und 7.16 präsentiert.

Der Unterschied zwischen beiden Anfragen besteht hauptsächlich darin, dass bei einer direkten Reservierungsanfrage (siehe Abbildung 7.15) zwei Endpunkte der zu reservierenden Teilstrecke explizit angegeben werden müssen, denn bei der Informationsanfrage können mehrere Verbindungsmöglichkeiten gemeldet werden. Bei der indirekten Anfrage über Proxy-SP wird dagegen die bei der Pfadsuche mitgeteilte REFERENCEID erforderlich, damit der Proxy-SP anhand dieser ID die gefundenen Teil-

```
<REQUEST>
    <RESERVATION>
        <CONNECTION>

            <RequestedConnection>
                <FromSCP>
                    <SCP_ID>
                        URI:http://namespaceSP1.com/SCP_ID/SCP_1_3/
                    </SCP_ID>
                </FromSCP>
                <ToSCP>
                    <SCP_ID>
                        URI:http://namespaceSP1.com/SCP_ID/SCP_1_2/
                    </SCP_ID>
                </ToSCP>
            </RequestedConnection>

            <ConcatenatedServiceProvider>
                <Domain_ID>
                    URI://http://ConcatenatedServiceNamespace.com/Domains/SP1/
                </Domain_ID>
                <CommunicationDSM>
                    http://dsm.domainSP1.com/E2ELinkDSM/SCP13-SCP32-12/
                </CommunicationDSM>
            </ConcatenatedServiceProvider>

            <RequestedProperties>

                <TimePeriod>...

                <QuantitativeQoS>...

                <QuantitativeQoS>...

                <ManagementFunctionality>...

                <ManagementFunctionality>...

            </RequestedProperties>

        </CONNECTION>
    </RESERVATION>
</REQUEST>
```

Abbildung 7.15.: Anfrage für Reservierung einer Teilstrecke

dienste identifizieren kann. Im Übrigen müssen in beiden Fällen die angeforderten Eigenschaften für die jeweilige direkte bzw. zusammengesetzte Teilstrecke spezifiziert werden.

Die Bestätigung beider Arten der Reservierungsanfrage ist gleich strukturiert. Die Bestätigung der an SP_1 gerichteten Anfrage ist in Abbildung 7.17 dargestellt. Außer den bestätigten Diensteigenschaften beinhaltet diese Nachricht auch die Dauer, für die die dafür notwendigen Ressourcen reserviert wurden, sowie eine REFERENCEID und

```
 1 <REQUEST>
 2     <MGMTFCT>
 3
 4         <ReferenceID>
 5             URI:http://namespaceSP4.com/ReferenceID/ProxySrv/id74/
 6         </ReferenceID>
 7
 8         <RESERVEROUTE>
 9
10             <RequestedProperties>
11
12                 <TimePeriod>...
16
17                 <QuantitativeQoS>...
26
27                 <QuantitativeQoS>...
36
37                 <ManagementFunctionality>...
65
66                 <ManagementFunctionality>...
77
78             </RequestedProperties>
79
80         </RESERVEROUTE>
81     </MGMTFCT>
82 </REQUEST>
```

Abbildung 7.16.: Anfrage für Reservierung eines gefundenen Pfades

eine optionale Kommunikationsadresse für die Bestellung des reservierten Teildienstes.

Auch wenn sich die XML-Nachrichten für die Bestellung der reservierten Teildienste (siehe Aktivität A_{12} in Abbildung 6.1 ohne größeren Aufwand aus den vorangegangenen Beispielen und den jeweiligen Prozessdefinitionen ableiten ließen, werden sie hier vollständigkeitshalber – jedoch ohne ausführliche Erläuterungen – in den Abbildungen 7.18 und 7.19 dargestellt. Beide Anfragen beziehen sich auf die REFERENCEID des zuvor reservierten Teildienstes. Bei der Bestellung wird auch eine Möglichkeit eingeräumt, die Anforderungen situationsbedingt anzupassen. Um den Kommunikationsumfang möglichst gering zu halten, kann dies als eine optionale Angabe betrachtet werden, die nur bei Abweichungen von reservierten Werten spezifiziert werden soll.

Wesentlich interessanter als die Bestellungsanfragen sind die zugehörigen Bestätigungen darauf. Die beispielspezifischen XML-Antworten sind in den Abbildungen 7.20 und 7.21 dargestellt. In beiden Fällen werden ein oder mehrere Teildienste zurückgemeldet, deren Benennung entsprechend dem UML-Diagramm für die Dienstzusammensetzung (siehe Abbildung 5.3) gewählt wurde: <CONNECTIONSERVICE> und <CONCATENATEDSERVICE>.

In beiden Fällen richtet sich die Strukturierung der bestätigten Eigenschaften, die in <COMMITTEDPROPERTIES> Blöcken spezifiziert werden, nach dem UML-Diagramm

```
 1 <RESPOND>
 2     <SUCCESS>
 3
 4         <ReferenceID>
 5             URI:http://namespaceSP1.com/ReferenceID/RsvdConn/id258/
 6         </ReferenceID>
 7         <CommunicationDSM>
 8             http://dsm.domainSP1.com/SrvDSM/RsvdConn/id258/
 9         </CommunicationDSM>
10
11         <ReservedProperties>
12
13             <TimePeriod>...
17
18             <QuantitativeQoS>...
27
28             <QuantitativeQoS>...
37
38             <ManagementFunctionality>...
66
67             <ManagementFunctionality>...
78
79         </ReservedProperties>
80
81         <ReservationTime>
82             <SingleValue>
83                 <Value>10</Value>
84                 <Metric>min</Metric>
85             </SingleValue>
86         </ReservationTime>
87
88     </SUCCESS>
89 </RESPOND>
```

Abbildung 7.17.: SP_1-Bestätigung der Reservierungsanfrage

aus Abbildung 4.52. Das gilt auch für die Strukturierung der zuvor beschriebenen Antwort auf eine Reservierungsanfrage. Die Identifikation der jeweiligen Teilstrecke geschieht weiterhin durch die Angabe der SCPs, die die jeweilige Teilstrecke begrenzen.

Im Fall von <CONNECTIONSERVICE> ist vor allem die Angabe der Kommunikationsadressen interessant. Es wird sowohl die Kommunikationsadresse für weitere Managementoperationen, wie z.B. CHANGE oder DECOMISSIONING, spezifiziert (siehe Zeilen 9 bis 11 in Abbildung 7.20) als auch die Adresse für die Anbindung der Single-Domain Überwachung in das Multi-Domain-Monitoring (siehe Zeilen 90 bis 92 in der o.g. Abbildung).

Bei <CONCATENATEDSERVICE> bezieht sich die erste Kommunikationsadresse (siehe Zeilen 8 bis 10 in Abbildung 7.21) dagegen auf den Proxy-SP, der alle entsprechenden Anfragen an die involvierten SP-Domänen weiterleitet. Die teilstreckenbezogene Adresse für die Kopplung des Monitoring-Dienstes kommt jetzt mehrmals vor, da der Proxy-SP vier weitere Teilstrecken bestellt hat.

```
<REQUEST>
    <RESERVEDSERVICE>

        <ReferenceID>
            URI:http://namespaceSP1.com/ReferenceID/RsvdConn/id258/
        </ReferenceID>

        <RequestedProperties>

            <TimePeriod>...

            <QuantitativeQoS>...

            <QuantitativeQoS>...

            <ManagementFunctionality>...

            <ManagementFunctionality>...

        </RequestedProperties>

    </RESERVEDSERVICE>
</REQUEST>
```

Abbildung 7.18.: Anfrage für die Bestellung reservierter Teilstrecke

```
<REQUEST>
    <MGMTFCT>

        <ReferenceID>
            URI:http://namespaceSP4.com/ReferenceID/ProxySrv/id74/
        </ReferenceID>

        <ORDERROUTE>

            <RequestedProperties>

                <TimePeriod>...

                <QuantitativeQoS>...

                <QuantitativeQoS>...

                <ManagementFunctionality>...

                <ManagementFunctionality>...

            </RequestedProperties>

        </ORDERROUTE>
    </MGMTFCT>
</REQUEST>
```

Abbildung 7.19.: Anfrage für die Bestellung einer reservierten Route

```
<RESPOND>
    <SUCCESS>

        <ConnectionService>

            <ReferenceID>
                URI:http://namespaceSP4.com/ReferenceID/ConnectionSrv/id478/
            </ReferenceID>
            <CommunicationDSM>
                http://dsm.domainSP1.com/ConnectionSrv/id478/
            </CommunicationDSM>

            <FromSCP>
                <SCP_ID>
                    URI:http://namespaceSP4.com/SCP_ID/SCP_4_2/
                </SCP_ID>
            </FromSCP>
            <ToSCP>
                <SCP_ID>
                    URI:http://namespaceSP5.com/SCP_ID/SCP_5_1/
                </SCP_ID>
            </ToSCP>

            <CommittedProperties>

                <TimePeriod>...

                <QuantitativeQoS>...

                <QuantitativeQoS>...

                <ManagementFunctionality>...

                <ManagementFunctionality>
                    <MONITORING>
                        <OperationalState>...
                        <AdministrativeState>...

                        <CommunicationDSM>
                            http://dsm.domainSP4.com/SDMonitoring/id478/
                        </CommunicationDSM>

                    </MONITORING>
                </ManagementFunctionality>

            </CommittedProperties>

        </ConnectionService>

    </SUCCESS>
</RESPOND>
```

Abbildung 7.20.: Antwort auf die Anfrage für die Bestellung einer reservierten Teilstrecke

```
<RESPOND>
    <SUCCESS>
        <ConcatenatedService>

            <ReferenceID>
                URI:http://namespaceSP4.com/ReferenceID/ProxySrv/id74/
            </ReferenceID>
            <CommunicationDSM>
                http://dsm.domainSP4.com/ProxyMgmt/id74/
            </CommunicationDSM>

            <FromSCP>
                <SCP_ID>
                    URI:http://namespaceSP5.com/SCP_ID/SCP_5_1/
                </SCP_ID>
            </FromSCP>
            <ToSCP>
                <SCP_ID>
                    URI:http://namespaceSP3.com/SCP_ID/SCP_3_2/
                </SCP_ID>
            </ToSCP>

            <CommittedProperties>...

            <ConnectionService>
                <FromSCP>
                    <SCP_ID>
                        URI:http://namespaceSP5.com/SCP_ID/SCP_5_1/
                    </SCP_ID>
                </FromSCP>
                <ToSCP>
                    <SCP_ID>
                        URI:http://namespaceSP2.com/SCP_ID/SCP_2_3/
                    </SCP_ID>
                </ToSCP>

                <CommittedProperties>
                    <TimePeriod>...

                    <QuantitativeQoS>...

                    <QuantitativeQoS>...

                    <ManagementFunctionality>...

                    <ManagementFunctionality>
                        <MONITORING>
                            <OperationalState>...
                            <AdministrativeState>...
                            <CommunicationDSM>
                                http://dsm.domainSP5.com/ConnectionMgmt/id482/
                            </CommunicationDSM>
                        </MONITORING>
                    </ManagementFunctionality>
                </CommittedProperties>

            </ConnectionService>

            <ConnectionService>...

            <ConnectionService>...

            <ConnectionService>...

        </ConcatenatedService>
    </SUCCESS>
</RESPOND>
```

Abbildung 7.21.: Antwort auf die Anfrage für die Bestellung einer reservierten Route

```
<RESPOND>
    <SUCCESS>

        <ConnectionService>...

        <ConnectionService>...

        <ConnectionService>...

        <ConnectionService>

            <ReferenceID>
                URI:http://namespaceSP4.com/ReferenceID/ConnectionSrv/id478/
            </ReferenceID>
            <CommunicationDSM>
                http://dsm.domainSP1.com/ConnectionSrv/id478/
            </CommunicationDSM>

            <FromSCP>
                <SCP_ID>
                    URI:http://namespaceSP4.com/SCP_ID/SCP_4_2/
                </SCP_ID>
            </FromSCP>
            <ToSCP>
                <SCP_ID>
                    URI:http://namespaceSP5.com/SCP_ID/SCP_5_1/
                </SCP_ID>
            </ToSCP>

            <CommittedProperties>...

        </ConnectionService>

        <ConcatenatedService>

            <ReferenceID>
                URI:http://namespaceSP4.com/ReferenceID/ProxySrv/id74/
            </ReferenceID>
            <CommunicationDSM>
                http://dsm.domainSP4.com/ProxyMgmt/id74/
            </CommunicationDSM>

            <FromSCP>
                <SCP_ID>
                    URI:http://namespaceSP5.com/SCP_ID/SCP_5_1/
                </SCP_ID>
            </FromSCP>
            <ToSCP>
                <SCP_ID>
                    URI:http://namespaceSP3.com/SCP_ID/SCP_3_2/
                </SCP_ID>
            </ToSCP>

            <CommittedProperties>...

            <ConnectionService>...

            <ConnectionService>...

            <ConnectionService>...

            <ConnectionService>...

        </ConcatenatedService>
    </SUCCESS>
</RESPOND>
```

Abbildung 7.22.: Antwort des Routing-Verantwortlichen auf die Bestellungsanfrage

Die Struktur bei <CONCATENATEDSERVICE> zeichnet sich durch eine Verschachtelungsmöglichkeit aus. Der Detaillierungsgrad der Angaben über die Zusammensetzung des delegierten Dienstes wird durch die Wahl des Delegationstyps gesteuert (siehe Zeile 107 in Abbildung 7.4). Diese Delegationsart wurde für das Beispiel absichtlich gewählt, da sie im Gegensatz zu *Full-Proxy*, bei der der interne Aufbau durch den Proxy-SP komplett verschattet wird, eine wesentlich komplexere Form der Delegation darstellt (für die ausführliche Diskussion der Delegationsformen siehe Abschnitt 4.3.4.2). Bei einem *Full-Proxy* wären die Angaben einzelner Teildienste (siehe Zeilen 462 bis 721 in Abbildung 7.22) überflüssig; stattdessen wäre die Angabe eines für den ganzen Verantwortungsbereich des Proxy zuständigen Monitoring-Dienstes im <COMMITTEDPROPERTIES> Block (siehe Zeile 392 in der o.g. Abbildung) notwendig.

Nachdem die Antworten von allen direkt oder indirekt (über Proxy-SP) bestellten Teildiensten angetroffen sind, kann der für das Routing zuständige SP_R die gesamte Routen-Information an seinen Auftraggeber schicken. Die entsprechende XML-Nachricht an SP_1 ist in Abbildung 7.22 dargestellt. Diese stellt nichts anderes dar als eine Konkatenation aller erhaltenen Bestätigungen.

Nach dem Erhalt der Erfolgsmeldung von SP_R können die Routeninformationen verwendet werden, um den reservierten Monitoring-Dienst zu bestellen (siehe Aktivität A13 in Abbildung 6.1). Eine entsprechende XML-Nachricht von SP_1 an SP_M ist in Abbildung 7.23 dargestellt. Zusätzlich zur REFERENCEID, die bei der Dienstreservierung zurückgeschickt wurde, spezifiziert die Anfrage eine Reihe zu überwachender Verbindungen. Am wichtigsten sind dabei die Angaben der Kommunikationsschnittstellen sowie der Methode, wie die Monitoring-Informationen abgefragt werden können. Die Angabe von zwei SCPs pro zu überwachende Verbindung ist optional, denn diese sollen auch zur Identifikation der einzelnen überwachten Abschnitte verwendet werden. Insbesondere ist sie wichtig, wenn zum Abfragen der Monitoring-Informationen mehrerer Teilstrecken dieselbe DSM-Schnittstelle verwendet wird. Auf der anderen Seite kann die explizite Angabe der zu erwartenden SCPs erlauben, eine syntaktische Korrektheitsüberprüfung durchzuführen (siehe dazu auch die Diskussion über Erfahrungen mit E2Emon im Abschnitt 8.1).

Nachdem sowohl alle Teilstrecken einer Verbindung als auch die Multi-Domain Managementdienste bestellt und die Kommunikationswege dabei festgelegt wurden, kann der *Concatenated Service Provider* die Routeninformationen für spätere Prozesse abspeichern und die Bestätigung der Dienstbereitschaft an die *End Site* senden (siehe Prozessdefinition in Abbildung 6.1).

```
<REQUEST>
    <RESERVEDSERVICE>

        <ReferenceID>
            URI:http://namespaceSPm.com/ReferenceID/Mon/id239/
        </ReferenceID>

        <MonitoredLink>...

        <MonitoredLink>...

        <MonitoredLink>...

        <MonitoredLink>

            <FromSCP>
                <SCP_ID>
                    URI:http://namespaceSP4.com/SCP_ID/SCP_4_2/
                </SCP_ID>
            </FromSCP>
            <ToSCP>
                <SCP_ID>
                    URI:http://namespaceSP5.com/SCP_ID/SCP_5_1/
                </SCP_ID>
            </ToSCP>

            <METHOD>PULL</METHOD>

            <CommunicationDSM>
                http://dsm.domainSP4.com/ConnectionMonitoring/id478/
            </CommunicationDSM>

        </MonitoredLink>

        <MonitoredLink>

            <FromSCP>
                <SCP_ID>
                    URI:http://namespaceSP5.com/SCP_ID/SCP_5_1/
                </SCP_ID>
            </FromSCP>
            <ToSCP>
                <SCP_ID>
                    URI:http://namespaceSP2.com/SCP_ID/SCP_2_3/
                </SCP_ID>
            </ToSCP>

            <METHOD>PULL</METHOD>

            <CommunicationDSM>
                http://dsm.domainSP5.com/ConnectionMonitoring/id482/
            </CommunicationDSM>

        </MonitoredLink>

        <MonitoredLink>...

        <MonitoredLink>...

        <MonitoredLink>...

    </RESERVEDSERVICE>
</REQUEST>
```

Abbildung 7.23.: Bestellung des reservierten Monitoring-Dienstes

7.3. Evaluation

Die gefundene Route sowie das bei der Pfadsuche erworbene Wissen über die vorhandenen Verbindungsmöglichkeiten sind in Abbildung 7.24 graphisch dargestellt.

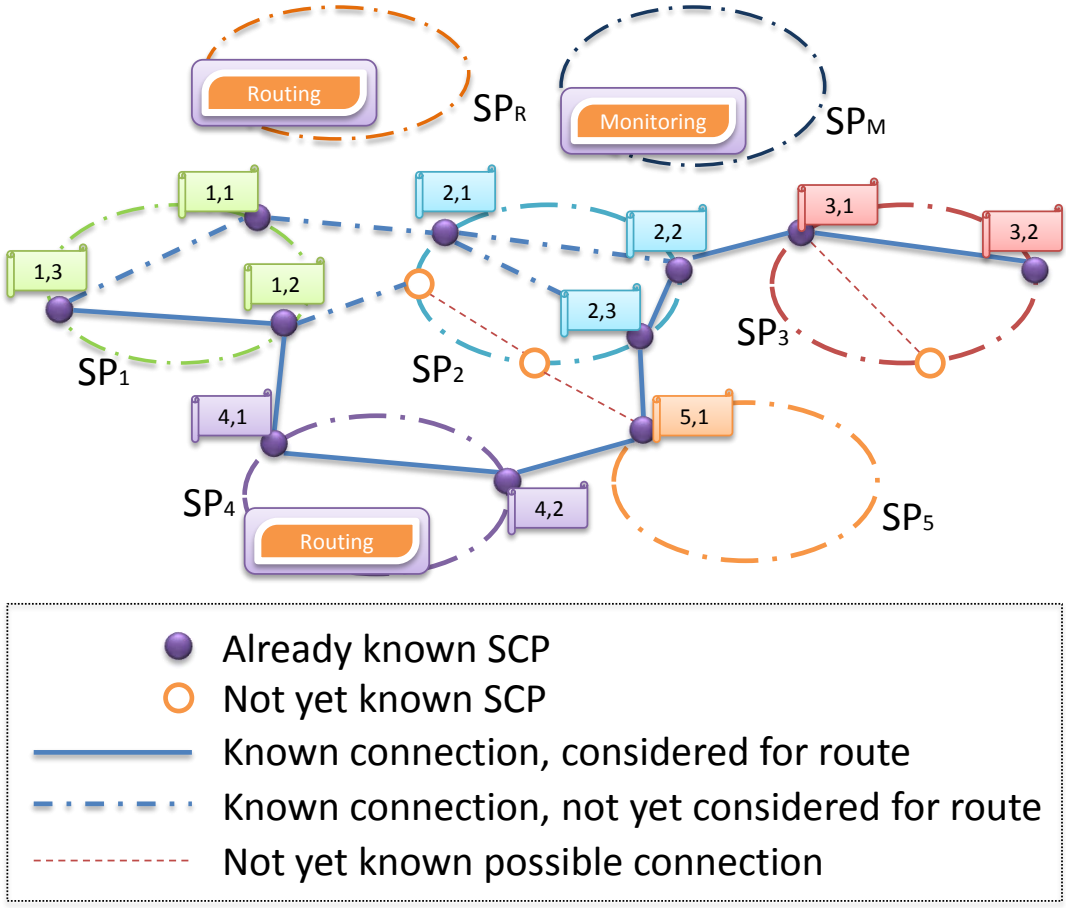


Abbildung 7.24.: Gefundenen Route und vorhandenes Wissen

Bei der Pfadsuche werden SP-Präferenzen berücksichtigt

Beim Durchspielen des Beispiels wurde gezeigt, dass die Abbildung der definierten UML-Diagramme auf die XML-Nachrichten ohne weiteres durchgeführt werden kann. Bei den Informationsabfragen lassen sich die unterschiedlichen Möglichkeiten entsprechend den SP-Präferenzen anordnen. Bei der Wahl der nächsten Teilstrecke wurde stets die vom jeweiligen Service Provider bevorzugtere Alternative ausgewählt. So wurde gleich am Anfang die Route von $SCP_{1,3}$ nach $SCP_{1,1}$ und nicht nach $SCP_{1,2}$ gewählt, obwohl die zweite bessere Eigenschaften aufwies (siehe Tabelle 7.2). Auch wenn auf dem – aus der Providersicht – bevorzugten Weg keine Route gefunden werden konnte, die die E2E-Kundenanforderungen erfüllt, konnte der Suchalgorithmus mit einer Alternativroute die Erfüllung der gestellten E2E-Anforderungen sicherstellen.

Globales Wissen wird nicht benötigt

Bei der Pfadsuche ist vor allem der Aspekt interessant, dass nicht der komplette Graph durchsucht werden muss, der die existierenden Netzverbindungen darstellt. Dies ist möglich, weil bei Informationsabfragen auf dem Wissen der jeweiligen SP-Domänen aufgebaut wird. Das bedeutet, dass für die Pfadsuche kein vollständiges globales Wissen erworben werden muss (siehe noch nicht bekannten Verbindungen und SCPs in Abbildung 7.24). Somit bietet das entwickelte Vorgehen eine echte Alternative zu den klassischen Ansätzen in der Graphentheorie, die auf der Kenntnis der vollständigen Topologie aufbauen.

Einfaches Vorgehen

Wie im Abschnitt 3.3 beschrieben wurde, wird das Optimalitätprinzip von BELLMAN bei mehrfachgewichteten Graphen nicht erfüllt. Dadurch werden fast zwangsläufig sehr komplexe Suchalgorithmen benötigt, um die Suchlaufzeit einzuschränken. Bei dem erarbeiteten Verfahren wird der Suchraum automatisch von den SP-Domänen verbindungspezifisch eingeschränkt, wodurch auch der Einsatz des Tiefensuche-ähnlichen Verfahrens gerechtfertigt wird. Eine Erweiterung des entwickelten Verfahrens mit den Ideen und Konzepten der Suchalgorithmen in mehrfachgewichteten Graphen kann sehr interessant sein.

Bessere Provider-Akzeptanz

Ein weiterer wichtiger Aspekt der gewählten Vorgehensweise besteht in einer wesentlich besseren Provider-Akzeptanz im Vergleich zu Abfragen über eine komplette Netz-Topologie. Mehr dazu wird projektbezogen in Kapitel 8 diskutiert.

Verschiedene Beziehungsformen können gleichzeitig unterstützt werden

Zu den mit Abstand kritischsten Aspekten in Multi-Domain Kooperationen gehören Verantwortungsbereiche und Kommunikationswege, die die einzelnen SP-Domänen miteinander in Verbindung bringen. Das Beispiel wurde so konstruiert, dass die Verantwortungsbeziehungen sowie die Kommunikationsbeziehungen beim Routing und beim Monitoring sich voneinander unterscheiden. Das soll vor allem die Flexibilität der entwickelten Lösung bei der Etablierung unterschiedlicher Beziehungsformen zeigen.

Kommunikationsbeziehungen während des Routing-Prozesses

In Abbildung 7.25 sind die Kommunikationsbeziehungen während des Routingprozesses dargestellt. Insbesondere entspricht diese Abbildung der Situation, nachdem die Route gefunden wurde und alle beteiligten SP-Domäne sowie deren Verantwortungsbereiche festgelegt wurden. Die Domäne SP_R wird von SP_1 beauftragt, stellvertretend für SP_1 eine geeignete Route zu finden, zu reservieren und zu bestellen. Deswegen befindet sich SP_R am Wurzel des Kommunikationsbaumes in Abbildung 7.25. Auch wenn SP_1 der Auftraggeber von SP_R ist, bei der Pfadsuche nimmt SP_1 gleichzeitig die Rolle des Verbindungsdienste-Providers ein. Diese Rolle nimmt auch der Provider SP_4 ein. Gleichzeitig nimmt SP_4 auch die *Proxy-SP* Rolle ein, in der er weitere Teildienste von SP_5, SP_2 und SP_3 beauftragt.

Verantwortungs- bzw. Vertragsbeziehungen bei der bestellten Dienstinstanz

Da SP_R alle Teilstrecken der gefundenen Route nur stellvertretend für SP_1 abfragt, reserviert und anschließend bestellt (siehe Zeilen 7 bis 14 in Abbildung 7.8 sowie Zeilen 18 bis 25 in Abbildung 7.15), weichen die Verantwortungs- bzw. Vertragsbeziehungen der etablierten Route von den Kommunikationsbeziehungen während der Pfadsuche ab (siehe Abbildung 7.26). Das bedingt auch die Notwendigkeit, die Informationen über

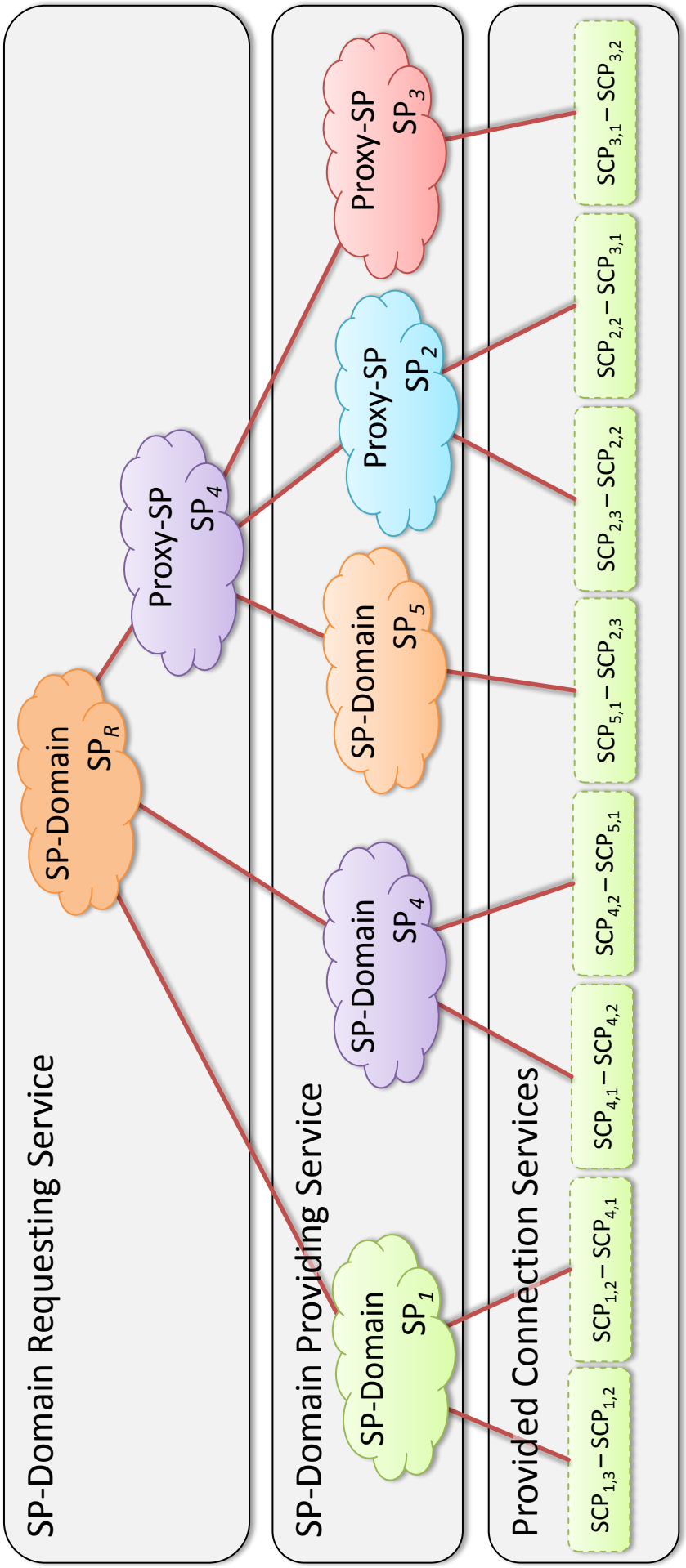


Abbildung 7.25.: Kommunikationsbeziehungen der Bestellung der Route

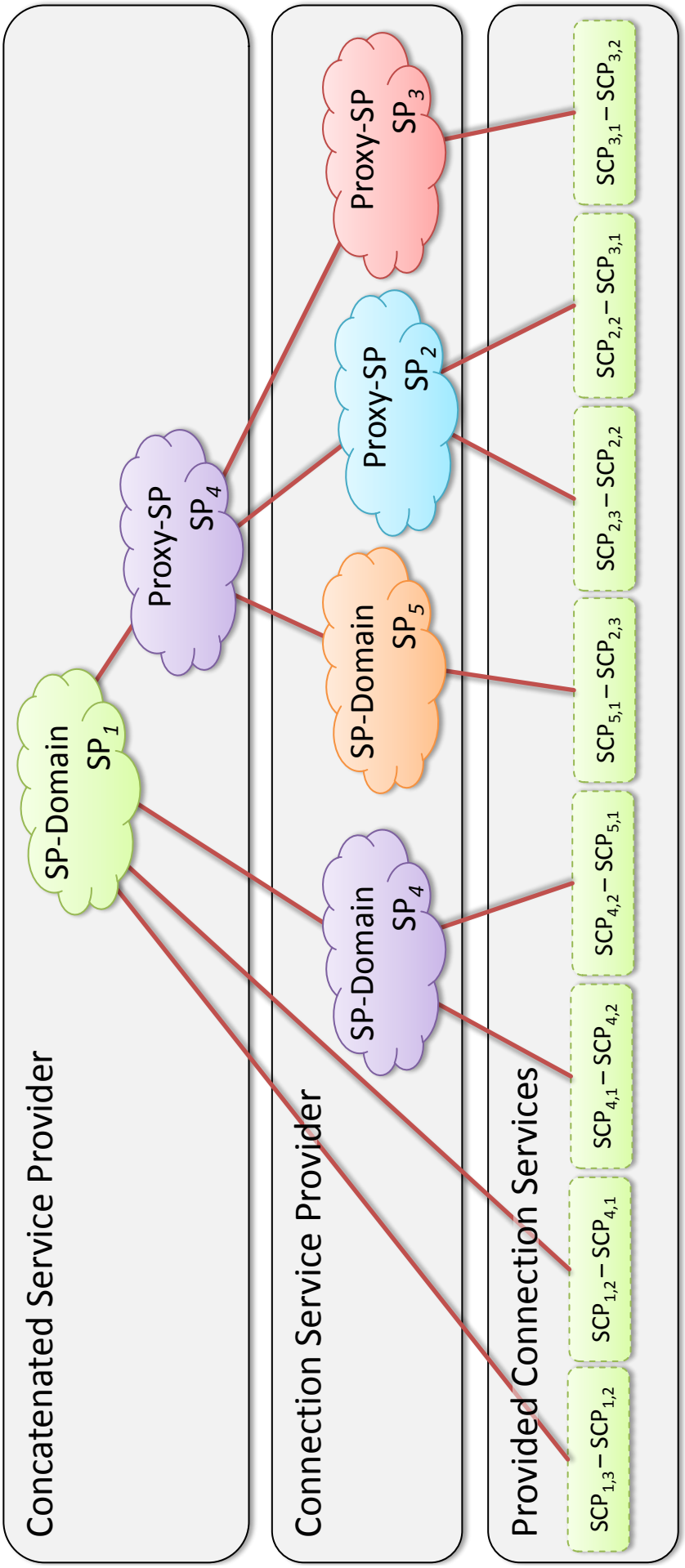


Abbildung 7.26.: Verantwortungsbeziehungen nach der Bestellung der Route

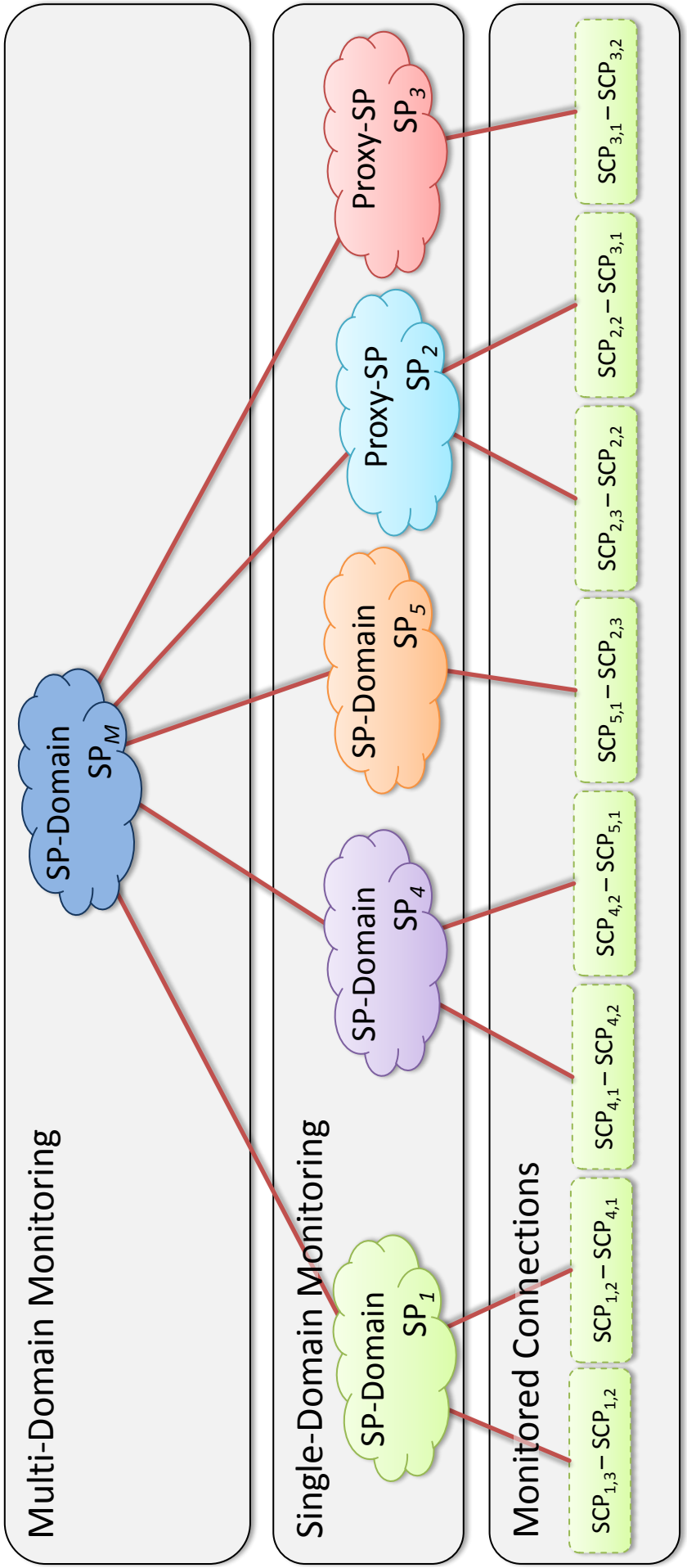


Abbildung 7.27.: Kommunikationsbeziehungen beim Monitoring

die gefundene Route an SP_1 zu melden (siehe Zeilen 4 bis 808 in Abbildung 7.22). Die Verantwortungsbeziehungen sind später dafür entscheidend, wie die Aufgaben wie z.B. CHANGE oder DECOMISSIONING aufgerufen und weitergereicht werden können. In Abbildung 7.26 ist klar erkennbar, dass nach der Bestellung der Route die SP-Domäne SP_1 für den gesamten Verketteten Dienst des Beispiels zuständig ist. Die Dienstinstanz besteht aus zwei Teilstrecken unter der direkten Eigenverantwortung, aus zwei weiteren Teilstrecken, die bei SP_4 bestellt wurden, sowie aus einem Verketteten Dienst für die Teilstrecke zwischen $SCP_{5,1}$ und $SCP_{3,2}$, für den der Proxy-SP SP_4 zuständig ist.

Kommunikationsbeziehungen beim Monitoring

Bei den Kommunikationsbeziehungen für das Monitoring ändert sich die Situation noch einmal (siehe Abbildung 7.27). Das liegt daran, dass SP_1 bei der Bestellung des Routing-Dienstes von SP_R die TRANSPARENTPROXY-Option gewählt hat (siehe Zeile 107 in Abbildung 7.4), wodurch auch bei der Delegation die Wiederverwendung der initial ausgewählten Provider der Multi-Domain Managementdienste (im Falle des Beispiels – nur SP_M für den Monitoring-Dienst) gefordert wird. Der große Vorteil dieser Delegationsart besteht darin, dass die Kommunikationswege zwischen den Single- und Multi-Domain Managementdiensten unabhängig von der Anzahl der Delegationen kurz bleiben. Im Gegensatz dazu bietet die *Full-Proxy*, die den internen Aufbau komplett verschattet, eine wesentlich einfachere Kommunikationsstruktur, die mit den Vertragsbeziehungen übereinstimmt. Der größte Nachteil von Full-Proxy besteht in der direkten Abhängigkeit der Länge der Kommunikationswege von der Anzahl der benötigten Delegationen.

Situationsbedingte Anpassungsmöglichkeiten

In Bezug auf Monitoring sind nicht nur die Kommunikationswege, sondern auch die Verantwortungsbereiche einzelner SPs interessant. Die SP-Domäne SP_M ist für die Abfrage der Zustandsinformationen einzelner Teildienste sowie für die Aggregation dieser Informationen zuständig. Die restlichen in Abbildung 7.27 dargestellten SPs stellen SP_M die Monitoring-Informationen der einzelnen Teildienste zur Verfügung, für die sie zuständig sind (in der Abbildung durch die Verbindungslinien angedeutet). Dabei zeichnet sich ein Nachteil der entwickelten Lösung auf, der durch die per-Teilstrecke Abfragen verursacht wird. Dadurch werden jeweils zwei Informationsabfragen bei SP-Domänen benötigt, die für zwei Teilstrecken zuständig sind, obwohl sie zu derselben Dienstinstanz gehören. Anhand dieses Beispiels kann z.B. die Erweiterung im Sinne der Dienstinstanz-bezogenen Abfragen interessant sein. Im Kapitel 8 wird zudem eine weitere Erweiterung diskutiert – per-Domain Abfragen. Die Wahl für eine dieser Varianten muss bei der Umsetzung der Lösung situationsbedingt getroffen werden, denn durch die Veränderung zur per-Dienstinstanz- oder per-Domain-Variante geht die Feingranularität verloren. Darüberhinaus kann die Unterstützung mehrerer unterschiedlicher Varianten die Komplexität einzelner Komponenten erhöhen.

8 Anwendung

Diese Dissertation entstand gleichzeitig mit der Mitarbeit im Géant2 Projekt. Dies hat es ermöglicht, Ideen aus dieser Arbeit in die Teilprojekte einfließen zu lassen und im Gegenzug Erfahrungen über die Tragfähigkeit der entwickelten und angesetzten Konzepte zu sammeln.

In diesem Kapitel werden zwei Teilprojekte beschrieben, die besonders von dieser gegenseitigen Bereicherung profitiert haben – E2E-Link-Monitoring-System (E2Emon) und *Information Sharing across Heterogeneous Administrative Regions* (I-SHARe). Beide Teilprojekte sind im Rahmen des *Géant2* Dienstes E2E Links entstanden (siehe dazu Abschnitt 2.3.2) und richten sich auf unterschiedliche Betriebs- und Managementaspekte.

Beim E2E-Monitoring-System handelt es sich um einen Baustein des Service-Level-Managements – die kontinuierliche Überwachung des Dienstinstanz-Zustandes. Da die Géant2 E2E Links zu der Dienstklasse *Concatenated Service* gehören, sind die Überschneidungen zwischen E2Emon und den Ergebnissen dieser Arbeit sehr groß. Das E2E Monitoring System wird zudem seit ca. 3 Jahren produktiv eingesetzt, weswegen viele Erfahrungen vorliegen. Wegen des Umfangs wird die Beschreibung von E2Emon in drei Unterabschnitte strukturiert: zunächst wird das Projektumfeld und die Ziele von E2Emon beschrieben, es folgt die Beschreibung der eingesetzten Konzepte und der notwendigen Anpassungen. Abschließend werden die Erfahrungen mit dem Produktivansatz geschildert und bewertet.

Der Fokus beim I-SHARe Teilprojekt liegt auf der Unterstützung der Géant2 E2E-Link-Betriebsprozesse durch Verbesserung des Informationsaustauschs zwischen den NRENs. Bislang wurden im I-SHARe Teilprojekt die Anforderungsanalyse, das Systemdesign und die Entwicklung eines ersten Prototyps abgeschlossen. Obwohl der I-SHARe-Prototype bereits im Testbetrieb ist, ist die Menge der bislang gesammelten Erfahrungen gering. Aus diesem Grund wird die Beschreibung des I-SHARe-Teilprojekts abweichend von der E2Emon-Beschreibung strukturiert: nach der Beschreibung der

Ziele des Teilprojekts werden eingesetzte Konzepte und die dabei erworbene Erfahrungen gemeinsam beschrieben.

Die Struktur des Kapitels ist graphisch in Abbildung 8.1 dargestellt.

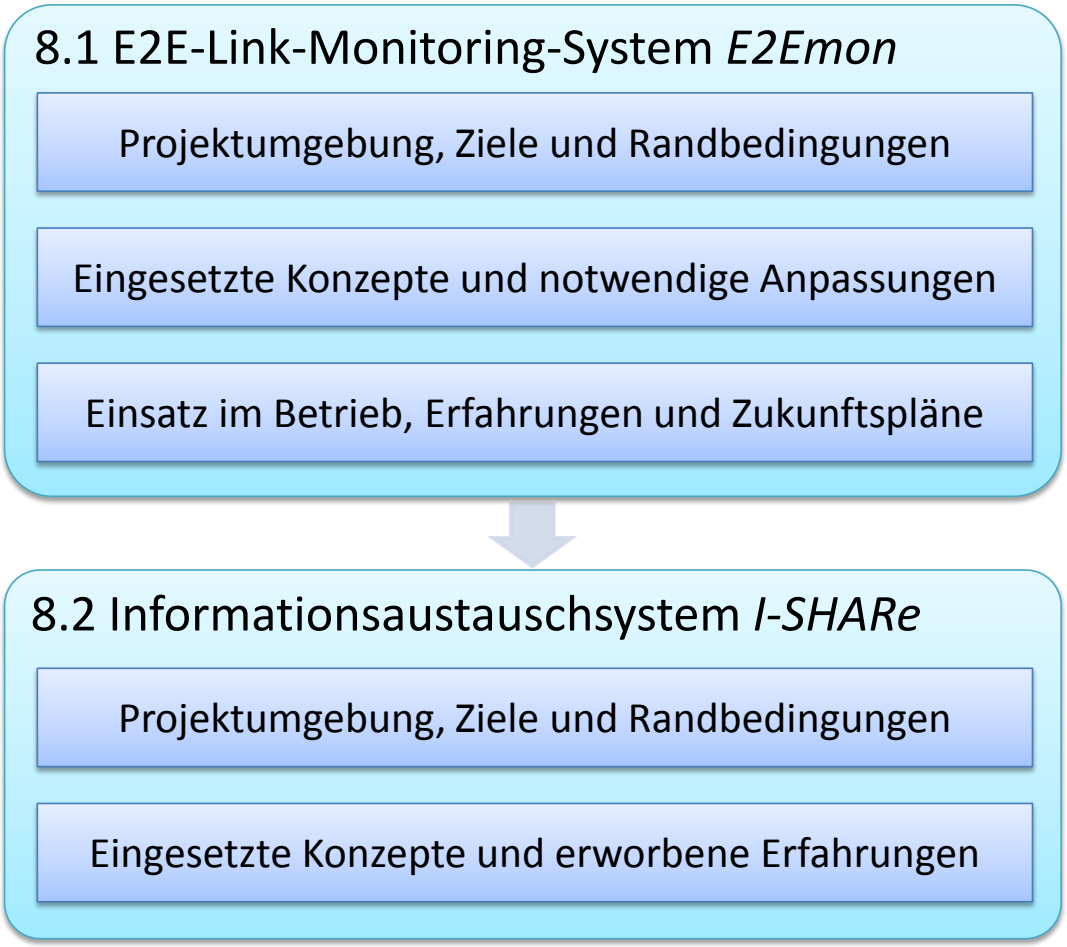


Abbildung 8.1.: Aufbau dieses Kapitels

8.1. E2E-Link-Monitoring-System E2Emon

Das E2E-Link-Monitoring-System (E2Emon) wurde konzipiert und entwickelt, um die operationalen und administrativen Zustände von Géant2 E2E Links (siehe Abschnitte 1.2 und 2.3.2) zu überwachen.

8.1.1. Projektumgebung, Ziele und Randbedingungen

Die Problematik des E2E-Link-Monitorings hängt direkt mit dem internen Aufbau der E2E Links zusammen, der wiederum von den Nutzungseigenschaften abgeleitet wurde. Wie im Abschnitt 2.3.2 beschrieben wurde, sind E2E Links dedizierte permanente Verbindungen, die für die maximale Ausnutzung der vorhandenen Übertragungsraten ausgelegt wurden. Dadurch entfällt die Notwendigkeit einer Routinginfrastruktur und die Verbindungen werden von den beteiligten NRENs überwiegend auf ISO/OSI Netzschichten 1 und 2 realisiert.

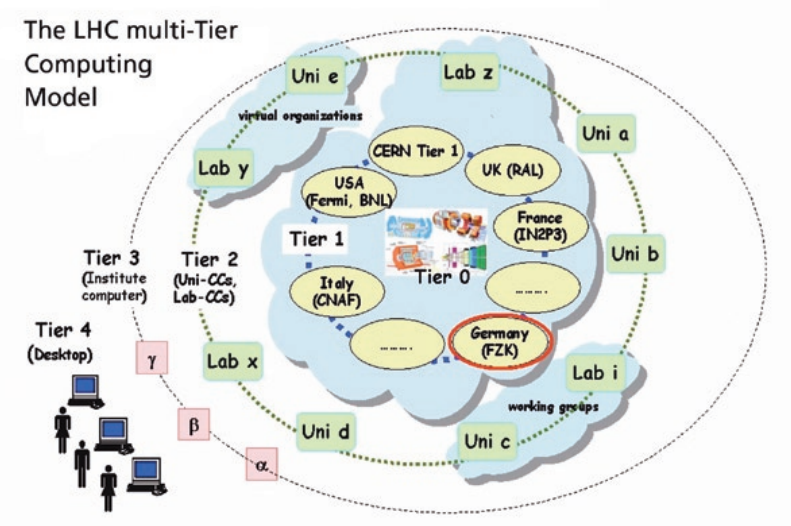


Abbildung 8.2.: LHC Multi-Tier Model [Sch07a]

Betrachtet man die Größenordnung der Forschungsprojekte wie LHC oder DEISA, die momentan die Hauptnutzer von E2E Links sind, so müssen im Rahmen dieser Projekte dutzende bis hunderte internationale Rechenzentren und Forschungseinrichtungen durch E2E Links miteinander verbunden werden. Zur Illustration sind in den Abbildungen 8.2 und 8.3 die groben Anordnungsstrukturen zwischen Rechenzentren in beiden o.g. Projekten dargestellt. So werden in Rahmen des LHC Projekts die 11 sog. Tier-1-Rechenzentren, die für die Speicherung der Experimentdaten zuständig sind, sternförmig an das Tier-0-Zentrum in CERN sowie untereinander durch E2E Links verbunden. Die ca. 100 für die Datenbearbeitung zuständigen Tier-2-Rechenzentren

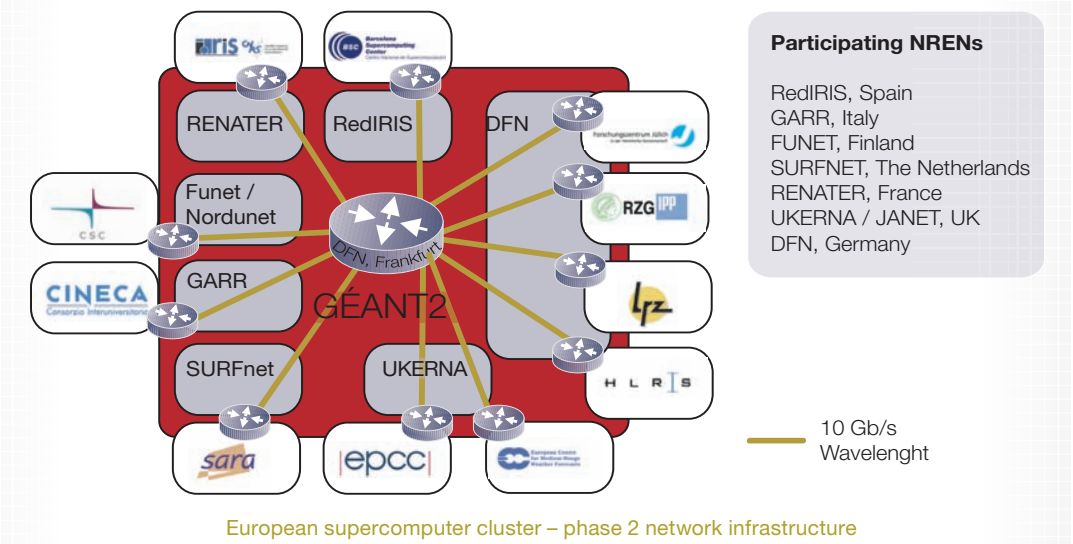


Abbildung 8.3.: DEISA Netz Infrastruktur [Dei08b]

(darunter auch das Leibniz-Rechenzentrum, LRZ) greifen auf die abgespeicherten Experimentdaten momentan überwiegend über die konventionelle Routinginfrastruktur zu. Es wird im Projekt jedoch angestrebt, mit der Zeit auch die Tier-1 zu Tier-2 Verbindungen auf Basis von E2E Links zu realisieren.

Bei der benötigten Anzahl der E2E Links ist vor allem der Kostenfaktor ein triftiges Argument, der die Einschränkung auf die Netzinfrastruktur der ISO/OSI Schichten 1 und 2 rechtfertigt. Neben der Kostenersparnis hat diese Entscheidung allerdings Konsequenzen in Bezug auf das E2E Link Management in sich, denn die für die ISO/OSI Netzschichten 3+ entwickelten Techniken können bei E2E Links nicht eingesetzt werden.

In dem Betriebskonzept für die verbindungsorientierten Netzdienste in Géant2 wird die Notwendigkeit einer Reihe domänenübergreifender Betriebsprozesse identifiziert [CRE+07]. Im Rahmen der Maßnahmen zur Zusicherung der E2E-Dienstgüte einzelner Dienstinstanzen wird das domänenübergreifende Monitoring benötigt. Zu den Zielen des Monitoring-Prozesses gehören:

- Erkennung der Störungen von E2E Links
- Lokalisation gestörter Abschnitte
- Möglichst automatische Initiierung des Fault-Managementprozesses

Für die Durchführung dieser Aufgaben wurde eine Kombination aus organisatorischen und technischen Mitteln konzipiert (siehe Abbildung 8.4). Für die Koordination der – zunächst nur Fault-Management bezogenen – Maßnahmen einzelner NRENs wurde eine sog. *E2E Coordination Unit* (E2ECU) eingerichtet. Die E2ECU kommuniziert

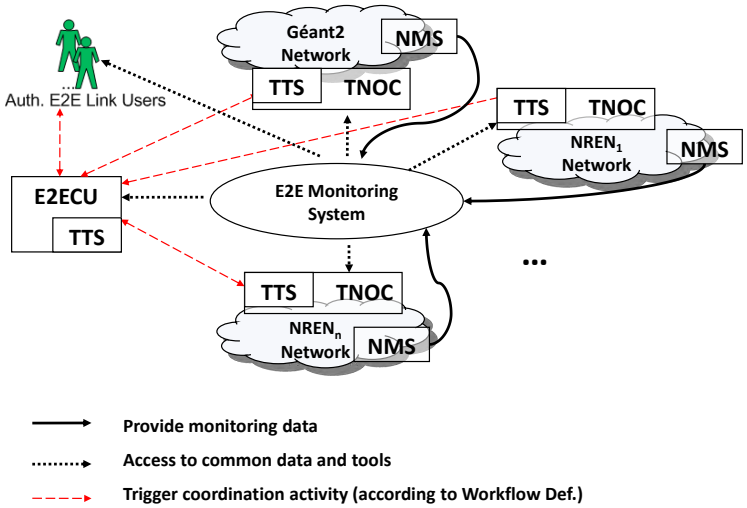


Abbildung 8.4.: Betriebsorganisation für Géant2 E2E Links [US06]

mit den für die Schicht-2-Datenstrecken zuständigen Betriebsgruppen der einzelnen NRENs, den sog. TNOCs (Transmission Network Operating Centre). Die E2ECU stützt sich bei ihrer Tätigkeit auf die Informationen des E2E Monitoring Systems, das die Informationen der *Netzmanagement-System* (NMS) einzelner NRENs zu einer domänenübergreifenden Sicht aggregiert. Neben der E2ECU dürfen auf die Informationen des E2E Monitoring Systems auch die TNOCs und autorisierte Nutzer (engl.: *authorized E2E Link User*) zugreifen. Als authorized E2E Link User sind dabei projektabhängig entweder die tatsächlichen Nutzer der E2E Links als auch spezielle technische Teams möglich. So wird bei LHC Computing Grid (LCG) im Falle eines E2E Link-Ausfalls mit einer dafür zuständigen Betriebsgruppe (dem sog. ENOC) kommuniziert, die auch ein zentraler Ansprechpartner der Benutzer für Probleme innerhalb des Projekts ist [BMM05, Kno05, EGE08, EGE09] (siehe Abbildung 8.5).

Somit wurden für das E2E-Monitoring-System folgende Aufgaben vorgesehen:

- Mit den involvierten NRENs kommunizieren, um die Monitoring-Daten einzelner NRENs zu sammeln
- Teilstrecken-Zustandsinformationen aggregieren, die zu demselben E2E Link gehören und von unterschiedlichen NRENs gemeldet werden
- E2E-Links-Zustandsinformationen analysieren und die E2ECU in Problemfällen automatisch benachrichtigen
- Bei Ausfällen den E2E-Link-Zustand für die spätere Untersuchung abspeichern
- Die laufende Statistik der E2E-Link-Zustände sammeln
- Bei der Berechnung des Gesamtzustandes ggf. laufende Wartungsarbeiten berücksichtigen

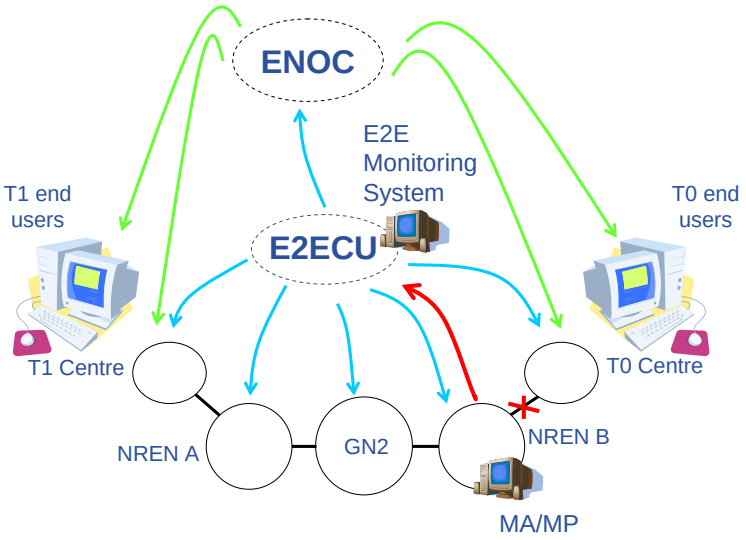


Abbildung 8.5.: Integration der E2ECU in das Fault Management des LCG [Rod08]

- Die aktuelle Zustandsinformationen der E2ECU, allen beteiligten NRENs und den authorised Users zur Verfügung stellen

Bei der Durchführung dieser Aufgaben sollen vom E2E-Monitoring-System auch die folgende Eigenschaften der Diensterbringung berücksichtigt werden:

- Die E2ECU (und somit auch das E2E Monitoring System) ist für alle E2E Links aus allen Projekten zuständig
- NRENs werden sich i.A. an der Erbringung mehrerer E2E Links beteiligen, die wiederum zu unterschiedlichen Projekten gehören können

Die Art der Zusammenarbeit der einzelnen NRENs wurde in einem *Memorandum of Understanding* (MoU) [LHC] festgelegt. Trotz einer engen Kollaboration bleiben die NRENs unabhängige Organisationen. So können alle NRENs – zwar mit technisch notwendigen Absprachen mit den Partner-NRENs – in Eigenregie entscheiden, welche Technologie und welcher Hardware-Anbieter bei der Realisierung eigener Teilstrecken eines E2E Links gewählt wird. Die Unabhängigkeit der NRENs bedeutet auch, dass u.U. sehr restriktive Sicherheits-Policies angewandt werden, um den Informations- und/oder Managementzugriff auf die NREN-interne Infrastruktur zu regeln. Dadurch werden weitere Anforderungen an das E2E Monitoring System motiviert:

- Die Abfrage der Monitoring-Informationen einzelner Teilstrecken soll ohne direkten Zugriff auf die Netzinfrastruktur der jeweiligen NRENs möglich sein
- Es muss ein Weg gefunden werden, auch bei heterogenen Monitoring-Informationen einzelner Teilstrecken eines E2E Links eine Aussage über den E2E-Zustand zu errechnen

- Auch ohne Uhr-Synchronisation der einzelnen NRENs muss das E2E Monitoring System die Zustandsinformationen einzelner NRENs synchronisieren können

8.1.2. Eingesetzte Konzepte und notwendige Anpassungen

Ausgehend von den beschriebenen Anforderungen und Randbedingungen wurde am LRZ das E2E-Monitoring-System *E2Emon* entwickelt. Die Systemarchitektur ist in Abbildung 8.6 dargestellt. Das Konzept sieht eine Aufteilung in zentrale (in der Abbildung oben) und NREN-spezifische (in der Abbildung unten, auf grauem Hintergrund) Komponenten vor. Während die zentralen Komponenten nur einmal vorkommen, müssen die NREN-spezifischen Komponenten bei allen NRENs implementiert und installiert werden.

Strukturierung des Unterabschnittes

Bei der Beschreibung der im Projekt eingesetzten Ideen aus dieser Arbeit wird in diesem Unterabschnitt zunächst die Kommunikationsschnittstelle zwischen der zentralen Komponente des Monitoring Systems erklärt, dann werden die relevanten Bestandteile der NREN-Komponenten und anschließend der Aufbau der zentralen Komponente besprochen.

Client-Servier Kommunikation

Die Kommunikation zwischen den zentralen und den lokalen Komponenten ist entsprechend des Client-Server-Prinzips realisiert und erfolgt über eine vordefinierte Schnittstelle via Web Services (vergleiche Abschnitte 3.1 und 5.1 sowie Einführung zu Kapitel 7). Um die Interoperabilität mit anderen existierenden oder zukünftigen Tools in Géant2 zu ermöglichen, wurde bei der Kommunikation das *perfSONAR* Kommunikationsschema verwendet [pSH09, Swa09]. Dabei handelt sich um die Kommunikation mittels SOAP und die Nutzung von XML-Nachrichten, die entsprechend dem *NMWG* Schema (NMWG steht für *Network Monitoring Working Group*) des *Global Grid Forums* (GGF!) definiert sind. Die Verwendung dieses Schemas hat sich auch in der DCN-Kooperation (siehe Abschnitt 2.3.4) etabliert, was auch die Interoperabilität mit den in Internet2 entwickelten Tools erleichtert.

Periodische Informationsabfragen

Das Konzept des Géant2 E2E-Monitoring-Systems [HY08b] sieht vor, dass die zentrale E2Emon-Komponente periodisch Informationsanfragen an alle NRENs schickt (vergleiche Abschnitte 5.10, 6.6 und insbesondere 6.7). Die XML-Anfrage der aktuellen Informationen ist in Abbildung 8.7 dargestellt. Durch die Spezifikation NOW im Feld TIME werden die aktuellen Zustandsinformationen angefordert. Es ist vorgesehen, dieses Feld bei der Weiterentwicklung der E2E Monitoring Systems auch für die Abfrage vergangener Zustandsinformationen zu verwenden.

Daten-Synchronisation durch gleichzeitige Abfragen

Durch diese zentral ausgeführten Anfragen wird auch die Synchronisation der Monitoring-Informationen gewährleistet. Diese Synchronisation ist jedoch nicht 100% genau. So werden die Anfragen nicht gleichzeitig, sondern sequentiell versendet, d.h. die Anfrage für einen in der Abfrageliste nachfolgenden NREN wird erst nach dem Erhalt der Antwort des vorherigen NREN geschickt. Im Projekt hat sich ein 5-Minutiger

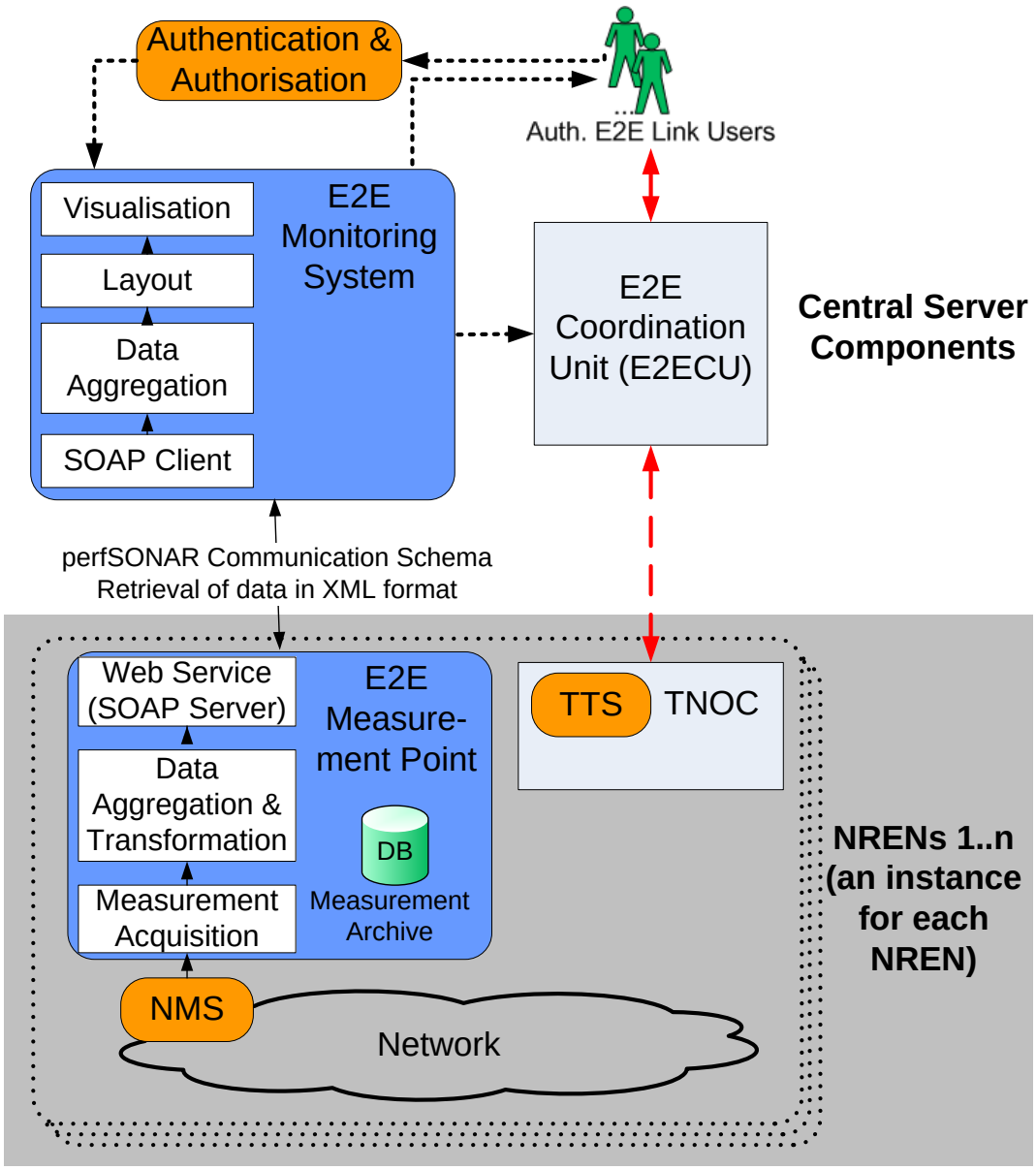


Abbildung 8.6.: E2E Monitoring System, Systemarchitektur [YH07]

```
<nmwg:message type="SetupDataRequest"
          xmlns:nmwg="http://ggf.org/ns/nmwg/base/2.0/">

   <nmwg:metadata id="meta1">
      <nmwg:eventType>Path.Status</nmwg:eventType>
    </nmwg:metadata>

    <nmwg:metadata id="meta2">
        <select:parameters>
            <select:parameter name="time">now</select:parameter>
            </select:parameters>
     </nmwg:metadata>

</nmwg:message>
```

Abbildung 8.7.: Abfrage der Monitoring-Informationen (generiert bei E2Emon) [HY08b]

Polling-Zyklus als akzeptabel etabliert. Bei der Berechnung der Verfügbarkeitsstatistik wird daher die momentane Zustandsaufnahme als für das komplette Polling-Intervall gültig angenommen. Das bedeutet wiederum, dass kurzfristige Zustandsveränderungen (engl.: *spikes*) - in Abhängigkeit davon, was vor der Antwort an die zentrale Monitoring-Komponente gemessen wurde - entweder überhaupt nicht erkannt oder deren Zustand als für den kompletten Polling-Intervall gültig angenommen werden.

Up-to-date vs. Historische Informationen bei NRENs

Wie die Monitoring-Informationen domänenintern durch einzelne NRENs dem E2E Monitoring System zur Verfügung gestellt werden ist graphisch in Abbildung 8.8 dargestellt. Dafür wurden zwei Alternativen definiert. In beiden Fällen liegt es in der Verantwortung des jeweiligen Service Providers, die vom NMS gesammelten Statusinformationen der eigenen Netzinfrastruktur mittels eines technologiespezifischen Skripts zu analysieren. Dabei werden die Technologie- und Infrastruktur-spezifischen Statusinformationen in das Datenformat transformiert, die von E2Emon erwartet wird. In diesem Schritt werden die Zustandsinformationen mit den topologischen Informationen in Verbindung gebracht, d.h. es muss spezifiziert werden, auf welchen Abschnitt welches E2E Links ein Zustand sich bezieht. Im Falle eines sog. *Measurement Points* (MP) werden diese Informationen zunächst in einer XML-Datei abgespeichert (siehe Abbildung 8.8 links). Diese Datei wird bei der Domain-internen Netzüberwachung kontinuierlich aktualisiert. Bei der Abfrage durch die zentrale Komponente des E2Emon-Monitoring-Systems wird diese Datei von dem Web Service MP als Antwort zurück geschickt. Im Falle eines sog. *Measurement Archives* (MA) sieht die Situation theoretisch nur wenig anders aus - die neuesten Status-Informationen werden jedoch nicht in eine Datei, sondern in eine Datenbank geschrieben und mit einem Zeitstempel versehen. Dadurch soll es in Zukunft ermöglicht werden, auch historische Statusinformationen abzufragen.

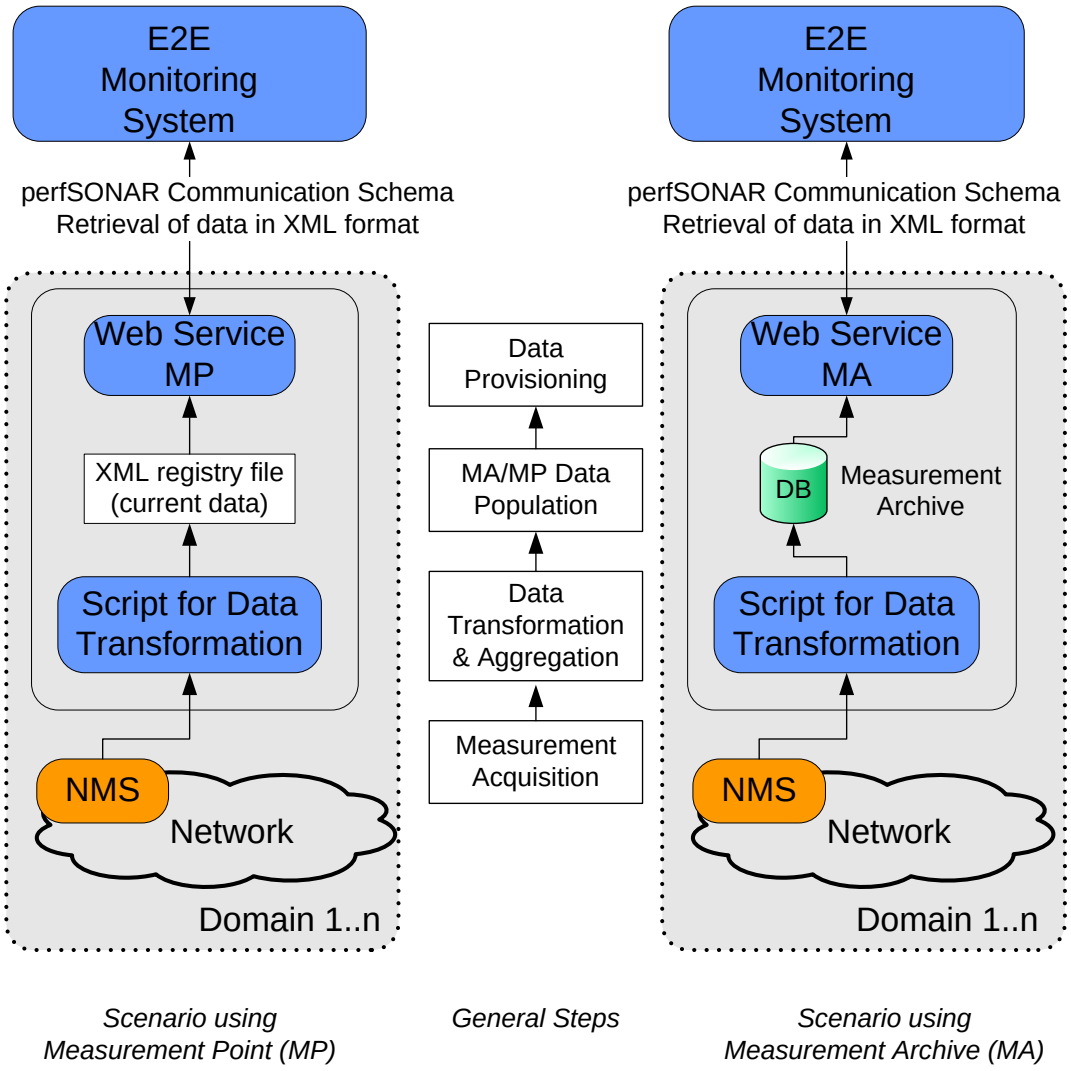


Abbildung 8.8.: Abholung der Monitoring-Informationen [HY08b]

Unterschiedliche Single-Domain Überwachungs-methoden

Die Abbildung betont insbesondere zwei Aspekte. Zu einem ist es nicht festgelegt, wie die Statusinformationen domänenintern aus den NMS abgefragt werden. Im Projektumfeld bei unterschiedlichen NRENs haben sich sowohl das regelmäßige Polling als auch der Einsatz von SNMP Traps durchgesetzt. Das heißt, dass die XML-Datei im Falle von MP mehrmals überschrieben werden kann, bevor die Informationsabfrage von der zentralen Monitoring-Komponente kommt. Auch konnte zwischen den NRENs keine Einigung erzielt werden, mit welchem Datum die Messwerte versehen werden sollen – von der letzten Zustandsmessung oder von der letzten Zustandsänderung. Der andere Aspekt bezieht sich ausschließlich auf die Verwendung von MAs (rechts im Bild). Da die NRENs derzeit keine synchronisierten Uhren verwenden, bleibt die Frage ungeklärt, wie die historischen Informationen aus unterschiedlichen MAs retro-

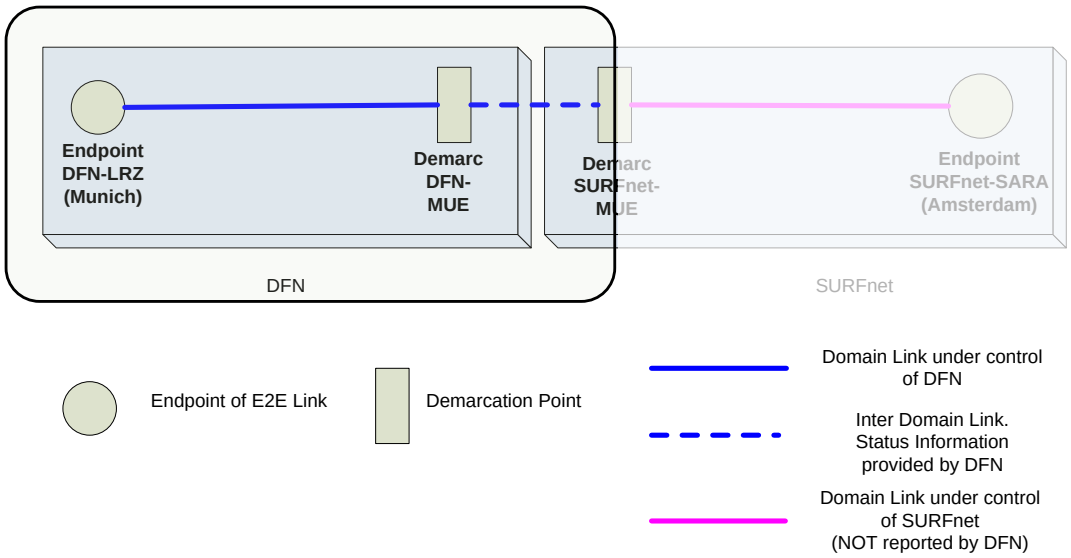


Abbildung 8.9.: Verantwortungsbereiche für Monitoring-Informationen, Variante 1 [HY08b]

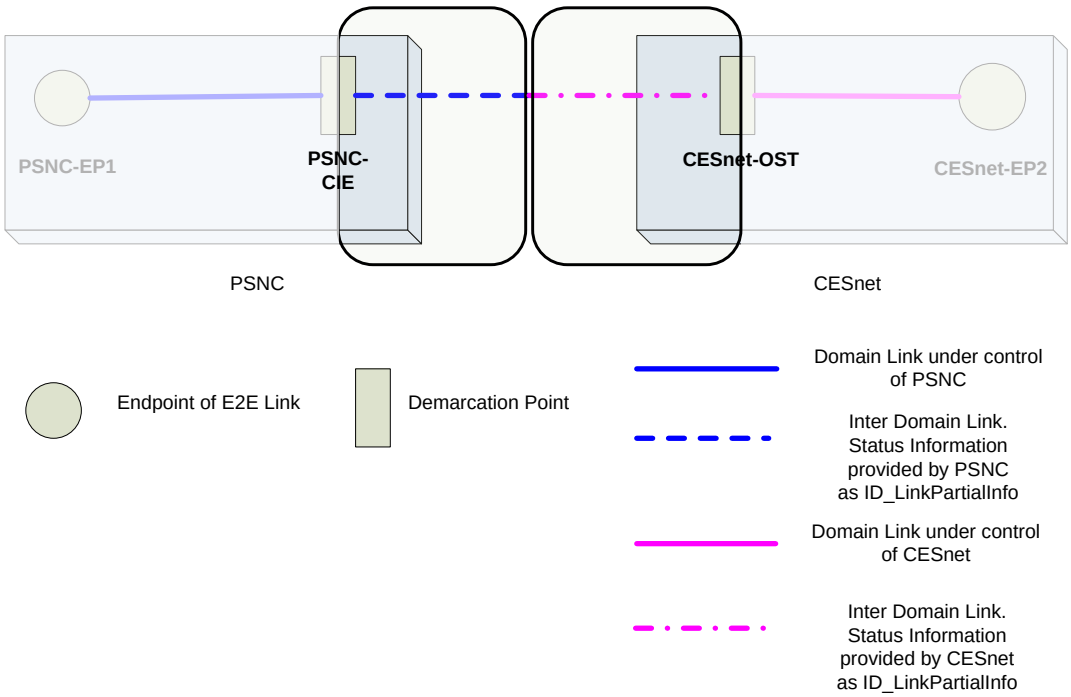


Abbildung 8.10.: Verantwortungsbereiche für Monitoring-Informationen, Variante 2 [HY08b]

spektiv miteinander in Verbindung gebracht werden können. Daher wird derzeit ein alternativer Weg diskutiert, historische Informationen nicht bzw. nicht nur bei den NRENs abzuspeichern.

Beschreibung der topologischen Strukturen

Sieht man von den Abweichungen bei der Terminologie ab (die SCPs an der Grenzen der Domäne werden als *Demarcation Points* (DP) bezeichnet), haben sich im Projekt bei der Beschreibung der topologischen Strukturen dieselben Konzepte durchgesetzt, wie sie im Kapitel 4 definiert wurden (siehe Abbildungen 8.9 und 8.10).

Beschreibung der Teildienst-Eigenschaften

Bei der Beschreibung der Teildienst-Eigenschaften hat man sich zunächst auf zwei – einen sog. *operativen* und einen *administrativen* – Zustandswert beschränkt. Der *Operational State* wird von den NMS-Messungen abgeleitet und entspricht der Aussage über die Funktionalität der Teilstrecke in den für sie vorgesehenen Wertebereichen. Der *Administrative State* dagegen gibt zusätzliche Informationen der Teilstrecke an, die meist auf administrative Vorgänge zurückzuführen sind, wie z.B., ob die Teilstrecke im Betrieb ist oder ob momentan Wartungsarbeiten durchgeführt werden, die diese Teilstrecke betreffen. Dadurch ist es möglich, bei der Fehlererkennung sowie bei der Statistikberechnung den *Administrative State* berücksichtigen. Das E2E Monitoring System generiert z.B. keine Fehlerbenachrichtigung, wenn auf der Teilstrecke eines E2E Links Wartungsarbeiten durchgeführt werden. Auch wenn die Realisierung solcher Interdependenzen zwischen unterschiedlichen Teilstreckeneigenschaften im Rahmen der entwickelten Lösung ohne weiteres bei der Definition der Aggregatfunktionen realisierbar ist (siehe Abschnitt 4.2.2), kann eine systematische Untersuchung solcher Situationen und vor allem deren verständlichere Beschreibung als eine Weiterentwicklung dieser Arbeit angesehen werden (siehe auch Kapitel 10).

Die erlaubten Werte für den operationalen und administrativen Zustand sind in den Tabellen 8.1 und 8.2 dargestellt (vergleiche Diskussion in Abschnitt 4.1 und insbesondere das UML-Diagramm in Abbildung 4.47). Durch die Wahl dieser grob-granularen erlaubten Wertezustände wurde eine Abstraktionsebene geschaffen, die für alle NRENs unabhängig von der eingesetzten Technologie und Infrastruktur gültig ist. Wie die Abbildung von den tatsächlichen Messergebnissen auf die abstrakten Zustände geschehen soll, wurde im Projekt nicht festgelegt, sondern den NRENs überlassen.

Aggregationsvorschriften

Die linke Spalte spezifiziert die erlaubten Werte, die in XML-Nachrichten verwendet werden dürfen. In Absprache mit der E2ECU und den Kooperationspartnern wurden mit den Werten Gewichte (Spalte rechts) assoziiert. Diese Gewichte werden vom E2E-Monitoring-System für die Berechnung des aggregierten E2E-Zustandes aus den Teildienste-Zuständen verwendet. Die Aggregationsvorschrift für beide Eigenschaftenzustände lautet "das größere Gewicht wird als der Aggregatwert übernommen" (vergleiche die Diskussion in Abschnitten 4.1, 4.2.2 und 4.2.6 über die mit den Eigenschaften assoziierten Aggregationsvorschriften).

Verglichen mit den UML-Diagrammen 5.3, 4.54 und insbesondere 4.50, die ein sehr allgemeines Modell mit Unterstützung für beliebig viele Eigenschaften und unter-

Operational State Value	Description	Weight
Unknown	Domain could not acquire information about operational state	0
Up	Link is up	1
Degraded	Link is up, but has reduced performance	2
Down	Link is down	3

Tabelle 8.1.: Operational State, erlaubte Wertebereiche [HY08b]

Administrative State Value	Description	Weight
Unknown	Domain could not acquire information about administrative state	0
NormalOperation	No administrative work is performed	1
Maintenance	Planned maintenance activity in progress	2
TroubleShooting	Trouble shooting is in progress	3
UnderRepair	Repair process is in progress	4

Tabelle 8.2.: Administrative State, erlaubte Wertebereiche [HY08b]

schiedliche Wertebereiche darstellen, konnte im Projekt dank der Einschränkungen der benötigten Informationen ein wesentlich einfacheres Datenmodell erstellt werden (siehe Abbildung 8.11). Die Vereinfachungen der Eigenschaftenbeschreibung im Projekt kann als ein Spezialfall der in dieser Arbeit entwickelten Lösung angesehen werden. Im Gegenzug zu diesen Vereinfachungen bei der Eigenschaftenbeschreibung musste das E2Emon-Datenmodell mit zusätzlichen Informationen angereichert werden, die zur besseren Nutzerfreundlichkeit und Nutzbarkeit des Systems beitragen sollen. Dazu gehören z.B. Felder wie *City* und *Institution* der Klasse "TopologyPoint". Wichtig ist auch zu bemerken, dass das Feld *LocalName* der Klasse "MonitoredLink" semantisch mit der REFERENCEID übereinstimmt, die mit jeder bestellten Teilstrecke assoziiert ist, d.h. die E2ECU nutzt diesen Namen als NREN-spezifische ID bei der Kommunikation mit dem jeweiligen Teilstreckenprovider.

Kommunikationsaufwand Minimierung

Da die NRENs sich i.A. bei der Erbringung mehrerer E2E Links beteiligen können und da die E2ECU für alle Projekte zuständig ist, werden bei den Abfragen der Monitoring-Informationen von jedem NREN gleichzeitig alle Informationen zu allen überwachten Teilstrecken der E2E Links zurückgemeldet. Dies geschieht, um den Kommunikationsaufwand möglichst gering zu halten. Zu Illustrationszwecken wird in Abbildung 8.12 der Ausschnitt einer Antwort an E2Emon dargestellt. Da die – in der Projektsprache – *Topology Points*[1] auch mehrmals in unterschiedlichen Teilstrecken verschiedener E2E Links vorkommen dürfen, wurde hier eine weitere Optimierung getroffen, indem die Topology Points nur ein Mal definiert und bei der Beschreibung der Teilstrecken ggf. mehrmals referenziert werden sollen. Das illustriert, dass es unter Berücksichtigung Projekt- bzw. Dienst-spezifischer Optimierungs-

[1] Die Topology Points können als Synonymen für SCPs betrachtet werden.

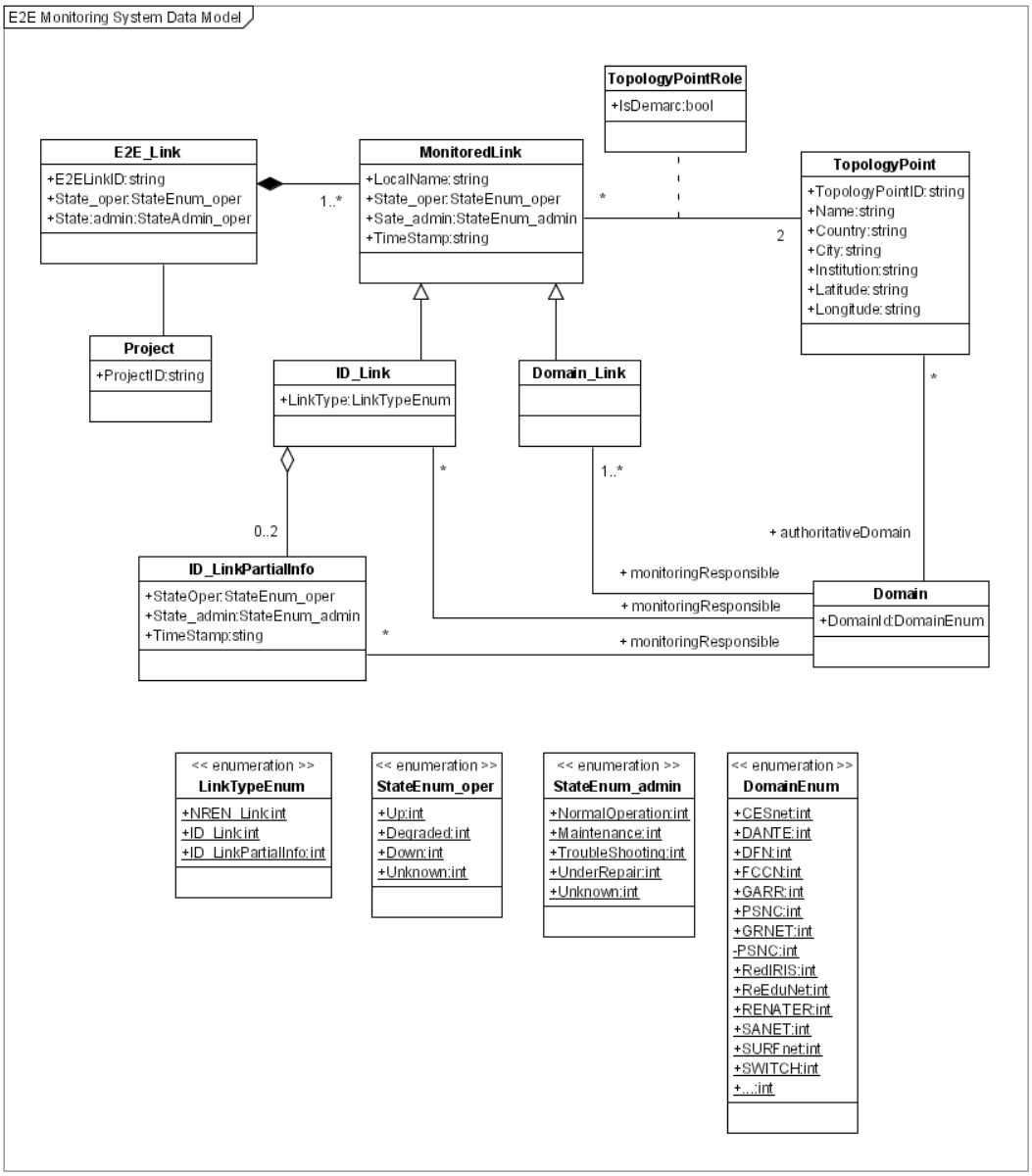


Abbildung 8.11.: E2Emon, Data Model [HY08b]

kriterien unterschiedliche syntaktische Definitionen der XML-Struktur für semantisch identische Inhalte geben kann (vergleiche die im Kapitel 7 im Beispiel verwendeten XML-Nachrichten).

Namenskonventionen für IDs

Im Gegensatz zu den Definitionen im Abschnitt 4.6.10 werden im Projekt wesentlich einfachere Namenskonventionen verwendet (vgl. die Namen der Topology Points und E2E Links in Abbildung 8.12). Als Grundregel gilt, dass der ID eines Topology Points aus zwei durch ein Minus-Zeichen getrennten Teilen besteht – einem global eindeu-

```
            <nmwgtopo3:name type="logical">DFN-LRZ</nmwgtopo3:name>
            <nmwgtopo3:country>Germany</nmwgtopo3:country>
            <nmwgtopo3:city>Munich</nmwgtopo3:city>
            <nmwgtopo3:institution>Leibniz Rechenzentrum
              </nmwgtopo3:institution>
            <nmwgtopo3:latitude>48 15 42.20 N</nmwgtopo3:latitude>
            <nmwgtopo3:longitude>11 39 59.51 E</nmwgtopo3:longitude>
      </nmwgtopo3:node>
    </nmwg:subject>
</nmwg:metadata>

<nmwg:metadata id="md2">
    <nmwg:subject id="sub-DFN-MUE">
      <nmwgtopo3:node id="DFN-MUE">
            <nmwgtopo3:type>TopologyPoint</nmwgtopo3:type>
            <nmwgtopo3:name type="logical">DFN-MUE</nmwgtopo3:name>
            <nmwgtopo3:country>Germany</nmwgtopo3:country>
            <nmwgtopo3:city>Muenster</nmwgtopo3:city>
            <nmwgtopo3:institution>DFN-Verein</nmwgtopo3:institution>
            <nmwgtopo3:latitude>50 8 00.01 N </nmwgtopo3:latitude>
            <nmwgtopo3:longitude>8 27 47.94 E </nmwgtopo3:longitude>
      </nmwgtopo3:node>
    </nmwg:subject>
</nmwg:metadata>

<nmwg:metadata id="md3">
    <nmwg:subject id="sub1">
      <nmtl2:link>
            <nmtl2:name type="logical">DFN-link-1234</nmtl2:name>
            <nmtl2:globalName type="logical">LRZ-SARA-DEISA-001
              </nmtl2:globalName>
            <nmtl2:type>DOMAIN_Link</nmtl2:type>

            <nmwgtopo3:node nodeIdRef="DFN-LRZ">
              <nmwgtopo3:role>EndPoint</nmwgtopo3:role>
            </nmwgtopo3:node>

            <nmwgtopo3:node nodeIdRef="DFN-MUE">
              <nmwgtopo3:role>DemarcPoint</nmwgtopo3:role>
            </nmwgtopo3:node>

      </nmtl2:link>
    </nmwg:subject>
</nmwg:metadata>

<nmwg:metadata id="md4">
    <nmwg:subject id="sub2">
      <nmtl2:link>
            <nmtl2:name type="logical">DFN-Surfnet-Link-5678</nmtl2:name>
            <nmtl2:globalName type="logical">LRZ-SARA-DEISA-001
              </nmtl2:globalName>
            <nmtl2:type>ID_Link</nmtl2:type>

            <nmwgtopo3:node nodeIdRef="DFN-MUE">
              <nmwgtopo3:role>DemarcPoint</nmwgtopo3:role>
            </nmwgtopo3:node>
```

Abbildung 8.12.: Antwort eines NRENs an die Abfrage der Monitoring-Informationen (Ausschnitt) [HY08b]

tigen NREN-Akronym und einer innerhalb des NRENs eindeutigen lokalen ID. In der Abbildung sind zwei solche IDs vorhanden: "DFN-LRZ" und "DFN-MUE". Die E2E Link ID setzt sich aus fünf Teilen zusammen, die wiederum durch ein Minus-Zeichen voneinander getrennt sind: Die Akronyme der zwei *End Points* (meistens werden dafür die Akronyme der mit E2E Link zu verbindenden Organisationen verwendet), einem Akronym des Projekts, für das der E2E Link bestellt wurde, sowie einer fortlaufenden Nummer, die zur Unterscheidung zwischen mehreren E2E-Links dient, die zwischen denselben Endpunkten für dasselbe Projekt verwendet werden. Neben einer guten Lesbarkeit und der Einfachheit, diese Namen im User Interface darzustellen, hat diese Entscheidung auch eine Reihe Schwierigkeiten verursacht, die genauer im nächsten Unterabschnitt beschrieben werden.

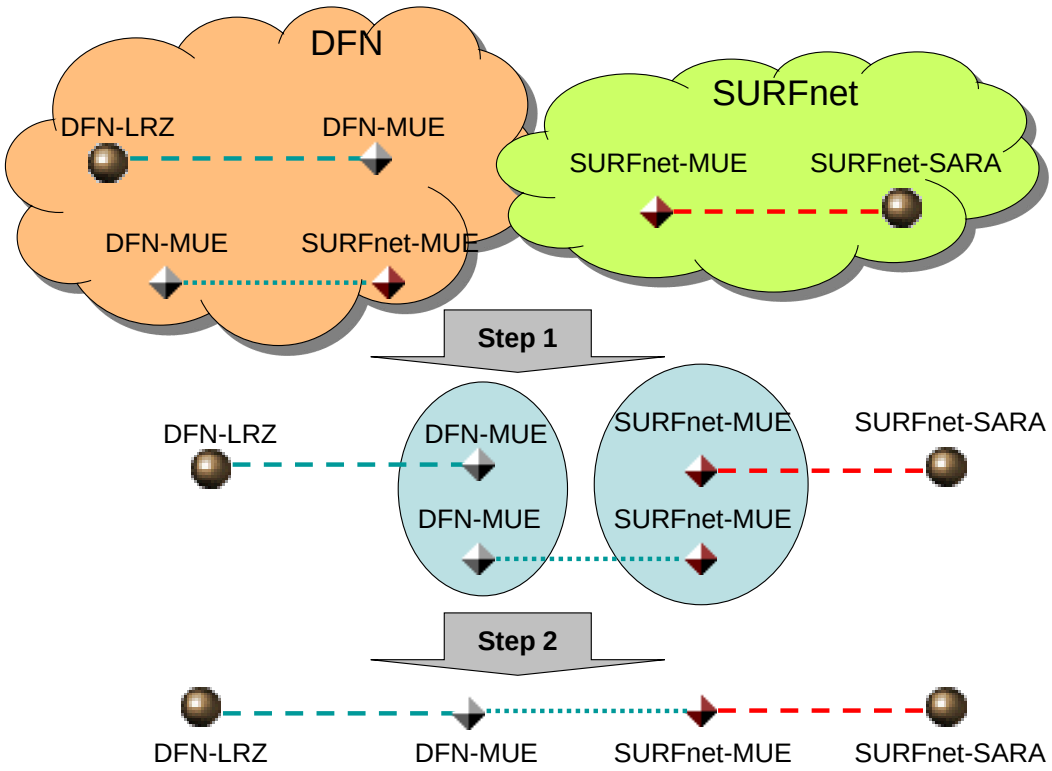


Abbildung 8.13.: Name Matching: Rekonstruktion der Zusammensetzung eines E2E Links [HY08b]

Name Matching für Topologie-Rekonstruktion

Im Gegensatz zur Überwachung von Géant2 E2E-Links ist bei der in dieser Arbeit entwickelten Lösung dem Monitoring System bekannt, aus welchen Teilstrecken sich die zu überwachende E2E-Verbindung zusammensetzt. Dennoch konnte beim Géant2 E2E Monitoring System ein anderes Konzept wangewendet werden, das im Kapitel 4 zur "Zusammensetzung" der Domänen-Sichten zu einer (semi-)globalen Sicht auf die vorhandenen Kapazitäten vorgeschlagen wurde – nämlich das *Name Matching*.

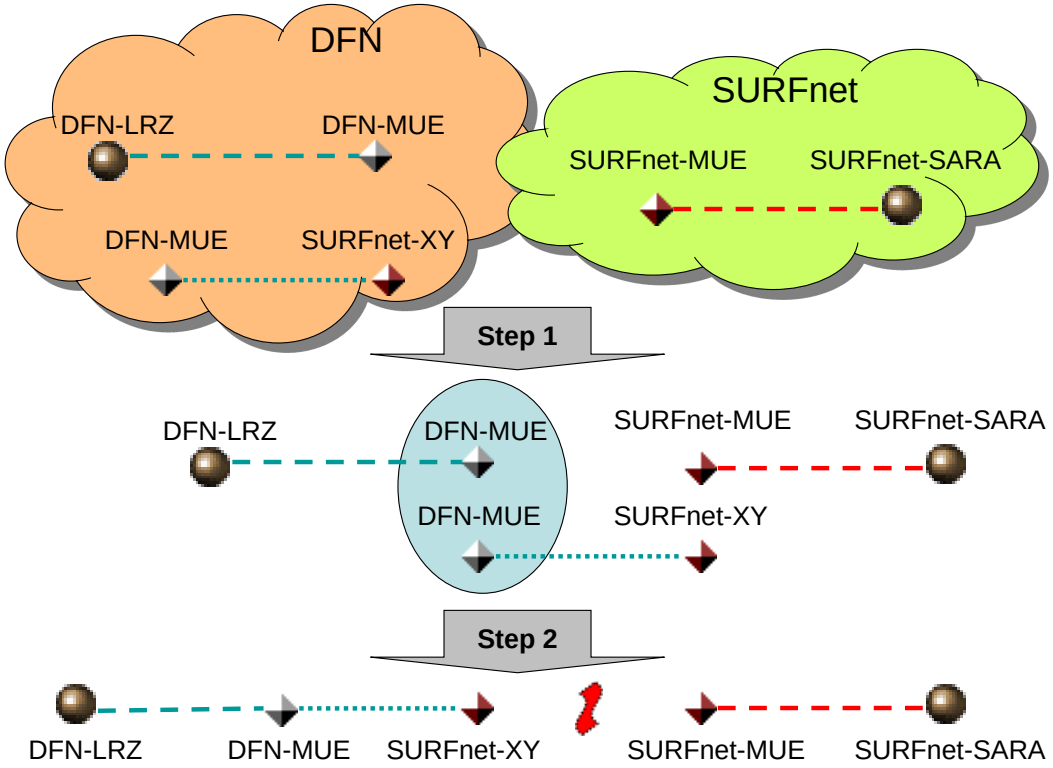


Abbildung 8.14.: Name Matching: Vollständige Rekonstruktion der Zusammensetzung eines E2E Links unmöglich [HY08b]

Das zeigt vor allem, dass die entwickelten Konzepte im Einzelfall nicht nur an den in dieser Arbeit für sie vorgesehenen Stellen eingesetzt werden können, sondern auch bei der Dienst-spezifischen Optimierung entsprechend angepasst bzw. auf andere Gebiete übertragen werden können.

Das Verfahren des Name Matchings ist graphisch in Abbildung 8.13 dargestellt. Dabei werden die Topology Points IDs aller Teilstrecken, die zu ein und demselben E2E Link gehören, auf Übereinstimmung untersucht. Sollte das der Fall sein, können die Teilstrecken im nächsten Schritt an den jeweiligen Endpunkten "zusammengeklebt" werden. Die perfekte Situation, dass alle Teilstrecken eines E2E Links zusammengesetzt werden können, ist nur dann möglich, wenn Informationen über alle Teilstrecken vorhanden sind und die Benennung der Topology Points korrekt ist. Dies ist allerdings nicht immer der Fall, weswegen E2Emon auch Fehlersituationen erkennen, darstellen (siehe Abbildung 8.14) und dementsprechend reagieren muss.

Visualisierung

Die abgefragten Monitoring-Informationen werden nach deren Aggregation und der Zusammensetzung zu zusammenhängenden Verbindungen semi-graphisch dargestellt.

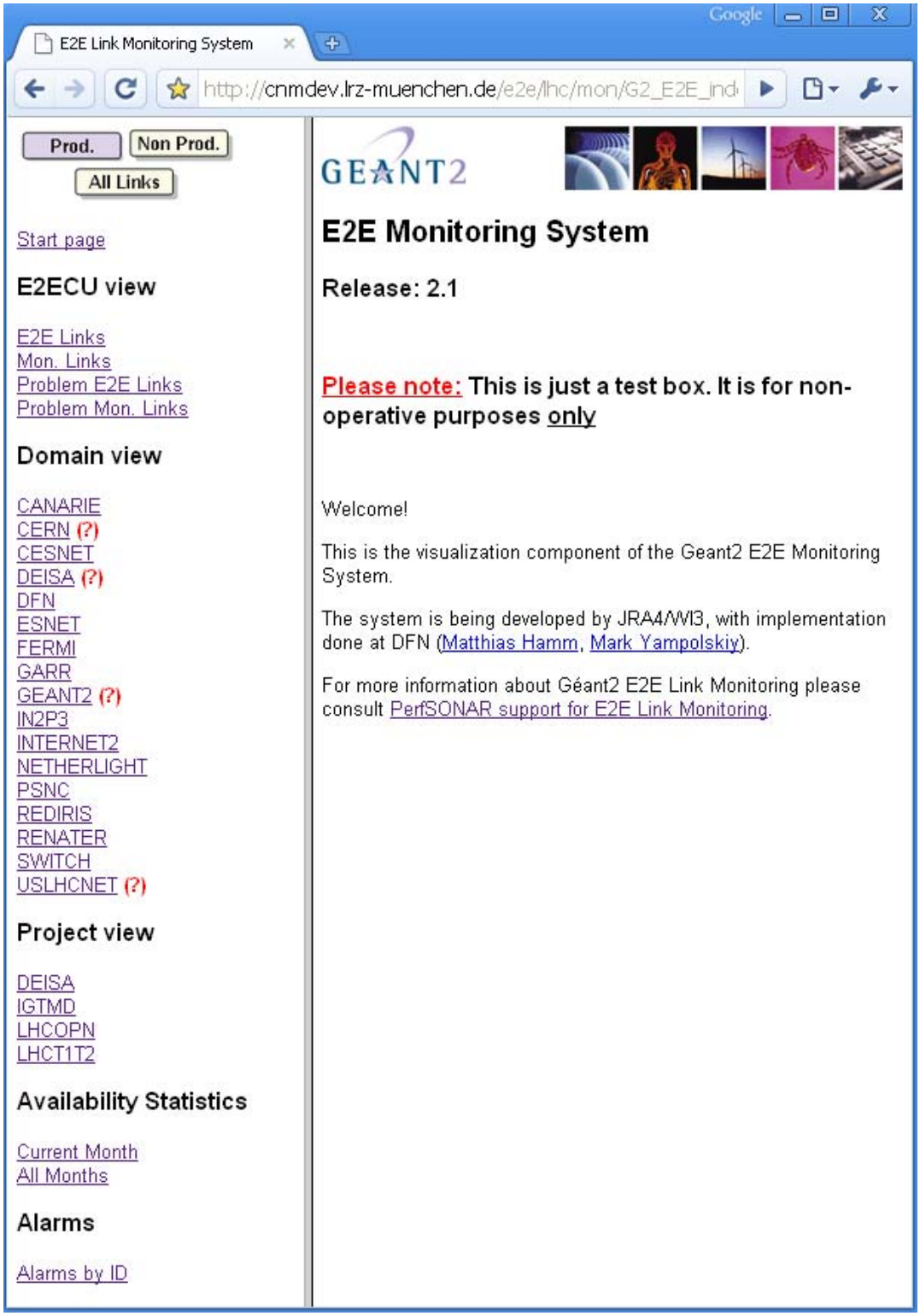


Abbildung 8.15.: E2Emon Entwicklerinstallation, Startseite [E2E09]

Abbildung 8.16.: E2Emon Entwicklerinstallation, semi-graphische E2E Link Anzeige

E2E Link ID	Endpoint A	Endpoint B	Monitored Domains	Availability (%)	Monitored Time (min)	Up-Time (min)	Degraded-Time (min)	Down-Time (min)	Uncertain-Time (min)
CSC-FRA-DEISA-001	DEISA-COP_FRA	DEISA-FRA_COP	GEANT2 DEISA	95.06	26548	25237	0	1302	9
FZJ-FRA-DEISA-001	DEISA-FRA_JUE	DEISA-JUE_FRA	DFN DEISA	99.62	26548	26448	0	100	0
SARA-FRA-DEISA-001	DEISA-AMS_FRA	DEISA-FRA_AMS	NETHERLIGHT GEANT2 DEISA	0.03	26548	8	0	0	26540
IDRIS-FRA-DEISA-001	DEISA-FRA_PAR	DEISA-PAR_FRA	GEANT2 DEISA	99.23	26548	26344	0	195	9
HLRS-FRA-DEISA-001	DEISA-FRA_STU	DEISA-STU_FRA	DFN DEISA	99.62	26548	26448	0	100	0
CINECA-FRA-DEISA-001	DEISA-FRA_MIL	DEISA-MIL_FRA	GEANT2 GARR DEISA	98.70	26548	26202	0	184	162
EPCC-FRA-DEISA-001	DEISA-FRA_LON	DEISA-LON_FRA	GEANT2 DEISA	99.13	26548	26317	0	230	1
RZG-FRA-DEISA-001	DEISA-FRA_GAR	DEISA-GAR_FRA	DFN DEISA	99.62	26548	26448	0	100	0
BSC-FRA-DEISA-001	DEISA-FRA_MAD	DEISA-MAD_FRA	GEANT2 DEISA	97.65	26548	25924	0	615	9

E2E Link ID	Endpoint A	Endpoint B	Monitored Domains	Availability (%)	Monitored Time (min)	Up-Time (min)	Degraded-Time (min)	Down-Time (min)	Uncertain-Time (min)
FERMI-IN2P3-IGTMD-002	FERMI-IGTMD	IN2P3-IGTMD2	INTERNET2 GEANT2 RENATER FERMI ESNET	80.42	26548	21350	0	269	4929

Abbildung 8.17.: E2Emon Entwicklerinstallation, E2E Link Statistics [E2E09]

Auch wenn die Visualisierungsaspekte nicht im Fokus der entwickelten Lösung liegen, lassen sich dadurch im Hintergrund ablaufende Prozesse und Optimierungsentscheidungen besser erläutern.

In Abbildung 8.15 ist die Start-Seite des Géant2 E2E-Monitoring-Systems dargestellt, das am Leibniz-Rechenzentrum (LRZ) installiert ist. Im Gegensatz zur Installation der E2ECU, die ausschließlich für autorisierte Nutzer zugänglich ist, ist die Installation am LRZ frei zugänglich. Diese Installation wird von den E2Emon-Entwicklern verwendet, um die neuesten Versionen des Systems realitätsnah zu testen und Feedback von den E2Emon-Nutzern vor dem endgültigen Release zu sammeln.

Für die Visualisierung der Monitoring-Informationen werden in E2Emon statische HTML-Seiten generiert. Um die Navigation zu Informationen für unterschiedliche Nutzergruppen zu vereinfachen, teilt sich die Ansicht auf E2E Links in drei große Bereiche: "E2ECU"-, "Domain"- und "Projekt"-Views (siehe linkes Frame in Abbildung 8.15). Für diese Views werden in Abhängigkeit vom Interesse der jeweiligen Gruppe die relevanten Informationen entweder tabellarisch oder semi-graphisch dargestellt. Zu Illustrationszwecken wird in Abbildung 8.16 gezeigt, wie die semi-graphische Anzeige eines E2E Links, der entsprechend dem "Name Matching" zusammengesetzt wurde (siehe Abbildungen 8.13 und 8.14), in E2Emon dargestellt wird. Zusätzlich ist im Monitoring System die Anzeige für die gesammelten E2E Link Statistiken und die Alarm vorgesehen, die hauptsächlich für die Nutzung von E2ECU vorbehalten ist.

Mit Ausnahme von "Available Statistics" können alle übrigen Views danach gefiltert werden, ob die E2E Links produktiv oder noch nicht produktiv sind (siehe drei Knöpfe links oben in Abbildung 8.15). Die Festlegung, welche E2E Links als produktiv zu betrachten sind, konfiguriert der E2Emon-Betreiber. Dafür kann entweder die mitgelieferte Administrations-GUI verwendet werden oder direkt die entsprechende Config-Datei editiert werden. Die Notwendigkeit für diese Unterscheidung ist dadurch gegeben, dass die einzelnen NRENs mit der Überwachung eigener Teilstrecken beginnen können, noch bevor alle Teilstrecken zusammengeschaltet sind und dem Kunden als ein einsatzfähiger E2E Link angeboten wird. Aus diesem Grund werden für noch nicht produktive E2E Links keine aktiven Alarme generiert oder deren Verfügbarkeit überwacht.

Sonderfall bei Statistik-Berechnung

Bei der Statistik-Berechnung ist vor allem der Fakt wichtig, dass u.U. nicht alle MPs oder MAs abgefragt werden können. Diese Situation wurde in der entwickelten Lösung bislang völlig vernachlässigt unter der Annahme, dass jede SP-Domäne die Verfügbarkeit der vereinbarten DSM-Schnittstellen im Betrieb gewährleisten kann (siehe Abschnitte 5.10, 6.6 und 6.7). Auch wenn das meistens der Fall ist, ist in der Realität die Gewährleistung einer 100%-er Verfügbarkeit kaum möglich. In E2Emon wurde neben den Zählern für E2E Link Up- und Down-Time ein zusätzlicher Zähler hinzugefügt, der die Zeit widerspiegelt, wann die Informationen von mindestens einem der beteiligten NRENs nicht verfügbar waren (siehe Spalte "Uncertain-Time" rechts in Abbildung

8.17). Da solche Situationen für Multi-Domain Dienste allgemein und nicht nur für Verkettete Dienste typisch sind, kann eine Untersuchung der Verhaltensmuster in solchen Situationen und der Empfehlungen deren Einsatzgebieten als eine wichtige weiterführende Arbeit angesehen werden (siehe Kapitel 10).

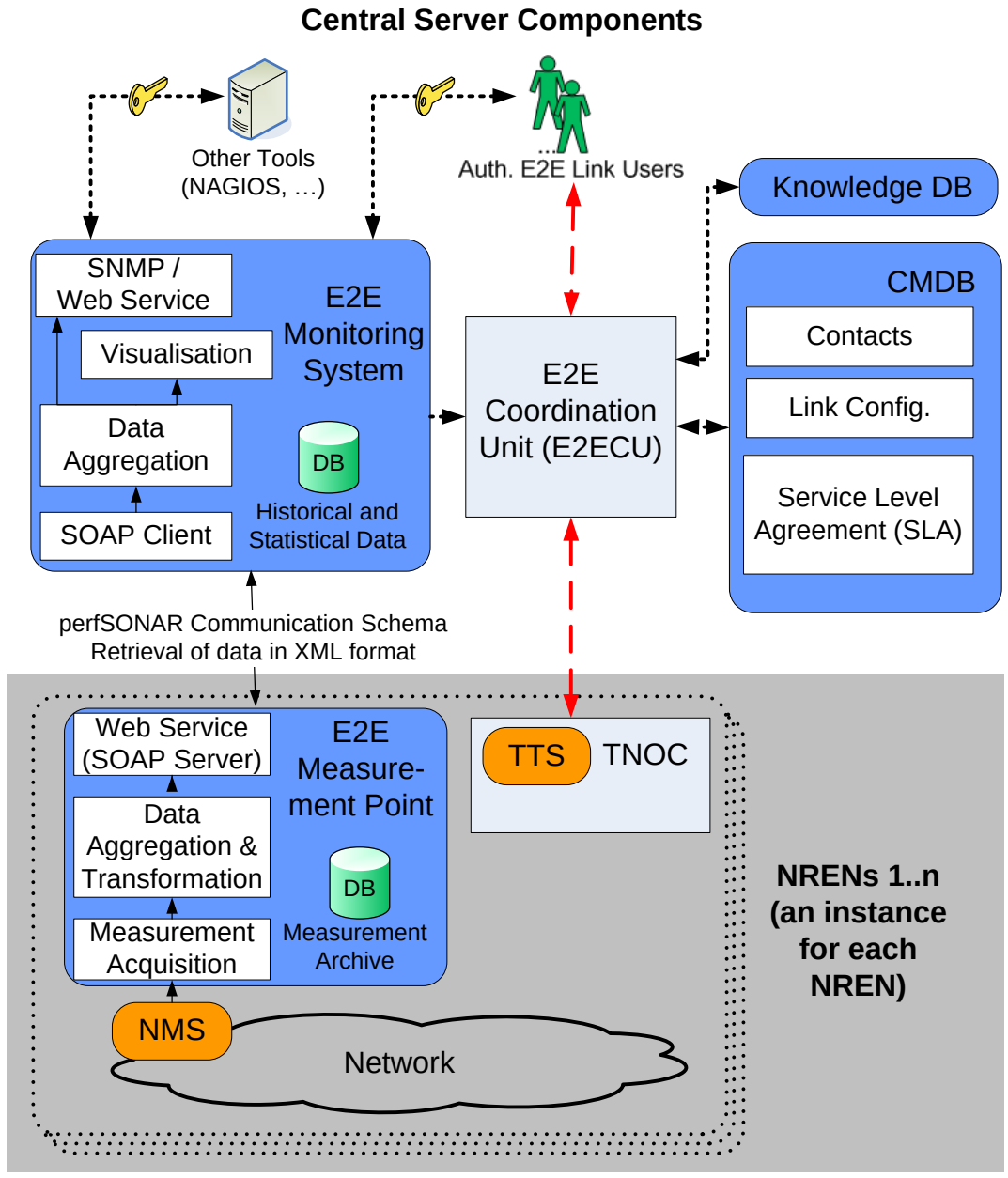


Abbildung 8.18.: E2E Monitoring System, geplannte Systemarchitektur-Erweiterung

Abbildung 8.19.: Intergierter Ansatz, CNM-View mit Statusinformationen aus unterschiedlichen Monitoring-Tools (Ausschnitt)

Geplante Architekturerweiterung und Schnittstellen nach Außen

Die semi-graphische Anzeige der E2E Link Zustände, wie in Abbildung 8.6 dargestellt, war bei der Planung von E2Emon Versionen 1.x als das einzige Interface nach außen vorgesehen. Inzwischen (Stand Mitte 2009) ist die Version 2.1 des E2E Monitoring Systems aktuell, die eine Reihe von Erweiterungen der ursprünglich geplanten Architektur implementiert. Die geplante Softwarearchitektur des E2Emon, die sowohl bereits implementierte als auch noch in Entwicklung befindliche Features umfasst, ist in Abbildung 8.18 dargestellt. Vor allem ist da zu bemerken, dass neben der Visualisierung auch eine Reihe von Schnittstellen nach außen vorgesehen wurden. Dadurch soll die bessere Integrierbarkeit mit anderen Tools gewährleistet werden.

Derzeit wird z.B. die automatische SNMP-Benachrichtigung bei der Erkennung neuer Fehler implementiert (vergleiche mit den vorgesehenen Ereignisbenachrichtigungen im Abschnitt 5.12). In der E2ECU wird diese Option aktiv genutzt, um die erkannten Fehler an eine Nagios[2]-Installation der E2ECU zu melden.

Viel interessanter – im Sinne der Übereinstimmungen mit den Lösungsideen dieser Arbeit – ist die Unterstützung der Web-Service-Schnittstelle, über die alle Monitoring-Informationen abgefragt werden können. Dadurch wird es möglich, die Managementfunktionalität auszulagern und sie dann transparent zu nutzen (vergleiche Diskussion über Delegation der Management-Dienste im Abschnitt 4.4 sowie das im Kapitel 7 durchgespielte Beispiel). Diese Schnittstelle wird vom CNM[3]-Tool genutzt, um die Monitoring-Informationen von E2Emon und anderen Quellen miteinander in Verbindung zu bringen und graphisch darzustellen (ein Ausschnitt der CNM-Anzeige siehe in Abbildung 8.19). Der Einsatz beschränkt sich momentan auf die T0-T1 Verbindungen für das LHC Projekt.

8.1.3. Einsatz im Betrieb, Erfahrungen und Zukunftspläne

Die Beschreibung der Erfahrungen folgt grob dem Datenfluss im Architekturkonzept folgen – von den NMS-Abfragen in den jeweiligen SP-Domänen (NRENs) bis hin zur E2Emon-Schnittstelle nach außen mit den aggregierten Zustandsinformationen.

Kein direkter Infrastrukturzugriff seitens E2Emon

Die Entscheidung, in E2Emon direkte Infrastrukturzugriffe zu vermeiden, hat sich als sehr gut erwiesen. Vor allem wurden dadurch die Sicherheitsbedenken der jeweiligen Netzbetreiber weitgehend ausgeräumt und deren Akzeptanz in Bezug auf den Ansatz erhöht. Dadurch wurde auch eine der wesentlichen Voraussetzung zur Beteiligung der NRENs bei E2E Monitoring erfüllt. Es hat sich allerdings herausgestellt, dass durch

[2] Nagios ist ein Tool, das häufig zur Überwachung der IT-Infrastruktur eingesetzt wird.

[3] CNM steht für Customer Network Management. Dabei handelt sich um ein am LRZ entwickeltes Tool, das sich für die User-freundliche Anzeige von Netzzustandsüberwachungsinformationen bewährt hat.

fehlende Ressourcen und die Heterogenität der in unterschiedlichen NRENs eingesetzten Infrastruktur die Umsetzung der Komponente "Data Aggregation & Transformation" (siehe Abbildung 8.6 oder 8.18) in einzelnen NRENs und dadurch auch bei der Ende-zu-Ende Überwachung sich verzögert hat.

Interpretationsfreiheit und Konsequenzen

Zu einer Reihe von Problemen hat die Entscheidung geführt, die Interpretation der einzelnen Zustandswerte (siehe Tabellen 8.1 und 8.2) den NRENs zu überlassen. So konnten sich viele NRENs nicht einigen, wann ein Zustand einer Verbindung als "Degraded" einzustufen ist. Das hat dazu geführt, dass die Verwendung dieses Zustandes von den meisten NRENs vermieden wird. Die entwickelte Lösung geht zwar von einer klar definierten Semantik der verwendeten Eigenschaften und deren Wertebereiche aus, die Praxistauglichkeit solcher Definitionen sollte bei der tatsächlichen Implementierung jedoch nicht vernachlässigt werden.

Anbindung der Single-Domain Managementsysteme

Eine weitere Erfahrung ist mit dem administrativen Zustand verbunden. Obwohl die Ziele und die Verwendungsprinzipien dieser Eigenschaft breite Zustimmung zwischen den NRENs fanden, hat es sich herausgestellt, dass eine automatische Kopplung der in den NRENs verwendeten Managementtools mit der "Data Aggregation & Transformation" Komponente in meisten Fällen unmöglich war. Das hat dazu geführt, dass die meisten NRENs diese Eigenschaft permanent entweder auf NORMALOPERATION oder auf UNKNOWN gesetzt haben (siehe Warnings in Abbildung 8.20, die einen Überblick über produktive E2E Links darstellt). Weil die Korrelation zwischen dem Operational und dem Administrative State im Projekt erwünscht ist, werden in E2Emon weiterhin beide Zustände unterstützt in der Hoffnung, dass die Situation bei den NRENs sich mit der Zeit ändert.

Verwendung abstrakter Topologie-Beschreibung

Die Entscheidung, die tatsächliche Netztopologie hinter einer abstrahierten zu "verstecken", die zudem von den Netzeigentümern bestimmt ist, hat sich als Erfolg erwiesen (vergleiche die Definition der Topologie-Beschreibung im Kapitel 4, insbesondere das XML-Diagramm in Abbildung 4.50). Der Vorschlag, in E2Emon auch die tatsächliche Netzinfrastruktur anzuzeigen, wurde von den NRENs hauptsächlich aus Sicherheitsgründen zurückgewiesen. Auf der anderen Seite wurde von einigen NRENs die Möglichkeit genutzt, mehrere verkettete *Domain Links* eines E2E Links an das E2Emon Monitoring System zu melden. Diese Option wurde von den NRENs gebraucht, die mehrere technische Domänen innerhalb ihrer administrativen Grenzen haben. In solchen Situationen war es aus technischen Gründen für die NRENs einfacher, die diese technische Domäne durchlaufenden Teilstrecken eines E2E Links getrennt zu überwachen und an das E2Emon ohne eine domäneninterne Aggregation zu melden. Eine solche Topologie-Darstellung ist auch mit der entwickelten Lösung möglich, wenn dies auch in der Beschreibung nie explizit erwähnt wurde. Das heißt allerdings, dass diese Option bei der Umsetzung der Lösung berücksichtigt werden muss.

Ein weiterer Topologie-Aspekt bezieht sich auf die Nutzung der *Interdomain-Link*-Beschreibung. Die Konzepte für die abstrakte Topologie-Beschreibung in der entwickelten Lösung und bei E2Emon stimmen überein (siehe insbesondere Abschnitt 4.1.3). Al-

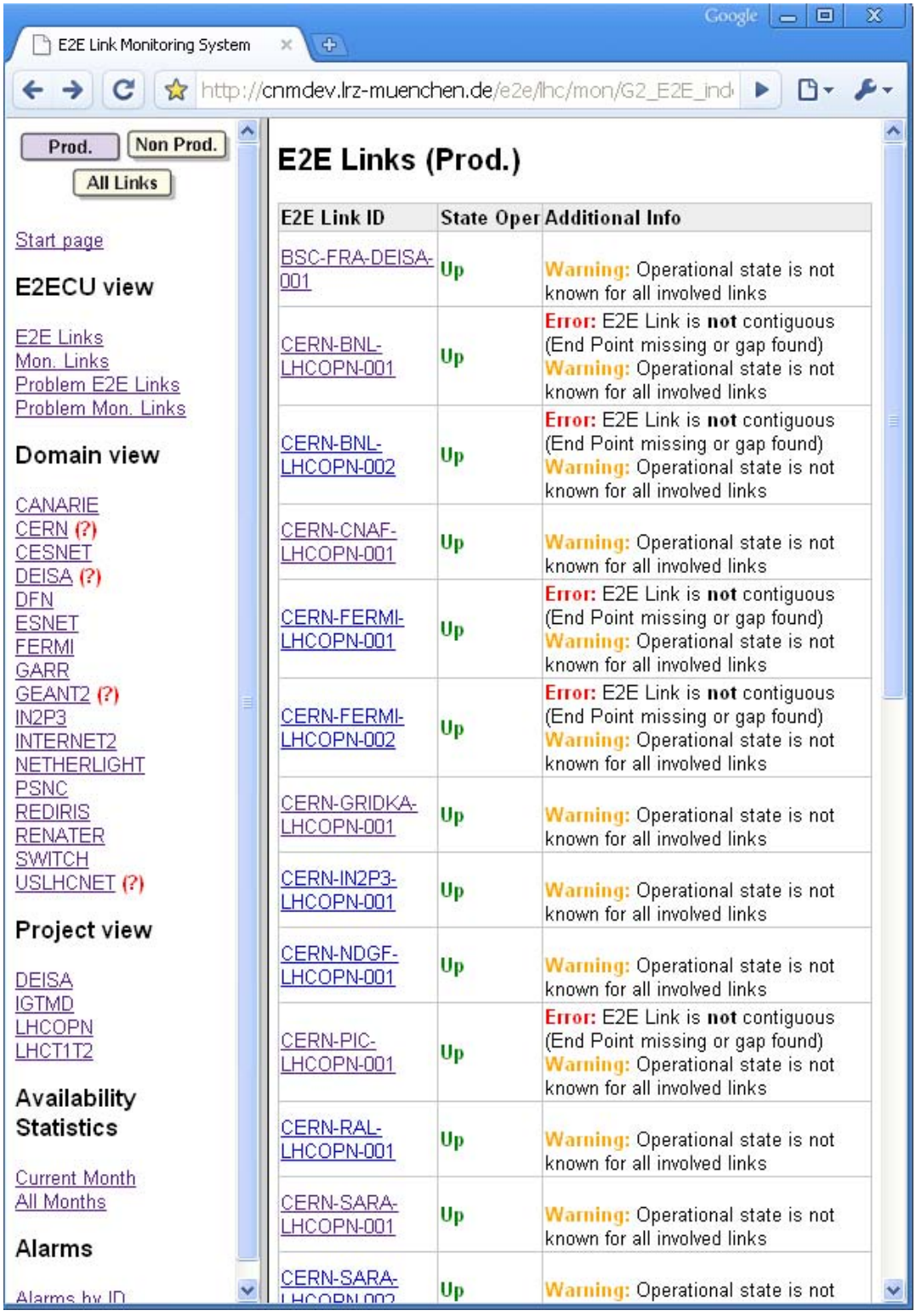


Abbildung 8.20.: E2Emon Entwicklerinstallation, Überblick produktiven E2E Links [E2E09]

lerdings liegt zwischen den beiden Ansätzen ein wesentlicher Unterschied darin, wie ein *Interdomain Link* ausschließlich von einer SP-Domäne gemeldet werden kann. Bei der Integration von E2Emon wurde vorgeschlagen, dass eine der Nachbar-Domänen einen eingeschränkten Zugriff auf die Netzinfrastruktur des angeschlossenen Partners bekommen kann, so dass der Verbindungsabschnitt ähnlich wie beim *Intra-Domain* Fall überwacht werden kann. Diese Option hat sich zwar als technisch möglich, aus Sicherheits- und Policy-Gründen allerdings überhaupt nicht als praktikabel gezeigt. Dem E2Emon werden daher fast ausschließlich die Teilsichten der aneinander angeschlossenen NRENs gemeldet. Die Mitteilung dieser Teilsicht-Informationen über die Web-Service-Schnittstelle hat mit keiner der Policies kollidiert. Aus diesem Grund wird in der Lösung dieser Arbeit vorgeschlagen, dass die Teilsicht-Informationen über die DSM-Schnittstelle ausgetauscht werden (siehe Abschnitte 4.1.3, 5.2 und 5.4).

Topologie-Rekonstruktion anhand IDs

Sowohl Erkennung der E2E-Link-Zusammensetzung bei E2Emon als auch die Rekonstruktion der abstrakten Netztopologie in der entwickelten Lösung werden anhand ID-Matching durchgeführt (siehe Abbildungen 8.13 und 8.14). Die größte Schwierigkeit besteht darin, dass beide benachbarte NRENs die DPs (in der Sprache der entwickelten Lösung – SCPs) identisch bezeichnen. Sollte diese Hürde genommen werden, dann ist dieses Verfahren sehr robust und die abstrakte Multi-Domain Netz-Topologie kann ohne jegliche manuelle Konfiguration von den Single-Domain-Informationen abgeleitet werden.

Probleme mit Vergabeverfahren und Kollisionen bei E2Emon-IDs

Als problematisch erwies sich das Vergabeverfahren für IDs in E2Emon. Die IDs für E2E Links sollten von der E2ECU und die IDs von Demarcation Points von den jeweiligen NRENs vergeben werden. Durch das steigende Interesse an E2E Links von anderen Forschungsprojekten und vor allem durch die aktive Beteiligung bei der Erbringung von E2E Links nordamerikanischer Forschungsnetze haben sich zwei gravierende Nachteile dieser Methode herausgestellt. Zu einem wurde der Vergabeprozess für E2E Link IDs als zu zentralistisch empfunden, was zu Diskussionen über Alternativen wie z.B. einen Registrierungsbaum geführt hat. Zu anderem hat es sich herausgestellt, dass unterschiedliche Forschungsnetze u.U. dieselben Akronyme haben können, was wiederum zu Namenskollisionen bei Demarcation Point IDs führen kann. Trotz dieser Nachteile und der Diskussionen über die Alternativen werden bislang (Stand Mitte 2009) immer noch die ursprünglich geplanten ID-Struktur und -Vergabeverfahren verwendet (vergleiche dazu die im Abschnitt 3.9 geführte Diskussion über Schwierigkeiten der Änderungen im Betrieb).

Überwachung aktueller Zustände

Obwohl die Möglichkeit, historische Daten von NRENs abzufragen, theoretisch sehr attraktiv erscheint, hat sie sich im Projekt bislang noch nicht durchgesetzt. Auf die Analyse der dazu geführten Gründe wird an dieser Stelle verzichtet. Interessant ist die Tatsache, dass aus E2ECU-Perspektive ein 5-Minutiges Polling-Interwall für die Abfrage der derzeit aktuellen Monitoring-Informationen zusammen mit der Synchronisation dieser Informationen durch E2Emon für den Betrieb und die E2E-Überwachung der E2E Link völlig ausreichen. Die kurzfristigen Ausfälle, die innerhalb des 5-Minutigen Raster anfallen, werden als nicht kritisch vernachlässigt. Der Bedarf für historische

Informationen entsteht nur dann, wenn die Situation bei Ausfällen untersucht werden soll. Für diesen Fall wird derzeit eine Erweiterung von E2Emon geplant, historische Daten direkt in der zentralen Komponente abzuspeichern. Diese Projekterfahrung hat dazu geführt, dass in der entwickelten Lösung ein relativ schlichtes, dafür aber praktikables Modell für die Überwachung definiert wurde (siehe Abschnitte 6.6 und 6.7).

Einsatz von Web Services

Der Einsatz von Web Services als Kommunikationsschnittstelle zum Austausch von XML-Nachrichten (vergleiche Vorschlag im Kapitel 7) hat sich insbesondere bei der Weiterentwicklung von E2Emon bewährt. Vor allem hat es ermöglicht, diverse notwendige Erweiterungen, deren Bedarf in der Anforderungsanalyse- und Planungsphasen nicht erkannt wurden, relativ einfach zu implementieren.

Optimierung der Kommunikation

Zur Kommunikation zwischen E2Emon und den bei NRENs installierten MPs oder MAs wurde eine anderere Optimierungsmethode angewendet. In dieser Arbeit wurde davon ausgegangen, dass für jede SP-Domäne die Kommunikation auf eine für E2E Link vorgesehene Schnittstelle umgeleitet werden kann. Dadurch wird allen SP-Domänen die Möglichkeit für eine dynamische Lastverteilung eingeräumt und die Menge der jeweils übertragenen Informationen reduziert. Bei E2Emon wurde dagegen jeweils eine Kommunikationsschnittstelle pro NREN spezifiziert, was eine andere Optimierung bedingt hat – alle Informationen werden gleichzeitig übermittelt, um die Anzahl der notwendigen Kommunikationsvorgänge zu begrenzen. Jede Optimierung kann nur im Kontext unterschiedlicher Faktoren, wie z.B. Nutzungsverhalten, entschieden werden.

Aggregationsvorschriften

Die Aggregationsvorschriften, wie sie in Abschnitten 4.2 und 4.6.10 definiert wurden, konnte bei E2Emon nur indirekt und bei weitem nicht vollständig eingesetzt werden. Interessant ist vor allem der Fakt, dass sich alle Beteiligten auf die Aggregatfunktionen für die nicht direkt messbaren Diensteigenschaften "Operational State" und "Administrative State" einigen konnten.

Gegenseitige Abhängigkeiten der Dienstgüteeigenschaften

Wie bereits erwähnt wurde, existieren insbesondere bei der Statistik-Berechnung in E2Emon auch gegenseitige Abhängigkeiten zwischen den verwendeten Monitoring-Parametern. Solche Situationen wurden in der entwickelten Lösung bislang nicht berücksichtigt und sollen daher in weiterführenden Arbeiten untersucht werden (siehe Kapitel 10).

Sicherheitsaspekte

Obwohl das nicht direkt zum Thema dieser Arbeit gehört, soll an dieser Stelle die Wichtigkeit der Sicherheitsaspekte bei allen Kommunikationsschnittstellen betont werden. Ausgehend von einer engen Kooperation und guten Vertrauensbeziehungen wurden in E2Emon diese Aspekte vernachlässigt, was bei der wachsenden Popularität der E2E Links zu unerwünschten Situationen geführt hat, wie z.B. Einblicke in die Daten anderer Forschungsprojekte. Diese Projekterfahrung hat dazu geführt, dass in der entwickelten Lösung die Entscheidungs- und Informationsfilterung-Komponenten durchgängig vorgesehen wurden (siehe "Decide" und "Filter" Komponenten in Abbildung 4.57 sowie "Check Credentials"-Aktivitäten in Kapiteln 5 und 6).

8.2. Informationsaustauschsystem I-SHARe

Genauso wie E2Emon bezieht sich auch *Information Sharing across Heterogeneous Administrative Regions* (I-SHARe) auf Géant2 E2E Links. Der Zweck dieses System besteht jedoch in der Unterstützung manuell ausgeführter Managementprozesse in allen Dienst-Lebenszyklusphasen.

8.2.1. Projektumgebung, Ziele und Randbedingungen

Bei E2E Links handelt es sich um einen neuartigen Dienst. Das bedeutet vor allem, dass viele providerübergreifende Managementprozesse nicht von vornhinein festgelegt werden konnten und oft *ad hoc* ausgeführt werden müssen. Die fehlende Koordination zwischen NRENs hat im Jahr 2006 unter anderem zu extrem langen Bereitstellungszeiten für E2E Links geführt [CRE+07].

Inzwischen (Stand Mitte 2009) sind die beteiligten Mitarbeiter mit den etablierten Multi-Domain Managementprozessen vertraut. Die notwendigen Tätigkeiten werden inzwischen intuitiv ausgeführt, ohne dass eine formale Beschreibung dafür definiert wurde. Dadurch lässt sich die derzeitige Situation in das COBIT-Reifegradmodell [ITG07] mit der Reifegradstufe 2 – INTUITIV, WIEDERHOLBAR – einordnen (siehe Abbildung 8.21). Zur Erfüllung der Anforderungen von DEISA und LHC – insbesondere eine Beschränkung der Prozessdurchlaufzeiten – ist jedoch mindestens die Reifegradstufe 4 – GEMANAGED anzustreben [Ham09].

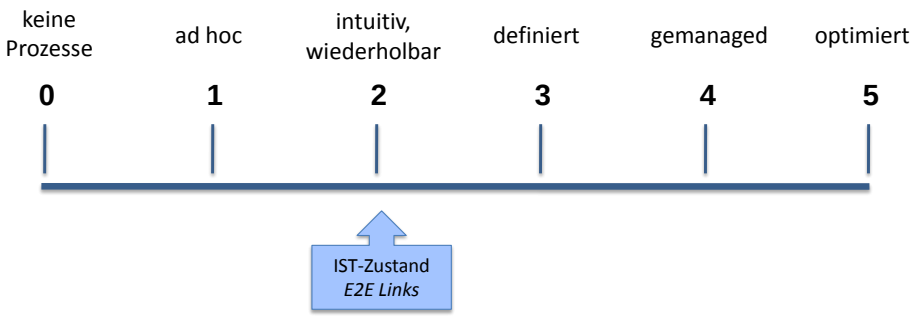


Abbildung 8.21.: Einordnung des Managements von E2E Links in das COBIT-Reifegradmodell (nach [Ham09])

Um dieses Ziel zu erreichen, wurde Ende 2007 in Géant2 die *I-SHARe* Aktivität gestartet. Die Ziele dieser Aktivität lassen sich grob in zwei Phasen aufteilen:

Momentan angestrebt: Unterstützung von Informationsaustausch bei der Durchführung definierter Managementprozesse

Im Anschluss geplant: Unterstützung der Managementprozesse durch die Kontrolle des Prozessablaufs

Bei den auszutauschenden Informationen handelt es sich sowohl um organisatorische als auch um technische Aspekte, deren Austausch die Managementprozesse unterstützt. So fallen unter die organisatorischen Aspekte der Name und die Arbeitszeiten des verantwortlichen Betriebspersonals sowie deren Kontaktinformationen. Als die technischen können nicht nur solche Aspekte, wie z.B. die eingesetzte Netztechnologie oder verwendete Wellenlänge, betrachtet werden, sondern auch die Art der Verbindung zwischen den NRENs.

Um diese Ziele zu erreichen, wurden zunächst folgende Aktivitäten in enger Kooperation mit den Betriebsgruppen mehrerer NRENs und DANTE durchgeführt:

- Managementprozesse, die sich etabliert haben, wurden in einer standardisierten Form erfasst
- Die erfassten Prozesse wurden analysiert und die zwischen NRENs auszutauschenden Informationen identifiziert
- Die identifizierten Informationen wurden von den beteiligten Projektpartnern evaluiert und vervollständigt

Im nächsten Schritt wurde das I-SHARe Tool konzipiert und ein Prototyp mit einer eingeschränkten Funktionalität entwickelt. Zurzeit wird der Prototyp von der E2ECU und einigen NRENs bei der Planung der neuen E2E Links evaluiert.

8.2.2. Eingesetzte Konzepte und erworbene Erfahrungen

Der Fokus von dieser Arbeit und von I-SHARe liegt relativ weit auseinander. Dennoch, da I-SHARe zur Unterstützung von Managementprozessen von E2E Links konzipiert wird, die zur Klasse Verketteter Dienste gehören, gibt es auch einige Überschneidungen und gegenseitige Ideenbereicherungen, die in diesem Abschnitt präsentiert werden.

Architekturkonzept und Verantwortlichkeiten

Beim I-SHARe-Architekturkonzept (siehe Abbildung 8.22) wurde auf die bei E2Emon bewährte Kopplung zwischen Single-Domain und Multi-Domain Komponenten über eine Web-Service-Schnittstelle (in der Abbildung - *ISHARe Domain Interface*) zurückgegriffen. Die Übereinstimmung mit der Lösung dieser Arbeit zeigt sich insbesondere darin, dass die SP-Domänen selbst in der Verantwortung für die eigene Informationen sind und in Eigenregie entscheiden, welche Single-Domain Informationen mitgeteilt werden und welche nicht [HHS+08]. Für die Entwicklung des Prototyps wurde jedoch entschieden, die für die produktive Version geplanten Architektur deutlich zu vereinfachen (siehe Abbildung 8.23). Das Grundkonzept von der Trennung der Domänen-eigenen und Multi-Domain Daten blieb dabei aber erhalten. In Gesprächen mit den Betriebsverantwortlichen in unterschiedlichen NRENs hat sich dieser Aspekt als einer der ausschlaggebendsten für die Tool-Akzeptanz erwiesen. In dem Konzept wird die Annahme gemacht, dass die NRENs über das *ISHARe Domain Interface* ausschließlich up-to-date Informationen zur Verfügung stellen. Momentan fehlt aber die

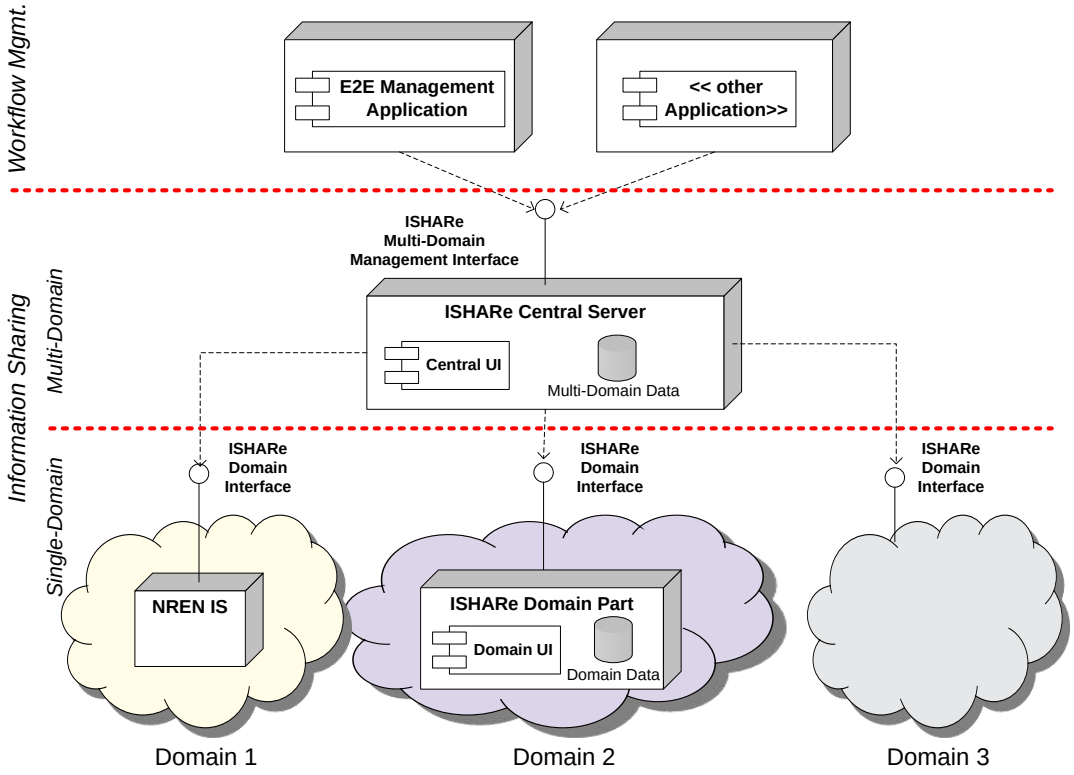


Abbildung 8.22.: I-SHARe Software-Architektur (geplant) [CHS+08]

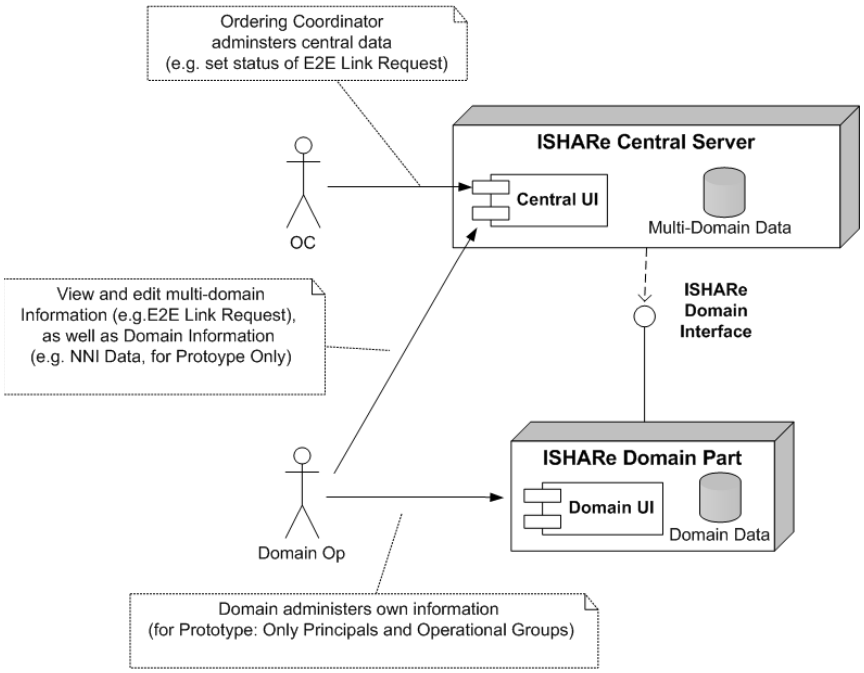


Abbildung 8.23.: I-SHARe Software-Architektur Prototyp [CHS+08]

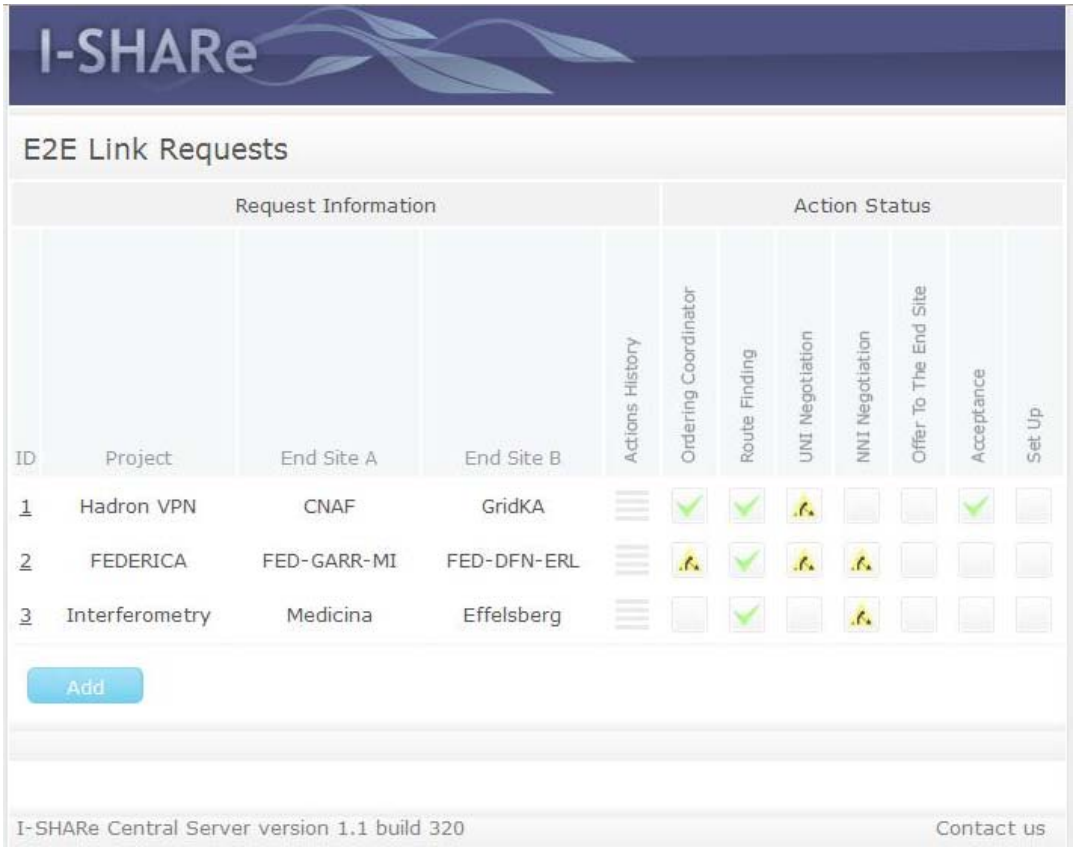


Abbildung 8.24.: I-SHARe Prototype, Übersicht über E2E Links in Planung [CHS+08]

Betriebserfahrung, um über die Tragfähigkeit dieser Annahme hier berichten zu können.

Routen-Suche für E2E Links

Die mit Abstand wichtigste Überschneidung zwischen der entwickelten Lösung und I-SHARe gibt es nicht bei dem Prototypen, sondern bei den Prozessen, die in der Vorbereitungsphase erfasst wurden. So hat sich in dem Projekt etabliert, dass bei der Routensuche die Netzplanungs-Teams unterschiedlicher NRENs miteinander Informationen darüber austauschen, welche Teilstrecken realisierbar sind. Ähnlich wie in der entwickelten Lösung werden Informationen über die Endpunkte, den Übergang in die eigene Domäne und die Dienstgüteanforderungen ausgetauscht. Der prinzipielle Unterschied zwischen den beiden Lösungen besteht darin, dass bei E2E Link bezogenen Betriebsprozessen immer nur eine Alternative betrachtet wird und eine weitere nur dann angeboten wird, wenn die vorherige nicht ausreicht [DMHH+08]. Bei den überwiegend manuell geplanten Verbindungen, wie es bei E2E Links der Fall ist, führt diese Vorgehensweise zur Reduktion des Planungsaufwandes einzelner SP-Domänen.

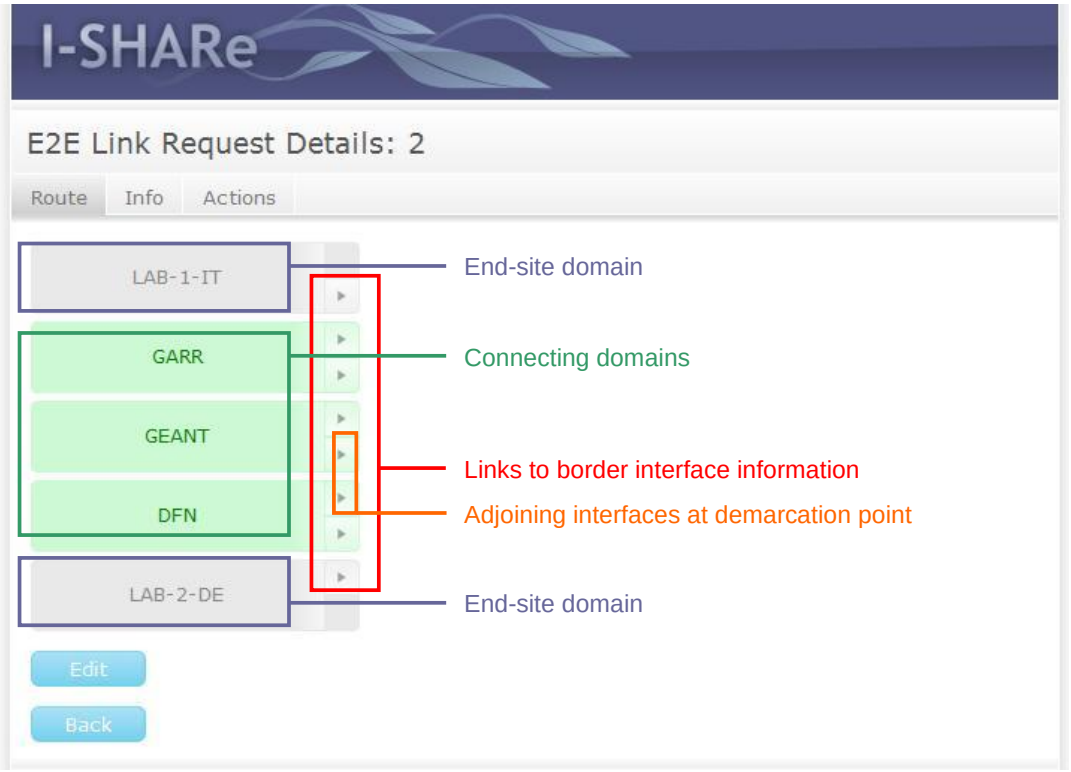


Abbildung 8.25.: I-SHARe Prototype, E2E Link Route [CHS+08]

Die in dieser Arbeit entwickelte Lösung orientiert sich eher an automatisch geschalteten Diensten und geht davon aus, dass die SP-Domänen die möglichen Verbindungen automatisiert aufbauen können. Die entwickelte Lösung mit der Abfrage für gleichzeitig mehrere alternative Möglichkeiten (siehe Abschnitte 4.3.4.1, 5.2 und 6.2) ist für die Reduktion der Kommunikation zwischen den SP-Domänen optimiert. Abgesehen von diesem Unterschied sowie von der Struktur der Kommunikationsartefakte und den Kommunikationswegen (im Géant2 Projekt wird das derzeit per e-Mail und Excel-Sheets gemacht) sind beide Vorgehen sehr ähnlich. Sehr wichtig ist daher der Fakt, dass es für die SP-Domäne akzeptabel ist, Dienstinstanz-bezogene Informationen auf dem Abstraktionsniveau "von einer Domänengrenze zu der anderen" preiszugeben.

Zu Illustrationszwecken werden in den Abbildungen 8.24 und 8.25 zwei Screen-Shots des I-SHARe Prototypen dargestellt. Bei der ersten Abbildung handelt es sich um eine Ansicht, die einen Überblick über den Status der ausgeführten E2E Link Planungsarbeiten vermitteln soll. Im zweiten Bild ist die Anzeige dargestellt, die bei einem bereits geplanten groben Verlauf über mehrere SP-Domäne die Eingabe der UNI/NNI Spezifikationen ermöglicht.

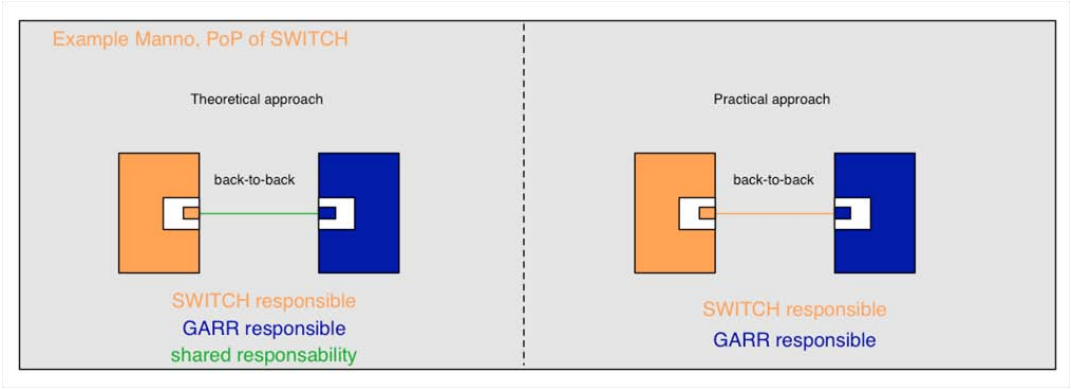


Abbildung 8.26.: NNI-NNI Connection, Directly connected equipment [HH09]

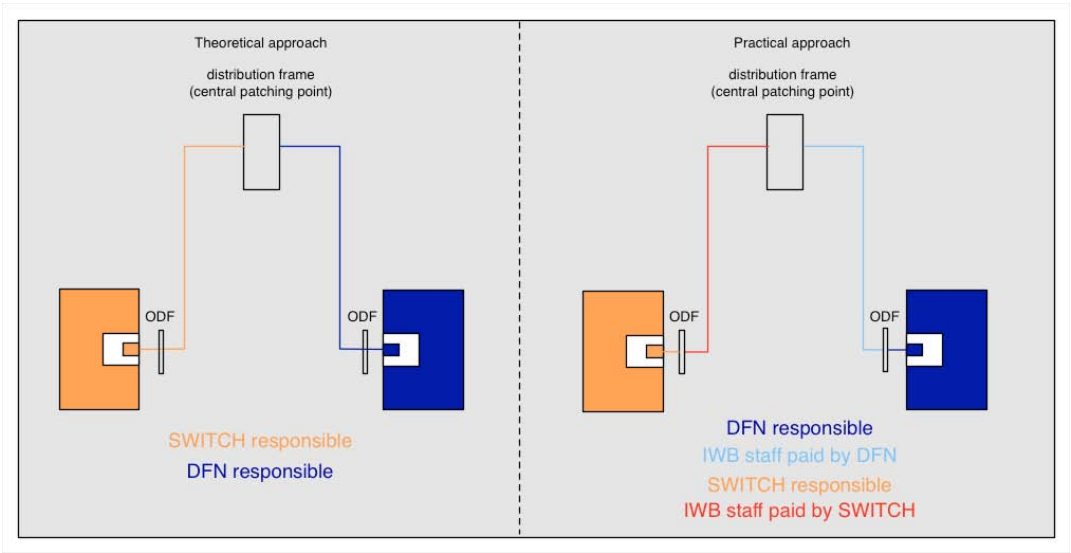


Abbildung 8.27.: NNI-NNI Connection, Distribution frame [HH09]

Semantik der Übergangspunkte

Ein anderer wichtiger Aspekt, der an dieser Stelle unbedingt erwähnt werden soll, hat sich erst vor Kurzem bei der Evaluation des I-SHARe Prototype gezeigt. Obwohl die Definition von *Demarcation Points* als Grenzpunkte der Domänenverantwortlichkeit bei E2Emon seit einigen Jahren erfolgreich verwendet wurde, kann diese Definition bei der physischen Zusammenschaltung zwischen benachbarten SP-Domänen nicht immer eindeutig festgelegt werden.

Zur Illustration dieser Behauptung sind in den Abbildungen 8.26 und 8.27 zwei Fälle dargestellt, wie das Equipment benachbarter SP-Domänen aneinander angeschlossen werden kann. In Abbildung 8.26 ist die sog. "back-to-back" Verbindung dargestellt, bei der Geräte nebeneinander stehen und mit einem kurzen Patch-Kabel verbunden werden. Die Abbildung 8.27 stellt eine nur ein wenig komplexere Variante dar, bei

	SWITCH	GARR
General Information		
Transfer Capacity [Gbps]	10	10
Housing location:		
Name	CSCS	CSCS
Full address	Centro Galleria 2, Via Cantonal, Manno	Centro Galleria 2, Via Cantonal, Manno
Working hours	9:00-17:00	9:00-17:00
Contact		
Onsite staff Information	Marco Consoli, Luca Bacchetta	Marco Consoli, Luca Bacchetta
Emergency Number	+41 44 268 15 30	+41 44 268 15 30
NREN contact Information	Ernst Heiri	Marco Marletta
Additional information	during office hours contact staff in Manno	try to contact SWITCH first
Physical Layer information:		
Hardware Name	mMA12.switch.ch	adva_manno.garr.it
Hardware Model	Sorrento	ADVA
Hardware description	DWDM	DWDM
Active equipment location	MAN-E154-RCSCS4	rack CSCS x
Presence of patch panels	☐	☐
Interconnection point	direct connection to GARRs ADVA, singlemode fiber 15 meters with special ADVA connectors	direct cable to SWITCHs Sorrento, singlemode fiber 15 meters with special ADVA connectors
Interface	10GE	10GE

Abbildung 8.28.: Directly connected equipment, in I-SHARe Prototype [HH09]

der ein zentraler Patch Panel verwendet wird und eine dritte Organisation für das Management dieser Verbindungen von beiden SP-Domänen beauftragt wird. In der Praxis werden auch wesentlich komplexere Verbindungsformen eingesetzt, die hier nicht behandelt werden.

Nach den Konsultationen mit den Betriebsverantwortlichen wurde entschieden, dass die Eingabe nur der eigenen Interfaces in I-SHARe eine akzeptable Lösung darstellt. Die NRENs können dann zusätzliche (u.U. auch Sub-Provider bezogenen) Informationen in I-SHARe pflegen. Die Beschreibungen der beiden präsentierten Verbindungsmöglichkeiten in I-SHARe sind in den Abbildungen 8.28 und 8.29 dargestellt.

Aus dieser Erfahrung kann vor allem die Lehre gezogen werden, dass bei der Umsetzung der Lösung die eindeutige Definition der SCP-Semantik sehr wichtig ist. Vor

	SWITCH	DFN
General Information		
Transfer Capacity [Gbps]	10	10
Housing location:		
Name	bâldata	bâldata
Full address	Margarathenstr. 40, 4002 Basel	Margarathenstr. 40, 4002 Basel
Working hours	24x7	24x7
Contact		
Onsite staff Information	bei Störungen, Telehouse +41 61 275 9640	+ 41 61 275 9640
Emergency Number	+41 44 268 15 30	+41 44 268 15 30
NREN contact Information	Ernst Heiri	Bruno Höhn
Additional information	access with badge always possible to rack	some DFN comment
Physical Layer information:		
Hardware Name	mBA13.switch.ch	Huawei_dfn.dfn.de
Hardware Model	Sorrento	Huawei
Hardware description	DWDM	DWDM
Active equipment location	Jupiter, M115, 1.OG, rack E1	Jupiter, M115, 1.OG, rack yz
Presence of patch panels	☑	☑
Interconnection point	connected through distribution frame via breakout cable with E2000 connectors, patching must be done through telehouse staff, cablelenght must be asked @ telehouse	connected through distribution frame
Interface	10GE	10GE

Abbildung 8.29.: Distribution frame, in I-SHARe Prototype [HH09]

allem bezieht sich diese Aussage auf den Zusammenhang zwischen dem abstrakten Begriff "SCP" und der physischen Infrastruktur. Diese Zusammenhänge können, bedingt durch mehrere Einflussfaktoren, unterschiedlich definiert werden. Daher kann eine solche Entscheidung nicht in dieser Arbeit "im Voraus" festgelegt werden, sondern sie muss bei der tatsächlichen Umsetzung der Lösung getroffen werden.

8.3. Nicht oder nicht vollständig evaluierte Konzepte

Zur Vollständigkeit müssen auch die in dieser Arbeit erarbeiteten Grundkonzepte besprochen werden, die nicht oder nicht vollständig in den Teil-Projekten eingesetzt und daher auch nicht bewertet werden konnten.

Routing-Verfahren

Auch wenn dieses Thema im Abschnitt 8.2.2 bereits kurz aufgegriffen wurde, soll hier zunächst das im Abschnitt 4.3.4 entwickelte *hybride Routing-Verfahren* angesprochen werden. Der Grund dafür liegt darin, dass dieses Verfahren eine zentrale Stellung bei der entwickelten Lösung einnimmt.

Im Géant2 Projekt wurde die Problematik der Dienstgütezusicherung bei Verketteten Diensten erkannt. Wegen einer fehlenden technischen Lösung hat man versucht, die Problematik durch persönliche Absprachen und eine manuelle Routenplanung zu bewältigen. Zu dem Zeitpunkt, als das Routing-Verfahren entwickelt wurde, hatten sich manuelle Abläufe bereits etabliert.

Beiden Verfahren liegt die Berücksichtigung der Domänen-Präferenzen über den Verlauf einer Route zugrunde. Daher kann das im Abschnitt 4.3.4 entwickelte Verfahren auch als eine für das automatische Routing aufbereitete Weiterentwicklung der manuellen Prozesse betrachtet werden. Nachdem das hybride Routing-Verfahren entwickelt wurde, konnten die prinzipiellen Unterschiede zwischen den beiden Verfahren in den persönlichen Gesprächen mit dem für Route-Planung verantwortlichen Betriebspersonal unterschiedlicher NRENs erläutert werden. Diese Gespräche haben ergeben, dass, solange die Informationsanfragen Dienstinstanz-bezogen sind, es für die NRENs sowohl technisch möglich als auch akzeptabel ist, mehrere Alternativen mitzuteilen. Die einzige dabei geäußerte Sorge galt der Einhaltung der Domänen-Präferenzen bei der Wahl zwischen alternativen Verbindungsmöglichkeiten. Die Möglichkeit für die Delegation der Routing-Aufgabe ist bereits in den manuellen Prozessen verankert. Der Unterschied besteht jedoch darin, dass bei der Aufgabenweitergabe die gesamten Informationen über den bereits definierten Routenverlauf mitgeteilt werden. In der entwickelten Lösung wurde dies durch die Mitteilung der Zwischensumme für die relevanten Dienstgüteeigenschaften ersetzt.

Eigenschaftenbereiche und Einschränkung der Informationsmenge

Neben den Aspekten des Routing-Verfahrens wurde in diesen Gesprächen auch nach der Meinung der Betriebsverantwortlichen zu einigen anderen Lösungsideen dieser Arbeit gefragt. Dabei zeigte sich, dass z.B. die Angaben von mehreren unterstützten Dienstgüteeigenschaften für dieselbe Verbindungsmöglichkeit sowohl technisch realisierbar als auch mit Domänen-Policies vereinbar ist, was den Konzepten von mehreren *Component Links* und den damit assoziierten unterstützten Wertebereichen entspricht (siehe vor allem Abschnitt 4.1.2). Die Bekanntgabe aller technisch realisierbaren Verbindungen oder gar der vollständigen Topologie wurden allerdings aus Policy-Gründen als nicht akzeptabel empfunden. Dies entspricht auch dem im Abschnitt 4.8 beschriebenen Einfluss der Policies auf die Entscheidungsfindung (vergleiche auch mit der ähnlichen Diskussion im Abschnitt 8.1.3).

Eigenschaften-IDs und ID-bezogenen Operationen

Zu den Grundkonzepten der entwickelten Lösung, die weder durch Projekte noch durch Interviews evaluiert werden konnten, gehören die im Abschnitt 4.2 beschlossenen Operationen auf Basis der Eigenschaften-IDs und die im Abschnitt 4.8 dafür vorgesehenen Identifizierungsmöglichkeiten. Die Gründe dafür unterscheiden sich zwischen den Planungs- und Betriebsphasen.

Bei der Routen-Planung werden alle relevanten Dienstgüteeigenschaften anhand ihrer Namen referenziert, damit die manuelle Bearbeitung erleichtert wird. Die Aggregation der unterstützten Teilstrecken-Eigenschaften und der Vergleich mit den E2E-Anforderungen werden wiederum manuell, basierend auf persönlichen Kenntnissen und Erfahrungen durchgeführt, was die Definition der entsprechenden Funktionen überflüssig macht.

Im Betrieb sieht die Situation anders aus, weil die Verbindungsgüte mehrerer E2E Links durch das E2Emon-System automatisch überwacht und bewertet werden soll. Die IDs für die zwei unterstützten Überwachungsparameter (Operational und Administrative State) wurden allerdings nicht in einem Registrierungsbaum, sondern ausschließlich bei der Spezifikation der Kommunikationsartefakte festgelegt. Auch die Operationen auf diesen Eigenschaften wurden direkt im Programm-Code festgelegt[4]. Die Entwicklung einer generischen ID-basierten Lösung verursacht auch einen wesentlich größeren Aufwand und bedingt i.A. auch einen komplexeren Programm-Code. Für die Unterstützung von lediglich zwei festgelegten Überwachungseigenschaften ist dieser Aufwand kaum zu rechtfertigen. Sollte jedoch für die Zukunft Unterstützung weiterer Eigenschaften geplant sein – was bei E2Emon weder gefordert wurde noch bislang der Fall war –, dann ist dieser zusätzliche Aufwand gerechtfertigt. Der Grund dafür liegt in einer i.A. größeren Flexibilität und wesentlich leichteren Erweiterbarkeit der ID-basierten Ansätze.

Multi-Domain Managementfunktionalität, Rollenzuordnung

Ein weiteres Lösungskonzept dieser Arbeit, das im Géant2 Projekt nicht getestet wurde, ist die dynamische Bestimmung der Verantwortlichen für Multi-Domain Managementrollen (siehe Abschnitt 4.4). Das liegt hauptsächlich an der übersichtlichen Größe der Kooperation sowie an der relativ geringen Anzahl der gleichzeitigen Anfragen für neue E2E Links. Das macht die Einbindung mehrerer SP-Domänen in die Durchführung derselben Multi-Domain Aufgaben überflüssig und kostenineffizient. In Géant2 wird jedoch eine statische Rollenzuordnung für einige Aufgaben unterstützt, wie es z.B. mit der E2ECU der Fall ist. Das entspricht wiederum dem Konzept der Festlegungen bei festen Kooperationen, das im Abschnitt 4.7 beschrieben wurde.

[4]Die entsprechenden Festlegungen in der Tool-Spezifikation werden hier nicht angesprochen, da sie keinen unmittelbaren Einfluss auf die durchgeführte Berechnung haben.

Kommunikationsprotokoll: Kommunikationsartefakte und Basisprozesse

Auch wenn das im Kapitel 5 definierte Kommunikationsprotokoll auf den Konzepten aufbaut, die sich bei OSI- und Internet-Management bewährt haben, so werden dabei auch viele dienstspezifische Festlegungen getroffen, vor allem bzgl. der Kommunikationsartefakte und der Basisprozesse. In Projekten konnte dies allerdings nicht getestet werden. Das liegt hauptsächlich daran, dass der Großteil der Anfragen, für die sie konzipiert wurden, bei den manuell gemanagten Géant2 E2E Links per e-Mail oder Telefonkommunikation erledigt werden. Die Entwicklung des E2Emon Systems wurde noch vor der Entwicklung der in dieser Arbeit präsentierten Lösung abgeschlossen. Somit konnte zwar das definierte Kommunikationsprotokoll von den Erfahrungen profitieren, die bei E2Emon gesammelt wurden, aber nicht umgekehrt.

SLM-Prozesse

Dasselbe betrifft auch die im Kapitel 6 definierten SLM-Prozesse. Die in den Abschnitten 6.6 und 6.7 definierten Monitoring- und Reporting-Prozesse entsprechen zwar in vielerlei Hinsicht dem Ablauf, der auch bei E2Emon eingesetzt wurde, alle anderen Prozesse wurden aber in keinem der Projekte produktiv getestet.

9 Bewertung der entwickelten Lösung

Dieses Kapitel untersucht die Güte der entwickelten Lösung. Zu diesem Zweck wird zunächst diskutiert, wie gut und durch welche technische Mittel die im Kapitel 2 aufgestellten Anforderungen abgedeckt sind. Anschließend wird im Abschnitt 9.2 die entwickelte technische Lösung anderen existierenden Ansätzen gegenübergestellt. Der Vergleich wird anhand des Erfüllungsgrades der aufgestellten Anforderungen durchgeführt.

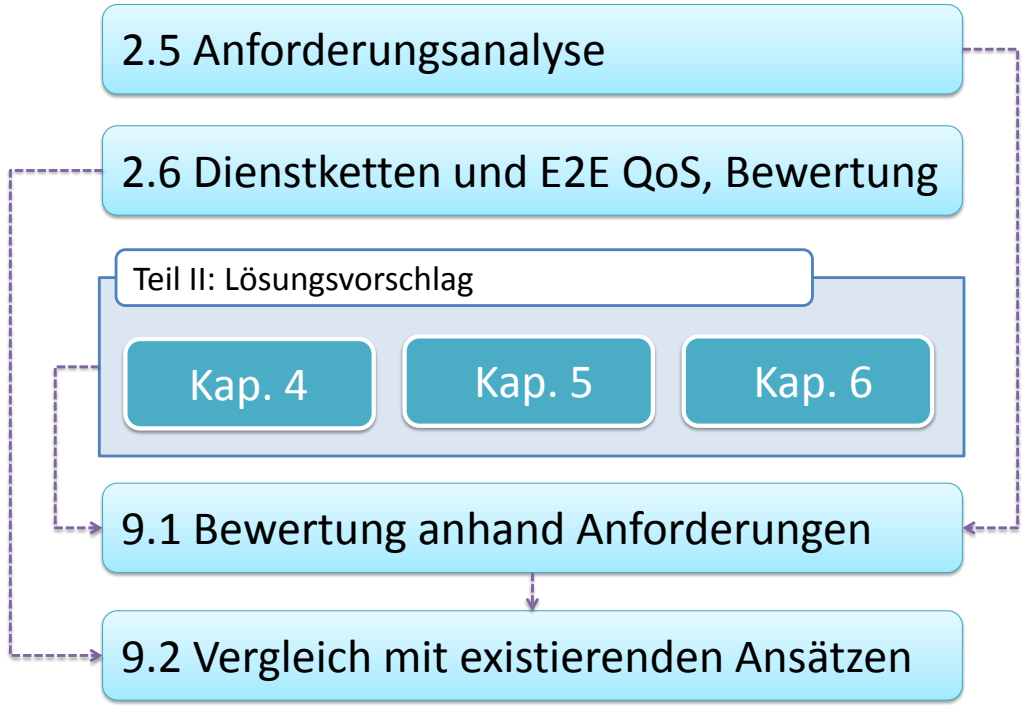


Abbildung 9.1.: Interdependenzen mit anderen Kapiteln

9.1. Bewertung anhand der aufgestellten Anforderungen

Die Reihenfolge der Anforderungsbewertung richtet sich nach der Reihenfolge ihrer Definition im Abschnitt 2.5. Für die bessere Referenzierbarkeit sind die funktionalen und die nichtfunktionalen Anforderungen samt der relevanten Lösungsteile entsprechend in den Tabellen 9.1 und 9.2 zusammengefasst.

Die in Anforderung FA-01 geforderte Abdeckung beliebiger QoS-Parameter ist hauptsächlich dadurch gelöst, dass jeder QoS-Parameter anhand seiner global eindeutigen ID referenziert wird. Diese IDs werden in einer einheitlichen Weise in allen Kommunikationsartefakten verwendet (siehe Abschnitt 4.6.10). Die im Abschnitt 4.2 bestimmte Assoziation der Operationen mit diesen IDs ergänzt die generische Definition der QoS-Parameter.

Die Anforderung FA-02 fordert Unterstützung für beliebige Managementfunktionalität sowie deren zugehörige Parameter. Die Erfüllung dieser Anforderung erfolgt mit derselben Prinzipien und Vorgehensweise, wie bei den QoS-Parametern. Der Unterschied besteht lediglich in der Strukturierung der Beschreibung in den Kommunikationsartefakten (siehe Abschnitt 4.6), die deren semantische Bedeutung sowie Zusammenhänge widerspiegelt.

Die Anforderung FA-03 fordert die gleichzeitige Unterstützung von mehreren Eigenschaften bei einer Dienstinstanz. Die Basis dafür wurde durch die bereits angesprochene generische Beschreibung von QoS-Parametern, Managementfunktionalität und der zugehörigen Parameter gelegt. Durch die Spezifikation in den Kommunikationsartefakten mittels "*"-Multiplizität bei den Assoziationen mit den Klassen, die für die o.g. Eigenschaften stehen, werden auch beliebige Kombinationen aller unterstützter Eigenschaften erlaubt (siehe insbesondere Abschnitt 4.6). Allerdings wird erst durch die Kombination aus den im Abschnitt 4.2 definierten Operationen auf mehreren Eigenschaften und der Verwendung dieser Operationen bei dem im Abschnitt 4.3.4 beschriebenen Routing-Verfahren die Anforderung vollständig erfüllt. Die Anforderung NFA-01 fordert die Beachtung der individuellen Möglichkeiten der Service Provider, die zudem mit der Zeit sich verändern können. Die Aktualität der vorhandenen Informationen über SP-Möglichkeiten wird dadurch gesichert, dass beim Routing-Prozess stets Informationsanfragen an die SP-Domäne gesendet werden (siehe vor allem Abschnitte 5.2 und 6.2).

In der Anforderung NFA-02 wird gefordert, bei der Pfadsuche auch die potentiell möglichen Teildienste zu berücksichtigen. In der Lösung wird dies dadurch erreicht, dass bei Informationsanfragen die Unterscheidung zwischen der Übertragung "bereits vorhandener" und "potentiell möglicher" Teildiensten einer Domäne spezifiziert werden kann (siehe insbesondere Attribut `UncertainityType_ID` im UML-Diagramm 4.49).

Die Anforderung NFA-03 fordert die Erweiterbarkeit in Bezug auf die unterstützten Diensteigenschaften. Diese Anforderung ist vor allem durch die hohe Dynamik im IT-

Anf.	Bezeichnung	Erfüllt durch…
FA-01	Unterstützung beliebiger QoS-Parameter	• Referenzieren der QoS anhand ihrer global eindeutigen IDs • Spezifikation der Operationen auf der QoS im Registrierungsbaum für die IDs • Generische/einheitliche Beschreibung der zwei unterstützten QoS-Klassen: qualitative und quantitative QoS-Parameter
FA-02	Unterstützung beliebiger Managementfunktionalität	• Referenzieren der Managementfunktionalität sowie der zugehörigen Parameter anhand global eindeutiger IDs • Spezifikation der Operationen auf der Managementfunktionalität und deren zugehörigen Parameter in dem Registrierungsbaum für die IDs • Generische/einheitliche Beschreibung der Managementfunktionalität und der zugehörigen Parameter in Kommunikationsartefakten
FA-03	Gleichzeitige Unterstützung mehrerer Eigenschaften	• Generische (ID-bezogene) Bezeichnung der QoS-Parameter, Managementfunktionalität sowie der zugehörigen Parameter • Verweise auf i.A. mehrere Eigenschaften bei der Beschreibung der Kommunikationsartefakte • Verallgemeinerte Operationen auf mehreren Eigenschaften • Berücksichtigung mehrerer Eigenschaften beim Routing-Verfahren
FA-04	Unterstützung aller Use Cases	• SLM-Prozesse • Kommunikationsprotokoll
FA-05	Ziele der Anpassung im Betrieb	• Basisprozess für die Anpassung einzelner Teildienste • SLM-Prozess für die Anpassung der E2E-Dienstinstanz
FA-06	Initiator der Abbestellung	• SLM-Prozess für Abbestellung einer Dienstinstanz • Basisprozess für Abbestellung der Teildienste

Tabelle 9.1.: Erfüllung der Funktionalen Anforderungen (FA) durch Lösungsteile

Umfeld motiviert. Die Grundlage dafür wird dadurch gelegt, dass alle Eigenschaften-IDs sowie die zugehörigen Operationen in einem Registrierungsbaum festgehalten werden (siehe Abschnitt 4.6.10). Dadurch ist auch die Spezifikation der IDs für noch nicht berücksichtigte Diensteigenschaften möglich. In Kombination mit der bereits besprochenen generischen Behandlung aller Diensteigenschaften wird die vollständige Erfüllung dieser Anforderung gewährleistet.

Mit der Anforderung FA-04 wird allgemein die Unterstützung für alle im Abschnitt 2.4.3 erfassten Use Cases gefordert. Diese Anforderung wird durch die im Kapitel 6 definierten SLM-Prozesse direkt angesprochen.

Die Anforderung NFA-04 verbietet einen direkten Zugriff auf die Infrastruktur einer fremden SP-Domäne. Zudem wird gefordert, dass jede SP-Domäne den Informationsumfang und den Detaillierungsgrad bezüglich der eigenen Teildienste selbst bestimmen kann. Dieser Anforderung wird vor allem durch die im Abschnitt 4.1.1 eingeführte DSM-Schnittstelle für die gesamte Kommunikation entsprochen. Die Kontrolle der ausgetauschten Informationen wird zum einen durch die im Abschnitt 4.8 vorgeschlagene Softwarearchitektur in einer einzigen SP-Domäne und zum anderen durch

Anf.	Bezeichnung	Erfüllt durch…
NFA-01	Beachtung der Service Provider Unterstützung	• Per-Dienstinstanz Informationsabfragen der vorhandenen Möglichkeiten
NFA-02	Unterstützung potentiell möglichen (Teil-)Dienste	• Unterscheidung zwischen potentiell möglichen und bereits vorhandenen Diensten anhand des `UncertainityType_ID` Attributs
NFA-03	Erweiterbarkeit in Bezug auf unterstützte Diensteigenschaften	• Möglichkeit neue Eigenschaften-IDs und zugehörigen Operationen im Registrierungsbaum zu spezifizieren • Generische Beschreibung der QoS-Parameter, Managementfunktionalität und zugehöriger Parameter
NFA-04	Zugriffseinschränkung auf die Domain-Informationen	• DSM-Schnittstelle • Überprüfung der Vertrauensbeziehungen in allen Basisprozessen
NFA-05	Begrenzung der Prozessdurchlaufzeit	• Abbruch bei Zeitüberschreitungen in Prozessen • Mitteilung der Zeiteinschränkung bei Funktionsanfragen
NFA-06	Dekomposition der QoS-Parameter	• Routing-Verfahren • Bestimmung der Grenzwerte anhand von Wertebereichen
NFA-07	Dekomposition der Management-funktionalität	• Routing-Verfahren • Bestimmung der Managementfunktionalitätsparameter • Bestimmung involvierter Akteure und Kommunikationswege • Delegation der Multi-Domain Managementfunktionalität und Verantwortungsbereiche
NFA-08	Zustimmung der involvierten SPs	• Kommunikationsprotokoll • Entscheidungsmöglichkeit in Basisprozessen
NFA-09	Erkennung (drohender) E2E-Dienstgüte-verletzungen	• Überwachung der Dienstgüte aller Teildienste • Ableitung des E2E-Zustandes von den Teildienste-Zuständen
NFA-10	Erkennung eines Verursacher-SP	• Überwachung der Dienstgüte aller Teildienste
NFA-11	Skalierbarkeit	• Aufbau des Routing-Verfahrens auf dem Domain-Wissen • *Load Balancing* durch Kommunikationswege
NFA-12	Robustheit	• Berücksichtigung aktuell möglicher Teildienste • Ausweichen bei Problemen auf eine Alternativroute • Anstoßen des *Incident&Problem Managementprozesses*
NFA-13	Anpassbarkeit an die veränderte Anforderungen	• Modularer Lösungsaufbau • Anpassbarkeit unterschiedlicher Lösungsteile kann ohne große Auswirkung auf andere durchgeführt werden

Tabelle 9.2.: Erfüllung der Nicht-Funktionalen Anforderungen (NFA) durch Lösungsteile

die festgelegte Überprüfung der Vertrauensbeziehungen in allen Basisprozessen (siehe dazu Kapitel 5) sichergestellt.

Die Anforderung NFA-05, die die Begrenzung der Laufzeit aller Prozesse fordert, wird durch folgende zwei Lösungsaspekte angesprochen: In den Prozessdiagrammen in den Kapiteln 5 und 6 sind alle "Wait for ..."-Aktivitäten jeweils mit einem Abbruch bei der Zeitüberschreitung versehen. Weiterhin wird bei den in Abschnitten 5.9 und 5.10 definierten `CHANGE`- und `MGMTFCT`-Anfragen eine Übergabe der Zeiteinschränkung vorgese-

hen, wodurch auch Verkettungseffekte von mehreren hintereinandergeschalteten Proxies eliminiert werden können (vergleiche Abschnitt 4.3.3).

In der Anforderung NFA-06 wird die Ableitung der erforderlichen Grenzwerte für die Teildienste-QoS von den E2E-Kundenanforderungen gefordert. Diese Anforderung wird zunächst durch das im Abschnitt 4.3.4 definierte Routing-Verfahren adressiert, das eine Route bestimmt, bei der die Erfüllung der E2E-Kundenanforderungen möglich ist. Weiterhin wird im Abschnitt 4.2.4 eine Vorgehensweise definiert, mit der von den Wertebereichen, die für die involvierten Teildienste möglich sind, auf die erforderlichen Grenzwerte geschlossen werden kann.

In der Anforderung NFA-07 wird eine ähnliche Anforderung in Bezug auf die Managementfunktionalität gefordert. An Stelle der QoS-Parameter werden bei dem Routing-Verfahren für die Erfüllung dieser Anforderung die Parameter der erforderlichen Managementfunktionalität bestimmt. Bei der Managementfunktionalität müssen zudem die involvierten Akteure für die unterschiedlichen Rollen sowie die Kommunikationswege bestimmt werden. Die Mitteilung der erwünschten Kommunikationswege geschieht dabei über die Kommunikationsartefakte (siehe die Verwendung der Klasse COMMUNICATIONDSM und die zugehörige Beschreibung im Abschnitt 4.6).

In der Anforderung NFA-08 wird die Entscheidungsfreiheit der diensterbringenden Domänen gefordert. Diese wird einerseits in dem Kommunikationsprotokoll "verankert", indem jede SP-Domäne die Informations- und Dienstanfragen ablehnen darf. Zudem wird in jedem definierten Basisprozess eine entsprechende Entscheidungsmöglichkeit vorgesehen. Beide Aspekte sind im Kapitel 5 definiert.

Die in NFA-09 geforderte Erkennung von (drohenden) Verletzungen der E2E-Zusicherungen geschieht in der entwickelten Lösung nur auf einem indirekten Wege. Da die direkten E2E-Messungen i.A. nicht möglich sind, werden die E2E-Dienstgütewerte von den Messwerten einzelner Teildienste abgeleitet (siehe Abschnitt 6.7). Diese Vorgehensweise beruht auf der Korrektheit der Aggregatfunktionen, die laut der Festlegung im Abschnitt 4.2 mit jedem QoS-Parameter assoziiert werden sollen. Weiterhin ist diese Lösung auf eine lückenlose Überwachung aller involvierten Teildienste angewiesen. Da sowohl die lückenlose Überwachung aller Teilstrecken durch die erbringenden SP-Domänen als auch die Korrektheit der mitgeteilten Überwachungsinformationen bei heterarchischen Organisationsformen nur sehr schwer zu durchsetzen sind, kann diese Anforderung nur als "bedingt erfüllt" bewertet werden.

Da E2E-Dienstgüteverletzungen nur durch die Verletzung von Zusicherungen für einen oder mehrere Teildienste verursacht werden können, wird in Anforderung NFA-10 gefordert, verursachende SP-Domänen identifizieren zu können. Da die Dienstinstanz-Überwachung auf Basis von Teilstrecken aufgebaut ist, kann diese Anforderung direkt erfüllt werden (siehe Abschnitt 6.7). In Bezug auf den Erfüllungsgrad dieser Anforderung gelten dieselben Bedenken wie bei NFA-09, deswegen kann sie nur als "bedingt erfüllt" bewertet werden.

In der Anforderung FA-05 werden Ziele aufgelistet, die bei dem Use Case "Change" verfolgt werden sollen. Die Grundlage für die meisten Ziele werden in dem Basisprozess für die Anpassung der einzelnen Teildienste gelegt (siehe Abschnitt 5.9). Dadurch wird die Anpassung der Teildienst-Zielwerte sowie der Kommunikationswege ermöglicht. Obwohl der im Abschnitt 6.8 definierte SLM-Prozess keine Unterstützung für das Re-Routing im Betrieb vorsieht, kann die Anforderung dennoch als erfüllt bewertet werden, weil eine entsprechende Erweiterung des SLM-Prozesses anhand der bereits definierten Hilfs- und Basisprozesse möglich ist.

Die im Kapitel 6 definierten SLM-Prozesse haben Referenz-Charakter. Grundsätzlich sollen sie illustrieren, wie die Managementprozesse aufbauend auf dem Kommunikationsprotokoll und den Basisprozessen definiert werden können. Dadurch kann sowohl die Anpassbarkeit der SLM-Prozesse an Dienst- bzw. Projekt-spezifische Anforderungen als auch die Verständlichkeit der Referenzprozesse bewahrt werden.

Eine ähnliche Überlegung ist auch auf die Anforderung FA-06 anwendbar. Diese Anforderung sieht vor, dass eine Dienstinstanz sowohl vom Kunden als auch von einem der involvierten SP-Domänen aufgelöst werden kann. Der entsprechende SLM-Prozess, der im Abschnitt 6.9 definiert ist, unterstützt allerdings nur die erste Möglichkeit. Die Unterstützung der zweiten Option wurde aufgrund deren Dienstspezifik nicht explizit definiert. Die entsprechende Erweiterung bleibt ohne weiteres auf Basis des im Abschnitt 5.12 definierten Benachrichtigungsmechanismus möglich.

Mot Anforderung NFA-11 werden Aspekte der Skalierbarkeit erfasst. Die Skalierbarkeit bei der Bestellung einer neuen Dienstinstanz wird vor allem durch das Routing-Verfahren gewährleistet, das das Hintergrundwissen und die Präferenzen der beteiligten SP-Domäne berücksichtigt (siehe Abschnitt 4.3.4). Die Skalierbarkeit im Betrieb wird hauptsächlich dadurch gewährleistet, dass die Managementaufgaben und die Kommunikationswege zwischen den Beteiligten beliebig definiert werden können (siehe Abschnitt 4.4). Bei Bedarf können die Kommunikationswege auch im Betrieb angepasst werden (siehe Abschnitt 5.9).

Ähnlich werden in der Anforderung NFA-12 Aspekte aufgelistet, in Bezug auf die die entwickelte Lösung robust sein soll. Während beim Routing auf auftretende Probleme direkt reagiert wird (siehe vor allem die Abschnitte 6.1, 6.2, 6.3 und 6.4), ist für die Betriebsphase das Anstoßen des *Incident&Problem Managementprozesses* vorgesehen (siehe Abschnitt 6.6). Da das Anstoßen des *Incident&Problem Managementprozesses* im Betrieb abhängig ist vom Erkennen des Problems (siehe Bewertung der Anforderung NFA-09), kann diese Anforderung nur als "größtenteils erfüllt" bewertet werden.

Die Anforderung NFA-13 fordert eine möglichst einfache Anpassbarkeit an veränderte Anforderungen. Dieser Anforderung entspricht vor allem der modulare Lösungsaufbau. Die Veränderung an einem der Lösungsteile, die in Kapitel 4, 5 und 6 definiert wurden, führt nur bedingt zu Anpassungen bei den anderen Teilen. Weiterhin wurden

im Abschnitt 4.7 eine Reihe denkbarer Anpassungen der Routing-Architektur aufgezeigt. Diese Anforderung kann somit als "erfüllt" bewertet werden.

9.2. Vergleich mit existierenden Ansätzen

Die im Abschnitt 9.1 durchgeführte Bewertung der entwickelten Lösung ist in Tabelle 9.3 dargestellt. Um den Vergleich mit existierenden Ansätzen zu erleichtern, wird diese Bewertung zusammen mit den Ergebnissen aus der Tabelle 2.6 dargestellt.

Auch wenn die entwickelte Lösung nicht alle Anforderungen vollständig erfüllt, so zeigt der Vergleich, dass die entwickelte Lösung ein deutlich ausgewogeneres Bild in Bezug auf den Erfüllungsgrad der aufgestellten Anforderungen aufweist als das bei existierenden Ansätzen der Fall ist. Somit kann die entwickelte Lösung als ein wesentlicher Fortschritt gegenüber der Status Quo bewertet werden.

Szenario 1: Telefonnetz/PSTN	Szenario 2: Géant2 E2E Links	Szenario 3: GLIF	Szenario 4: DCN	Szenario 5/1: IntServ	Szenario 5/2: DiffServ	Entwickelte Lösung		
☐☐☐	🟧🟧☐	☐☐☐	☐☐☐	☐☐☐	☐☐☐	🟩🟩🟩	FA-01	Unterstützung beliebiger QoS-Parameter
☐☐☐	🟧🟧☐	☐☐☐	☐☐☐	☐☐☐	☐☐☐	🟩🟩🟩	FA-02	Unterstützung beliebiger Managementfunktionalität
🟥☐☐	🟩🟩🟩	☐☐☐	🟥☐☐	☐☐☐	☐☐☐	🟩🟩🟩	FA-03	Gleichzeitige Unterstützung mehrerer Eigenschaften
🟧🟧☐	🟧🟧☐	🟧🟧☐	🟧🟧☐	🟥☐☐	🟥☐☐	🟩🟩🟩	FA-04	Unterstützung aller Use Cases
☐☐☐	🟥☐☐	☐☐☐	☐☐☐	☐☐☐	🟥☐☐	🟩🟩🟩	FA-05	Ziele der Anpassung im Betrieb
🟩🟩🟩	🟥☐☐	🟧🟧☐	🟧🟧☐	🟩🟩🟩	🟩🟩🟩	🟩🟩🟩	FA-06	Initiator der Abbestellung
🟩🟩🟩	🟩🟩🟩	🟧🟧☐	🟧🟧☐	🟧🟧☐	☐☐☐	🟩🟩🟩	NFA-01	Beachtung der Service Provider Unterstützung
☐☐☐	🟩🟩🟩	☐☐☐	☐☐☐	☐☐☐	☐☐☐	🟩🟩🟩	NFA-02	Unterstützung potentiell möglicher (Teil-)Dienste
🟧🟧☐	🟩🟩🟩	☐☐☐	🟥☐☐	☐☐☐	☐☐☐	🟩🟩🟩	NFA-03	Erweiterbarkeit in Bezug auf unterstützte Diensteigenschaften
🟩🟩🟩	🟧🟧☐	🟥☐☐	🟥☐☐	☐☐☐	🟧🟧☐	🟩🟩🟩	NFA-04	Zugriffseinschränkung auf die Domain-Informationen
🟩🟩🟩	🟥☐☐	☐☐☐	☐☐☐	☐☐☐	☐☐☐	🟩🟩🟩	NFA-05	Begrenzung der Prozessdurchlaufzeit
🟥☐☐	🟩🟩🟩	🟧🟧☐	🟧🟧☐	☐☐☐	☐☐☐	🟩🟩🟩	NFA-06	Dekomposition der QoS-Parameter
☐☐☐	🟧🟧☐	🟥☐☐	🟥☐☐	☐☐☐	☐☐☐	🟩🟩🟩	NFA-07	Dekomposition der Managementfunktionalität
🟩🟩🟩	🟩🟩🟩	🟥☐☐	🟥☐☐	☐☐☐	☐☐☐	🟩🟩🟩	NFA-08	Zustimmung der involvierten SPs
☐☐☐	🟥☐☐	🟥☐☐	🟥☐☐	☐☐☐	☐☐☐	🟥☐☐	NFA-09	Erkennung (drohender) E2E-Dienstgüteverletzungen
☐☐☐	🟥☐☐	☐☐☐	☐☐☐	☐☐☐	☐☐☐	🟥☐☐	NFA-10	Erkennung eines Verursacher-SP
🟩🟩🟩	🟥☐☐	🟧🟧☐	🟧🟧☐	🟩🟩🟩	🟩🟩🟩	🟩🟩🟩	NFA-11	Skalierbarkeit
🟩🟩🟩	🟥☐☐	🟥☐☐	🟥☐☐	🟧🟧☐	🟩🟩🟩	🟧🟧☐	NFA-12	Robustheit
🟥☐☐	🟧🟧☐	🟥☐☐	🟥☐☐	🟥☐☐	🟥☐☐	🟩🟩🟩	NFA-13	Anpassbarkeit an veränderte Anforderungen

Erfüllungsgrad der Anforderungen:

☐☐☐ gar nicht 🟥☐☐ bedingt/kaum 🟧🟧☐ größtenteils 🟩🟩🟩 vollständig

Tabelle 9.3.: Bewertung der Lösung anhand Kriterienkatalog

10 Zusammenfassung und Ausblick

Das moderne Netz- und Telekommunikationsumfeld ist von Verbindungsdiensten geprägt, die durch die horizontale Verkettung mehrerer Teildienste realisiert werden. Im Allgemeinen werden diese Teildienste durch unterschiedliche IT Service Provider erbracht. Die Ende-zu-Ende Dienstgüte sowie deren Zusicherung ist bei derartig aufgebauten Diensten kein prinzipiell neuer bzw. bisher unbekannter Aspekt. Dennoch haben sich bislang in diesem Zusammenhang nur zwei Herangehensweisen etabliert, die nicht alle möglichen Fälle abdecken. So ist für die Zusicherung von Dienstgüteeigenschaften der Aufbau hierarchischer Organisationsformen üblich. Bei Diensten mit einer *Best-Effort*-Strategie (zu denen auch Internet- und Telefonverbindungen gehören) wird die Dienstgüte-Problematik durch den Einsatz von *Overprovisioning* begegnet.

In der modernen vernetzten Welt sind Verkettete Dienste zu einem integralen Teil für andere *Value-Added Services* geworden, die sowohl im Forschungs- als auch im Businessumfeld benötigt werden. Wachsende Anforderungen an die kundenorientierten Dienste spiegeln sich in neuen Anforderungen an die Netz-Dienste wider. Wie im Kapitel 1 gezeigt wurde, wird eine Möglichkeit benötigt, die E2E-Dienstgüte für Dienstketten auch dann zuzusichern, wenn weder der Aufbau hierarchischer Organisationsbeziehungen noch das *Overprovisioning* im benötigten Maße möglich oder akzeptabel sind. Diese Arbeit hat sich mit den technischen Aspekten der aufgezeigten Problematik befasst und dafür eine geeignete Lösung erarbeitet.

Dieses Kapitel ist wie folgt aufgebaut: Im folgenden Abschnitt 10.1 wird ein kurzer Rückblick der Arbeit gegeben und dabei die wichtigsten Aspekte zusammengefasst. Im Abschnitt 10.2 werden Weiterentwicklungsmöglichkeiten geschildert. Die Arbeit wird mit einem Ausblick auf verwandte Forschungsfragestellungen im Abschnitt 10.3 abgeschlossen.

10.1. Zusammenfassung dieser Arbeit im Rückblick

Das Kapitel 2 hat sich mit der Aufstellung der Anforderungen auf die zu entwickelnde Lösung befasst. Zunächst wurde in diesem Kapitel die Zielsetzung dieser Arbeit präzisiert. Ausgehend von der Zielsetzung wurden für die Anforderungsanalyse fünf Dienstketten-Szenarios hinzugezogen, die jeweils die bekanntesten und/oder aussichtsreichsten Vertreter in unterschiedlichen Kategorien sind – etablierte und neue kundenorientierte Dienste, Forschungsprojekte und -Kooperationen, sowie die bekanntesten Techniken zur Dienstgütezusicherung. Bei den ausgewählten Szenarios wurden unterschiedliche Aspekte untersucht und analysiert, darunter vor allem die oft einander entgegengerichteten Interessen der Dienstnutzer und der Service Provider. Das Ergebnis dieser fundierten Szenarien-Analyse mündete in einen Anforderungskatalog. Der Katalog umfasst alle identifizierten Anforderungen, die bei Dienstgütezusicherungsmaßnahmen für Verkettete Dienste erfüllt werden sollten. Das Kapitel schloss mit der Bewertung aller ausgewählten Szenarios anhand des aufgestellten Anforderungskataloges. Das Ergebnis dieser Bewertung zeigt deutlich, dass die Erfüllung aller aufgestellten Anforderungen durch keine punktuelle Verbesserung der vorgestellten Szenarios möglich ist. Dies motiviert die Notwendigkeit für die Entwicklung einer neuen Lösung.

Der Lösungsteil begann mit Kapitel 3. Als erstes wurde in diesem Kapitel eine grobe Lösungsskizze präsentiert. Entsprechend dieser Skizze besteht die angestrebte Lösung aus drei Teilen: einer Routing-Architektur, die die Aspekte der E2E-Dienstgütezusicherung berücksichtigt, einem Kommunikationsprotokoll zur Signalisierung unterschiedlicher Anfragen und zum Informationsaustausch, sowie den darauf aufgebauten Service-Level-Managementprozessen. Resultierend aus der Zielsetzung dieser Arbeit sowie aus der Lösungsskizze wurden im weiteren Verlauf dieses Kapitels unterschiedliche Ansätze zur Thematik detailliert untersucht. Das Ergebnis dieses Abschnittes war eine Analyse möglicher Lösungsbausteine und Erfahrungen, die bei der Entwicklung der Lösung in den weiteren drei Kapiteln einfließen.

Die SLM-aware Routing-Architektur, die den Kern der Lösung bildet, wird im Kapitel 4 entwickelt. Diese Architektur legt nicht nur den Verlauf einer Route fest, sondern berücksichtigt dabei auch die Besonderheiten der Verketteten Dienste sowie die Vorgaben des Service-Level-Management bei dieser Dienstform. Dafür sind insbesondere die Definition und das Zusammenspiel folgender drei Lösungsteile entscheidend:

Beschreibung möglicher Teilstrecken und Eigenschaften: Dieser Lösungsteil wurde auf Basis von ITU-T Empfehlungen für die Beschreibung optischer Transportnetze entwickelt. Die notwendigen Anpassungen und Erweiterungen wurden aus der Zielsetzung sowie von der Spezifik der Verketteten Dienste abgeleitet. Dabei werde insbesondere auf eine vernünftige Balance zwischen den für die Dienstgütezusicherung notwendigen Informationen und den i.A. sehr restriktiven Informations-Policies der autonomen SP-Domäne geachtet.

Operationen auf Eigenschaften: Dieser Lösungsteil profitierte vor allem von den Erfahrungen und Vorgehensweisen, die in der Graphentheorie gesammelt bzw. entwickelt wurden. Die notwendigen Erweiterungen resultierten daraus, dass die Spezifik der zu unterstützenden Dienstgüteeigenschaften und Managementfunktionalität in der Graphentheorie nicht unmittelbar unterstützt wird.

SLM-aware Routing-Verfahren: Aufbauend auf *Routing by Delegation* und *Source Routing* wurde in dem Kapitel ein hybrides Routing-Verfahren entwickelt, das in sich die – in Bezug auf die aufgestellten Anforderungen – besten Eigenschaften dieser etablierten Verfahren vereint. Neben der Bestimmung des Routen-Verlaufs werden bei diesem Verfahren auch die Dienstinstanz-bezogenen E2E-Anforderungen auf Teilstrecken-bezogene Anforderungen abgebildet sowie alle für das Ende-zu-Ende Service-Level-Management benötigten Rollen und Kommunikationswege festgelegt.

Neben den zentralen Konzepten einer Routing-Architektur wurden in diesem Kapitel auch eine Reihe von Optimierungs-, Umsetzungs- und Integrationsaspekten erarbeitet. Zu den wichtigsten gehören die Möglichkeit der Bestellung fehlender Multi-Domain Managementfunktionalität bei einer anderen SP-Domäne, wodurch die Spezialisierung unterschiedlicher Service Provider an unterschiedlichen Aufgaben ermöglicht wird, die Festlegung der benötigten Kommunikationsartefakte und Identifizierungsmöglichkeiten sowie die Softwarearchitektur-Skizze einer SP-Domäne.

Die technische Integration zwischen unabhängigen SP-Domänen wird grundsätzlich von einem Signalisierungs- bzw. Kommunikationsprotokoll übernommen. Das im Kapitel 5 definierte Kommunikationsprotokoll baut auf den in OSI- und Internet-Managementarchitekturen bewährten Kommunikationsmustern auf. Dieses auf Anfrage-, Antwort- und Benachrichtigungsnachrichten basierende Kommunikationsmuster wird anhand des Zustandsdiagramms sowie der erlaubten Dienstzusammensetzung und Managementoperationen verfeinert. Mit jeder so definierten Dienstanfrage wurde in diesem Kapitel ein Basisprozess assoziiert, der das erwartete Vorgehen bei einer übermittelten Anfrage eindeutig spezifiziert. Die Definition der Basisprozesse erfolgte in Anlehnung an die Methode *ITSMCooP*, die zur Spezifikation von Multi-Domain Prozesse bei nicht-hierarchischen Kooperationsformen entwickelt wurde. Neben dem Verhalten wurden bei der Prozessdefinition auch die möglichen Abfolgen der erlaubten Signalisierungsnachrichten sowie die damit verbundenen Kommunikationsartefakte festgelegt.

Referenzprozesse für das Service-Level-Management bei Verketteten Diensten wurden im Kapitel 6 definiert. Die SLM-Prozesse bauen ausschließlich auf dem zuvor definierten Kommunikationsprotokoll und den Basisprozessen auf. Dadurch werden nicht nur SLM-Prozesse definiert, die – aus der Sicht des Autors – in den meisten Fällen bei Verketteten Diensten eingesetzt werden können, sondern auch die Anpassbarkeit an die Providerkooperation- bzw. Dienstkatalog-spezifischen Anforderungen gewährleistet.

Der Evaluationsteil dieser Arbeit wurde vom Kapitel 7 eingeleitet. In diesem Kapitel wurde an einem Beispiel mit fünf SP-Domänen illustriert, wie der Bestellprozess in der ganzen Tiefe der dabei ablaufenden Aktivitäten und der dabei benötigten Kommunikation zwischen Domänen umgesetzt werden kann. Für die Umsetzung des zuvor definierten Kommunikationsprotokolls wurden in diesem Kapitel *Web Services* gewählt, die – gegenüber den *in-band* Protokollen – sowohl bessere Erweiterungseigenschaften aufweisen als auch vergleichsweise gut für derartige Illustrationen geeignet sind. Neben der Abbildung der Protokollanfragen und Kommunikationsartefakte auf die XML-Nachrichten wird in diesem Kapitel ein besonderes Augenmerk auf die Verdeutlichung der kritischen Eigenschaften der entwickelten Lösung gelegt, wie z.B. die vorgesehene Verteilung der Managementaufgaben sowie die Etablierung der Kommunikationswege zwischen beteiligten SP-Domänen.

Im Kapitel 8 wurden zwei Géant2-Teilprojekte beschrieben, in denen unterschiedliche Grundkonzepte der in dieser Arbeit präsentierten Lösung angewendet werden konnten. Die dabei gesammelten Erfahrungen werden Teilprojekt-bezogen aufgelistet und kritisch bewertet. Zum Schluss dieses Kapitels wurden auch Lösungskonzepte besprochen, die bislang nicht oder nicht vollständig in den Projekten eingesetzt werden konnten.

Im Kapitel 9 wurde die entwickelte Lösung anhand der aufgestellten Anforderungen diskutiert und bewertet. Dabei wurden auch die Lösungsteile kurz aufgelistet, durch die die jeweiligen Anforderungen erfüllt werden. Die Gegenüberstellung der Gesamtgüte der entwickelten Lösung und existierender Ansätze haben dieses Kapitel abgeschlossen.

10.2. Weiterentwicklung der Ergebnisse dieser Arbeit

Auch wenn die entwickelte Lösung in Bezug auf die aufgestellten Anforderungen bereits eine deutliche Verbesserung gegenüber bislang existierenden Ansätzen zeigt, zeigten sich im Laufe der Arbeit einige Aspekte, die durch nachfolgende Arbeiten weiter entwickelt werden sollten:

- Die entwickelte Lösung vertritt eine Dienstinstanz-zentrische Sicht, bei der alle Kommunikationswege und Kommunikationsartefakte sich ausschließlich auf eine einzige Dienstinstanz beziehen. Diese Vorgehensweise ermöglicht größtmögliche Flexibilität in Bezug auf die bei der Diensterbringung teilnehmenden SP-Domänen sowie auf die Gestaltung der Kommunikationswege. Im Kapitel 8 wurde aber gezeigt, dass diese Flexibilität oft überflüssig oder sogar kontraproduktiv sein kann, insbesondere wenn mehrere Dienstinstanzen dieselben Akteure und Kommunikationswege miteinander teilen.

  Dieser Aspekt ist insbesondere für ein Monitoring der Dienstinstanzen im Betrieb wichtig, denn zu diesem Zeitpunkt sind bereits alle Festlegungen getroffen. Bei der Weiterentwicklung der Lösung sollte es daher möglich sein, die Monitoring-Informationen über mehrere Dienstinstanzen gleichzeitig anzufragen bzw. mitzuteilen.

- Ein weiterer Aspekt, der sich auf das Dienstinstanz-Monitoring bezieht, wurde im Kapitel 9 erläutert. Die Erkennung von Verletzungen der Vereinbarungen sowie der verursachenden SP-Domänen hängt davon ab, ob die Überwachung aller Teildienste lückenlos ist oder nicht.

  Diese Situation kann durch den Einsatz von *Overlapping Monitored Connections* verbessert werden (siehe Abschnitt 3.6). Diese Vorgehensweise ist allerding sehr stark technologieabhängig und kann nicht pauschal bei allen Diensten gefordert werden. Eine Weiterentwicklung des Routing-Verfahrens sollte jedoch dies als eine mögliche Option unterstützen.

  Weiterhin soll auch der Fall genauer betrachtet werden, wenn *Overlapping Monitored Connections* nicht realisierbar sind. Es muss genau untersucht werden, welche Verhaltensmuster bei fehlenden Informationen über Teilstrecken denkbar und sinnvoll sind (vergleiche ähnliche Diskussion über das E2E Monitoring System im Abschnitt 8.1). Die Lösung sollte dann um entsprechende Verhaltensmuster erweitert werden.

- Bei der im Abschnitt 8.1 geführten Diskussion über das E2E Monitoring System wurde die Notwendigkeit erkannt, auch die Interdependenzen zwischen unterschiedlichen Dienstgüteeigenschaften beschreiben und verwenden zu können. Wie das generisch spezifiziert werden kann, muss auch gesondert untersucht werden.

10.3. Ausblick auf verwandte offene Fragestellungen

Die entwickelte Lösung fokussiert sich auf Dienstgütezusicherungen bei dedizierten Verbindungen. Somit kann diese Technik ohne weiteres auf die Netztechniken, wie z.B. VPN, übertragen werden. In modernen Rechnernetzen zeichnet sich jedoch eine zunehmende Bedeutung von p2p-Verbindungen ab. Ursprünglich überwiegend für *File-Sharing* eingesetzt, wird diese Technik mittlerweile in unterschiedlichen Bereichen verwendet, wie das z.B. bei *Skype* für *Internet-Telefonie* der Fall ist. Auch die Provider von multimedialen Inhalte zeigen ein wachsendes Interesse an dieser Technik. Da für beides, die Kommunikation und Video-on-Demand, die Einhaltung der E2E-Dienstgüte unabdingbar ist, stellt sich die Frage, ob sich die entwickelte Lösung bzw. Lösungsteile auf p2p-Netze übertragen lassen. Falls ja, stellt sich die Frage, welche Anpassungen an die Spezifik von p2p-Netzen dabei notwendig sind.

Unabhängig davon, ob bei dedizierten Verbindungen oder bei p2p-Netzen stellt sich die folgende Frage, die nicht allein mit Informatikmitteln geklärt werden kann. In dieser Arbeit wurde davon ausgegangen, dass die Zusagen einer SP-Domäne, einen oder mehrere Teildienste mit einer definierten Dienstgüte zu erbringen, verbindlich sind. Die Signierung einer Nachricht bietet zwar ein technisches Hilfsmittel, es muss jedoch geklärt werden, welche organisatorischen und juristischen Rahmen notwendig sind, damit eine solche "Unterschrift" tatsächlich verbindlich wird.

Da bei der Diensterbringung Kosten entstehen, die i.A. an den Kunden weitergegeben werden, stellen sich Fragen nach dem *Accounting* und dem *Billing* auch bei *Verketteten Diensten*. Aus technischer Sicht ist vor allem interessant, durch wen und wie das Accounting geführt wird und an wen und wie oft relevante Informationen weitergegeben werden. Aus wirtschaftlicher Sicht stehen dagegen die Umlage der Kundenzahlungen oder umgekehrt der Strafzahlungen (bei SLA-Verletzungen) an die involvierten SP-Domänen im Vordergrund.

Insgesamt zeichnet sich damit ab, dass die entwickelte Lösung zwar einen essentiellen Beitrag zur E2E-Dienstgütezusicherung bei *Verketteten Diensten* liefert. Darüberhinaus sind Weiterentwicklungen nötig – auch in Zusammenarbeit mit anderen Fachgebieten – damit der Einsatz der entwickelten Lösung bei kundenorientierten Diensten möglich wird.

Abkürzungen

AS	Autonomes System
BPEL4WS	Business Process Execution Language for Web Services
BPMN	Business Process Modeling Notation
CMDB	Configuration Management Database
E2E	End-to-End
E2Emon	E2E-Link-Monitoring-System
eTOM	Enhanced Telecom Operations Map
GLIF	Global Lambda Integrated Facility
I-SHARe	Information Sharing Across Heterogeneous Administrative Regions
ITIL	IT Infrastructure Library
ITSM	IT-Service-Management
ITSMCooP	IT Service Management Processes for Co-Operating Providers
ITU-T	International Telecommunications Union Technical Standards Group
MIB	Management Information Base
MNM	Munich Network Management
NNI	Network-Network Interface
NREN	National Research and Educational Network
OGC	Office of Government Commerce

OMG	Objects Management Group
QoS	Quality of Service
SAP	Service Access Point
SID	Shared Information/Data Model
SLA	Service Level Agreement
SLM	Service-Level-Management
TMF	Telemanagement Forum
TNOC	Transmission Network Operating Centre
UML	Unified Modeling Language
WfMS	Workflow Management System
XML	Extensible Markup Language
XPDL	XML Process Definition Language
LHC	Large Hadron Collider
DEISA	Distributed European Infrastructure for Supercomputing Appications
CSM	Customer Service Management
CSMAP	CSM Access Point
NGOSS	New Generation Operations Systems and Software
EP	End Point
MO	Managed Objects
PSTN	Public Switched Telephone Network
SS7	Signalling System No. 7
ISDN	Integrated Services Digital Network
DCN	Dynamic Circuit Network
DRAGON	Dynamic Resource Allocation via GMPLS Optical Networks
OSCARS	On-demand Secure Circuits and Advance Reservation System
AutoBAHN	Automated Bandwidth Allocation across Heterogeneous Networks
MPLS	Multiprotocol Label Switching
RSVP	Resource Reservation Protocol
OSPF	Open Shortest Path First

DiffServ	Differentiated Services
IntServ	Integrated Services
ATM	Asynchronous Transfer Mode
MCP	Multi-constrained Path
CSP	Constrained Shortest Path
MCSP	Multi-constrained Shortest Path
TNA	Technology Neutral Architecture
UC	Underpinning Contract
OTN	Optical Transport Network
TCM	Tandem Connection Monitoring
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
URN	Uniform Resource Name
DSM	Domain Service Management
SCP	Service Connection Point

Literaturverzeichnis

[3CO08] 3COM: *Understanding IP Addressing: Everything You Ever Wanted To Know*. Nummer 19.11.2008. 3COM, 2008 (letzter Zugriff: 19.11.2008). Elektronische Quelle URL: `http://www.3com.com/other/pdfs/infra/corpinfo/en_US/501302.pdf`.

[ADF+01] ANDERSSON, L., P. DOOLAN, N. FELDMAN, A. FREDETTE und B. THOMAS: *RFC 3036: LDP Specification*. RFC 3036, IETF, 2001.

[Adl09] ADLER, H.-M.: *Neues im X-WiN*, 2009 (letzter Zugriff: 03.03.2009). Elektronische Quelle URL: `http://www.dfn.de/fileadmin/3Beratung/Betriebstagungen/bt50/plenum-xwin-hma.pdf`.

[Aga08] *AGAVE Homepage*, 2008 (letzter Zugriff: 29.11.2008). Elektronische Quelle URL: `http://www.ist-agave.org/`.

[AH93] ALTER, C. und J. HAGE: *Organizations Working Together*. Sage Library of Social Research 191. Sage, Newbury Park, London, New Delhi, 1993.

[AMA+99] AWDUCHE, D., J. MALCOLM, J. AGOGBUA, M. O'DELL und J. MCMANUS: *RFC 2702: Requirements for Traffic Engineering Over MPLS*. RFC 2702, IETF, 1999.

[AMT07] ANDERSSON, L., I. MINEI und B. THOMAS: *RFC 5036: LDP Specification*. RFC 5036, IETF, 2007.

[Aut08] *Bandwidth on Demand with AutoBAHN*, 2008 (letzter Zugriff: 04.03.2008). Elektronische Quelle URL: `http://www.geant2.net/server/show/ConWebDoc.2544`.

[BBC+98] BLAKE, S., D. BLACK, M. CARLSON, E. DAVIES, Z. WANG und W. WEISS: *RFC 2475: An Architecture for Differentiated Services.* RFC 2475, IETF, 1998.

[BCS94] BRADEN, R., D. CLARK und S. SHENKER: *RFC 1633: Integrated Services in the Internet Architecture: an Overview.* RFC 1633, IETF, 1994.

[Bel57] BELLMAN, R.: *Dynamic Programming.* Princeton University Press, 1957.

[BFF96] BERNERS-LEE, T., R. FIELDING und H. FRYSTYK: *RFC 1945: Hypertext Transfer Protocol – HTTP/1.0.* RFC 1945, IETF, Mai 1996.

[BFM05] BERNERS-LEE, T., R. FIELDING und L. MASINTER: *RFC 3986: Uniform Resource Identifier (URI): Generic Syntax.* RFC 3986, IETF, 2005.

[BGSS06] BRENNER, M., M. GARSCHHAMMER, M. SAILER und T. SCHAAF: *CMDB - Yet another MIB? On Reusing Management Model Concepts in ITIL Configuration Management.* In: *DSOM 2006*, LNCS 4269, Seiten 269–280. Springer, 2006.

[BK04] BLECKER, THORSTEN und BERND KALUZA: *Heterarchische Hierarchie: Ein Organisationsprinzip flexibler Produktionssysteme.* Technischer Bericht, Institut für Wirtschaftswissenschaften der Universität Klagenfurt, 2004.

[Ble07] BLECHAR, MIKE: *Magic Quadrant for Business Process Analysis Tools.* Technischer Bericht, Gartner Group, 2007.

[BMM94] BERNERS-LEE, T., L. MASINTER und M. MCCAHILL: *RFC 1738: Uniform Resource Locators (URL).* RFC 1738, IETF, 1994.

[BMM05] BOS, ERIK-JAN, EDOARDO MARTELLI und PAOLO MORONI: *LHC Tier-0 to Tier-1 High-Level Network Architecture.* Technischer Bericht, CERN, 2005.

[Bou09] BOURSAS, LATIFA: *TrustBased Access Control in Federated Environments.* Doctoral Thesis, Ludwids-Maximilians-Universität, 2009.

[BPGO+05] BELA, B., C. PINART, J. GONZALES ORDAS, J. JIMENEZ, P. DEMEESTER, K. CASIER, R. THEILLAUD, V. PIPERAUD und D. PAPADIMITRIOU: *An Experience on Implementing Network Managementfor a GMPLS Network.* 2005.

[Bro08] BROCKNERS, FRANK: *Ethernet OAM Overview: Making Ethernet Manageable.* In: MÜLLER, PAUL, BERNHARD NEUMAIR und GABI DREO RODOSEK (Herausgeber): *Erstes DFN-Forum Kommunikationstechnologien - Verteilte Systeme im Wissenschaftsbereich. Beiträge der Fachtagung 28. Mai bis 29. Mai 2008, Kaiserslautern*, Seiten 35–44. GI-Verlag, Bonn, 2008.

[BS94] BJERRING, L.H. und J.M. SCHNEIDER: *End-to-end Service Management with Multiple Providers.* In: KUGLER, H.-J., A. MULLERY und N. NIEBERT (Herausgeber): *Towards a Pan-European Telecommunication Service Infrastructure - IS&N '94*, Band 851 der Reihe *LNCS*, Seiten 303–318. Springer, Berlin u.a., 1994.

[BSC01] BHOJ, P., S. SINGHAL und S. CHUTANI: *SLA Management in Federated Environments.* Computer Networks, 35(1):5–24, 2001.

[BSS09] BRENNER, MICHAEL, THOMAS SCHAAF und ALEXANDER SCHERER: *An Information Model for IT Service Management Processes.* In: *Making Management Scalable, Robust, Cost-Effective and Revenue-Generating (Proceedings of the 11th IFIP/IEEE Symposium of Integrated Network Management).* New York, 2009.

[BZB+97] BRADEN, R., L. ZHANG, S. BERSON, S. HERZOG und S. JAMIN: *RFC 2205: Resource ReSerVation Protocol (RSVP).* RFC 2205, IETF, 1997.

[CCS96] CASTINEYRA, I., N. CHIAPPA und M. STEENSTRUP: *RFC 1992: The Nimrod Routing Architecture.* RFC 1992, IETF, 1996.

[CHS+08] CESARONI, GIOVANNI, MATTHIAS K. HAMM, FRANCK SIMON, GLORIA VUAGNIN, MARK YAMPOLSKIY, MACIEJ LABEDZKI und MARCIN WOLSKI: *I-SHARe: Prototype Specification.* Technischer Bericht, Géant2, 2008.

[CIO08a] *IT-Beauftragter der Bundesregierung, Homepage*, 2009 (letzter Zugriff: 19.11.2008). Elektronische Quelle URL: `http://www.cio.bund.de/`.

[CIO08b] *Vertragstypen zur Beschaffung von IT für die öffentliche Hand*, 2009 (letzter Zugriff: 19.11.2008). Elektronische Quelle URL: `http://www.cio.bund.de/cln_102/DE/IT-Angebot/IT-Beschaffung/it-beschaffung_node.html`.

[Cob08] *CobiT (Control Objectives for Information and Related Technology) 4.1*, 2007 (letzter Zugriff: 25.04.2008). Elektronische Quelle URL: `http://www.isaca.org/Template.cfm?Section=COBIT6&Template=/TaggedPage/TaggedPageDisplay.cfm&TPLID=55&ContentID=31519`.

[CRE+07] CHEVERS, JOHN, DALE ROBERTSON, MICHAEL ENRICO, MARIAN GARCIA-VIDONDO und XAVIER MARTIN-RIVAS: *Deliverable DN3.0.5: Processes and Provisioning of Point-to-Point Services in GÉANT2.* Technischer Bericht DN 3.0.5, Géant2, 2007.

[Dan07] DANCIU, VITALIAN: *Application of policy-based techniques to process-oriented IT service management.* Dissertation, Ludwig-Maximilians-Universität München, 2007.

[DCN08] *DCN Homepage*, 2008 (letzter Zugriff: 04.03.2008). Elektronische Quelle URL: `http://www.internet2.edu/network/dc/`.

[DCN09] *How to Connect: Internet2's Dynamic Circuit Network*, 2009 (letzter Zugriff: 12.09.2009). Elektronische Quelle URL: `http://www.internet2.edu/pubs/DCN-howto.pdf`.

[DEI08a] *DEISA Homepage*, 2007 (letzter Zugriff: 18.06.2008). Elektronische Quelle URL: `http://www.deisa.eu/`.

[Dei08b] *DEISA Homepage*, 2008 (letzter Zugriff: 13.03.2008). Elektronische Quelle URL: `http://www.deisa.eu/organisation/network_operation.php`.

[DH95] DEERING, S. und R. HINDEN: *RFC 1883: Internet Protocol, Version 6 (IPv6)*. RFC 1883, IETF, 1995.

[DH98] DEERING, S. und R. HINDEN: *RFC 2460: Internet Protocol, Version 6 (IPv6)*. RFC 2460, IETF, 1998.

[Dij59] DIJKSTRA, E. W.: *A note on two problems in connexion with graphs*. Numerische Mathematik, 1:269271, 1959.

[DLRRS08] DOUVILLE, R., J.-L. LE ROUX, J.-L. ROUGIER und S. SECCI: *A service plane over the PCE architecture for automatic multidomain connection-oriented services*. Communications Magazine, IEEE, 46:94–102, 2008.

[DMHH+08] DE MARINIS, ELEONORA, MATTHIAS HAMM, ANDREAS HANEMANN, GLORIA VUAGNIN, MARK YAMPOLSKIY, GIOVANNI CESARONI und STELLA-MARIA THOMAS: *Deliverable DS3.16.1v8: Use Cases and Requirements Analysis for I-SHARe*. Technischer Bericht, Géant2, 2008.

[DR02] DREO RODOSEK, G.: *A Framework for IT Service Management*. Habilitationsschrift, Ludwigs-Maximilians-Universität, 2002.

[DRA08] *DRAGON Homepage*, 2008 (letzter Zugriff: 25.02.2008). Elektronische Quelle URL: `http://dragon.maxgigapop.net/`.

[DvGIF02] DAIGLE, L., D.W. VAN GULIK, R. IANNELLA und P. FALTSTROM: *RFC 3406: Uniform Resource Names (URN) Namespace Definition Mechanisms*. RFC 3406, IETF, 2002.

[E2E09] *Geant2 E2Emon Entwicklerinstallation*, 2009 (letzter Zugriff: 23.07.2009). Elektronische Quelle URL: `http://cnmdev.lrz-muenchen.de/e2e/lhc/`.

[EGE08] EGEE: *Operational Interface between EGEE and Geant/NRENs*. Elektronische Quelle URL: `https://edms.cern.ch/file/565449/3/EGEE-MSA2.3-565449-v3.0.pdf`, 2006 (letzter Zugriff: 12.04.2008).

[EGE09] EGEE: *EGEE SA2 - Networking Support.* Elektronische Quelle URL: http://press.eu-egee.org/fileadmin/documents/infosheets_egee3/infosheet_SA2.pdf, 2008 (letzter Zugriff: 29.03.2009).

[FGM+99] FIELDING, R., J. GETTYS, J. MOGUL, H. FRYSTYK, L. MASINTER, P. LEACH und T. BERNERS-LEE: *RFC 2616: Hypertext Transfer Protocol – HTTP/1.1.* RFC 2616, IETF, 1999.

[FT87] FREDMAN, M. L. und R. E. TARJAN: *Fibonacci heaps and their uses in improved network optimization algorithms.* Journal of the ACM, 34:596615, 1987.

[FVA06] FARREL, A., J.-P. VASSEUR und J. ASH: *RFC 4655: A Path Computation Element (PCE)-Based Architecture.* RFC 4655, IETF, 2006.

[GAR08] GARSCHHAMMER, M., R. HAUCK H.-G. HEGERING B. KEMPTER I. RADISIC H. RÖLLE UND H. SCHMIDT: *A CaseDriven Methodology for Applying the MNM Service Model.* IFIP/IEEE, Florence, Italy, April 2002 (letzter Zugriff: 17.02.2008). Elektronische Quelle URL: http://www.mnm-team.org/pub/Publikationen/ghhk02/PDF-Version/ghhk02.pdf.

[Gea09] *Geant2 Homepage*, 2007 (letzter Zugriff: 14.04.2009). Elektronische Quelle URL: http://www.geant2.net/.

[GG] GALIS, ALEX und DAVID GRIFFIN: *A comparison of approached to Multi Domain Connection Management.*

[GHH+01] GARSCHHAMMER, M., R. HAUCK, H.-G. HEGERING, B. KEMPTER, I. RADISIC, H. RÖLLE, H. SCHMIDT, M. LANGER und M. NERB: *Towards generic Service Management Concepts. A Service Model Based Approach*, 2001.

[GHH+02] GARSCHHAMMER, M., R. HAUCK, H.-G. HEGERING, B. KEMPTER, I. RADISIC, H. RÖLLE und H. SCHMIDT: *A Case-Driven Methodology for Applying the MNM Service Model*, 2002.

[GHK+01] GARSCHHAMMER, M., R. HAUCK, B. KEMPTER, I. RADISIC, H. RÖLLE und H. SCHMIDT: *The MNM Service Model - Refined Views on Generic Service Management.* Journal of Communications and Networks, 3(4):297–306, 2001.

[GJ79] GAREY, M. und D.S. JOHNSON: *Computers and Intractability: A Guide to the Theory of NP-Completeness.* W.H. Freeman and Company, 1979.

[Gle09] GLENFIS AG: *ISO/IEC 20000 IT Service Management Standard.* Elektronische Quelle URL: http://www.itil.org/de/itgovernance-itilundcobit/index.php, 2009 (letzter Zugriff: 05.03.2009).

[GLI08a] GLIF: *GLIF: Linking the World with Light*. Elektronische Quelle URL: `http://www.glif.is/publications/info/brochure.pdf`, 2007 (letzter Zugriff: 22.01.2008).

[GLI08b] GLIF: *GLIF Homepage*. Elektronische Quelle URL: `http://www.glif.is/`, 2008 (letzter Zugriff: 25.03.2008).

[Gri08] *GridKa Homepage*, 2008 (letzter Zugriff: 12.03.2008). Elektronische Quelle URL: `http://grid.fzk.de/`.

[Gro07] GROUP, OBJECT MODELLING: *Business Process Modeling Notation (BPMN) Specification, Final Adopted Specification, dtc/06-02-01*, 2006 (letzter Zugriff: 08.02.2007). Elektronische Quelle URL: `http://www.omg.org/cgi-bin/apps/doc?dtc/06-02-01.pdf`.

[Hal96] HALL, JANE: *Management of Telecommunication Systems and Services, Modelling and Implementing TMN-Based Multi-Domain Management*, Band Vol. 1116 der Reihe *Lecture Notes in Computer Science*. Springer, 1996.

[Ham09] HAMM, MATTHIAS: *Eine Methode zur Spezifikation der IT-Service-Managementprozesse Verketteter Dienste*. Doctoral Thesis, Ludwids-Maximilians-Universität, 2009.

[HAN99] HEGERING, H.-G., S. ABECK und B. NEUMAIR: *Integriertes Management vernetzter Systeme. Konzepte, Architekturen und deren betrieblicher Einsatz*. dpunkt, Heidelberg, 1999.

[HAs05] HEILMANN, H., R. ALT und H. ÖSTERLE (Herausgeber): *Virtuelle Organisationen*, Band 242 der Reihe *HMD*. dpunkt, Heidelberg, 2005.

[HGB06] HATEM, RENÉ, ALMAR GIESBERTS und ERIK-JAN BOS: *The Ordering and Fault Resolution Process for Multi-Domain Lightpaths Across Hybrid Networks*. 2006.

[HH09] HUBER, BEATRICE und ERNST HEIRI: *Demarcation Points? Attempt to clarify*. Technischer Bericht, Géant2, 2009.

[HHS+08] HAMM, MATTHIAS, ANDREAS HANEMANN, KARIN SCHAUERHAMMER, KLAUS ULLMANN und MARK YAMPOLSKIY: *Unterstützung von IT Service Management-Prozessen in Multi-Domain-Umgebungen*. In: MÜLLER, PAUL, BERNHARD NEUMAIR und GABI DREO RODOSEK (Herausgeber): *Erstes DFN-Forum Kommunikationstechnologien - Verteilte Systeme im Wissenschaftsbereich. Beiträge der Fachtagung 28. Mai bis 29. Mai 2008, Kaiserslautern*, Seiten 23–32. GI-Verlag, Bonn, 2008.

[HK09] HOMMEL, WOLFGANG und SILVIA KNITTL: *Zielorientierte Datenmodellierung für ITIL-basierte inter-organisationale Configuration Management Databases.* In: *9. Internationale Tagung Wirtschaftsinformatik*, Wien, Österreich, 2009.

[HMY08] HAMM, MATTHIAS, PATRICIA MARCU und MARK YAMPOLSKIY: *Beyond Hierarchy: Towards a Service Model supporting new Sourcing Strategies for IT Services.* In: *Proceedings of the 2008 Workshop of HP Software University Association (HP-SUA)*, Marrakesch, Marokko, 2008. Infonomics-Consulting.

[Hom07] HOMMEL, WOLFGANG: *Architektur- und Werkzeugkonzepte für föderiertes Identitäts-Management.* Doctoral Thesis, Ludwids-Maximilians-Universität, 2007.

[Hua08] HUANG, JENNY: *eTOM and ITIL: Should you be Bi-lingual as an IT Outsourcing Service Provider?*, January 2005 2005 (letzter Zugriff: 27.04.2008). Elektronische Quelle URL: `www.bptrends.com`.

[HY08a] HAMM, M. und M. (DFN) YAMPOLSKIY: *IT Service Management verketteter Dienste in MultiDomain Umgebungen.* PIK, (31(2)), 2008.

[HY08b] HAMM, MATTHIAS K. und MARK YAMPOLSKIY: *E2E Link Monitoring: System Design and Documentation.* Technischer Bericht, Géant2, 2008.

[ISO05a] ISO/IEC: *International Standard ISO/IEC 20000-1:2005(E). Part 1: Specification.* Genf, 2005.

[ISO05b] ISO/IEC: *International Standard ISO/IEC 20000-1:2005(E). Part 2: Code of Practice.* Genf, 2005.

[ITG07] ITGI (IT GOVERNANCE INSTITUTE): *Control Objectives for Information and related Technology, Version 4.1.* ITGI, Rolling Meadows, 2007.

[ITI04] *ITIL Managing IT services. Service Delivery.* Technischer Bericht 03.08.2007, Office of Government Commerce, 2004.

[ITI08] *ITIL Homepage*, 2008 (letzter Zugriff: 30.09.2008). Elektronische Quelle URL: `http://www.itil-officialsite.com/`.

[ITU93] ITU-T: *Q.700: Specifications of Signalling System No. 7.* ITU-T Recommendation, 1993.

[ITU94a] ITU-T: *X.200: Information technology - Open Systems Interconnection - Basic Reference Model: The basic model.* ITU-T Recommendation, 1994.

[ITU94b] ITU-T: *X.680: OSI Networking and System Aspects - Abstract Syntax Notation One (ASN.1).* ITU-T Recommendation, 1994.

[ITU96] ITU-T: *Q.703: Specifications of Signalling System No. 7 – Message transfer part.* ITU–T Recommendation, 1996.

[ITU00] ITU-T: *G.805: Generic functional architecture of transport networks.* ITU–T Recommendation, 2000.

[ITU01] ITU-T: *G.872: Architecture of optical transport networks.* ITU–T Recommendation, 2001.

[ITU03a] ITU-T: *G.7041/Y.1303: The Generic Framing Procedure (GFP).* ITU–T Recommendation, 2003.

[ITU03b] ITU-T: *G.709: Interfaces for the Optical Transport Network (OTN).* ITU–T Recommendation, 2003.

[ITU03c] ITU-T: *G.809: Functional architecture of connectionless layer networks.* ITU–T Recommendation, 2003.

[ITU04] ITU-T: *G.7042/Y.1305: Link capacity adjustment scheme (LCAS) for virtual concatenated signals.* ITU–T Recommendation, 2004.

[ITU05] ITU-T: *E.164: The international public telecommunication numbering plan.* ITU–T Recommendation, 2005.

[ITU06] ITU-T: *G.8080/Y.1304: Architecture for the automatically switched optical network (ASON).* ITU–T Recommendation, 2006.

[Jaf84] JAFFE, J.: *Algorithms for finding path with multiple constraints.* Networks, 14:95–116, 1984.

[Khu06] KHURRAM, K. (Herausgeber): *Optical Networking Standards.* Springer, Berlin, 2006.

[Kie03] KIEPUSZEWSKI, B.: *Expressiveness and Suitability of Languages for Control Flow Modelling in Workflows.* Doktorarbeit, Queensland University of Technology, 2003.

[KKS04] KLEIN, RALF, FLORIAN KUPSCH und AUGUST-WILHELM SCHEER: *Modellierung inter-organisationaler Prozesse mit Ereignisgesteuerten Prozessketten.* Veröffentlichungen des Instituts für Wirtschaftsinformatik, Heft 178, Inititut für Wirtschaftsinformatik, 2004.

[KMRS08] KRAUSS, P., MYSID, RJGODOY und SURACHIT: *WikipediA Homepage: URI*, 2007 (letzter Zugriff: 20.11.2008). Elektronische Quelle URL: `http://en.wikipedia.org/wiki/Image:Domain_name_space.svg`.

[Kno05] KNOBLOCH, J.: *LHC Computing Grid. Technical Design Report.* Technischer Bericht CERN-LHCC-2005-024, CERN, 2005.

[KNS92] KELLER, G., MARKUS NÜTTGENS und AUGUST-WILHELM SCHEER: *Semantische Prozessmodellierung auf der Grundlage "Ereignisgesteuerter Prozeßketten (EPK)".* Veröffentlichungen des Instituts für Wirtschaftsinformatik, Heft 89, Inititut für Wirtschaftsinformatik, 1992.

[KR88] KERNIGHAN, B. und D. RITCHIE: *The C Programming Language (2nd ed.).* Prentice Hall, 1988.

[KtHvdA03] KIEPUSZEWSKI, B., ARTHUR H.M. TER HOFSTEDE und WIL M.P. VAN DER AALST: *Fundamentals of Control Flow in Workflows.* Acta Informatica, 39(3):143–209, 2003.

[Kui04] KUIPERS, F. A.: *Quality Of Service Routing In The Internet: Theory, Complexity and Algorithms.* Dissertation, Technische Universität Delft, 2004.

[Lan01] LANGER, M.: *Konzeption und Anwendung einer Customer Service Management Architektur.* Dissertation, Technische Universität, 2001.

[LCG09] *LCG Homepage*, 2007 (letzter Zugriff: 11.05.2009). Elektronische Quelle URL: `http://lcg.web.cern.ch/LCG/`.

[LHC] LHC COMPUTING GRID: *Memorandum of Understanding for Collaboration in the Deployment and Exploitation of the Worldwide LHC Computing Grid.*

[LHC08a] *LHC Homepage*, 2007 (letzter Zugriff: 06.03.2008). Elektronische Quelle URL: `http://lhc.web.cern.ch/lhc/`.

[LHC08b] *LHC Homepage*, 2007 (letzter Zugriff: 12.03.2008). Elektronische Quelle URL: `http://lhc-machine-outreach.web.cern.ch/lhc-machine-outreach/components/lhc-manufacturing.htm`.

[LHH05] LI, YUXI, J. HARMS und R. HOLTE: *IDA*_MCSP: a fast exact MCSP algorithm.* Communications, 2005. ICC 2005. 2005 IEEE International Conference on, 1:93– 99, 2005.

[Liv08] *Paul Baran Invents Packet Switching.* `http://www.livinginternet.com/i/ii_rand.htm`, 2000 (letzter Zugriff: 09.11.2008).

[LN07] LANGER, M. und M. NERB: *Onlineordering of endtoend connectivity services over the internet*, Juni, 2000 2000 (letzter Zugriff: 02.05.2007). Elektronische Quelle URL: `http://www.hpovua.org/PUBLICATIONS/PROCEEDINGS/7_HPOVUAWS/papers/session4-1.pdf`.

[LTM+] LEWIS, D., T. TIROPANIS, A. MCEWAN, C. REDMOND, V. WADE und R. BRACHT: *Experiences in Integrated Multi-Domain Service Management.*

[LYG+07] LEHMAN, T., XI YANG, C.P. GUOK, N.S.V. RAO, A. LAKE, J. VOLLBRECHT und N. GHANI: *Control Plane Architecture and Design Considerations for Multi-Service, Multi-Layer, Multi-Domain Hybrid Networks.* High-Speed Networks Workshop, Seiten 67–71, 2007.

[McC45] MCCULLOCH, WARREN S.: *A Heterarchy of Values determined by the Topology of Nervous Nets.* Bull. Math. Biophysics, 7:89–93, 1945.

[MES08] *MESCAL Homepage*, 2008 (letzter Zugriff: 29.11.2008). Elektronische Quelle URL: `http://www.mescal.org/`.

[Mey02] MEYER, M.: *Kommunikationstechnik: Konzepte der modernen Nachrichtenübertragung.* Vieweg+Teubner, 2002.

[Mey08] MEYNELL, KEVIN: *GLIF Overview. Presentation at CLARA Meeting, Quito, Ecuador.* Elektronische Quelle URL: `http://www.glif.is/publications/presentations/20060725KM_CLARA.ppt`, 2006 (letzter Zugriff: 25.03.2008).

[MGL+09] MARCU, PATRICIA, GENADY GRABARNIK, LAURA LUAN, DANIELA ROSU, LARISA SHWARTZ und CHRIS WARD: *Towards an Optimized Model of Incident Ticket Correlation.* In: *In Making Management Scalable, Robust, Cost-Effective and Revenue-Generating (Proceedings of the 11th IFIP/IEEE Symposium of Integrated Network Management).* New York, 2009.

[Moc87a] MOCKAPETRIS, P.: *Domain Names - Concepts and Facilities.* Technischer Bericht RFC-1034, IETF, 1987.

[Moc87b] MOCKAPETRIS, P.: *Domain Names - Implementation and Specification.* Technischer Bericht RFC-1035, IETF, 1987.

[Moc87c] MOCKAPETRIS, P.: *RFC 1034: DOMAIN NAMES - CONCEPTS AND FACILITIES.* RFC 1034, IETF, 1987.

[Moc87d] MOCKAPETRIS, P.: *RFC 1035: DOMAIN NAMES - IMPLEMENTATION AND SPECIFICATION.* RFC 1035, IETF, 1987.

[MOF08] *MOF (Microsoft Operations Framework) 4.0*, 2008 (letzter Zugriff: 25.04.2008). Elektronische Quelle URL: `http://technet.microsoft.com/en-us/library/cc506049.aspx`.

[Moy98] MOY, J.: *OSPF Version 2.* Technischer Bericht RFC-2328, IETF, 1998.

[MSC05] MCFARLAND, M., S. SALAM und R. CHECKER: *Ethernet OAM: key enabler for carrier class metro ethernet services.* Communications Magazine, IEEE, 43:152–157, 2005.

[MvdA05] MULYAR, N.A. und WIL M.P. VAN DER AALST: *Patterns in Colored Petri Nets.* Technischer Bericht, Eindhoven University of Technology, 2005.

[NBBB98] NICHOLS, K., S. BLAKE, F. BAKER und D. BLACK: *RFC 2474: Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers*. RFC 2474, IETF, 1998.

[Ner01] NERB, M.: *Customer Service Management als Basis für interorganisationales Dienstmanagement*. Dissertation, Technische Universität, 2001.

[NM08] NIEDERBERGER, R. und O. (FZJ) MEXTORF: *The DEISA project Network operation and support first experiences*. TERENA, (13.03.2008), 2005 (letzter Zugriff: 13.03.2008). Elektronische Quelle URL: `http://tnc2005.terena.org/programme/presentations/show.php?pres_id=98`.

[OAS07] OASIS: *Web Services Business Process Execution Language Version 2.0*. Elektronische Quelle URL: `http://docs.oasis-open.org/wsbpel/2.0/wsbpel-v2.0.pdf`, 2007 (letzter Zugriff: 02.07.2007).

[Obe96] OBERWEIS, ANDREAS: *Modellierung und Ausführung von Workflows mit Petri-Netzen*. Teubner, Stuttagrt, Leipzig, 1996.

[ODvdATH08] OUYANG, CHUN, MARLON DUMAS, WIL M.P. VAN DER AALST und A. H.M. TER HOFSTEDE: *From Business Process Models to Process-oriented Software Systems: The BPMN to BPEL Way*, 2006 (letzter Zugriff: 24.09.2008).

[Off00] OFFICE OF GOVERNMENT COMMERCE (Herausgeber): *Service Support*. TSO, Norwich, GB, 2000.

[Off01] OFFICE OF GOVERNMENT COMMERCE (Herausgeber): *Service Delivery*. TSO, Norwich, GB, 2001.

[Off04a] OFFICE OF GOVERNMENT COMMERCE (Herausgeber): *Business Perspective: The IS View on Delivering Services to the Business*. TSO, Norwich, GB, 2004.

[Off04b] OFFICE OF GOVERNMENT COMMERCE (Herausgeber): *Software Asset Management*. TSO, Norwich, GB, 2004.

[Off07a] OFFICE OF GOVERNMENT COMMERCE: *ITIL Service Design*. TSO, London, 2007.

[Off07b] OFFICE OF GOVERNMENT COMMERCE: *ITIL Service Operation*. TSO, London, 2007.

[Off07c] OFFICE OF GOVERNMENT COMMERCE: *ITIL Service Strategy*. TSO, London, 2007.

[Off07d] OFFICE OF GOVERNMENT COMMERCE: *ITIL The Business Perspective, Volume 1*. TSO, London, 2007.

[OMG07a] OMG (OBJECT MANAGEMENT GROUP): *Unified Modeling Language: Infrastructure*. Elektronische Quelle URL: `http://www.omg.org/cgi-bin/doc?formal/07-02-06`, 2007 (letzter Zugriff: 18.12.2007).

[OMG07b] OMG (OBJECT MANAGEMENT GROUP): *Unified Modeling Language: Superstructure*. Elektronische Quelle URL: `http://www.omg.org/cgi-bin/doc?formal/07-02-05`, 2007 (letzter Zugriff: 18.12.2007).

[OMG09] OMG (OBJECT MANAGEMENT GROUP): *Business Process Modeling Notation (BPMN) Specification, Version 1.2*. Elektronische Quelle URL: `http://www.omg.org/spec/BPMN/1.2/PDF`, 2008 (letzter Zugriff: 08.01.2009).

[OSC08] *OSCRAS Homepage*, 2008 (letzter Zugriff: 04.03.2008). Elektronische Quelle URL: `http://www.es.net/oscars/`.

[Pav07] PAVLOU, G.: *IM2007 Workshop: Traffic Engineering and Quality of Service Management for IP-based Next Generation Networks*, May 2007.

[PB00] PERELSON, STEPHEN und REINHARDT A. BOTHA: *Conflict analysis as a means of enforcing static separation of duty requirements in workflow environments*. South African Computer Journal, 26:212–216, 2000.

[PK99] PETKE, R. und I. KING: *RFC 2717: Uniform Resource Identifier (URI): Generic Syntax*. RFC 2717, IETF, 1999.

[Poh71] POHL, I.: *Bi-directional Search*. Machine Intelligence, 6:127–140, 1971.

[Pos81] POSTEL, J.: *RFC 1981:Internet Protocol*. RFC 791, IAB, September 1981.

[PRI08] *PRINCE (Projects in Controlled Environments)*, 1996 (letzter Zugriff: 25.04.2008). Elektronische Quelle URL: `http://www.ogc.gov.uk/methods_prince_2.asp`.

[pSH09] *perfSONAR Homepage, Protocols and Messages*, 2009 (letzter Zugriff: 21.10.2009). Elektronische Quelle URL: `http://www.perfsonar.net/protocols.html`.

[Rei98] REIHLEN, MARKUS: *Die Heterarchie als postbürokratisches Organisationsmodell der Zukunft*. Technischer Bericht, Universität Köln, 1998.

[Res00] RESCORLA, E.: *RFC 2818: HTTP Over TLS*. RFC 2818, IETF, Mai 2000.

[RM90] ROSE, M. und K. MCCLOGHRIE: *RFC 1155: Structure and Identification of Management Information for TCP/IP-based Internets*. RFC 1155, IETF, Mai 1990.

[Rod08] RODWELL, TOBY: *The End-to-End Coordination Unit (E2ECU) and EGEE Network Operations Centre (ENOC). TERENA NRENs&Grids Workshop.* Elektronische Quelle URL: `http://www.terena.org/activities/nrens-n-grids/workshop-04/slides/rodwell-nrens-n-Grids-ENOC-e2ecu.pdf`, 2006 (letzter Zugriff: 15.04.08).

[RTF+01] ROSEN, E., D. TAPPAN, G. FEDORKOW, Y. REKHTER, D. FARINACCI, T. LI und A. CONTA: *RFC 3032: MPLS Label Stack Encoding.* RFC 3032, IETF, 2001.

[RVC01] ROSEN, E., A. VISWANATHAN und R. CALLON: *RFC 3031: Multiprotocol Label Switching Architecture.* RFC 3031, IETF, 2001.

[Sai05] SAILER, M.: *Towards a Service Management Information Base*, Dezember, 2005 2005.

[Sas08a] *Computer Science Tutorials and Applets, 2.2 Complexity of BFS.* `http://www.cs.usask.ca/content/resources/tutorials/csconcepts/1998_3/BFS/2-2.html`, 2009 (letzter Zugriff: 23.11.2008).

[Sas08b] *Computer Science Tutorials and Applets, 2.2 Complexity of DFS.* `http://www.cs.usask.ca/content/resources/tutorials/csconcepts/1998_3/DFS/2-2.html`, 2009 (letzter Zugriff: 23.11.2008).

[Sch07a] SCHAUERHAMMER, KARIN: *X-WiN als Netzressource im Grid.* DFN Mitteilungen, 69(Dezember):16–19, 2005 (letzter Zugriff: 23.09.2007). Elektronische Quelle URL: `http://www.dfn.de/fileadmin/5Presse/DFNMitteilungen/heft69.pdf`.

[Sch07b] SCHIFFERS, MICHAEL: *Management dynamischer Virtueller Organisationen in Grids.* Doctoral Thesis, Ludwids-Maximilians-Universität, 2007.

[Sch08] SCHUMM, DAVID: *Graphische Modellierung von BPEL Prozessen unter Verwendung der BPMN Notation.* Diplomarbeit, Universität Stuttgart, 2008.

[SH06] STILLER, B. und D. HAUSHEER: *State-of-the-Art in Economic Management of Internet Services.* 2006.

[SHS04] SAILER, M., A. HANEMANN und D. SCHMITZ: *Variety of QoS - the MNM Service Model Applied to Web Hosting Services*, 2004.

[Sig07] *Signaling System 7 (SS7), 2. What is Out-of-Band Signaling?* `http://www.iec.org/online/tutorials/ss7/topic02.asp`, 2009 (letzter Zugriff: 23.10.2007).

[SPG97] SHENKER, S., C. PARTRIDGE und R. GUERIN: *RFC 2212: Specification of Guaranteed Quality of Service.* RFC 2212, IETF, 1997.

[SRP08] SECCI, S., J.-L. ROUGIER und A. PATTAVINA: *On the selection of optimal diverse AS-paths for inter-domain IP/(G)MPLS tunnel provisioning*. Telecommunication Networking Workshop on QoS in Multiservice IP Networks, 2008. IT-NEWS 2008. 4th International, Seiten 235–241, 2008.

[Ste93] STEVENSON, D.: *Electropolitical Correctness and High-Speed Networking, or, Why ATM is like a Nose*. April 1993.

[Ste00] STEINMETZ, R.: *Multimedia-Technologie. Grundlagen, Komponenten und Systeme*. Springer, 2000.

[Str00] STROUSTRUP, B.: *The C++ Programming Language (3rd ed.)*. Addison-Wesley, 2000.

[SW94] SYDOW, J. und A. WINDELER: *Management interorganisationaler Beziehungen. Vertrauen, Kontrolle und Informationstechnik*. Westdeutscher Verlag, 1994.

[SW97] SHENKER, S. und J. WROCLAWSKI: *RFC 2215: General Characterization Parameters for Integrated Service Network Elements*. RFC 2215, IETF, 1997.

[SW06] SCHAUERHAMMER, K. und M. WILHELM: *Fasern ohne Grenzen. Cross-Border-Fibres als Ergänzung der GÉANT-Konnektivität*. DFN Mitteilungen, 71(Dezember):18–19, 2006.

[Swa09] SWANY, MARTIN: *NM-WG/perfSONAR Topology Schema. Presentation at The 21st Open Grid Forum - OGF21, Seattle, Washington*. Technischer Bericht, 2007 (letzter Zugriff: 23.07.2009).

[Tan03] TANENBAUM, ANDREW S.: *Computernetzwerke*, Band 4., überarbeitete Auflage. Pearson Studium, München, 2003.

[Tar72] TARJAN, R.: *Depth-first search and linear graph algorithms*. SIAM Journal on Computing, 1(2):146–160, 1972.

[Tat07] *TAT-14 Cable System Homepage*, 2007 (letzter Zugriff: 14.03.2007). Elektronische Quelle URL: `https://www.tat-14.com/tat14/`.

[Teq08] *TEQUILA Homepage*, 2008 (letzter Zugriff: 29.11.2008). Elektronische Quelle URL: `http://www.ist-tequila.org/`.

[TJ97] TISCHER, M. und B. JENNRICH: *Internet intern, Technik & Programmierung*. DATA BECKER, Düsseldorf, 1997.

[TMF04a] *The NGOSS Technology-Neutral Architecture*. Technischer Bericht TMF 050, Version 3.1, Tele Management Forum, 2004.

[TMF04b] *Shared Information/Data (SID) Model. System View Concepts and Principles*. Technischer Bericht NGOSS Release 4.0, GB926, Version 1.1, Tele Management Forum, August 2004.

[TMF04c] *SLA Management Handbook. Volume 1. Executive Overview.* Technischer Bericht GB917-1, Tele Management Forum, 2004.

[TMF04d] *SLA Management Handbook. Volume 2. Concepts and Principles.* Technischer Bericht GB917-2, Tele Management Forum, 2004.

[TMF04e] *SLA Management Handbook. Volume 3. Service and Technology Examples.* Technischer Bericht GB917-3, Tele Management Forum, 2004.

[TMF04f] *SLA Management Handbook. Volume 4. Enterprise Perspective.* Technischer Bericht GB917-4, Tele Management Forum, 2004.

[TMF05] TMF (TELEMANAGEMENT FORUM): *Shared Information/Data (SID) Model. Addendum U - Using the SID.* Technischer Bericht GB922-1U, Version 6.4, 2005.

[TMF07a] *Enhanced Telecom Operations Map (eTOM). The Business Process Framework.* Technischer Bericht GB921, Tele Management Forum, 2007.

[TMF07b] *Enhanced Telecom Operations Map (eTOM). The Business Process Framework. Addendum B.* Technischer Bericht GB921B, Tele Management Forum, 2007.

[TMF08] TMF (TELEMANAGEMENT FORUM): *Information Framework (SID) – Common, Service, Resource Domains. Performance Business Entitites. Release 8.0.* Technischer Bericht GB922 Addendum 1, Version 1.2, 2008.

[Toe02] TOEMENDAL, M.: *Virtuelle Organisationen am Rand des Chaos.* Strategie- und Informationsmanagement. Rainer Hamp, München, 2002.

[US06] ULLMANN, KLAUS und KARIN SCHAUERHAMMER: *Operational Model for E2E links in the NREN/GÉANT2 and NREN/Cross-Border-Fibre supplied optical platform.* Technischer Bericht, Géant2, 2006.

[vdA00] AALST, WIL M.P. VAN DER: *Loosely Coupled Interorganizational Workflows: modeling and analyzing workflows crossing organizational boundaries.* Information and Management, 37(2):67–75, 2000.

[vdAtH04] AALST, WIL M.P. VAN DER und ARTHUR H.M. TER HOFSTEDE: *Design and Implementation of the YAWL System.* In: PERSSON, A. und J. STIRNA (Herausgeber): *Proceedings of the 16th International Conference on Advanced Information Systems Engineering (CAiSE'04)*, Band 3084 der Reihe *Lecture Notes in Computer Science*. Springer, Berlin, 2004.

[vdAtH05] AALST, WIL M.P. VAN DER und ARTHUR H.M. TER HOFSTEDE: *YAWL: Yet Another Workflow Language.* Information Systems, 30(4):245–275, 2005.

[vdAW01] AALST, WIL M.P. VAN DER und M. WESKE: *The P2P approach to Interorganizational Workflows.* In: *Proceedings of the 13th International Conference on Advanced Information Systems Engineering (CAiSE'01)*, Lecture Notes in Computer Science, Vol. 2068, Seiten 140–156. Springer, Berlin, 2001.

[vdHDGdLP09] HAM, JEROEN VAN DER, FREEK DIJKSTRA, PAOLA GROSSO und CEES DE LAAT POSTER: *Pathfinding with Aggregated Topologies.* Terena Networking Conference 2009, 2009.

[WfM09] WFMC (WORKFLOW MANAGEMENT COALITION): *Workflow Management Coalition Workflow Standard. Process Definition Interface – XML Process Definition Language.* Technischer Bericht WFMC-TC-1025, Version 2.1.a, 2009.

[WIK08] *WikipediA Homepage: DNS*, 2008v(letzter Zugriff: 18.11.2008). Elektronische Quelle URL: `http://en.wikipedia.org/wiki/Image:Domain_name_space.svg`.

[WN98] WINAND, U. und K. NATHUSIUS (Herausgeber): *Unternehmungsnetzwerke und virtuelle Organisationen.* Schäffer-Poeschel, Stuttgart, 1998.

[WvdADtH07] WOHED, PETIA, WIL M.P. VAN DER AALST, MARLON DUMAS und ARTHUR H.M. TER HOFSTEDE: *Analysis of Web Services Composition Languages: The Case of BPEL4WS*, October 2003 2003 (letzter Zugriff: 08.11.2007). Elektronische Quelle URL: `http://citeseer.ist.psu.edu/cache/papers/cs/32128/http:zSzzSztmitwww.tm.tue.nlzSzresearchzSzpatternszSzdownloadzSzbpel_er.pdf/analysis-of-web-services.pdf`.

[YH07] YAMPOLSKIY, M. und M. HAMM: *Management of Multidomain End-to-End Links. A Federated Approach for the Pan-European Research Network Géant 2.* In: *Moving from Bits to Business Value: Proceedings of the 2007 Integrated Management Symposium (to appear).* IFIP/IEEE, München, Germany, May 2007.

[YLT+06] YANG, XI, T. LEHMAN, C. TRACY, J. SOBIESKI, SHUJIA GONG, P. TORAB und B. JABBARI: *Policy-Based Resource Management and Service Provisioning in GMPLS Networks.* Proceedings of the 25th IEEE International Conference on Computer Communications (INFOCOM 2006), Seiten 1–12, 2006.

[Zie01] ZIEGELMANN, M.: *Constrained Shortest Paths and Related Problems: Constrained Network Optimization.* Dissertation, Naturwissenschaftlich-Technischen Fakultät I der Universität des Saarlandes, 2001.

Index

A

D

E

F

G

H

I

K

M

N

O

P

R

S

U

V