



G-Lab Phase 1

Studien und Experimentalplattform für das Internet der Zukunft

Projektkoordinator:

Universität Würzburg (Prof. Dr. Phuoc Tran-Gia)

Projektpartner:

TU Berlin (Prof. Dr. Anja Feldmann)

TU Darmstadt (Prof. Dr. Ralf Steinmetz)

TU München (Prof. Dr. Jörg Eberspächer)

Universität Karlsruhe (TH) (Prof. Dr. Martina Zitterbart)

TU Kaiserslautern (Prof. Dr. Paul Müller, Prof. Dr. Hans Schotten)

Kurzfassung

Das heutige Internet besitzt eine große wirtschaftliche Bedeutung, basiert jedoch größtenteils noch auf Mechanismen und Algorithmen, die in den 70er und 80er Jahren entwickelt wurden. Neue Anwendungen im geschäftlichen und privaten Bereich stellen Anforderungen, für die das Internet ursprünglich nicht konzipiert war und sehen sich Sicherheitsproblemen gegenüber, die auf Defizite in der Architektur des Internet hinweisen. Von besonderem Interesse ist dabei das Wechselspiel zwischen den Möglichkeiten der Technik und den Anforderungen der Applikationen. Dies wird bei Untersuchungen im Rahmen der Studien in G-Lab explizit mit betrachtet. Mit mathematischen Analysen und computergestützten Simulationen alleine ist die Erforschung und Entwicklung von neuen Architekturen, Protokollen und vor allem Diensten nicht mehr zu bewältigen. Neue Ideen, die zunächst im theoretischen Umfeld entwickelt werden, müssen vielmehr zusätzlich in einer realistischen Umgebung im praktischen Einsatz getestet werden. Um bei diesen Entwicklungen (vgl. die amerikanischen Initiativen FIND und GENI) nicht wie beim aktuellen Internet nur eine Mitläufer-Rolle, sondern eine technologisch führende Position einnehmen zu können, ist es für die deutsche Wirtschaft unerlässlich, sich an den weltweiten Bestrebungen zu beteiligen und die Grundlagen für ein zukünftiges Internet mittels geeigneter Studien und Experimentalplattformen aktiv zu erforschen. Nur über frühzeitigen Kompetenzaufbau kann so die Basis für die strategische Definition zukünftiger Standards und die Entwicklung innovativer Produkte geschaffen werden.

Zunächst muss im Rahmen von Studien erforscht werden, welche Anforderungen neue Dienste und Applikationen an das Netzwerk stellen werden. Danach gilt es diese Mechanismen zu entwickeln und erste lokale Untersuchungen in Richtung Machbarkeit, Skalierbarkeit und Leistungsfähigkeit durchzuführen. Um die Funktionalität der vielversprechendsten Ansätze unter möglichst realistischen Bedingungen nachzuweisen, müssen anschließend ausführliche Studien in einer realitätsnahen und modifizierbaren Experimentierplattform durchgeführt werden. Die Ergebnisse liefern dann die Einsicht, wie neue Architekturen gestaltet werden können, um die Vielfalt der existierenden und sich in der Entwicklung befindlichen Dienste bestmöglich unterstützen zu können. In diesem Zusammenhang bieten allerdings weder das Internet, noch bereits existierende Testnetze wie das PlanetLab ausreichende Möglichkeiten, neue Kommunikationsprotokolle sowie neue Architekturen, auf allen Schichten der Kommunikationssysteme und insbesondere auch über Schichten hinweg, zu untersuchen. Nur mit voller Kontrolle über alle Schichten der Testumgebung und der Möglichkeit entsprechende Änderungen an der Hardware vorzunehmen, lassen sich neue Softwarelösungen auch in der Praxis realisieren. Das deutschlandweit angelegte G-Lab geht in seiner Funktionalität über ein einfaches Rechnercluster hinaus und legt besonderen Wert auf die Wechselbeziehung zwischen zukünftigen Netzwerkarchitekturen und der Anwendungsschicht.

Im Laufe der einzelnen Studien bzw. des gesamten Vorhabens wird sich herausstellen, welche Dienste, Komponenten und Funktionen auf welcher Ebene des Netzes bereitgestellt werden müssen. Dazu gehört vor allem die Frage der Ansiedlung des Netzwerkmanagements, aber auch Aspekte wie unterschiedlich starke Sicherheitsmechanismen und Konzepte zur Vertrauensbildung, die einfach durch den Benutzer konfiguriert werden können. Eine weitere Kernfrage besteht darin, ob Eigenschaften wie Robustheit, Verfügbarkeit und Dienstgüte zentral in das Netz integriert werden müssen oder eher verteilt bzw. endsystemorientiert umgesetzt werden können. Nicht zuletzt wird auch die skalierbare Unterstützung von unterschiedlichen mobilen und drahtgebundenen Zugangsnetzen auf einer gemeinsamen Infrastruktur eine wichtige Rolle spielen.

Inhalt

1. Ziele und Bezüge	4
1.1 Gesamtziel des Vorhabens	4
1.2 Wissenschaftliche und technische Arbeitsziele des Vorhabens	6
2. Technische Studien zum Future Internet	7
2.1 Die Arbeitsschwerpunkte	7
ASP0: Koordination und Konsolidierung	8
ASP1: Architekturkonzepte für das Future Internet	8
ASP2: Routing und Adressierung	10
ASP3: Mobilitätsaspekte und drahtlose Netze	12
ASP4: Monitoring- und Managementkonzepte	13
ASP5: Dienstgüteunterstützung und Sicherheitskonzepte	14
ASP6: Dienstarchitekturen und Dienstkomposition	16
ASP7: Experimentalplattform	19

1. Ziele und Bezüge

1.1 Gesamtziel des Projektes G-Lab

Das Gesamtziel von G-Lab ist die Entwicklung und Untersuchung innovativer (inter-) networking Paradigmen. Dies soll sowohl auf Basis inkrementeller, als auch grundlegend neuer Ansätze geschehen, was im Folgenden ausführlich motiviert wird.

Ausgangssituation: Das Internet schwächelt

Das Internet ist mittlerweile zum Rückgrat der modernen Industriegesellschaft und der globalen Wirtschaft gewachsen, und es besitzt eine immense wirtschaftliche Bedeutung. Gleichmaßen steigen die Anforderungen an das Internet immer weiter und man geht heute davon aus, dass über die Vernetzung „traditioneller“ Rechner in Zukunft eine große Anzahl an Alltagsgegenständen über das Internet vernetzt sein werden (Stichwort: Internet der Dinge). Wie das Internet der u.a. daraus resultierenden Vielfalt an unterschiedlichen Anforderungen gerecht werden kann oder ob neue Architekturkonzepte benötigt werden ist heute noch unklar und soll im Rahmen von G-Lab untersucht werden. Geeignete Konzepte und Architekturen sollen entworfen werden und in einer äußerst realitätsnahen Experimentalplattform untersucht werden.

Innovationen sind im Internet heute auf der Applikationsebene stark von „Community“ bezogenen Anwendungen wie Skype, YouTube oder Flickr und anderen interaktiven und nichtlinearen IPTV Diensten geprägt. Unter dem Schlagwort Web 2.0 werden neuere Web-Anwendungen zusammengefasst, die einen hohen Grad an Interaktivität erlauben. Andererseits gewinnen geschäftliche Anwendungen erheblich an Bedeutung (Virtuelle Private Netze, eCommerce u.a.), die vor allem durch hohe Anforderungen an die Ausfallsicherheit gekennzeichnet sind. Auf den unteren Schichten ergeben sich sowohl durch Streaming-Dienste, als auch durch die Integration von drahtlosen Zugängen und durch immer heterogenere Transportnetze deutlich steigende Anforderungen an Bandbreite, Architektur, Mobilität und Unterstützung eines breiten Spektrums an weiteren Dienstanforderungen.

Diesen sich schnell weiterentwickelnden Anforderungen hat die technische Evolution des Internet nicht standhalten können. Zahlreiche Beschränkungen des Internet behindern effiziente Implementierungen neuer Anwendungen und Protokolle vor allem auf den Schichten 3 und 4 bzw. können deren Auf- und Ausbau sogar gänzlich verhindern. Tatsächlich entwickelt sich das Internet schrittweise zu einem „Flickenteppich“, wobei immer öfter die ursprünglichen Architekturprinzipien missachtet werden. Deutlich wird dies unter anderem an dem Infrage stellen des Schichten-Prinzips (cross-layer design). Immer mehr „Zwischenschichten“, wie z.B. MPLS auf Schicht 2,5 werden eingefügt oder auch das Ende-zu-Ende Prinzip wird durch Firewalls, NATs, Proxies, Caches, etc. verletzt. Die Notwendigkeit hierfür folgt aus den gestiegenen Anforderungen der Applikationen. Doch die Veränderungen erfolgen ohne langfristige Planung oder Zielsetzung. Als Konsequenz nimmt die Komplexität des Internet ständig zu, so dass heute Innovationen verhindert und neue Anforderungen nur mit immer größerem Aufwand erfüllt werden können. Bereits die Komplexität der aktuellen Internetarchitektur erfordert einen hohen Konfigurations- und Verwaltungsaufwand, während sie kaum Sicherheit, Dienstgüte, Robustheit und Flexibilität bietet.

Clean Slate versus evolutionäre Weiterentwicklung: Studien und Experimente weisen den Weg

Weltweit sind in den letzten Monaten in allen Hochtechnologieregionen Forschungsprogramme zur Weiterentwicklung des Internet initiiert worden. Hierbei werden sowohl das Transportnetzwerk mit seiner Übertragungstechnik und Architektur, als auch die Protokolle und Service-Enabler kritisch diskutiert. Um das Internet der Zukunft wieder für wirkliche Innovationen zu öffnen, werden dabei zurzeit zwei wesentliche Ansätze diskutiert. Zum einen

sind dies ein evolutionärer und zum anderen ein revolutionärer „clean-slate“ Ansatz. Für beide Ansätze ist es notwendig neue Architekturen, Mechanismen und Techniken zu entwerfen und zu entwickeln, die die oben beschriebenen Nachteile vermeiden, aber zugleich erweiterte Möglichkeiten für neue zukünftige Dienste bieten. In diesem Vorhaben soll daher zum einen versucht werden, die bestehenden Möglichkeiten des Internet auszureizen und zum anderen untersucht werden, ob vollkommen neue Architekturansätze einen Weg in die Zukunft ermöglichen. Dabei muss darauf geachtet werden, dass alle Vorschläge technisch sinnvoll implementierbar sind. Hierbei muss der konzeptionelle Entwurfs-, bzw. Entwicklungsprozess durch eine geeignete Experimentalplattform ergänzt werden, die es erlaubt, theoretische Ergebnisse möglichst früh in einer echt verteilten Umgebung zu testen. Dies ist gegenwärtig nur in engen Grenzen auf der Basis von Simulationen und mathematischen Analysen möglich, wobei naturgemäß stark von realen Gegebenheiten abstrahiert wird. Verlässliche Aussagen über die Eigenschaften neuer Netzarchitekturen und Anwendungen lassen sich daher nur treffen, wenn diese unter praxisnahen Bedingungen eingesetzt wurden. Je realistischer die Umgebung ist, in der Experimente stattfinden können, desto größer ist der Wert der gewonnenen Erfahrungen, da diese wesentlich leichter auf reale Einsatzbedingungen projiziert werden können als rein theoretisch gewonnene Erkenntnisse. Kommunikationssysteme sind zudem prinzipiell verteilte Systeme und müssen daher auch in einer entsprechenden Umgebung, die aus verteilten aber unabhängigen Komponenten besteht, getestet werden.

Für zahlreiche Fragestellungen erlaubt erst ein verzahnter Ansatz aus Experiment und Studien neue Netzkonzepte zu untersuchen, Aspekte der Integration in das bestehende Internet zu beobachten und die Funktion neuer Mechanismen unter realistischen Randbedingungen zu demonstrieren. Diese Schritte sind sowohl für die wissenschaftliche Arbeit, als auch für die Akzeptanz der Ergebnisse in Industrie und Standardisierung und damit für die wirtschaftliche Umsetzbarkeit von hoher Bedeutung. Dies kann durch eine verteilte Struktur mit mehreren Inselsystemen, die anfangs noch durch das traditionelle Internet verbunden sind, später aber „zusammenwachsen“ können, erreicht werden.

Das hier vorgestellte Vorhaben G-Lab hat zum Ziel, den oben begründeten Randbedingungen entsprechend, einen Rahmen für Studien zu Mechanismen, Protokollen und Basistechnologien für das Internet der Zukunft zu schaffen und gleichzeitig eine Experimentalplattform zur Verfügung zu entwickeln und aufzubauen, um ausgewählte Studien in einer realen Umgebung weiterzuführen, zu testen und die Ergebnisse zu demonstrieren.

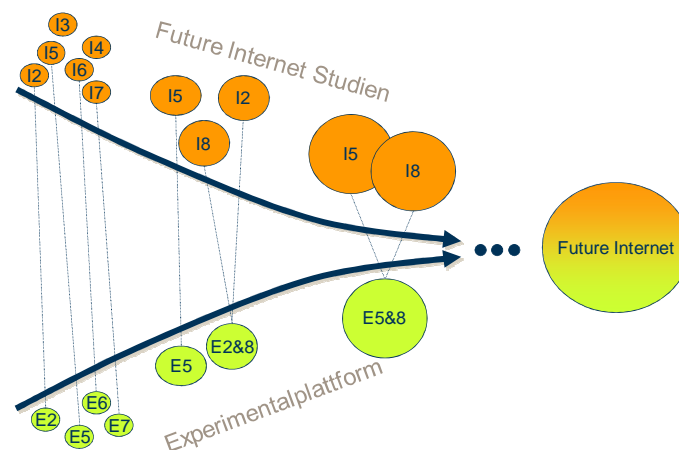


Abbildung 1: G-Lab: Studien und Experimentalplattform

Wie in Abbildung 1 dargestellt ist das Ziel aller im Rahmen von G-Lab durchgeführten konzeptionellen und experimentellen Studien, eine gemeinsame Vision für das zukünftige Internet zu entwickeln. Es ist zu erwarten, dass die Ergebnisse einiger konzeptioneller Studien einer detaillierten Untersuchung im Rahmen der Experimentalplattform bedürfen. Anderer-

seits werden die Ergebnisse der Untersuchungen im Experimentalsystem neue konzeptionelle Fragen aufwerfen, so dass sich ein iterativer Prozess entwickeln wird.

1.2 Wissenschaftliche und technische Arbeitsziele des Vorhabens

Das Ziel des Forschungsvorhabens G-Lab ist die Entwicklung von neuen Mechanismen für das Internet der Zukunft und deren experimentelle Umsetzung in einer Testumgebung. Das Gesamtvorhaben gliedert sich in einen Studienanteil zur theoretischen Untersuchung neuer Konzepte und in den Aufbau einer deutschlandweiten Experimentalplattform, die eine prototypenhafte Umsetzung der Konzepte ermöglicht.

Ausgangspunkt der Arbeiten ist die unbefriedigende Performanz, Sicherheit, Zuverlässigkeit, unzureichende Administrierbarkeit und Inflexibilität des heutigen Internet. Dies betrifft alle Schichten im Sinne des OSI-Referenzmodells.

Als Konsequenz aus dieser Diagnose muss man sich - je nach Funktion - teilweise oder vollständig von heutigen technischen Lösungen der Netzarchitektur lösen und neue Wege gehen. Neue Mechanismen für die Basisfunktionen *wie Adressierung, Routing, Switching, Sicherheit, Netzmanagement* sind in einem möglichst integrativen Gesamtansatz zu konzipieren. Dadurch sollen als Ziele die folgenden Eigenschaften eines künftigen Internet auf effiziente Weise realisierbar sein:

- Hohe Mobilität durch drahtlose Netze („Mobility as the common case“)
- Integration „existierender alter Dienste“ wie Telefonie Verlust an Funktionalität
- Integration von Diensten mit Echtzeit-Anforderungen
- Anbindung neuer Netztechnologien wie z.B. Sensornetze
- Zusammenspiel von Systemen mit höchst heterogenen Ressourcen (von Sensoren bis zu Höchstleistungs-Rechnern) und unterschiedlichsten physikalischen Anbindungen (von Nahbereichskommunikation über GPRS bis zu Optischen Netzen, von LAN bis zu Satellitenverbindungen)
- Hohe Informationssicherheit und Ausfallsicherheit

Als *Forschungsschwerpunkte* wurden im Einzelnen identifiziert:

- Konzepte zur Strukturierung des Netzes und zur vertikalen und horizontalen Funktionsverteilung
- Routing- und Adressierungsverfahren
- Unterstützung von Teilnehmermobilität und von drahtlosen Zugängen unterschiedlichster Art
- Schichtenübergreifende und netzweite Kontroll-, Monitoring- und Managementkonzepte
- Unterstützung von Dienstgüte (Quality of Service), Ausfallsicherheit (Resilience) und Informationssicherheit (Security)
- Dienstarchitekturen (Plattformen) und Komposition von Diensten

Diese Forschungsschwerpunkte, die in Kapitel 2 noch näher beschrieben werden, werden in standortübergreifenden Forschungsgruppen bearbeitet, wobei durchaus konkurrierende Teillösungen entstehen können und sollen, die im Gesamtprojekt diskutiert und bewertet werden. Methodisch gesehen werden hier sowohl theoretische, analytische sowie simulative Untersuchungen und prototypische experimentelle Studien durchgeführt. Als technische Plattform dient das gemeinsame Experimentalnetz, bestehend aus einer hinreichend großen Zahl von geografisch verteilten, geclusterten Netzknoten, auf die die Projektteilnehmer relativ ungehinderten Zugriff haben. Die bestehende Experimentalumgebung wird in Kapitel 2 im Arbeitsschwerpunkt 7 näher beschrieben.

2. Technische Studien zum Future Internet

Überlegungen und Aktivitäten zum Redesign des Internet müssen zumindest in einer ersten Phase angesichts der vielfältigen Möglichkeiten ein relativ breites Spektrum von Ansätzen verfolgen. Neben eher konservativen Konzepten, die im Sinne einer Evolution auf die Weiterentwicklung der heutigen IP-Netze setzen, wird verstärkt sogenannten clean-slate Ansätzen ein großes Potenzial bescheinigt. Dabei löst man sich von der traditionellen Internet-Architektur, in der Annahme, dadurch Freiheitsgrade für bessere zukünftige Architekturen gewinnen und nutzen zu können. International zeichnen sich in diesem Bereich vielseitige Forschungsvorhaben ab, die diesen sogenannten „clean-slate“ Ansatz verfolgen. Insbesondere die Arbeiten in den USA im Kontext der NSF-Vorhaben GENI und FIND sind hier zu nennen. Bei GENI stehen Experimentalplattformen im Vordergrund des Interesses, wohingegen sich die Projekte in FIND mit neuen Konzepten und Methoden für das Future Internet befassen. Die technischen Studien, die im Rahmen von G-Lab durchgeführt werden sollen, sind hinsichtlich ihrer Zielsetzung mit den Projekten in FIND vergleichbar. Der Standort Deutschland will hiermit an der Gestaltung des Future Internet mitwirken indem G-Lab Beiträge zu zukunftsweisenden Konzepten und Architekturen liefert.

Die Projektpartner wollen gemeinsam auf eine Gesamtarchitektur für das Future Internet bzw. für eine oder mehrere Netzarchitekturen im Rahmen des Future Internet hinarbeiten. „Pluralism of networks“ soll dabei ausdrücklich erlaubt werden – es ist nicht zu erwarten, dass das Future Internet einer einzigen „Leitinnovation“ folgt. Die Vielfalt der Arbeiten wird in thematische Arbeitsschwerpunkte gegliedert, an denen sich die Teilprojekte der Teilnehmer ausrichten. Gewisse übergreifende Zielsetzungen für das Future Internet wie Verfügbarkeit, Robustheit und Skalierbarkeit sind nicht gesondert aufgeführt.

2.1 Die Arbeitsschwerpunkte

Zur Koordination der Arbeiten in G-Lab:

ASP0: Koordination und Konsolidierung

Die folgenden Arbeitsschwerpunkte zu den Konzeptarbeiten werden in G-Lab bearbeitet:

ASP1: Architekturkonzepte für das Future Internet

ASP2: Routing und Adressierung

ASP3: Mobilitätsaspekte und drahtlose Netze

ASP4: Monitoring- und Managementkonzepte

ASP5: Dienstgüteunterstützung und Sicherheitskonzepte

ASP6: Dienstarchitekturen und Dienstkomposition

Zum Aufbau der Experimentalplattform:

ASP7: Experimentalplattform

Eine genaue Abgrenzung zwischen der Experimentalplattform und den Konzeptarbeiten bzw. der Studienplattform fällt schwer, da es Überschneidungen zwischen den beiden Plattformen gibt, denn die Entwicklung eines Prototypen oder Demonstrators lässt sich zu beiden Plattformen hinzuzählen. Der ungefähre Aufwand für die Experimentalplattform liegt bei 15-20% des Gesamtprojektaufwandes.

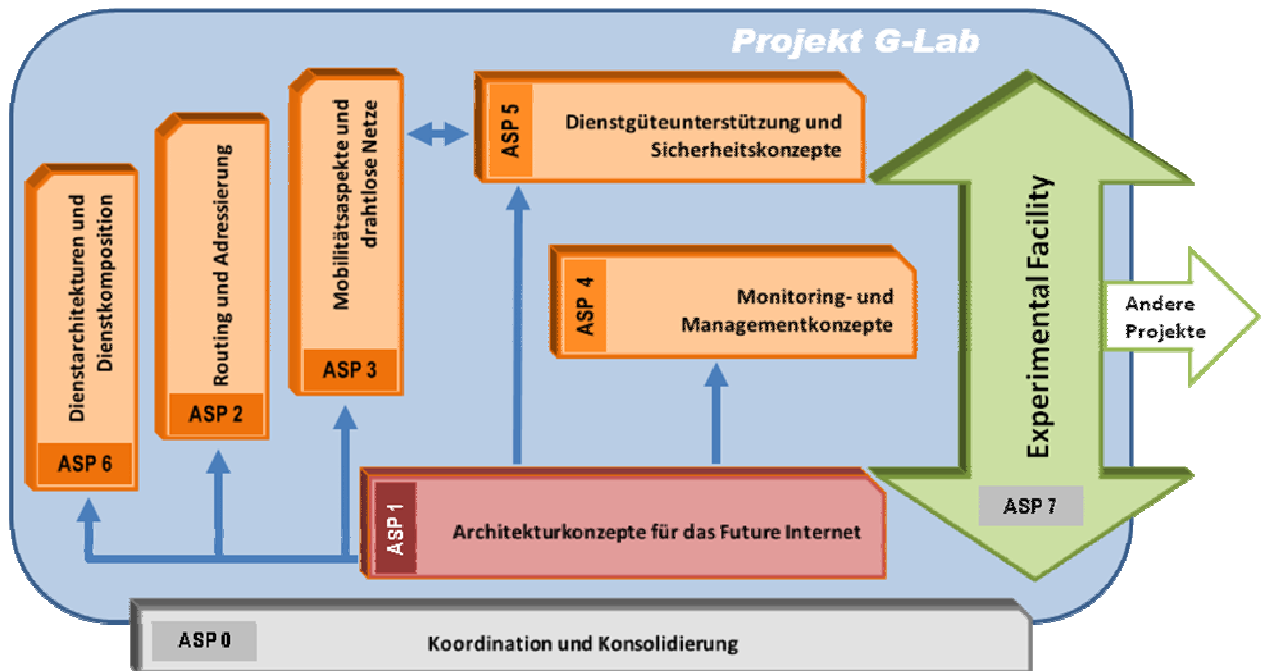


Abbildung 2: G-Lab ASP Struktur

ASP0: Koordination und Konsolidierung

Das ASP0 beinhaltet eine übergreifende Koordination, mit der sichergestellt werden soll, dass die zunächst eher individuellen Aktivitäten im Rahmen des Vorhabens in eine Gesamtsicht für das Future Internet münden.

Darunter fällt die Organisation unterschiedlicher Aktivitäten wie Workshops, Statusseminare und ähnlich gelagerte Veranstaltungen, bei denen die aktuellen Arbeiten der einzelnen Arbeitsschwerpunkte vorgestellt werden und eine mögliche Integration bzw. ein Interworking diskutiert wird.

Ein gemeinsamer Arbeitskreis dient zur Diskussion und Konsolidierung von Schlüsselkonzepten sowie von möglichen Standardisierungsinitiativen. Circa alle 6 Monate findet ein Workshop statt, bei dem ein kritischer Diskurs über alle ASP hinweg durchgeführt wird.

ASP1: Architekturkonzepte für das Future Internet

Dieser Arbeitsschwerpunkt beschäftigt sich mit neuartigen, grundlegenden Architekturkonzepten, die sich von den derzeitigen Konzepten und Modellen lösen, diese „aus der Distanz“ bewerten und neuartigen Konzepten gegenüber stellen. Dabei wird beispielsweise die Rolle der Schichten hinterfragt sowie Untersuchungen hinsichtlich der Platzierung von Funktionalitäten im Kommunikationssystem durchgeführt. Ziel ist nicht „die eine“ Architektur für das zukünftige Internet zu finden, sondern gegebenenfalls mehrere unterschiedliche Architekturen herauszukristallisieren. Diese können dann in virtuellen Netzen platziert werden. Interaktionen sind über geeignete Konzepte zum Interworking zwischen den Architekturen/Netzen möglich.

ASP1.1: Multilayer und Cross-Layer Designaspekte

In diesem ASP werden alternative Konzepte zur strengen schichtenorientierten Architektur untersucht. Die Arbeiten folgen dabei beispielsweise früheren Arbeiten zur funktionsbasierten Gliederung von Kommunikationssystemen und -protokollen und zu sogenannten Mikro-

protokollen sowie aktuelleren Arbeiten zu rollenbasierten Architekturen und ähnlichen Ansätzen wie sie beispielsweise auch im Rahmen der NewArch-Aktivitäten in den USA untersucht wurden.

Das Ziel dabei ist in einer einfacheren Gesamtarchitektur zu sehen, die möglichst offen für zukünftige Änderungen ist und durch Austauschen/Adaptieren einzelner Funktionen/Dienste eine Anpassung an sich ändernde Anforderungen ermöglicht. Dabei sollen die resultierenden Systeme im Vergleich zu rein schichtenorientierten Ansätzen leichtgewichtiger sein und mehrfache Platzierung gleicher Funktionalität in unterschiedlichen Schichten weitestgehend vermieden werden.

Ein möglicher Weg besteht darin, dienst-orientierte Konzepte auch in den „traditionellen unteren Schichten“ der Kommunikationssysteme konsequent zu verfolgen und damit letztendlich eine flexiblere Lösung mit wesentlich höherem Potenzial zur Adaptivität bereitzustellen. Auch die Integration neuer Funktionalitäten, die beim ursprünglichen Design nicht absehbar waren, soll damit deutlich erleichtert werden. Der Schwerpunkt liegt dabei auf Funktionalitäten, die für den Informationsaustausch zwischen Kommunikationspartnern erforderlich sind. Diese Funktionalitäten werden mit geeigneten Schnittstellen versehen sowie deren Interaktionen im Detail analysiert, insbesondere auch im Hinblick auf sehr unterschiedliche Netzbereiche (z.B. Backbone, Sensornetz). Besondere Beachtung nimmt eine detaillierte Bewertung der Schichtenauflösung im Hinblick auf Cross-Layer-Aspekte ein. Die Vor- und Nachteile werden gegenübergestellt, wobei unterschiedliche existierende Architekturen mit einbezogen werden (z.B. Internet, zelluläre Netze).

Cross-Layer-Aspekte spielen besonders bei drahtlosen Zugangstechniken eine wesentliche Rolle, um die Vorteile optimierter Übertragungsverfahren auf der physikalischen Schicht auch im Zusammenspiel mit höheren Schichten zu realisieren (z.B. Mobilität, Kanaleigenschaften). Die Fähigkeit von Cross-Layer Funktionen, z.B. die Gesamtkapazität eines Funknetzes zu maximieren sowie die Anforderungen der Teilnehmer hinsichtlich Datenrate, Delay und Übertragungsqualität optimal zu erfüllen, hängt wesentlich von der Verfügbarkeit aktueller und ausreichend genauer Information über den aktuellen Zustand verfügbarer Funkkanäle ab. Damit stellen Cross-Layer Funktionen insbesondere bei mobilen Teilnehmern spezielle Anforderungen an die Detektion der Funkkanaleigenschaften sowie deren Signalisierung an die Steuerungsinstanzen des Netzes. Im Rahmen der Untersuchungen zu Cross-Layer Aspekten sollen in diesem Zusammenhang Studien durchgeführt werden hinsichtlich der Eignung von Kanalinformationen zur Verbesserung der Leistungsfähigkeit eines Funksystems, und wie diese Informationen in realen Systemen optimal genutzt werden können.

Darüber hinaus werden Untersuchungen zu alternativen Konzepten zur strengen schichtenorientierten Architektur hinsichtlich der Auswirkungen auf paketorientierte Transportnetze durchgeführt. Dies betrifft insbesondere die Anbindung an flexible paketorientierte Hochgeschwindigkeitstransportnetze (BMBF Projekt Packet100 / EUREKA-Celtic 100GET). Hier sind schichtenübergreifende Ansätze insbesondere hinsichtlich der Steuerungsmechanismen von Bedeutung. Im Rahmen von G-Lab sollen hier auf nationaler Ebene über das Projekt EUREKA-Celtic 100GET weitergehende Machbarkeitsuntersuchungen und Systemexperimente durchgeführt werden, um das Zusammenwirken der neuartigen Layer 2 Pakettransportknoten mit Knoten anderer Partner, den im Rahmen von G-Lab entstehenden Architekturen und mit bisheriger Technik zu untersuchen und zu erproben.

Als Ziel dieses Arbeitsschwerpunktes ist ein dienstorientierter Entwurf für das zukünftige Internet, wobei die „klassischen“ unteren Schichten inkl. physikalischer Schicht (drahtloser Link, paketorientiertes Transportnetz) im Mittelpunkt des Interesses stehen. Wichtige Aspekte werden durch geeignete Evaluierungen (Simulation, Analyse, kleinere Prototypen) bewertet.

ASP1.2: Positionierung und Verteilung der Funktionen

Eine grundlegende Fragestellung bei der Entwicklung neuer Architekturkonzepte für zukünftige Netze ist die Anordnung der Intelligenz im Netz. In traditionellen Netzarchitekturen steckt der größte Teil der Intelligenz im Netz selbst. Moderne Ansätze die ein Peer-to-Peer-ähnliches Konzept verfolgen verschieben dagegen die komplette Funktionalität oder zumindest einen Großteil davon an den Rand des Netzes. Dadurch können Ressourcen wie Rechenleistung und Speicherplatz, welche durch den rapiden Fortschritt und Preisverfall in großem Maße am Rand des Netzes zur Verfügung stehen, genutzt werden. Andererseits ergeben sich durch die verteilte Natur dieser Systeme neue Problemstellungen. Die Sicherheit eines verteilten Systems ist beispielsweise schwerer zu gewährleisten als eine zentrale Instanz gegen Angreifer abzusichern. Außerdem werden Mechanismen benötigt um die Zusammenarbeit der dezentralen Instanzen zu gewährleisten.

In diesem ASP soll deshalb untersucht werden wie dezentrale mit zentralen Strukturen optimal zusammenarbeiten können. Zudem stellt sich die Frage welche Funktionen zwingend bzw. aus Kostengründen weiterhin zentral gestaltet werden müssen. Die Frage nach einer zentralen oder dezentralen Lösung wird dabei vermutlich für unterschiedliche Schichten der Netzarchitektur nicht einheitlich beantwortet werden können.

Eine weitere Frage ist, ob die einzelnen funktionalen Bausteine hierarchisch oder modular zueinander angeordnet werden sollen. Ergebnisse aus anderen Vorhaben wie ScaleNet werden aufgegriffen und ggfs. weiterentwickelt.

ASP1.3: Skalierbare Virtualisierung von Netzwerkressourcen

Die Virtualisierung von Netzwerk-Ressourcen in Festnetzen und in drahtlosen Netzen gilt als Basis für die Einführung eines neuen Internet und erfordert neue Ansätze über die heute bekannten Virtualisierungstechnologien hinaus, da hier sowohl die Netzknoten und Links als auch die drahtlosen Komponenten in die Betrachtung mit einbezogen werden müssen. Auch die Leistungscharakteristik von virtualisierten Netzknoten muss in diesem Szenario evaluiert werden. Es soll insbesondere ein skalierbares Virtualisierungs-Framework erarbeitet werden, welches die Bereitstellung von virtuellen Netzen und die Verwaltung dieser umfasst. Dazu müssen Signalisierungsmethoden und Protokolle analysiert werden, die in dem angestrebten Virtualisierungs-Framework verwendet werden sollen. Dieses Virtualisierungs-Framework stellt sozusagen die Basis für die in den ASP1.2 und ASP6.1 entwickelten Architekturen dar.

Als Anwendungsfall wird ein deutschlandweites virtuelles Netz angenommen, das GVNet (Germany Virtual Network), auf dem unterschiedliche Betreiberszenarien mit gegebenenfalls unterschiedlichen Protokollen analysiert werden sollen. Ein Anwendungsfall kann z.B. auch die Bereitstellung von Ressourcen für die zweite Phase des Projekts sein.

In Abstimmung mit den Projektpartnern soll eine prototypische Implementierung von Teilen eines virtuellen Netzes durchgeführt werden und einen Schwerpunkt in diesem ASP bilden. Dazu gehören die Weiterentwicklung von Virtualisierungslösungen als auch insbesondere die prototypische Entwicklung eines Signalisierungsprotokolls.

ASP2: Routing und Adressierung

In diesem Arbeitsschwerpunkt werden bestehende Routing- und Adressierungsmechanismen in Frage gestellt, da diese unter anderem die Flexibilität und Mobilität der Nutzer stark einschränken. Deshalb sollen neuartige Mechanismen entwickelt werden, die anschließend auf der Experimentalplattform implementiert und evaluiert werden.

ASP2.1: Namen und Adressierung / Invarianten

Einer der Hauptkritikpunkte im heutigen Internet ist die starke Kopplung zwischen Lokalität und Identität anhand der Netzwerkadressen. Hierdurch wird die Unterstützung vieler Dienste – wie beispielsweise der Mobilität – deutlich erschwert. Einige neue Ansätze wie beispiels-

weise FARA und HIP bauen darauf auf, diese enge Kopplung zu lösen und damit neue Freiheiten bei der Konzipierung zukünftiger Architekturen für das Internet zu erlangen.

Eine der Problematiken im heutigen Internet ist die Namensverwaltung. Die Benutzer müssen entweder den DNS-Namen der Maschine kennen, die einen gewünschten Dienst anbietet, oder sie müssen hoffen, dass die Antwort einer Suchmaschine, mit dem String als Eingabe, die gewünschten URL enthält, aus der der DNS-Name extrahiert werden kann. Zurzeit dient die IP-Adresse sowohl als Ortsbeschreibung als auch als Dienstidentifikator. Diese Verknüpfung verhindert im momentanen Internet das Remapping von Diensten, die Ortsänderung der Endpunkte, und effiziente alternative Kommunikationsparadigma, wie push und pull (unter Verwendung des Netzes als Zwischenspeicher), any-/multicast, etc.

In diesem Arbeitsschwerpunkt werden alternative Adressierungsvarianten für Informationen, Geräte, Dienste, etc. untersucht, die eine strikte Trennung dieser Funktionalitäten ermöglichen, aber auch eine einfache Bedienung durch den Benutzer erlauben. Deshalb müssen Informationen über die Adressen verteilt werden. Es wird untersucht auf welcher Abstraktionsschicht welche Informationen verwaltet und verteilt werden, und wie ein effizientes Mapping zwischen Namen und Ort im Internet vorgenommen werden kann. Das bedeutet signifikante Änderungen in der Steuerungsebene des Internet gegenüber den heutigen vorherrschenden Protokollen: BGP, OSPF, IS-IS, etc. Dazu gehört auch die Frage, wer welche Adressen kontrolliert und wer welchen Teil der Adressauflösung einsehen und kontrollieren kann.

In diesem Zusammenhang soll auch die weitere Verwendung hierarchischer Adressen (z.B. IPv6) berücksichtigt werden, beispielsweise als Basis für das Routing. Wichtig ist allerdings, dass jeder Nutzer eine eindeutige Adresse/Benutzerkennung erhält, über die er an jedem eingewählten Ort erreichbar ist – dies erfordert eine geeignete Adressauflösung. In diesem Arbeitsschwerpunkt soll deshalb eine dezentrale Adressauflösung ähnlich zu DNS und DynDNS entwickelt werden, die in der Lage ist Milliarden von Nutzern und Endgeräten zu verwalten und die mit der zunehmenden Mobilität der Nutzer effizient umgehen kann.

ASP2.2: Alternative Routingkonzepte

Packet Forwarding im Internet basiert auf Prefix Matching. Routing-Tabellen speichern für unterschiedliche IP-Nummernpräfixe die entsprechenden Interfaces, auf die die jeweiligen Pakete beim Forwarding durch den Router weitergeleitet werden. Dieses Prinzip hat seit dem Beginn des Internet gut funktioniert, aber mit zunehmendem Wachstum des Internet, mit der Vergabe kleiner Adressbereiche, mit dem Wechsel von Kunden zu anderen Providern und mit Multihoming werden Stimmen bezüglich der Skalierbarkeit dieses Konzeptes in den nächsten Jahren laut. Es gibt bereits mehrere Vorschläge für ein zukünftiges skalierbares Internet Routing, die zum Teil in der Routing Research Group der IRTF diskutiert wurden: a) Cisco propagiert das Locator/ID Separation Protocol (LISP), welches eine Trennung zwischen Locator und Identifier einführt; b) UCLA propagiert eFIT (enable Future Internet innovation through Transit wire) welches eine Trennung der Adressierung von Benutzer- und Provider-Netzen vorsieht; c) die Cornell University schlägt ein Core Router-Integrated Overlay (CRIO) vor, welches durch den Aufbau von Interdomain Tunnels Skalierbarkeit zu erreichen versucht; d) Olivier Bonaventure von der UCL fordert, dass sogenannte Locators automatisch zugewiesen werden sollen, um eine stetige Zersplitterung des Adressraumes zu verhindern.

Diese neuen Konzepte werden studiert, kombiniert und schließlich auf der Experimentalplattform implementiert werden, um die Machbarkeit der neuen Protokolle zu demonstrieren. Zudem werden aber intensive Simulationsstudien benötigt um Skalierbarkeitsfragen zu adressieren, die selbst in einem sehr großen Testnetz nicht beantwortet werden können. Ferner sollen neuartige Traffic Engineering Methoden entwickelt und getestet werden, die durch die

Locator/ID Trennung und die damit verbundene dynamischen Locator-Vergabe ermöglicht werden.

ASP3: Mobilitätsaspekte und drahtlose Netze

Dieser Arbeitsschwerpunkt beschäftigt sich mit der Mobilität der Nutzer und der Integration von Mesh- und Sensorknoten in das Internet. Es werden bestehende Mobilitätsmechanismen wie Mobile IP untersucht, erweitert und bei Bedarf komplett neu entwickelt. Ein unterbrechungsfreier Handover der Dienste zwischen verschiedenen Systemen (Sitzungsmobilität) soll ermöglicht werden, wobei der Nutzer gleichzeitig über mehrere Technologien mit dem Internet verbunden sein kann.

ASP3.1: Integrierte Mobilitätsunterstützung für drahtlose Netze

Für zukünftige Mobilkommunikationssysteme auf der Basis des Future Internet sind entsprechende neue Mechanismen zur Mobilitätsunterstützung zu erforschen, die nicht nur die bereits heute bestehenden Anforderungen erfüllen. Aus der Sicht der Protokollarchitekturen ist hierbei im Gegensatz zum bisher durch die IETF spezifizierten Mobile IP ein integrierter Ansatz zu verfolgen. Letzteres wurde gewissermaßen als Zusatzmechanismus auf der Basis des bestehenden Internet entwickelt, um den Ortswechsel eines mobilen Endgerätes transparent für die darüber liegenden Kommunikationsschichten zu gestalten. Tatsächlich bezieht sich diese Transparenz aber lediglich darauf, dass die IP- Adresse beibehalten wird und die Kommunikation auf diese Weise ohne Abbruch fortgesetzt werden kann. Wünschenswert wäre es jedoch, wenn ein Protokoll zur Mobilitätsunterstützung auch den Blick auf die darunterliegenden Schichten in strukturierter Art ermöglichen würde.

Darüber hinaus wird das für die globale Mobilitätsunterstützung gedachte Mobile IP tatsächlich oft nur domänenintern verwendet. Wichtig ist es daher auch, das Ziel einer „Global Seamless Mobility“ (Handover und Ressourcenmanagement) insbesondere aus der Benutzersicht zu beleuchten und vor allem abzugrenzen, wie viel Mobilitätssupport auf globaler Ebene bereit gestellt werden muss und wie viel bereits am Netzrand und im Netzzugang erbacht werden kann, insbesondere auch in „Multi-Access“ Systemen.

ASP3.2: Synergie-Effekte durch Integration von Sensornetzen

Ein drahtloses Sensornetz besteht sowohl aus einer Vielzahl von Sensorknoten als auch aus einer kleinen Menge an Datensammelstationen und Senken, die als Anbindung an das Internet dienen. Da die Sensorknoten zwar eine Vielzahl von Daten sammeln können, jedoch nur begrenzte Intelligenz, Übertragungs- und Verarbeitungsfähigkeiten haben, ist der Informationsfluss in diesen Netzen sehr eingeschränkt: die Senken leiten Anfragen von Nutzern außerhalb des Netzes an die Sensorknoten und versenden die gesammelten Daten dann aus dem Sensornetz in das Internet. Für das Weiterleiten der Anfragen von außerhalb gibt es viele Vorschläge. Dabei ist zu beachten, dass die Anfragen nie direkt an bestimmte Knoten adressiert sind, sondern dass diese Datenbankabfragen ähnlich aufgebaut sind (COUGAR) und nach geographischen (GHT, GPCR), meist jedoch nach inhaltlichen (Directed Diffusion, SPIN, TEEN) Gesichtspunkten versendet werden. Zudem sollen diese Mechanismen noch energieeffizient realisiert werden.

Durch die Integration von Sensornetzen ergeben sich Möglichkeiten das Internet um eine Vielzahl neuer Dienste zu erweitern. Beispielsweise können im Internet der Zukunft Daten aus mehreren jeweils weitflächig installierten Sensornetzen parallel abgefragt und aggregiert werden. Die Synergie-Effekte, aber auch die Probleme, die bei der Integration von Sensornetzen auftreten, sollen in diesem Arbeitsschwerpunkt erörtert werden. Hierfür sind Position und Art der Sensoren, die zu sammelnden Daten und vor allem die Standorte und Bandbreite der Internetanbindung zu planen und zu optimieren. Diese Einzelfragestellungen sollen zu einer systematischen Planungsmethodik beitragen, die für zukünftige Anwendungen wie Global Scale Sensor Networks eingesetzt werden können.

ASP3.3: Multi-Homing und Aspekte der Sitzungsmobilität

Es ist zu erwarten, dass zukünftige Endgeräte zumeist über mehrere Netzschnittstellen verfügen werden. Ziel sollte es sein, diese nicht nur im Sinne einer bestmöglichen Zustellung von Paketen zu nutzen, sondern tatsächlich hinsichtlich der unter Randbedingungen optimalen Erbringung von Telekommunikationsdiensten an sich. Dafür sind von Netzseite jedoch weitergehende Funktionen einschließlich einer fortgeschrittenen Mobilitätsverwaltung erforderlich, welche die gleichzeitige Kommunikation über mehrere Schnittstellen flexibel zu steuern vermag. Dabei sind nicht nur die unterschiedlichen Mechanismen zum Verfolgen des Aufenthaltsortes aktiver und zum Rufen passiver Teilnehmer zu berücksichtigen, sondern auch darüber hinausgehend die Kontexte der einzelnen Sitzungen.

ASP4: Monitoring- und Managementkonzepte

Dieser Arbeitsschwerpunkt widmet sich Fragestellungen, die im großen Kontext des Netzmanagements angesiedelt sind. Hierbei liegt der Fokus auf einem dezentralen Monitoring- und Managementkonzept, bei dem die Messinfrastruktur direkt in das Netz integriert ist.

ASP4.1: Monitoringkonzepte

Das Netzwerk-Monitoring und die Analyse von Messdaten haben maßgeblich zum Verständnis der Funktionsweise des Internet beigetragen. Die Erhebung von Messdaten ist für den reibungslosen Betrieb und den gezielten Ausbau eines Netzes unumgänglich. Ein Designziel für das zukünftige Internet ist, bereits im Architekturkonzept die Notwendigkeit von Messungen zu berücksichtigen und die Netzwerkanalyse zu unterstützen.

Speziell im Hinblick auf die grundlegend neuen Konzepte, die im G-Lab entwickelt werden, besteht ein erheblicher Bedarf an Werkzeugen zum Netzwerk-Monitoring. Prototypische Implementierungen aus den verschiedenen G-Lab Studien sollen es ermöglichen, in einer kontrollierten Umgebung reproduzierbare Aussagen über zukünftige Technologien zu machen. Hier gilt es, die erforderlichen Methoden zur Messung und Analyse der Leistungsfähigkeit neuer Netzwerkkonzepte bereitzustellen. Dies betrifft ein weites Spektrum an Kenngrößen, wie Dienstgüte, Robustheit und Verfügbarkeit des Netzes.

Das heutige Internet trennt strikt zwischen dem Netz und den Endsystemen und stellt nahezu keine Informationen über Netzwerkinterna zur Verfügung. Dies hat zur Folge, dass Anwendungs- und Transportprotokolle sich in ihren Entscheidungen, wenn überhaupt, auf ungenaue Informationen aus eigenen Messungen verlassen müssen. Die zunehmende Heterogenität und Komplexität der Netze erschwert dies jedoch erheblich. Das zukünftige Internet bietet dagegen die Möglichkeit, eine eigene Messinfrastruktur in das Netz zu integrieren. Die gesammelten Messdaten können in aufbereiteter Form über zu definierende Schnittstellen höheren Schichten bereitgestellt werden. Das Vorhandensein dieser Informationen kann grundlegend neue, adaptive Lösungen beispielsweise in den Bereichen Selbstorganisation, Dienstgüte und Verlässlichkeit, z.B. im ASP5.1 und ASP6.3 ermöglichen. Eine besondere Herausforderung an das Monitoring stellen zukünftige, dezentrale Systeme dar, wie beispielsweise drahtlose ad-hoc Netze. Aspekte wie Sicherheit, Verlässlichkeit und Dienstgüte können in solchen Netzen heute nicht sichergestellt werden. Es gilt, geeignete Monitoring-Konzepte für diese Netze zu entwickeln und hiermit eine Grundlage zur Untersuchung von Sicherheitsmechanismen in zukünftigen Netzen im ASP5.2 zu legen.

ASP4.2: Management- und Administrationskonzepte

Ziel ist die Spezifikation einer Steuerungs- und Management Plane für die Netze der Zukunft und der Funktionssplit zwischen beiden Planes. Hierzu findet eine Analyse bereits vorhandener Steuerungs- und Management Plane Ansätze sowohl im Bereich der klassischen Transportnetze, wie auch in den existierenden Paketnetzarchitekturen statt. Eine Unterscheidung in zentrale und dezentrale Ansätze ist hierbei enthalten. Durch die durchgeführte Analyse sollen Gemeinsamkeiten und somit mögliche Synergien verdeutlicht werden und

eine Bewertung einer Verschmelzung beider "Welten" ermöglicht werden. Es sollen Fehler-szenarien für die Netze der Zukunft definiert und die Fehlerbehebung analysiert werden - insbesondere wie sich die Ausfälle der Data Plane auf die Funktionsfähigkeit der Steuerungs- und Management Plane auswirken.

Weiterhin ist es von entscheidender Wichtigkeit sicherzustellen, dass alle Vorgänge entweder autorisiert oder anonym sind. Doch welcher kann/soll/muss autorisiert/anonym sein? Brauchen wir unterschiedliche Teilnetze mit unterschiedlichen Richtlinien? Ein Banknetz hat diametral andere Anforderungen als ein anonymes medizinischer Beratungsdienst. Eine Realisierung solch unterschiedlicher Anforderungen an die Architektur der Netze soll mittels Netzvirtualisierung untersucht werden.

Jedoch wenn mehrere Netze auf einer Infrastruktur realisiert werden ist sicherzustellen, dass diese unabhängig voneinander betrieben werden können. D.h. jedes Teilnetz braucht seine eigenen Ressourcen und eigene Kontrollstruktur. Das Management einer solchen Infrastruktur ist nicht trivial und beinhaltet, u.a.:

- automatische Ressourcenzuweisung
- Spezifikation von komplexen Netzen unterschiedlichster Architekturen
- Automatische Konfiguration der Spezifikation der Netze
- Monitoring und Überwachung

ASP5: Dienstgüteunterstützung und Sicherheitskonzepte

Ziel dieses ASPs ist es neue Mechanismen zu entwickeln, um den Nutzern Dienste mit hoher Qualität und Sicherheit zu garantieren. Hierbei liegt der Fokus auf dezentralisierten, verteilten Ansätzen. Eine sichere und verfügbare Kommunikation bildet dabei die Basis für weitere Optimierung der Dienstgüte. Außerdem helfen neue Mechanismen zur Erkennung und Behebung von Überlasten die Qualität der Übertragung zu gewährleisten.

ASP5.1: Zusammenhänge technischer und wahrgenommener Dienstgüte

Bei Echtzeit-Übertragungen, in denen viele Dienstanutzer zur selben Zeit den gleichen Inhalt konsumieren, wie z.B. bei Fernsehen über das Internet (IPTV), eignet sich nur Broadcast/Multicast. Anders verhält es sich mit Streaming-Inhalten, die zu beliebiger Zeit bzw. in einem hinreichend großen Zeitfenster konsumiert werden können. Ein typisches Beispiel sind hierfür die heute existierenden Podcasts, die auch als Video-on-Demand bekannt sind. Multicast kann hier nicht mehr das Verteilen der Inhalte lösen, da die Daten nicht mehr zeitgleich konsumiert werden. Es gibt nun mehrere Probleme bei IPTV: a) der Dienstanbieter muss möglicherweise sehr viele Streams unterstützen können; b) Nutzeranfragen können aufgrund der Popularität von Sendungen stark variieren; c) schwach angebundene Kunden können die Inhalte nur in geringer Auflösung erhalten; d) es wird sehr viel Netzverkehr erzeugt, indem dieselben Daten zeitversetzt mehrmals über dieselben Leitungen transportiert werden.

Diese Probleme können durch dezentrale und verkehrs- und inhaltssensitive Mechanismen gelöst werden. Bei der Verteilung der Inhalte muss die Netztopologie berücksichtigt werden, wobei durch Zwischenspeichern von Streams mehr Anfragen lokal gehalten und die Netzbelastung dadurch gesenkt werden kann. Es ergeben sich Kompromisse zwischen Effizienz, Kosten durch Overhead, Robustheit und Dienstqualität. Weiterhin müssen es solche Systeme erlauben, beim Abspielen zu pausieren, auf Bookmarks zu springen, schnellen Vor- und Rücklauf anzubieten, um so interaktives Fernsehen zu ermöglichen. Die Machbarkeit soll durch einen Prototypen gezeigt und seine Funktionalität durch den Einsatz im Testnetz überprüft werden. Zudem sollen Leistungsbewertungen hinsichtlich der Skalierbarkeit und der erfahrenen Dienstgüte (Quality of Experience) solcher Ansätze durchgeführt werden.

ASP5.2: Sicherheitskonzepte

Das zukünftige Internet ist bezüglich der verwendeten Kommunikationstechnologien sowie Dienst- und Anwendungsparadigmen keine "Monokultur" sondern durch Offenheit und Heterogenität gekennzeichnet. Neben etablierten, auf einer zentralisierten Architektur aufbauenden Client-Server Systemen wird die Bedeutung dezentraler Peer-to-Peer Systeme weiter zunehmen. Schon heute bieten diese Systeme sowohl für Wissenschaft als auch kommerziellen Einsatz eine flexible Plattform zur Entwicklung neuartiger Anwendungen. Weiterhin werden hochdynamische Funkzugangsnetze (d.h. drahtlose Ad hoc und Mesh-Netze) in Zukunft eine unverzichtbare Ergänzung zu kabelgebundenen Zugangstechnologien bieten. Die weite Verbreitung von Wireless LANs lässt diesen Trend schon heute erkennen.

Die durch diese Technologien gewonnen Freiheitsgrade bieten allerdings nicht nur aufrichtigen Anwendern, sondern auch Angreifern neue Möglichkeiten. Sicherheitsmaßnahmen müssen deshalb integraler Bestandteil zukünftiger Netzarchitekturen sein. Herkömmliche Sicherheitsmaßnahmen kabelgebundener Client-Server-Systeme basieren auf den dort gegebenen klaren Netzgrenzen und zentralen, vertrauenswürdigen Instanzen. Fehlen diese Voraussetzungen, ist der Einsatz bisher verwendeter Sicherheitsmaßnahmen nicht möglich. Ziel dieses Arbeitsschwerpunktes ist deshalb die Entwicklung neuartiger Mechanismen zur Gewährleistung der Sicherheit in dezentralen Systemen ohne klare Netzgrenzen.

Bisherige Ansätze in dieser Richtung sind meist gezielt auf wenige Angriffsmechanismen und einzelne Schichten (oft nur die Netzwerkebene) eines Kommunikationssystems ausgerichtet. Effektive Lösungen zur Einhaltung von Sicherheitsanforderungen müssen jedoch ein deutlich größeres Maß an Flexibilität zur Erkennung und Abwehr auch neuer Angriffe z.B. auf Ebene der Funkübertragung oder der eingesetzten Transport- und Anwendungsprotokolle bieten. Cross-Layer-Techniken wie sie in ASP1.1 betrachtet werden, können dabei zur Verknüpfung der Sicherheitsmaßnahmen auf verschiedenen Schichten dienen. Darüber hinaus können verschiedene Stufen der Angriffserkennung unterschieden werden, um eine bessere Skalierbarkeit des Systems zu ermöglichen. So wird zunächst auf einen „groben“ Verdacht geprüft und nur bei Vorliegen eines solchen dann weiter im Detail analysiert.

Zur Erkennung von Angriffen und zur Evaluierung der Wirksamkeit der entwickelten Sicherheitslösungen werden effektive Monitoring-Mechanismen, wie sie in ASP4.1 entwickelt werden, benötigt. Diese ermöglichen zudem eine kombinierte Betrachtung von Sicherheit und QoS Aspekten. Beide Bereiche beeinflussen sich direkt: Eine sichere und verfügbare Kommunikation bildet einerseits die Basis für weitere Optimierungen der Dienstgüte. Andererseits erzeugen Sicherheitsmaßnahmen eine unvermeidbare, zusätzlich Netzlast, die es zu minimieren gilt. Die Performanz der in diesem Arbeitsschwerpunkt zu entwickelnden neuartigen Mechanismen zur Gewährleistung von Sicherheit in dezentralen Systemen ohne klare Netzgrenzen ist ein entscheidender Faktor für deren Anwendbarkeit in der Praxis und soll deshalb durchgängig als Rahmenbedingung Beachtung finden.

ASP5.3: Advanced Congestion Control

Mit der Verbreitung von Hochgeschwindigkeitsnetzen bis zum Einzelbenutzer stoßen die heutigen TCP-Versionen an ihre Grenzen. In den letzten Jahren wurden TCP viele Optionen hinzugefügt, die aber nur in den Endsystemen Anwendung finden. Überlast wird bei TCP den Endsystemen in der Regel indirekt durch Paketverluste signalisiert, was eine sehr späte Form von Überlastbenachrichtigung ist und Übertragungswiederholungen nach sich zieht. Um die Effizienz von Transportprotokollen zu steigern, wurde die sogenannte Explicit Congestion Notification (ECN) eingeführt, welches Endsysteme frühzeitig durch Inband Signaling vor beginnendem Datenstau warnt und sie auffordert ihre Datenrate zu reduzieren. Darüber hinaus existieren weitere Trends in diesem Bereich, die zurzeit in IETF diskutiert werden und für die in hohem Maße Forschungsbedarf existiert. Ein Beispiel dafür ist "re-feedback & re-ECN". Im Rahmen einer Studie wollen wir das Verhalten dieser neuen Mechanismen unter-

suchen, welche auf das Feedback von Netzknoten angewiesen sind. Auf Grund dieser Interaktion müssen die Netzelemente sinnvoll konfiguriert werden um eine gute Netzauslastung bzw. einen guten Service für die Benutzer zu gewährleisten. Um die Studien möglichst praxisnah zu testen, wird eine Experimentalplattform benötigt, in dem die Knoten diese Interaktionen durchführen können. Da insbesondere TCP Quickstart und re-ECN den Sendern erlaubt erheblich mehr zu senden als herkömmliche TCP-Varianten, dürfen diese Protokolle zunächst auch nur in geschützten Umgebungen zum Einsatz kommen bis sie vollständig verstanden sind.

ASP6: Dienstarchitekturen und Dienstkomposition

Der Fokus dieses Arbeitsschwerpunktes liegt in dem Zusammenspiel zwischen Diensten und darunterliegenden Schichten. Dabei sollen in einer horizontalen Sicht gegenseitige Einflüsse der Schichten im Hinblick auf die Dienstkomposition der gesamten Architektur analysiert werden. In einer vertikalen Sicht soll das Zusammenspiel von Overlay und Underlay untersucht werden, um das System möglichst effizient zu realisieren und dadurch QoS zu ermöglichen.

ASP6.1: Dienstarchitekturen

Dienstorientierte Architekturen haben in den letzten Jahren insbesondere auch im Hinblick auf das Web eine zunehmend wichtige Rolle eingenommen. Dieses Arbeitspaket widmet sich den Architekturkonzepten, welche die Erbringung von Diensten und darauf aufsetzender Anwendungen unterstützen und erleichtern. Es soll insbesondere untersucht werden, wie Basisdienste, die für viele bestehende und neue Anwendungen relevant sind, im Sinne eines „generischen“ Satzes von Diensten definiert und dann in einer „mittleren Schicht“ (im Sinne der Cross-Layer-Konzepte aus ASP1.1 zwischen der Anwendungsschicht und der Transportschicht) platziert werden können. Dabei soll u.a. geklärt werden, ob diese Dienste hierarchisch oder modular zueinander angeordnet sind. Man verspricht sich dadurch eine höhere Effizienz und größere Flexibilität, aber auch eine verbesserte Kompatibilität unterschiedlicher Dienstkombinationen und Anwendungen.

Solche Dienste bzw. Funktionen sind u.a. Routing und Lookup (basierend auf unterschiedlichen schichtenübergreifenden Adressierungsformaten, vgl. ASP2.1), Sicherheitsfunktionen, Resilience-Funktionen (Ausfallsicherheit, schnelle Detektion von ausgefallenen Knoten), Speicherdienste (Daten werden an einem für den Nutzer transparenten Ort im System gespeichert und können von überall gelesen werden), Suchfunktionen (mit komplexen Suchmöglichkeiten), Mobilitätsunterstützung incl. Positionierung („Mobility as the common case“, Handover zwischen verschiedenen Zugangnetzen), und gewisse Ressourcenmanagement-Funktionen.

Im Vergleich zu netzbasierten Ansätzen wie dem IP Multimedia Subsystem (IMS) soll hier der aus der P2P-Welt vorgezeichnete Weg der weitgehenden Verlagerung von Funktionalitäten an den Netzrand verfolgt werden. Als offene Forschungsfragen sind in diesem ASP vor allem Skalierungsfähigkeit und Realtime-Fähigkeit ebenso wie Methoden des verteilten Managements zu untersuchen. Die Vorarbeiten aus Overlay-Netzen stellen dabei für unterschiedlichste Anwendungsszenarien eine gute Basis dar. Zu vermuten ist, dass sich letztendlich eine günstige Mischform von verteilten, dezentralen und teilzentralisierten Funktionen als Optimum ergibt. Für die praktische Umsetzung ebenso von Bedeutung sind flexible Dienstplattformen, um eine einfache Dienstkomposition nach ASP6.2 zu ermöglichen.

Weiterhin ist es wichtig zu bestimmen, in welcher Granularität Dienste gestaltet werden, um durch Komposition eine effiziente Lösung für eine Aufgabe zusammensetzen zu können. Die Dienste sollen dazu möglichst lösungsagnostisch spezifiziert werden. Erreicht werden kann dies durch eine Orientierung an Entitäten des Systems; vermieden werden sollte eine direkte aufgabenzentrische Dienstspezifikation, die eine Wiederverwendung limitiert. Die Aufgabenorientierung ist dann ein Ziel der Dienstkomposition.

ASP6.2: Dienstkomposition

Für einen dienstorientierten Ansatz, wie in ASP6.1 skizziert, ist eine Komposition des Systems aus den vorhandenen Diensten eine inhärente Notwendigkeit. Dies gilt über alle „klassischen“ Schichten hinweg und ist deshalb sowohl für die in ASP6.1 geschilderten Arbeiten als auch für die in ASP1.2 dargestellten Konzepte erforderlich. Diese übergreifende Komposition von Diensten ermöglicht es von vornherein, Wechselwirkungen zwischen den Diensten zu berücksichtigen und damit klassische Cross-Layer-Fragestellungen zu lösen.

Die in den Arbeitspaketen ASP1.2 und ASP6.1 erarbeiteten Schnittstellen (bzw. Servicebeschreibungen) ermöglichen die Definition lose gekoppelter, autonomer, wiederverwendbarer und zusammensetzbarer Dienste. Lösungsagnostische Dienste können zur Erfüllung unterschiedlicher Aufgaben beitragen und sind daher für die Komposition besonders gut geeignet. Für deren Entwurf sind jedoch neue Designprinzipien erforderlich.

Dabei sind das Suchen, das Auffinden und die Orchestrierung zentrale Aufgaben. Weiterhin ist die domänenübergreifende Choreografie geeigneter Dienste eine zentrale Fragestellung, sobald Dienste anderer Anbieter genutzt werden. Unter Choreografie wird das Aushandeln technischer und auch nicht-technischer Randbedingungen für eine Dienstnutzung in zwei gleichberechtigten Domänen verstanden.

Für die Komposition ist es notwendig, diese Dienste zu lokalisieren und technisch zusammenzubinden, so dass sie gemeinsam eine Aufgabe erfüllen. Die Lokalisierung der Dienste kann aufgrund funktionaler Anforderungen geschehen. Ausreichend ist dies aber nicht. Denn Dienste lassen sich auch mit unterschiedlicher Qualität (z.B. Performanz, Zuverlässigkeit oder Kosten) und unterschiedlicher Implementierungs-Semantik¹ bereitstellen. Diese Ausnutzung nicht-funktionaler Anforderungen an Dienste ist ein innovativer Aspekt in diesem Arbeitspaket. Beispielsweise soll nicht eine „komplette“ Robustheit bereitgestellt werden, sondern eine quantifizierbare Robustheit. Also nicht entweder 100% oder nichts, sondern auch dazwischen einstellbare Stufen. Evtl. können verschiedene Aspekte gegeneinander gewichtet werden, beispielsweise Robustheit gegen Energieverbrauch in einem Sensornetz. Um eine solche Dienstkomposition zu ermöglichen, ist eine entsprechende semantisch angereicherte Beschreibung der nicht-funktionalen Anforderungen an die Dienste zu entwerfen. Des Weiteren müssen Verfahren zur Verfügung stehen, um Dienste bezüglich ihrer qualitativen Eigenschaften bewerten zu können.

Auf der Anwendungsebene werden bereits einige Verfahren zur Komposition von Diensten (Orchestrierung- und Choreografie) erfolgreich eingesetzt, wie sie zum Beispiel BEPL4WS oder WS-Choreographie. Diese sind jedoch aufgrund ihrer XML-basierten Kommunikationsmuster nicht dazu geeignet, auf den unteren, architekturellen Schichten zum Einsatz zu kommen. Hier ist ein grundsätzlich neuer Ansatz zu entwerfen, der aber auf die Grundprinzipien der vorhandenen Lösungen aufsetzt. Die Beschreibung nicht-funktionaler Eigenschaften und die Bewertung qualitativer Eigenschaften sind für alle Ebenen, in denen Dienste genutzt werden können, noch nicht ausreichend gelöst. Um einen nahtlosen Übergang zwischen Diensten verschiedener Ebene zu ermöglichen, sollten diese Verfahren möglichst einheitlich und ebenen übergreifend anwendbar sein.

Für ein dienstorientiertes Kommunikationssystem ist die Dienstkomposition – anders als derzeit auf Applikationsebene üblich – in drei unterschiedlichen Varianten notwendig. Zum einen muss es möglich sein, Dienste schon vor der Auslieferung zusammenzusetzen, um damit einen Startpunkt zu erhalten, auf dem alles Weitere aufgesetzt werden kann. Weiterhin gibt es Dienste, die nicht entfernt genutzt werden können, sei es aufgrund der Performanz oder aufgrund der Funktionalität. Dann muss es eine Möglichkeit geben, diese Dienste zu lokalisieren und lokal nachzuintallieren. Die dritte Variante ist die entfernte Nutzung im Netzwerk vorhandener Dienste, so wie dies bei der klassischen SOA der Fall ist.

¹ Als Gegenteil zur Aufrufsemantik, die gleich sein muss aufgrund der vereinbarten Schnittstelle.

Eine weitere zentrale Fragestellung ist die Berücksichtigung unterschiedlicher Sicherheitsanforderungen bei der Komposition von Diensten. Die Anforderungen ergeben sich oft aus der Nutzungsart einer Dienstkomposition. Das heißt einfache Kommunikationsmuster wie „Web-Surfen“ brauchen keinen „Sicherheitsdienst“ in ihren Kommunikationsworkflow zu integrieren, während andere, wirtschaftlich sensible Kommunikationsbeziehungen hier Dienste einbauen, die einen hohen Sicherheitsstandard garantieren. Dies geht natürlich auch mit der Frage der Authentifizierung und Autorisierung (bin ich berechtigt einen solchen Dienst zu nutzen?), des Auditing (wer hat was wann wie genutzt?) und des Accounting (wie wird ein solcher Dienst abgerechnet?) einher. Ergebnis des ASPs sollen geeignete Verfahren zur Komposition entsprechender Dienste sein.

ASP6.3: Overlays und P2P

Dezentrale Overlays und die darauf aufbauenden Peer-to-Peer-Systeme verursachen bereits im heutigen Internet bis zu 80% des Verkehrsaufkommens. Dabei haben die Overlays in der Regel nur wenig Bezug zur darunter liegenden Netzwerktopologie. Aufgrund dieser „informationellen Asymmetrie“ können die Freiheiten, die beim Aufbau der Overlay-Topologie bestehen nicht zu einem effizienten Gebrauch des Underlays genutzt werden. Dies geschieht zum Nachteil sowohl der Anwender als auch der Internet Service Provider (ISPs). So kann z.B. eine direkte Verbindung zwischen zwei benachbarten Knoten im Overlay über physikalisch weit entfernte Router erfolgen, so dass unnötige Latenzzeiten entstehen und Ressourcen verschwendet werden. Insbesondere entstehen den ISPs oft vermeidbare Transitkosten dadurch, dass das Overlay Datenverkehr über Domänengrenzen leitet, obwohl die Daten oft auch lokal auf einem Peer innerhalb derselben Domäne vorliegen.

Weiterhin haben neue Overlay-basierte Anwendungen dedizierte Dienstgüteanforderungen, wie z.B. Peer-to-Peer-basierte IP-TV-Anwendungen wie Joost, Bablegum oder ZATTOO. Kommerziell wichtige Verkehrsflüsse werden in Zukunft nicht mehr überwiegend von zentralen Servern zu Endkonten verlaufen, sondern direkt zwischen Endkonten. Für ISPs wird es daher immer wichtiger, Kapazitäts- und Dienstgüteanforderungen zwischen Endknoten prognostizieren zu können. Auch hierfür ist die Auflösung der „informationellen Asymmetrie“ unverzichtbar.

Um dieses Problem zu überwinden bedarf es mehr Underlay-Wissen im Overlay. Die Bereitstellung entsprechender Informationen würde es den ISPs ermöglichen, effiziente Overlay-Topologien gezielt zu fördern. Beispielsweise wäre ein Overlay, welches in seiner Struktur die Grenzen der ISP-Domänen berücksichtigt, vorteilhaft sowohl für die ISPs als auch für die Benutzer. Unser Ziel ist es, die geschilderte Informationsasymmetrie zu überwinden, um eine effiziente Unterstützung von dezentral verwalteten Diensten zu ermöglichen. Dazu bedarf es eines zusätzlichen Informationsaustauschs zwischen den Overlays und dem Underlay. Mit diesen Informationen können Overlays im zukünftigen Internet möglichst optimal strukturiert werden. Es ist zu untersuchen, welche Art der Informationen hierzu benötigt wird, wie sie ausgetauscht werden kann und insbesondere welche Overlays diese Informationen nutzen können und in welchem Maße sie davon profitieren können.

Im Vordergrund muss dabei die Bewertung und Evaluierung der verschiedenen technischen Ansätze zu diesem Informationsaustausch aus industrieller Sicht stehen, vor allem im Zusammenhang mit der Zusicherung und gesicherten Bereitstellung von Konnektivität, Dienstgüte über eine heterogene Netzwerklandschaft mit einer Vielzahl von Domänen- und Dienstgüte- und Dienstanbietergrenzen hinweg.

Bisher dazu in der Standardisierung vorgeschlagene Rahmenwerke und Architekturen wie z.B. IETF NSIS (Next Steps in Signalling) und ETSI TISPAN (Telecoms & Internet converged Services & Protocols for Advanced Network) erwiesen sich als zu heterogen, oder als zu sehr auf nur einen kleinen Teil eines globalen Dienstgüte-Ansatzes konzentriert.

Eine sorgfältige Bewertung neuer, Overlay-basierender Ansätze zur globalen Berücksichtigung von Dienstgüteanforderungen Ende-zu-Ende ist insbesondere bezüglich der zu definierenden Virtualisierungs-Schnittstelle zwischen ISP und dem Overlay vonnöten, um eine zuverlässige Dienstsynchronisation bei zugesicherter Dienstgüte zu erreichen. Auch ist für eine erfolgreiche industrielle Umsetzung neuer Konzepte eine detaillierte Kenntnis und Berücksichtigung der Bedürfnisse aller Beteiligten wie z.B. der Netzwerkoperatoren zwingende Voraussetzung.

ASP7: Experimentalplattform

Die in den Arbeitsschwerpunkten ASP1 bis ASP6 definierten Forschungsaktivitäten beschreiben zum einen grundlegende, theoretische Forschungsarbeiten zum Thema Future Internet zum anderen aber auch experimentelle Ansätze (Simulation, Emulation) zur Überprüfung der abgeleiteten Ergebnisse unter realen Bedingungen. Routing-, Adressierungs-, Mobilitäts-, Kontroll- und Managementaspekte sowie die Interaktion der Funktionen weisen eine derartige Komplexität auf, dass sie mit rein analytischen Methoden nur schwer zu behandeln sind. Hier müssen neue und innovative verteilte Simulations-/Emulationsverfahren entwickelt werden die es erlauben auch auf den unteren Schichten des ISO/OSI Modells zu experimentieren. Darüber hinaus ist hier die Verteilung selbst Gegenstand der Forschung. Für die koordinierte Organisation und das Zusammenspiel dezentral eigenständiger Simulations-/Emulationsumgebungen sind neuartige Monitoring- und Managementkomponenten zu entwickeln die weit über die existierenden Ansätze in PlanetLab hinausgehen.

Die Ergebnisse in PlanetLab (<http://www.planet-lab.org/>) zeigen, dass diese Simulations- und Emulationsverfahren im klassischen Internet zielführend sind. Insbesondere die Untersuchungen zur Verteilung von Algorithmen und Funktionalitäten erfordern eine verteilte Umgebung, in der auch die Verzögerungen unter realistischen Bedingungen untersucht werden können.

Da die existierende PlanetLab Infrastruktur jedoch nur einem eingeschränkten Monitoring unterliegt und die Netzwerkverbindungen zwischen den Knoten nicht aufgezeichnet werden, sind die Ergebnisse zum Teil nur sehr schwer nachzuvollziehen bzw. zu interpretieren. Dies ist unter Qualitätsgesichtspunkten jedoch unverzichtbar. Die in G-Lab vorgeschlagene Experimentalplattform geht hier, auf der Basis der PlanetLab Software, einen anderen Weg. Hier wird versucht das Gesamtsystem (Software, Hardware, Netz) unter einem gemeinsamen, verteilten Monitoring-Ansatz zu betreiben. Dadurch wird eine 7x24 Stunden Verfügbarkeit, eine vereinfachte Administration und vor allem eine Qualitätssicherung gewährleistet. Qualitätssicherung bedeutet dabei, dass bei der Durchführung der Experimente die Randbedingungen unter denen ein Experiment durchgeführt worden ist, mit protokolliert werden.

Die wesentlichen Vorteile der hier vorgeschlagenen Infrastruktur gegenüber der existierenden PlanetLab Infrastruktur können wie folgt zusammengefasst werden:

- volle Kontrolle über das Testbett
 - Reservierung von einzelnen Testressourcen möglich
 - Ausschluss von Quereinflüssen
 - Möglichkeit Skalierbarkeit zu testen
- Möglichkeit, Ressourcen exklusiv zu reservieren
 - Testen von QoS Ansätzen
 - Dezentrale Komponenten sind eigenständig zu nutzen
 - Tests auf unteren Netzwerkebenen
- Möglichkeit, Funktionalität zu erweitern
 - Neue Technologien (Wireless, Sensor,...)
 - Testnetze (G-Lab mit PlanetLab Japan, WinLab, ...)

Da auf den Knoten dieses Systems ausschließlich die PlanetLab Software läuft (das System bootet mit dieser Software) stehen die Systeme ausschließlich den Experimenten im Rahmen von G-Lab zur Verfügung. Allgemeine Aufgaben können über diese Knoten nicht mehr abgewickelt werden.

Da die Knoten über Ethernet bzw. IP miteinander vernetzt sind, stellen die Untersuchungen auf den unteren Schichten der heutigen Netzarchitektur eine weitere Herausforderung dar. Aber auch hier kann zunächst in kleinen, kontrollierten Umgebungen die Funktionalität einer neuen Architektur untersucht werden. Der Aufbau der geplanten Experimentalplattform ist so angelegt, dass auch ein Zugang zur Layer-2 Funktionalitäten ermöglicht wird. So besteht z.B. die Möglichkeit mit der verwendeten Software die entwickelten Protokolle über die eingesetzte Hardware zu tunneln. Da die G-Lab Testumgebung von den Projektpartnern selbst administriert wird, lässt sich die Testumgebung nachträglich um zusätzliche Komponenten erweitern, die nicht zwangsweise auf dem IP Protokoll basieren müssen.

Die für die 1. Phase des G-Lab Projektes beschaffte Experimentalplattform besteht aus ca. 175 Netzknoten, die über 6 Standorte verteilt sind, wobei der Standort Kaiserslautern die Funktion des PlanetLab Central übernimmt. An jedem Standort gibt es einen Kopfknoten, der für Aufgaben wie DHCP, DNS, Boot images, Monitoring, etc. vorgesehen ist. Neben dem Kopfknoten gibt es noch weitere 24 Netzknoten an jedem Standort (in Kaiserslautern 58). Von den 24, bzw. 58 Netzknoten sind jeweils 2 mit 8 Ethernet Interfaces ausgerüstet, die vor allem für netz/routing-spezifische Tests genutzt werden sollen.

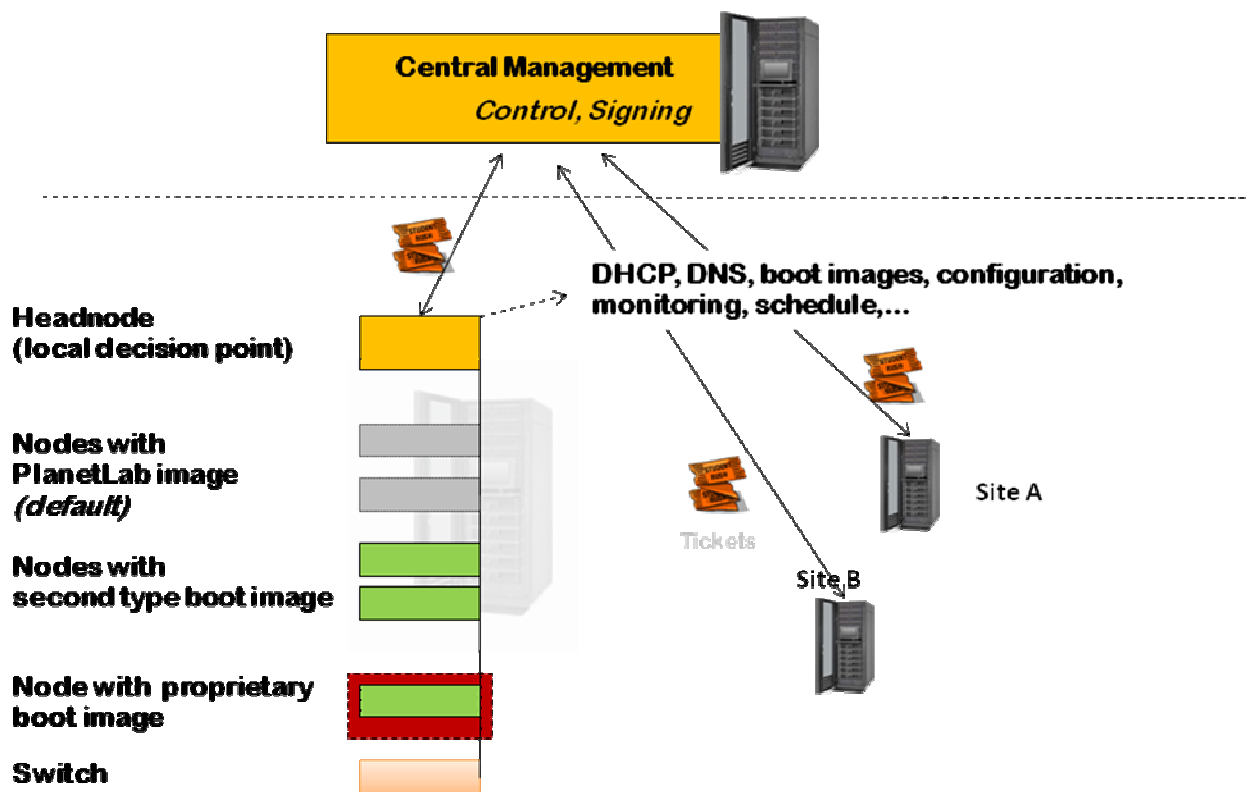


Abbildung 3: G-Lab: Experimentalplattform

Die genaue Spezifikation der Knoten ist in Tabelle 1 aufgelistet. Die Nutzungsrechte der Experimentalplattform werden in einer Konsortialvereinbarung geregelt. Hierbei besteht auch die Möglichkeit für später hinzukommende Partner, die Experimentalplattform zu nutzen und zu erweitern.

Typ	Beschreibung	Anzahl
Kopfknoten	Sun Fire X4250 mit 2x4 Kern Intel Xeon E5450 Prozessor (3.0 GHz), 16 GB RAM, 16x146 GB SAS Festplatten (10.000 UPM), 4x10/100/1000 Ethernet, ILOM	1
Netzknoten	Sun Fire X4150 mit 2x4 Kern Intel Xeon L5420 Prozessor (2.5 GHz), 16 GB RAM, 4x146 GB SAS Festplatten (10.000 UPM), 4 bzw. 8x10/100/1000 Ethernet, ILOM	24 (58)
Vernetzung	Cisco Catalyst 4506 (Kaiserslautern) Cisco Catalyst 4503 (andere) Unterstützung von GRE Tunneln Port: Uplink je 2 Mini-GBIC 1 Gbit/s; Intern 144 bzw. 72 1 Gbit/s (RJ-45)	