Hochschule
Bonn-Rhein-Sieg
Fachbereich Informatik

Netzmanagement von IPv4/v6-Dual-Stack-Umgebungen - Konzeption, Evaluierung und Implementierung

Abschlussarbeit

zur Erlangung des Grades Master of Science
im Studiengang Computer Science

vorgelegt von
Markus Becker

Erstbetreuer:	Prof. Dr. Martin Leischner Hochschule Bonn-Rhein-Sieg
Zweitbetreuer:	Prof. Dr. Kerstin Uhde Hochschule Bonn-Rhein-Sieg
Eingereicht am:	13. März 2013

Eidesstattliche Erklärung

Ich versichere an Eides statt, die von mir vorgelegte Arbeit selbstständig verfasst zu haben. Alle Stellen, die wörtlich oder sinngemäß aus veröffentlichten oder nicht veröffentlichten Arbeiten anderer entnommen sind, habe ich als entnommen kenntlich gemacht. Sämtliche Quellen und Hilfsmittel, die ich für die Arbeit benutzt habe, sind angegeben. Die Arbeit hat mit gleichem Inhalt bzw. in wesentlichen Teilen noch keiner anderen Prüfungsbehörde vorgelegen.

.....

(Ort, Datum) (Unterschrift)

Danksagung

Ich möchte mich an dieser Stelle bei all denen bedanken, die mich bei der Anfertigung meiner Bachelorarbeit so tatkräftig unterstützt haben. Besonderer Dank gilt:

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

1 Anforderungsanalyse

In diesem Kapitel werden zunächst Anforderungen an ein Netzmanagement für Dual-Stack-Umgebungen ermittelt. Auf Basis dieser Anforderungen wird in Kapitel **??** ein Konzept für ein Netzmanagement formuliert, das eine optimale Unterstützung von Dual-Stack-Umgebungen leistet.
Als Einstiegspunkt für das Sammeln von Anforderungen wird zunächst eine Analyse auf Basis der IPv6-Spezifikation durchgeführt. Durch die Analyse der mit IPv6 neu eingeführten Funktionalitäten, können neue Einsatzszenarien für das Netzmanagement erkannt und in einer späteren Konzeption berücksichtigt werden. Mit einem Vergleich bestehender Merkmale zwischen IPv4 und IPv6 können Anforderungen an sowohl neue, als auch bereits bestehende Managementmechanismen und -methoden, erkannt werden. In einem weiteren Schritt werden Anforderungen aus Sicht des IT-Service-Managements analysiert. Dafür werden Services aus den Netzlaboren herangezogen und in Bezug auf ITIL-Prozesse analysiert. Durch die Analyse von Services können Anforderungen, die aus dem Service-Management entstehen, wie es beispielsweise bei vielen mittleren und großen Unternehmen eingesetzt wird, aufgedeckt werden. In einem letzten Schritt werden Anforderungen auf Basis der Architektur einer Netzmanagementplattform analysiert. Insbesondere das Zusammenspiel von für eine Netzmanagementplattform charakteristischen Elementen kann durch eine Analyse der Architektur berücksichtigt werden. Da die Themenstellung bisher in keiner wissenschaftlichen Arbeit adressiert wurde, wird für die Anforderungsanalyse keine Literaturrecherche herangezogen.

1.1 Vergleich von IPv4 und IPv6

Für die Adressierung der mit IPv4 einhergehenden Probleme wurden mit IPv6 im Rahmen der Spezifikation diverse neue Funktionen eingeführt. Eine Konsequenz dieser Anpassungen und Erweiterungen ist die fehlende Abwärtskompatibilität von IPv6. Für die Analyse von Anforderungen, die durch die Integration von IPv6 entstehen, wird daher ein Vergleich zwischen IPv4 und IPv6 für die Analyse von Unterschieden verwendet. Eine vollständige Auflistung aller Unterschiede und Neuerungen von IPv6 befindet sich in [IBM12] und [DH98]. Viele dieser Änderungen und Neuerungen spielen für das Netzmanagement nur eine untergeordnet Rolle. Der Übersichtlichkeit halber werden in Tabelle 1.1 ausschließlich Unterschiede mit einer Relevanz für das Netzmanagement von Dual-Stack-Umgebungen aufgelistet.

	IPv4	IPv6
Adressnotation	- Dezimal - Trennung durch Punkte - 32 Bit	- Hexadezimal - Trennung durch Doppelpunkte - 128 Bit
Adressraum	- 32 Bit = 4,3 * 10^9	- 128 Bit = 3,4 * 10^{38}
Adresstypen	- Öffentliche Adressen - private Adressen	- Global-Unicast-Adressen - Link-Lokale Adressen
Ports	- Adressfamilie: AF_INET - TCP und UDP	- Adressfamilie: AF_INET6 - TCP und UDP
Zusatzprotokolle	- DHCP - ICMP - DNS	- DHCPv6 - ICMPv6 - DNSv6

Tabelle 1.1: Vergleich ausgewählter Unterschiede von IPv4 und IPv6

Adressnotation

Ein erster offensichtlicher Unterschied zwischen IPv4 und IPv6 ist die Notation der Adressen. Die bisher durch Punkte aufgeteilte IP-Adresse wird mit der Einführung von IPv6 durch Doppelpunkte getrennt. Des Weiteren wird die Adresse nicht mehr dezimal, sondern hexadezimal notiert. Zusätzlich wurde mit IPv6 der Adressraum von 32Bit auf 128Bit vergrößert. [DH98]
Die Berücksichtigung der neuen Adressnotation hat dabei nicht nur Einfluss auf die Größe von Formularfeldern. Zusätzlich führt sowohl die hexadezimale Schreibweise, als auch die Trennung der Adressblöcke durch Doppelpunkte und die Vervierfachung

der Adresslänge zu einer schlechteren Lesbarkeit und damit zu einer höheren Fehlerwahrscheinlichkeit bei der Eingabe von Adressen. Die softwareseitige Kontrolle der IPv6-Adresse wird im Vergleich zu IPv4 wichtiger. Im Kontext des Netzmanagements erfordert die neue Adressnotation somit eine syntaktische Prüfung der eingegebenen IPv6-Adresse, die beispielsweise bei der Konfiguration von Objekten, wie einem Host oder Service, angegeben werden müssen. [End12] Tabelle 1.2 listet alle Anforderungen, die durch die geänderte Adressnotation entstehen.

Adressnotation	- Unterstützung von IPv6-Adressen - Syntaktische Prüfung von Adresseingaben

Tabelle 1.2: Adressnotation: Anforderungen

Adressraum

Einer der Hauptbeweggründe für die Spezifikation von IPv6 war die mit IPv4 einhergehende Adressknappheit. Eine schon seit Jahren absehbare Verknappung von IPv4-Adressen wird in IPv6 mit einer 128 Bit langen Adresse entgegen gewirkt. Die Vergrößerung des Adressraums ermöglicht die Anbindung von theoretischen 3,4 * 10^{38} Endgeräten an das Internet. [DH98] Die Einführung von IPv6 wird auf lange Sicht zu einer Vergrößerung der zu managenden Netze führen. Eine Folge ist die durch den Dual-Stack-Betrieb einhergehende steigende Komplexität solcher Netze. Das Netzmanagement muss es also ermöglichen, solche Netze übersichtlich zu managen und zu verwalten. Filtermöglichkeiten gewinnen durch die Größe von IPv6-Netzen und den Dual-Stack-Betrieb an Bedeutung.
Auf der funktionalen Seite können Methoden wie das Auto-Discovery, die IPv4-Netze vollständig und sukzessive gescannt haben, durch die Größe von IPv6-Netzen nicht weiter verwendet werden und müssen überarbeitet werden. Der vergrößerte Adressraum von IPv6 führt zu den in Tabelle 1.3 aufgelisteten Anforderungen.

Adressraum	- Erweiterte Filtermöglichkeiten - Neukonzeption von Methoden, die einen Adressbereich als Eingabeparameter verwenden

Tabelle 1.3: Adressraum: Anforderungen

Adresstypen

IPv6 führt diverse neue Adresstypen ein. Die eindeutige und auch sehr einfache Einteilung in private und öffentliche IPv4 Adressen wird es infolgedessen nicht mehr geben. Jedes für IPv6 konfigurierte Interface muss mindestens über eine link-local IPv6-Adresse für die lokale Kommunikation verfügen. Zusätzlich können Interfaces

über die in Kapitel ?? erwähnten IPv6-Adressen parametrisiert werden.
Die neue Adressvielfalt sorgt für eine Aufspaltung der bisher eindeutigen Adressierung eines Interfaces. Einem Interface in einer Dual-Stack-Umgebung können, neben einer IPv4-Adresse, mehrere IPv6-Adressen zugeordnet. Für die globale Kommunikation eines Objektes müssen beispielsweise mindestens eine Link-Local und eine Global-Unicast IPv6-Adresse konfiguriert sein. Weiterhin erfordert die Integration von IPv6 eine Betrachtung der neuen Adresstypen auf Relevanz für das Netzmanagement. Adresstypen, die nicht für das Monitoring oder Management von Dual-Stack-Umgebungen benötigt werden, sollten aus Gründen der Übersicht nicht in das Netzmanagement integriert werden.
Zusätzlich werden die häufig im Kontext des Netzmanagements für z.B. das Auto-Discovery eingesetzte Broadcast-Adressen durch einen IPv6-Multicast simuliert. [Hag06] Durch den Wegfall der Broadcast-Kommunikation erfordern Methoden, die zuvor einen Broadcast für die Kommunikation verwendet haben, eine Anpassung. Tabelle 1.4 listet alle Anforderungen, die durch die mit IPv6 neu eingeführten Adresstypen entstehen.

Adresstypen	- Integration von relevanten IPv6-Adressen - Anpassung von Methoden, die Broadcast-Kommunikation verwenden

Tabelle 1.4: Adresstypen: Anforderungen

Ports

Einen weiteren funktionalen Unterschied stellen Ports dar. Ports werden sowohl in IPv6 als auch in IPv4 für die Unterscheidung von TCP- oder UDP-Verbindungen verwendet. Dennoch wird für die Differenzierung der Verbindungsendpunkte ein neuer Portbereich eingeführt. Durch die Hinzunahme der neuen Adressfamilie *AF_INET6* werden in der Übergangszeit also 4 Portbereiche verwendet. Eine Anwendung kann beispielsweise Port 22 sowohl in den Bereichen *AF_INET* (TCP & UDP) als auch *AF_INET6* (TCP & UDP) binden.
Ein Management von Services in Dual-Stack-Umgebungen erfordert eine Berücksichtigung von beiden Portbereichen, damit sowohl die Verfügbarkeit für IPv4 als auch für IPv6 überwacht werden kann. Die durch die neue Portfamilie resultierenden Anforderungen an das Netzmanagement werden in Tabelle 1.5 dargestellt.

Ports	- Zusätzliches Monitoring über Portbereich *AF_INET6*

Tabelle 1.5: Ports: Anforderungen

Zusatzprotokolle

Aus Kompatibilitätsgründen wurden viele Protokolle für IPv6 angepasst. Für das Netzmanagement relevante Protokolle sind beispielsweise ICMPv6 und DHCPv6. Die Implementierung der Protokolle basiert dabei letztendlich auf dem zugrundeliegenden Betriebssystem. Nichtsdestotrotz müssen Netzmanagementtools auf diese Protokolle im Rahmen von spezifischer Managementfunktionalität zurückgreifen. Ein Ping einer IPv4-Adresse muss beispielsweise über ICMP, ein Ping einer IPv6-Adresse über ICMPv6, erfolgen. Tabelle 1.6 listet alle Anforderungen, die durch für IPv6 angepasste Zusatzprotokolle entstehen, auf.

Zusatzprotokolle	- Anpassung von Methoden auf die für IPv6 angepasste Hilfsprotokolle

Tabelle 1.6: Zusatzprotokolle: Anforderungen

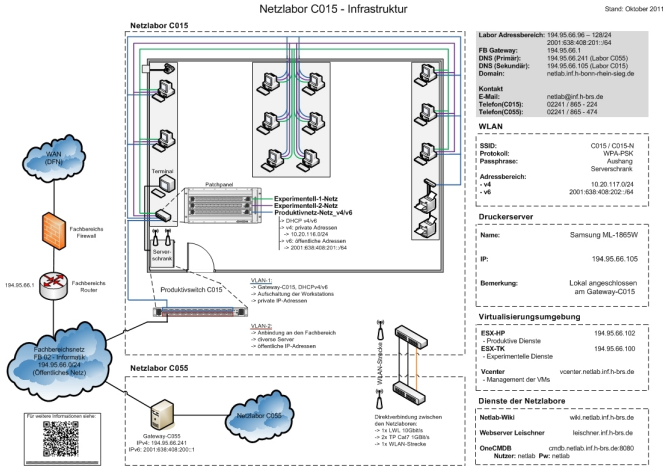
1.2 IT-Services

Nach der Analyse der mit IPv6 neu eingeführten Funktionalität werden Anforderungen aus Sicht des IT-Service-Managements analysiert. Das Netzmanagement wird im Rahmen des ITSM für die Unterstützung diverser Prozesse verwendet und erfordert eine Betrachtung inwieweit das integrierten Anbieten von Services durch den zusätzlichen IPv6-Stack beeinflusst wird.
Es werden zwei typische Services aus den Netzlaboren für die Anforderungsanalyse herangezogen. Als Servicebeispiele werden die Bereitstellung einer Webseite und die Anbindung der Netzlabore an das Internet verwendet.
Für ein besseres Verständnis der Services und der darunter liegenden Infrastruktur wird zunächst die Infrastruktur der Netzlabore näher erläutert. Der Fokus der Erläuterung liegt dabei auf der IPv6-Infrastruktur. Im Rahmen der Serviceanalyse wird nach der Erläuterung der Infrastruktur eine Beschreibung des Services und der damit verbundenen Einsatzszenarien gegeben. In einem weiteren Schritt wird der Leistungsumfang und die Leistungseigenschaften der Services in Form eines Service-Level-Agreements festgehalten. Darauf aufbauend werden die in Kapitel **??** beschriebenen Prozesse, die Kontaktpunkte mit dem Netzmanagement haben, für eine Anforderungsanalyse der jeweiligen Services herangezogen. Jeder dieser Prozesse wird auf Basis des Services und der damit verbundenen Integrationsaufgaben in Dual-Stack-Umgebungen untersucht.

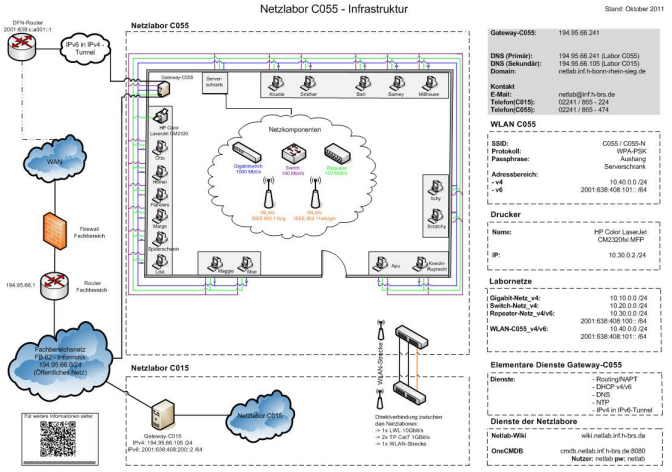
1.2.1 Die Netzlabore

Die Netzlabore in den Räumen C015 und C055 sind Teil des Schwerpunktes Telekommunikation im Fachbereich Informatik der Hochschule Bonn-Rhein-Sieg. Sie werden

für Übungen, Praktika, Praxisprojekte, Abschlussarbeiten und Forschungsprojekte eingesetzt. Das Ziel der Netzlabore ist dabei die Ergänzung und Vertiefung der Inhalte, die während der Vorlesung vermittelt wurden. Auf Basis der dafür angebotenen



(a) C015



(b) C055

Abbildung 1.1: Infrasturktur von C015 und C055

Services und der komplexen Infrastruktur werden eine Vielzahl von Anforderungen an das Netzmanagement gestellt. Die Infrastruktur der beiden Netzlabore wird in Abbildung 1.1 dargestellt. Das Netzlabor für Netzwerksysteme und Telekommunikation (C015) wird Studenten des Schwerpunktes Telekommunikation für das Arbeiten an Projekten bereitgestellt. Die vorhandenen Workstations und eigene Laptops können über Patchfelder für einen experimentellen Aufbau von Netzen miteinander verbunden werden. Eine Anbindung an das Internet erfolgt über ein Gateway, das mit dem Fachbereichsnetz der Hochschule verbunden ist.
Das Netzlabor für Hochleistungsnetze und Mobilkommunikation (C055) wird in erster Linie für Übungen, Praktika und Vorlesungen verwendet. Den Studenten werden zur Unterstützung von Übungen diverse Workstations, die über verschiedene logische

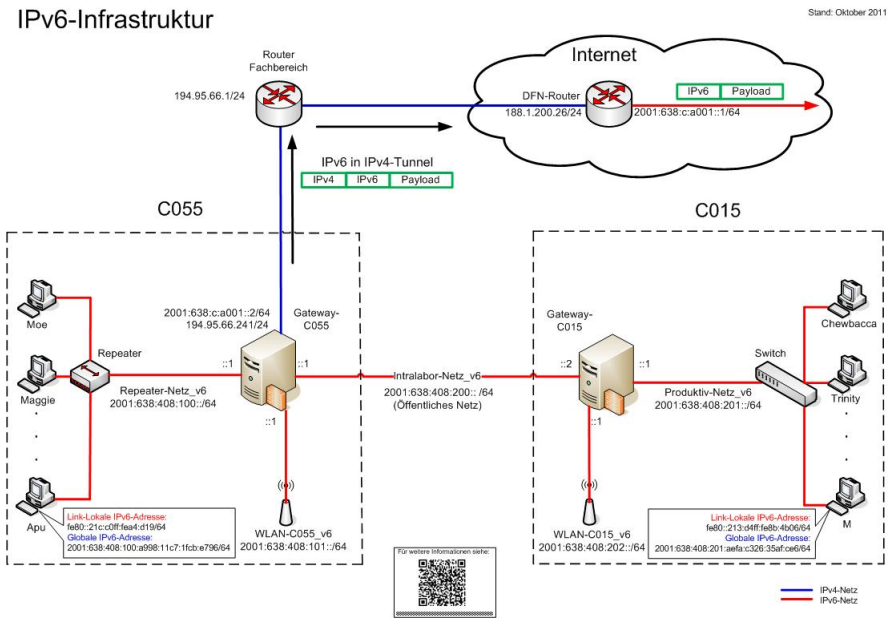


Abbildung 1.2: IPv6 Infrastruktur der Netzlabore

Netze miteinander verbunden sind, bereitgestellt.
Darauf aufbauend waren die Netzlabore bereits seit dem Jahr 2000 an das 6Bone mit IPv6 angebunden. Die heutige IPv6-Anbindung wird nach der Stilllegung des 6Bone über das Deutsche Forschungsnetz realisiert.[FH04] Die Netzlabore verfügen neben einer lokalen Infrastruktur somit auch über eine IPv6-Anbindung an das Internet. Dazu werden global gültige IPv6-Adressen aus dem Bereich 2001:638:408::/48 vergeben. Die Anbindung findet dabei nicht über eine native Lösung der Hochschule, sondern über eine Tunnellösung, statt. (siehe Grafik 1.2).
Neben der Anbindung der Workstations werden auch diverse Dienste der Labore über IPv6 angeboten. Darunter fallen alle angebotenen Webseiten (Webserver Leischner, Webseite der Netzlabore) als auch elementare Dienste wie DHCP und NTP. Eine vollständige Liste von managebaren Objekten kann auf der Webseite der Netzlabore ([Net12]) im Schwerpunkt Netzmanagement eingesehen werden.
Ein weiteres Merkmal der Netzlabore ist die umfangreiche Virtualisierungsumge-

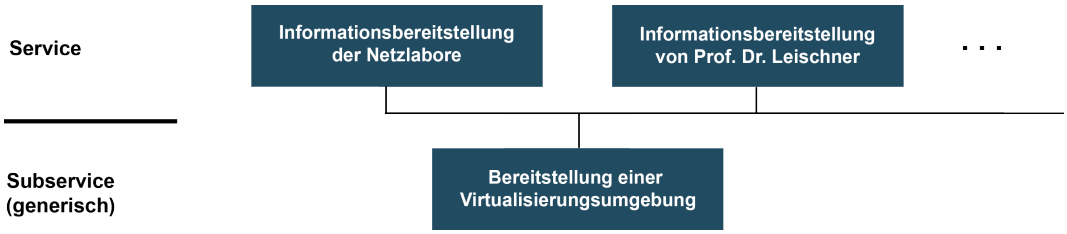


Abbildung 1.3: Nutzung eines generischen SLAs für eine Servicedefinition

bung, die einem Großteil von Services der Netzlabore zugrunde liegt. Die Netzlabore greifen dabei auf die Virtualisierungslösung VSphere von VMWare zurück. Abbil-

dung 1.3 zeigt den Zusammenhang der Virtualisierungsumgebung und der angebotenen Services auf Basis einer Servicedefinition.
Nachfolgend werden zwei Services der Netzlabore im Rahmen der für das Netzmanagement relevanten ITIL-Prozesse untersucht.

1.2.2 Service: Webserver

Die Webseite der Netzlabore dient primär der Informationsbereitstellung der Netzlabore. Typische Anwendungsszenarien sind die Bereitstellung von Übungsmaterial und die Beschreibung der Laborinfrastruktur.

Leistungsbeschreibung

Es wird für die folgende Vereinbarung über die Bereitstellung der Webseite der Netzlabore ein „interner SLA" verwendet. Die Anforderungen sind hinsichtlich der zu erbringenden Leistungen demnach nicht übermäßig streng definiert. Leistungsziele und Metriken werden lediglich informell festgehalten. Die Beschreibung in Tabelle 1.7 kann somit nicht als Vertrag, sondern als Absichtserklärung betrachtet werden.
Für eine vereinfachte Servicebeschreibung wird der in Abbildung 1.3 gezeigte Subservice "Bereitstellung einer Virtualisierungsumgebung" für die Servicedefinition herangezogen. So müssen Anforderungen, die an die zugrundeliegende Infrastruktur gestellt werden, nur einmal definiert werden und können direkt in einen neuen Service der innerhalb der Virtualisierungsumgebung betrieben wird, übernommen werden.
Nachfolgend wird der Service "Informationsbereitstellung der Netzlabore" im Rahmen der in Kapitel **??** beschriebenen ITIL-Prozesse analysiert.

SLA-Merkmal	Beschreibung
Kurzbeschreibung	- Hosting eines Webservers zur Bereitstellung von Inhalten der Netzlabore (netlab.inf.h-brs.de)
Serviceinhalte	- *Bereitstellung einer virtuellen Maschine* - *Sicherstellung des Zugriffs auf die virtuelle Umgebung* - *Regelmäßige Datensicherung der gespeicherten Daten* - Leistungsfähige Anbindung des Webservers an das Internet (v4/v6) - Sicherstellung des Zugriffs für den Anwender auf den Webserver
Service- und Reaktionszeiten	- Schnelle Reaktionszeit bei Ausfall der gesamten virtuellen Maschine oder Webseite (Servicelevel: gold) - Schnelle Wiederherstellung der vollen Einsetzbarkeit des Standardumfangs (Servicelevel: gold)
Mitwirkungspflichten	- *Störungen und Endstörungen müssen per E-Mail an die Verantwortlichen der virtuellen Maschine gemeldet werden* - *Als Ansprechpartner muss ein Labormitarbeiter über E-Mail erreichbar sein*

Von einem Subservice geerbte Merkmale werden kursiv dargestellt.

Tabelle 1.7: Leistungsbeschreibung für den Service „Informationsbereitstellung der Netzlabore"

Availability Management

Das Ziel des Availability Managements ist die Einhaltung der für den jeweiligen Service definierten Verfügbarkeit. Die nach ITIL definierten Hauptaktivitäten des Availability Managements umfassen neben der Definition der Serviceverfügbarkeit auch die jeweiligen Schritte zur Realisierung des Monitorings der Verfügbarkeit. [Bei08, S. 73]
Die Verfügbarkeit wird durch die in Tabelle 1.7 genannte Anforderungen nach einer Bereitstellung von Inhalten der Netzlabore definiert.
Das Monitoring der Verfügbarkeit wird von ITIL in reaktive und proaktive Maßnahmen aufgetrennt. Proaktive Maßnahmen, die eine Überwachung von Systemdaten, wie etwa der Festplattenkapazität vorsieht, spielen in Dual-Stack-Umgebungen nur eine untergeordnete Rolle und stellen keine neuen Anforderungen an das Netz-

management. Die Sicherstellung der Verfügbarkeit eines Webservers im Rahmen von reaktiven Maßnahmen wird in den Netzlaboren, wie in Abbildung 1.4 dargestellt, re-

DNS Resolution	OK	04-18-2012 1 DNS OK: 0.035 seconds response time. www.chaoticmoon.com returns 173.255.201.227
HTTP	OK	04-18-2012 1 HTTP OK HTTP/1.1 200 OK - 39986 bytes in 0.004 seconds
Ping	OK	04-18-2012 1 OK - www.chaoticmoon.com: rta 0.735ms, lost 0%

Abbildung 1.4: Beispielhaftes vollständiges Monitoring eines Webservers (IPv4)

alisiert. Mittels eines Pings wird ein einfacher Erreichbarkeitscheck durchgeführt. So kann sichergestellt werden, dass der Server für den Nutzer über den angesprochenen IP-Stack erreichbar ist. Dennoch gibt es auch Szenarien, in denen die Überwachung der Verfügbarkeit eines Webservers über einen Ping nicht ausreicht. Durch den Ausfall des Webservers (z.B. Apache) wäre der Server für den Nutzer der Webseite nicht mehr verfügbar, könnte aber noch durch einen Ping erreicht werden. Für eine vollständige Überwachung eines Webservers in einer IPv4-Umgebung sind folgende Schritte notwendig:

- Ping
- Abfrage eines Ports
- Dateianfrage über HTTP
- Überprüfung des DNS-Records

Abbildung 1.5 visualisiert die nötigen Schritte, die für eine Überwachung eines Webservers in einer Dual-Stack-Umgebungen realisiert werden müssen. Das Monitoring der Verfügbarkeit, wie es heute typischerweise in einer IPv4-Umgebung realisiert wird, muss für jeden beschriebenen Schritt um die erforderliche Methode für IPv6 erweitert werden. Die Überwachung der Erreichbarkeit eines IPv6-Servers wird durch

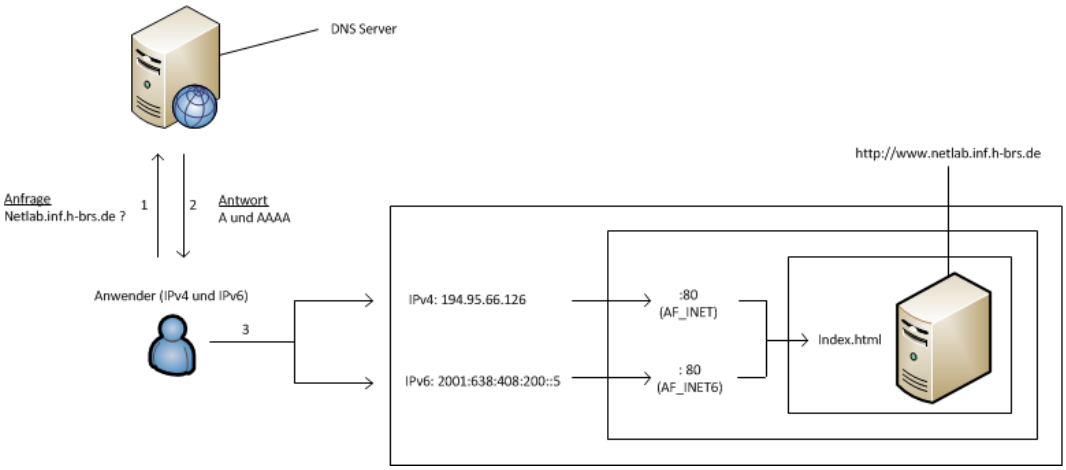


Abbildung 1.5: Monitoring eines Webservers in einer Dual-Stack-Umgebung

einen zusätzlichen Ping über ICMPv6 realisiert. Die Abfrage einer Webseite über

IPv6 erfordert eine weitere Methode, die eine HTTP-Verbindung über einen Port der Adressfamilie *AF_INET6* aufbaut. Durch die zusätzlich Abfrage eines AAAA-Records kann die Korrektheit des DNS-Entrys für IPv6 überwacht werden.
Als Voraussetzung für das Monitoring müssen somit zunächst die Methoden, die bisher ausschließlich für die Überwachung von IPv4-Funktionalität genutzt wurden, auf IPv6 angepasst werden. Sowohl der Ping, als auch das testweise Abrufen einer Datei über HTTP und das Überprüfen des jeweiligen DNS-Eintrags müssen doppelt, für jeweils IPv4 und IPv6, konfiguriert und angelegt werden. Da die Definition von zwei separaten Methoden für jeden Service einen Mehraufwand für das Netzmanagement bedeutet, sollte eine Integration von IPv6 in heutige Methoden angestrebt werden.

Availability Management	- Anpassung von bestehenden Methoden auf IPv6 - Integration von IPv6 in vorhanden Methoden - Zusätzliches Monitoring von Services über Portbereich *AF_INET6*

Tabelle 1.8: Availability Management: Anforderungen

Event/Incident Management

Im Rahmen des Netzmanagements umfassen sowohl das Event, als auch das Incident Management sehr ähnliche und zusammenhängende Aktivitäten, sodass eine Anforderungsanalyse beider Prozesse in einem Schritt durchgeführt wird.
Das Event und Incident Management befasst sich neben der Erkennung und Klassifizierung von Events bzw. Incident mit deren Behandlung. Das Erkennen und Klassifizieren von Events wird primär im Event Management abgehandelt. Die Analyse und Behebung von Events wird durch die für einen Service unkritische Ausprägung von Events im Rahmen des Event Managements sekundär behandelt. Durch die für einen Service kritischen Incidents liegt der Fokus des Incident Managments auf der Fehleranalyse und -behebung.
Die Analyse im Rahmen des Event und Incident Managements der Netzlabore wird entlang der in ITIL festgelegten Aktivitäten realisiert. Zur Erkennung von Events und Incidents werden für den Service "Webserver" folgenden Metriken und Schwellwerte genutzt:

Dienst	Metrik	warning	critical
HTTP	Antwortzeit	5s	10s
DNS	Antwortzeit	5s	10s
Ping	RTT	3000ms	5000ms
	Packet Loss	80%	100%

Tabelle 1.9: Schwellwerte des Services "Webserver"

Für jede genannten Metrik sind Schwellwerte für einen warnenden und einen kritischen Zustand definiert, über die ein Event klassifiziert werden kann.
Die zusätzliche Anbindung des Webservers über IPv6 wird nicht in den bereits für IPv4 definierten Triggern berücksichtigt. Antwortzeiten können auf Basis des zugrunde liegenden Internet Protocols variieren, sodass Events/Incident, die auf die IPv6-Anbindung zurück zu führen sind, nicht erkannt werden können. Für jede Methode muss somit ein zusätzlicher Trigger für IPv6 eingerichtet werden. Daraus folgt, dass die zusätzlichen Trigger im Fehlerfall weitere Events erzeugen. Ein Fehler, der nicht auf IPv4 oder IPv6 beruht, wie z.B. der Ausfall eines Servers, resultiert infolgedessen in zwei Events. Identisch zu einem Netzmanagement von IPv4-only-Umgebungen verlangt das Event Management nach einer Korrelation von Triggern und den daraus generierten Events. Der Ausfall eines DNS- oder Webservers würde in diesem Fall nur einen Event generieren. Die Beschreibung von Events muss im Rahmen einer Korrelation von Triggern angepasst werden, sodass der auslösende Trigger erkennbar ist.

Die durch einen Event oder Incident angestoßene Analyse eines Fehlers ist ein sehr individueller Prozess. Dennoch verlangt insbesondere das Incident Management nach einer optimalen Unterstützung bei der Analyse.
Die Herkunft eines Fehlers wird durch die weitere Anbindung des Webservers über IPv6 zusätzlich verkompliziert. Fehler können nicht mehr grundsätzlich einem ausgefallenen Router oder einer fehlerhaften Interfacekonfiguration zugeordnet werden. IPv6 führt somit, durch die zusätzliche Anbindung, eine weitere Fehlerdimension ein. IPv4- und IPv6-Traffic kann beispielsweise unterschiedlich geroutet werden und Fehler können von IP-spezifischer Natur sein. Folgende Fehlerkategorien sind in Dual-Stack-Umgebungen möglich:

- IPv4-spezifische Fehler (z.B. Fehlerhafte IPv4-Interface-Konfiguration)
- IPv6-spezifische Fehler (z.B. Ausfall eines Tunnels)
- IP-unabhängige Fehler (z.B. Defekte Festplatte, Ausfall eines Gateways)

Abhängig von der Fehlerursache bieten sich unterschiedliche Sichten für eine Fehleranalyse an. Wenn durch eine Incidentbeschreibung ersichtlich ist, dass es sich um ein IPv6-spezifisches Problem handelt muss ein Tool die Möglichkeit bieten Dienste bzw. Netze ausschließlich oder primär mit IPv6-relevanten Informationen anzuzeigen. Durch die Filterung von irrelevanten Informationen kann so ein Fehler schneller identifiziert und behoben werden. Auf der anderen Seite hilft eine integrierte Sicht auf eine Infrastruktur bei der Analyse von Fehlern, die IP-unspezifisch sind und beide Protokolle gleichermaßen betreffen. Der Ausfall einer Verbindung zu einem Gateway lässt sich beispielsweise besser durch eine Übersicht mit allen Objekten und Informationen diagnostizieren.
Im Kontext der Fehleranalyse werden somit primär Anforderungen an die Darstellung, die bei einer effizienten Fehleranalyse unterstützten muss, gestellt. Eine Fehlerbezogene Ansicht über Elemente wie Objekte, Incidents oder ganze Netze sind die Grundlage für eine schnelle Servicewiederherstellung. IP-Spezifische Fehler erfordern eine separierte Sicht, IP-unabhängige Fehler eine integrierte Sicht auf die für den Fehler relevante IT-Infrastruktur.

Event/Incident Management	- Zusätzlich Definition von Triggern für IPv6 - Korrelation von IPv4- und IPv6-Triggern - Separierte Sichten auf IPv4- und IPv6-Infrastruktur (z.B. durch Filtermechanismen) - Integrative Darstellung

Tabelle 1.10: Event/Incident Management: Anforderungen

Capacity Management

Das Capacity Management befasst sich mit der Bereitstellung von Kapazitäten auf Basis von aktuellen und zukünftigen Anforderungen. Mit Hilfe von Performancedaten können unter anderem Über- und Unterkapazitäten aufgedeckt und behoben werden. Zusätzlich können Aussagen über die Servicequalität durch die Auswertung von QoS-Parametern getroffen werden. [Bei08, S. 70]

Für das Monitoring eines Webservers werden typischerweise folgenden Metriken in einer IPv4-Umgebung gemessen:

- RTT
- HTTP-Antwortzeit
- DNS-Antwortzeit

Grafik 1.6 zeigt eine Ansicht auf die Round Trip Time (RTT) eines Webservers. In vielen Fällen muss im Rahmen des Capacity Management keine Unterscheidung zwischen IPv4- und IPv6-Daten stattfinden. Wenn der gesamte ausgehende Traffic eines Unternehmens gemessen werden soll, reicht eine Statistik über den Schicht-2 Traffic aus. Auf der anderen Seite verlangen andere Metriken, abhängig von der Infrastruktur, IP-spezifische Performancedaten. Durch die Tunnelanbindung der Netzlabore ist es beispielsweise wichtig, die RTT und die HTTP Response Time IP-abhängig zu messen. Neben der bereits zuvor geforderten Integration von IPv6 bei

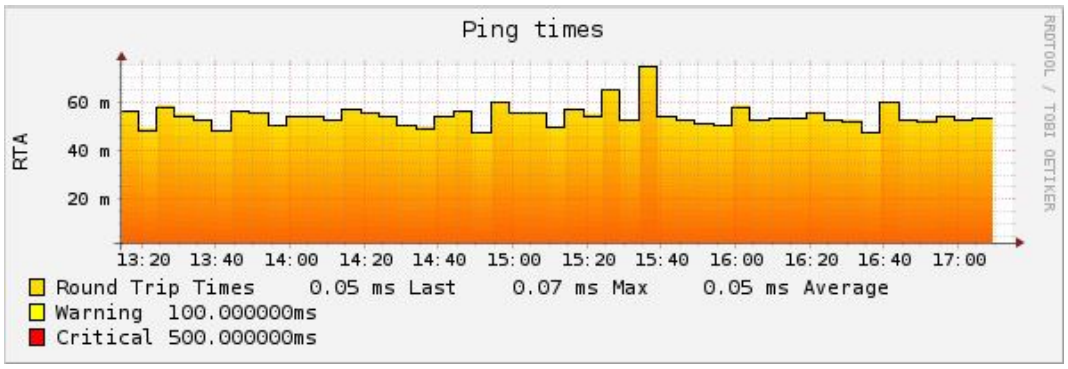


Abbildung 1.6: RTT eines Webservers

der Überwachung von Services und Generierung von Events verlangt das Performance Management eine separate Betrachtung von IPv6- und IPv4-Daten. Ein Messwert, wie etwa das Transferaufkommen, kann in meisten Fällen durch eine integrierte Sicht auf den Gesamttraffic über IPv4 und IPv6 realisiert werden. Andere Messwerte, wie eine RTT oder eine HTTP-Antwortzeit, erfordern in vielen Fällen eine separierte Betrachtung von IPv4 und IPv6. Ein Fehler, der auf die IPv6-Anbindung über den Tunnel zum Deutschen Forschungsnetz zurückzuführen ist, ist ein typischer Anwendungsfall in den Netzlaboren, der eine Separation der Antwortzeiten erfordert. Hierzu sollten in Dual-Stack-Umgebungen alle bisher erhobenen Messwerte auf eine Integration von IPv6 oder eine getrennte Betrachtung zu IPv4 untersucht werden.

Capacity Management	- Zu IPv4 korrespondierende Betrachtung von IPv6-QoS-Daten - Separative Betrachtung von QoS-Daten (z.B. RTT) - Integrative Betrachtung von QoS-Daten (z.B. Traffic)

Tabelle 1.11: Capacity Management: Anforderungen

1.2.3 Service: Internetanbindung des Netzlabors C055

Das Netzlabor C055 wird insbesondere für Übungen, Vorlesungen und Praktika verwendet. Es wird dazu eine Vielzahl von Workstations den Studenten bereitgestellt. Die Labor-PCs sind über diverse physisch voneinander getrennte Netze miteinander und dem Internet verbunden. Zusätzlich können zwei WLANs von den Studenten für die Anbindung eigener Laptops an das Internet verwendet werden. Sowohl die Kabelanbindung als auch das WLAN stellen eine IPv4- und eine IPv6-Anbindung für die Studenten und Mitarbeiter zur Verfügung. Viele Übungen und Praktika setzen für eine Durchführung der Aufgaben eine Internetverbindung voraus. Eine funktionierende Anbindung an das Internet ist also für den Betrieb des Labors von grundlegender Natur.

Leistungsbeschreibung

Es wird für die folgende Vereinbarung über die Bereitstellung einer Internetanbindung für das Netzlabor C055 ein „interner SLA" verwendet. Die Anforderungen sind hinsichtlich der zu erbringenden Leistungen also nicht übermäßig streng definiert. Leistungsziele und Metriken werden wie bei der Beschreibung des Webservers lediglich informell festgehalten. Die Beschreibung des Services "Internetanbindung des Netzlabors Hochleistungsnetze und Mobilkommunikation" in Tabelle 1.12 kann somit nicht als Vertrag, sondern als Absichtserklärung betrachtet werden. Durch die produktive Nutzung der Internetanbindung des Netzlabors während Vorlesungen und Übungen ist eine schnelle Reaktionszeit und Wiederherstellung der Konnektivität im Fehlerfall erforderlich. Dabei muss die Anbindung sowohl über IPv4 als auch über IPv6 gewährleistet sein. Viele Übungen verwenden für die Durchführung beide Anbindungen der Netzlabore.
Nachfolgend wird der Service "Internetanbindung des Netzlabores Hochleistungsnetze und Mobilkommunikation" im Rahmen der in Kapitel **??** beschriebenen ITIL-Prozesse analysiert.

SLA-Merkmal	Beschreibung
Kurzbeschreibung	- Bereitstellung einer Internetanbindung für das Netzlabor für Hochleistungsnetze und Mobilkommunikation (C055) - IPv4 und IPv6
Serviceinhalte	- Anbindung der Workstations an das Internet über IPv4 und IPv6 - Bereitstellung eines WLANs für studentische Laptops und Labormitarbeiter (v4/v6)
Service- und Reaktionszeiten	- Schnelle Reaktionszeit bei Ausfall der Internetverbindung (Servicelevel: gold) - Schnelle Wiederherstellung der vollständigen Internanbindung (Servicelevel: gold)
Mitwirkungspflichten	- *Störungen und Endstörungen müssen per E-Mail an die Verantwortlichen der Netzlabore gemeldet werden* - *Als Ansprechpartner muss ein Labormitarbeiter über E-Mail erreichbar sein*

Tabelle 1.12: Leistungsbeschreibung für den Service „Internetanbindung des Netzlabors Hochleistungsnetze und Mobilkommunikation"

Availability Management

Die Verfügbarkeit ist, wie in Tabelle 1.12 beschrieben, als die Bereitstellung der Internetanbindung über IPv4 und IPv6 definiert. Grafik 1.7 zeigt die vereinfachte Anbindung von C055 an das Deutsche Forschungsnetz (DFN), über das die Internetanbindung der Hochschule realisiert wird. Ein Merkmal der Internetanbindung ist die getrennte Anbindung von IPv4 und IPv6. Trotz, dass beide Anbindungen im DFN terminieren, wird die IPv6-Anbindung über einen IPv6-in-IPv4 Tunnel realisiert.
Ähnlich der Überwachung eines Webservers sind für die Überwachung der Verfügbarkeit der Internetverbindung über IPv4 folgende Schritte notwendig:

- Ping, externe Adresse
- Ping, Gateways (C015, C055 & Fachbereich)
- Abfrage eines Ressource Records (DNS)
- Beziehen einer IPv4-Adresse (DHCP)

Das Monitoring der IPv6-Anbindung des Netzlabors erfordert dabei identisch zu einem Monitoring eines Webservers auch hier die Definition weiterer Methoden für die jeweiligen Dienste und Hosts. Zusätzlich muss der Tunnelendpunkt des IPv6-Tunnels in das Monitoring mit aufgenommen werden. (siehe Abbildung 1.7) Folgende Schritte

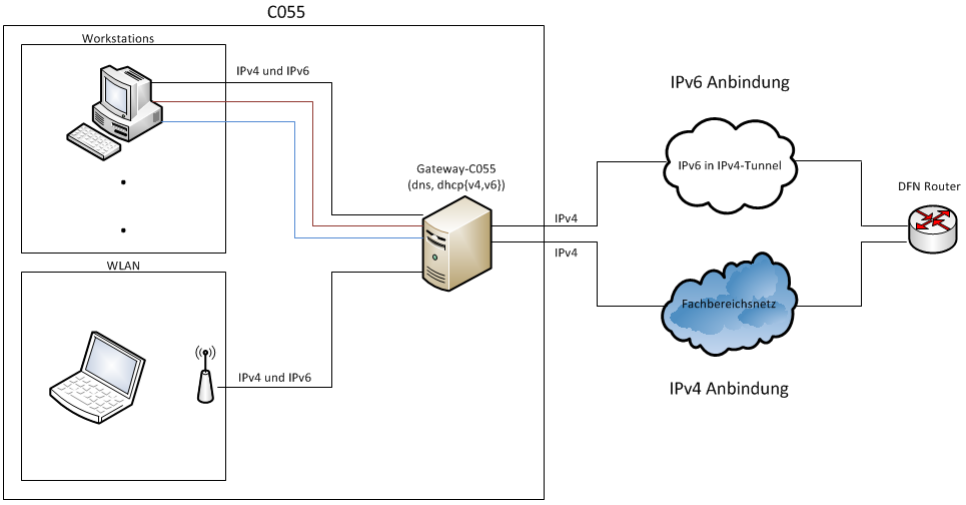


Abbildung 1.7: Internetanbindung des Netzlabors für Hochleistungsnetze und Mobilkommunikation

sind somit für das Monitoring der IPv6-Anbindung des Netzlabors erforderlich.

- Ping6, externe Adresse
- Ping6, Gateways (C015 & C055)
- Ping6, DFN-Gateway
- Abfrage eines Ressource Records (DNS)
- Beziehen einer IPv6-Adresse (DHCPv6)

Im Gegensatz zu DNS handelt es sich bei DHCPv6 um ein für IPv6 neu spezifiziertes Protokoll. [DBV+03] Die Kommunikation findet zudem über Multicast und Link-Local Adressen statt. Die Anpassung einer solchen Methode fordert somit eine tiefer gehende Anpassung der Funktionalität und Kommunikationsabläufe.

Die Überwachung der Verfügbarkeit eines komplexen Services, wie der Anbindung der Netzlabore an das Internet, erfordert durch die Dual-Stack-Umgebung eine Vielzahl von Anpassung und bedeutet für das Netzmanagement einen Mehraufwand. Viele Anforderungen, die sich aus der Analyse des Webservers ergaben, finden sich auch bei der Internetanbindung der Netzlabore wieder. Der Zugriff auf Protokolle wie ICMPv6 und das Monitoring von Diensten über die IPv6-Ports der Portfamilie *AF_INET6* gehört dabei zu den ersten grundlegenden Anforderungen. Eine mehrfache Definition von Servicechecks wie bei der Prüfung der Erreichbarkeit von Hosts über einen Ping

oder der Abfrage eines DNS-Servers bedeutet einen Mehraufwand für das Netzmanagement. Ähnlich der Überwachung eines Webservers fehlt es an dieser Stelle an einer integrierten Sicht auf einen Service.
Das Monitoring von DHCPv6 ist ein Beispiel für eine Methode, die nicht über eine simple Anpassung des Zugriffs auf den IP-Stack für den Einsatz über IPv6 verwendet werden kann. Somit müssen neben der Integration von IPv6 in bereits bestehende Methoden auch neue Methoden konzeptioniert und implementiert werden.

Availability Management	- Anpassung von bestehenden Methoden auf IPv6 - Integration von IPv6 in vorhandene Methoden - Zusätzliches Monitoring über *AF_INET6* - Neukonzeption von Methoden (z.B. DHCP6)

Tabelle 1.13: Event/Incident Management: Anforderungen

Event/Incident Management

Die Analyse im Rahmen des Event und Incident Managements wird wie bereits in Kapitel 1.2.2 entlang der Aktivitäten des Event und Incident Managements durchgeführt.
Aus folgenden Metriken werden bei einem Monitoring der Internetanbindung der Netzlabore über IPv4 Events erzeugen:

Dienst	Metrik	warning	critical
DHCP	Pool-Auslastung	80%	99%
	Antwortzeit	5s	10s
DNS	Antwortzeit	5s	10s
Ping	RTT	3000ms	5000ms
	Packet Loss	80%	100%

Tabelle 1.14: Schwellwerte des Services "Webserver"

Für jede Metrik ist sowohl ein warnender als auch ein kritischer Schwellwert definiert, anhand derer eine Klassifizierung vorgenommen wird.
Ähnlich zu den in Kapitel 1.2.2 definierten Schwellwerten bei der Überwachung eines Webservers decken die hier genannten Metriken die Internetanbindung über IPv6 nicht ab. Es müsste für jede der genannten Metriken zusätzliche Trigger für IPv6 definiert werden, sodass ein Event, der auf die IPv6-Anbindung der Netzlabore zurück zu führen ist, erkannt werden kann. Die Definition weiterer Trigger führt zu einem Anstieg von generierten Events. Der Ausfall des DHCP- oder DNS-Servers führt zu

doppelten Events, obwohl die Events auf eine Fehlerquelle zurück zu führen sind. Durch eine Korrelation der jeweiligen IP-spezifischen Trigger können Events auf die in IPv4-only-Umgebungen typische Anzahl an Events reduziert werden.
Für die Fehleranalyse ist die Bereitstellung und Darstellung von IP-spezifischen Informationen auch für diesen Service grundlegend. Der Ausfall des Tunnelendpunkts oder eine fehlerhafte IPv6-Konfiguration auf einem der Gateways würde zu einem Fehler führen, der für die Behebung ausschließlich IPv6-relevante Informationen benötigt.
Die Anforderungen des Event und Incident Managements überschneiden sich somit zu den bereits im Rahmen der Analyse des Webservers eruierten Anforderungen. Fehlerabhängig müssen sowohl separierte, als auch integrierte Sichten für die Fehleranalyse bereitgestellt werden.

Event/Incident Management	- Zusätzlich Definition von Triggern für IPv6 - Korrelation von IPv4- und IPv6-Triggern - Separierte Sichten auf IPv4- und IPv6-Infrastruktur - Integrative Darstellung

Tabelle 1.15: Event/Incident Management: Anforderungen

Capacity Management

Metriken, die bei der Überwachung der Internetanbindung des Netzlabors C055 über IPv4 genutzt werden sind:

- Auslastung des DHCP-Pools
- Traffic
- RTT
- DNS-Antwortzeit

Die Auslastung des DHCP-Pools ist eine Metrik, die einen kritischen Einfluss auf eine Internetanbindung haben kann. Durch einen zu klein dimensionierten Pool können bei einer hohen Auslastung keine weitere Adresse vergeben werden. Zusätzlich kann über die Messung der Antwortzeiten und des Traffics eine Aussage über die Auslastung und Funktion der Internetanbindung getroffen werden.
Identisch zu der Betrachtung von geeigneten Parametern für das Monitoring von Performancedaten im Rahmen des Services "Informationsbereitstellung der Netzlabore" muss eine Unterscheidung von Parametern in eine separate und eine integrierte Sicht vorgenommen werden. Die RTT ist ein Parameter, der durch die Anbindung über einen Tunnel eine von IPv4 isolierte Betrachtung erfordert. Der Traffic kann sowohl integriert (siehe Abbildung 1.8), als auch für einen besseren Informationsgehalt, separiert betrachtet werden. IPv6-Traffic wird im Umfeld der Hochschule und

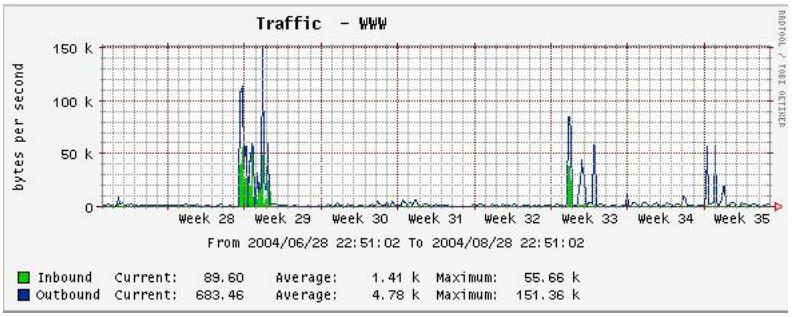


Abbildung 1.8: Trafficaufkommen der Internetanbingung (IPv4)

des Fachbereichs nicht gemessen. Somit ist es auch für die Labore wichtig festzustellen wie sich der Traffic auf Basis von IP aufteilt. Die DHCP-Pool Auslastung ist eine Metrik, die im Rahmen von Dual-Stack-Umgebungen in der Regel ausschließlich eine Betrachtung über IPv4 benötigt, da IPv6-Netze typischerweise überdurchschnittlich groß definiert werden.

Capacity Management	- Zu IPv4 korrespondierende Betrachtung von IPv6-QoS-Daten - Separative Betrachtung von QoS-Daten (z.B. RTT) - Integrative Betrachtung von QoS-Daten (z.B. Traffic) - Betrachtung von IPv4-QoS-Daten auf Relevanz für IPv6 (z.B. DHCP-Pool)

Tabelle 1.16: Capacity Management: Anforderungen

1.3 Architektur einer Netzmanagementplattform

Die Analyse der Unterschiede zwischen IPv4 und IPv6 hat erste Anforderungen an das Netzmanagement auf Basis der Protokollspezifikation aufgedeckt. Durch die Analyse der zwei Services der Netzlabore konnten Anforderungen des IT-Service-Managements eruiert werden. In einem weiteren Schritt wird in diesem Kapitel die Architektur von Netzmanagementtools untersucht. Als Basis für die Analyse wird die von Hegering in [HAN99] beschriebene Architektur einer Netzmanagementplattform verwendet. Die in Abbildung 1.9 dargestellte Architektur teilt den Aufbau einer Netzmanagementplattform in Basisfunktionalität, Managementfunktionalität und eine grafische Oberfläche ein. Die grafische Oberfläche (GUI) ermöglicht dem Benutzer den Zugriff auf die Funktionen und Methoden der Managementplattform. Gleichzeitig wird durch die GUI das zu überwachende Netz dargestellt. [HAN99, S. 282] Die unter der grafischen Benutzeroberfläche liegende Managementfunktionalität beinhaltet die für das Netzmanagement wichtigen Methoden, welche für die Überwachung

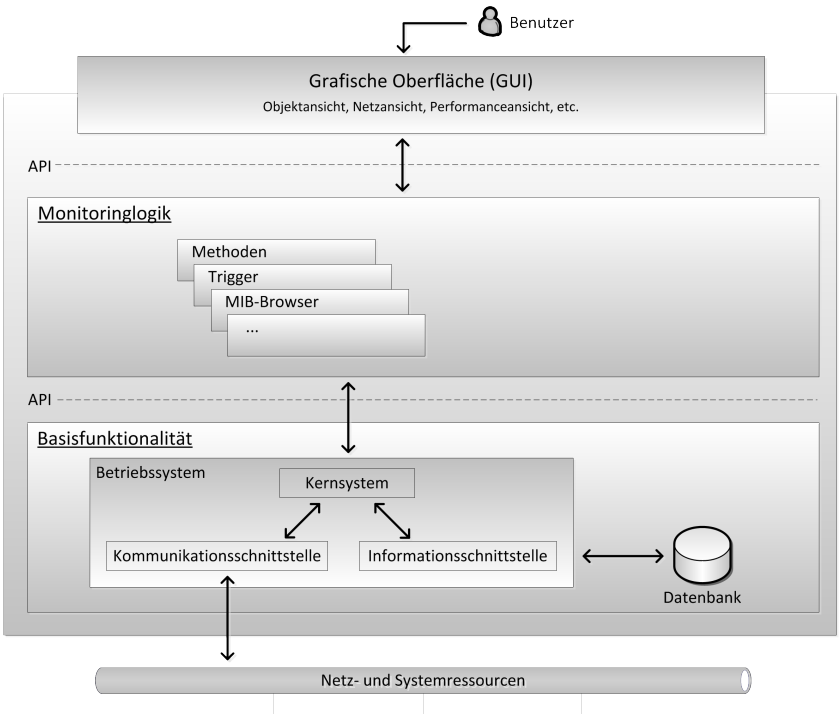


Abbildung 1.9: Aufbau einer Netzmanagementplattform (Vgl. [HAN99, S. 278])

der verschiedenen Objekte und Anwendungen verwendet werden. Durch die Basisfunktionalität werden den Anwendungen des Netzmanagementtools die benötigten Basisdienste, wie den Zugriff auf die Datenbank oder den IP-Stack, bereitgestellt. Insbesondere das Zusammenspiel der einzelnen Elemente einer Netzmanagement-Plattform kann durch eine Analyse der Architektur berücksichtigt werden. Eine Analyse von für das Monitoring genutzten spezifischen Managementfunktionalitäten und Sichten wird bereits durch die in Kapitel 1.2 durchgeführte Analyse von Services abgedeckt.

1.3.1 Basisfunktionalität

Das Betriebssystem ermöglicht dem Netzmanagement den Zugriff auf die Kommunikations- und Informationsschnittstelle über eine API. Nachfolgend wird eine Anforderungsanalyse entlang der bereitgestellten Dienste der jeweiligen Schnittstelle durchgeführt.

Informationsschnittstelle

Über die Informationsschnittstelle können Informationen abgespeichert und gelesen werden. Für Managementzwecke stellt eine Netzmanagementplattform in der Regel eine umfangreiche Datenbasis in Form einer Datenbank bereit. Über die Informationsschnittstelle können Informationen wie Meta-, Objekt- oder Topologiedaten abgespeichert und abgerufen werden. [HAN99, S. 280] Das Netzmanagement einer Dual-Stack-Umgebung erfordert nur wenige Anpassungen im Rahmen der Informationsverarbeitung des Betriebssystems. Es führt in einem ersten Schritt zu einer erhöhten

Datenmenge, resultierend aus der Speicherung von zusätzlichen IPv6-relevanten Informationen. Weiterhin müssen die bisher für IPv4 dimensionierten Datenbankfelder für die 128-Bit langen IPv6-Adresse angepasst werden. Ein identisches Bild zeigt sich bei einer für das Configuration Management verwendeten Datenbank (CMDB). Die bisher für die Speicherung von IPv4-Adressen genutzten Felder müssen auf die Länge von IPv6-Adressen angepasst werden. Die Umstrukturierung einer Datenbank ist von der jeweiligen Modellierung abhängig und wird daher nicht weiter betrachtet. Abgesehen von Anpassungen der Felder, werden keine weiteren Anforderungen seitens der Informationsschnittstelle gestellt.

Informationsschnittstelle	- Anpassung von den für IPv4-Adressen genutzten Datenbankfeldern.

Tabelle 1.17: Informationsschnittstelle: Anforderungen

Kommunikationsschnittstelle

Über die Kommunikationsschnittstelle wird der Zugriff auf externe Netz- und Systemressourcen (Objekte) ermöglicht. Abbildung 1.10 zeigt den Aufbau der Kommunikationsschnittstelle, die die Kommunikation mit Netzressourcen über den IP-Stack oder andere proprietäre Protokolle ermöglicht. Für das Management von Dual-Stack-

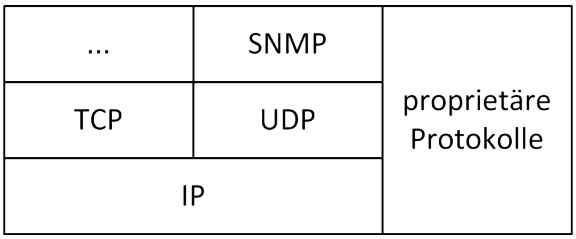


Abbildung 1.10: Kommunikationsschnittelle einer Netzmanagementplattform (Vgl. [HAN99, S. 279])

Umgebungen muss das Betriebssystem über die Kommunikationsschnittelle den Zugriff auf den zusätzlichen IPv6-Stack ermöglichen und dementsprechend mit einer link-local und globalen IPv6-Adresse konfiguriert sein. (siehe Kapitel 1.1)

Kommunikationsschnittstelle	- Bereitstellung des Zugriffs auf den IPv6-Stack.

Tabelle 1.18: Kommunikationsschnittstelle: Anforderungen

1.3.2 Managementfunktionalität

Die Managementfunktionalität einer Netzmanagementplattform basiert primär auf Methoden und damit verbunden Triggern. Die in Kapitel 1.2 durchgeführte An-

forderungsanalyse von Services der Netzlabore deckt Anforderungen aus diesen beiden Bereichen ab.
Neben spezifischen Methoden, die für das Monitoring und Management von Service verwendet werden, basiert die Managementfunktionalität auf Basismethoden. Insbesondere ein MIB-Browser als auch das Auto-Discovery von Netzressourcen findet sich in einem Großteil von Netzmanagementplattformen wieder. [HAN99] Im Folgenden werden sowohl der MIB-Browser, als auch das Auto-Discovery für eine Anforderungsanalyse herangezogen.

MIB-Browser

Netzmanagementplattformen unterscheiden sich, neben dem Funktionsumfang, durch die unterstützten Methoden und Anwendungen, über die Objekte überwacht werden können. Nichtsdestotrotz ist ein MIB-Browser eine grundlegende Anwendung, die von allen Netzmanagementplattformen implementiert wird. [HAN99, S. 288] Über den MIB-Browser können Managementinformationen eines Systems angezeigt und bearbeitet werden. Als Voraussetzung für die Bewegung in einer baumartig strukturi-

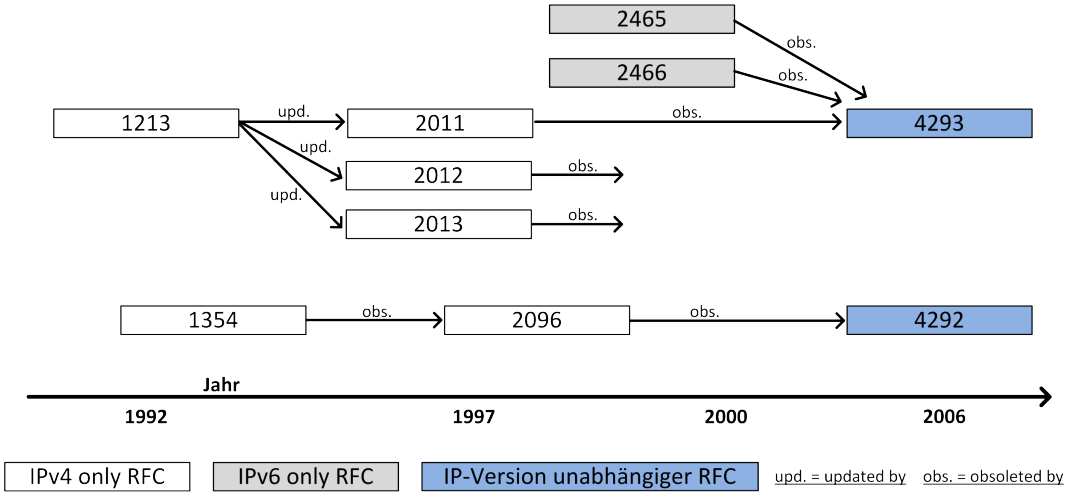


Abbildung 1.11: IP-spezifische MIB-Übergänge (Vgl. [cis12])

erten MIB muss sowohl das entfernte System als auch die Netzmanagementplattform über identische MIBs verfügen. Ähnlich den Anpassungen, die bereits im Rahmen der Datenbank gefordert wurden, mussten auch im Rahmen der MIBs Anpassungen von verschiedenen Feldern vorgenommen werden. MIBs, die für das Speichern von IP-Adressen einen 32-Bit breiten Datentyp verwendet haben, wurden für den Einsatz in einer Dual-Stack- oder IPv6-Umgebung angepasst. Abbildung 1.11 zeigt den Verlauf der jeweiligen Anpassungen der betroffenen MIBs für IPv6. Dazu wurde als Ersatz für die in RFC 2011 definierte MIB-2 durch RFC 2465 und RFC 2466 eine alternative MIB, die identische Informationen enthält, definiert. Erst mit der im Jahr 2006 spezifizierten MIB "Management Information Base for the Internet Protocol (IP)" können sowohl IPv4, als auch IPv6 Informationen über SNMP gle-

ichermaßen abgefragt werden. Ein identisches Bild zeigt sich bei der ebenfalls 2006 spezifizierten MIB "IP Forwarding Table MIB" (RFC 4292), die neben IPv4-Adressen auch IPv6-Adressen enthalten kann.

MIB-Browser	- Unterstützung von RFC 4292 und 4293 für das Abfragen von IPv6-Managementinformationen.

Tabelle 1.19: MIB-Browser: Anforderungen

Auto-Discovery

Das Auto-Discovery ist im Rahmen des Netzmanagements eine weitverbreitete Möglichkeit Netzressourcen innerhalb einer spezifizierten IP-Spanne aufzudecken. Abbildung 1.12

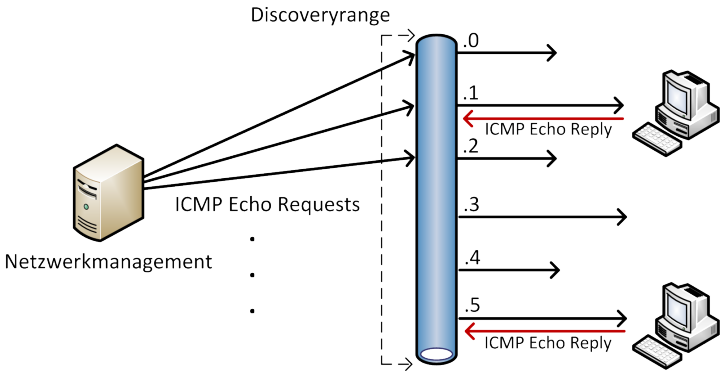


Abbildung 1.12: Auto-Discovery von Netzressourcen in IPv4-only-Umgebungen

zeigt die typische Funktionsweise des Auto-Discovery in IPv4-Umgebungen. Das Aufdecken von Netzressourcen innerhalb der spezifizierten IP-Spanne oder eines ganzes Netzes wird über einen Ping an jede einzelne Adresse realisiert. Ressourcen, die auf den Ping antworten werden in die Liste von aufgedeckten Objekten eingetragen. Der Administrator kann mit dieser Liste in einem nachfolgenden Schritt relevante Objekte durch eine weitergehende Konfiguration in das Netzmanagement aufnehmen. Das zeitaufwendige sukzessive Eintragen von IP-Adressen in die Eingabemaske der Objektdefinition entfällt somit.
Durch die Größe von IPv6-Netzen kann ein Scannen von ganzen Netzen oder größeren Netzabschnitten nicht mehr über ein Ping jeder einzelnen Adresse realisiert werden. Das Auto-Discovery muss infolgedessen für IPv6- und Dual-Stack-Umgebungen angepasst werden.
Eine Analyse der verschiedene Möglichkeiten eines Auto-Discoverys in einer IPv6-Umgebung wurde bereits in Ansätzen in der Veröffentlichung "Research of the topology auto-discovery approach in the IPv6 access network" ([Zen05])behandelt und wird an dieser Stelle nicht weiter betrachtet.

Auto-Discovery	- Anpassung des Auto-Discovery-Mechanismus.

Tabelle 1.20: Auto-Discovery: Anforderungen

1.3.3 Grafische Oberfläche

Netzmanagementplattformen unterscheiden sich neben einem teils abweichenden Umfang von Managementfunktionen durch die unterschiedliche Visualisierung von Informationen. Eine Formulierung von allgemeinen Anforderungen, die an die grafische Oberfläche durch das Netzmanagement von Dual-Stack-Umgebungen gestellt werden, ist durch die Serviceanalyse in Kapitel 1.2 berücksichtigt.
Ein wichtiges Merkmal der grafischen Oberfläche ist die Bereitstellung verschiedener *Views*, die den unterschiedlichen Benutzergruppen der Plattform eine für die jeweilige Aufgabenstellung angepasste Sicht auf das Netz anbieten. [HAN99, S. 284]
Eine Untermenge an Sichten, die durch eine Netzmanagementplattform für das Netzmanagement bereitgestellt werden sollen lässt sich durch die von Hegering beschriebenen Darstellung einer Infrastruktur definieren. Demnach lässt sich durch eine Sicht auf Objekte und einer weiteren Sicht auf Objektrelationen (z.B. Netze) die Darstellung einer Infrastruktur realisieren. [HAN99, S. 284] Die Analyse von Services in Kapitel 1.2 hat gezeigt, dass über die Darstellung von Infrastruktur nicht alle ITIL-Prozesse optimal unterstützt werden können.

ITIL-Prozess	Relevante Elemente
Event Management	Infrastruktur, Events
Incident Management	Infrastruktur, Incidents
Capacity Management	Performancedaten

Tabelle 1.21: Nutzung von Sichten innerhalb von ITIL-Prozessen

Sowohl das Event, als auch das Incident Management benötigen für die Analyse von Fehlern eine Übersicht über die jeweilige Infrastruktur und greifen somit auf die zuvor definierte Objekt- und Netzansicht zurück. Die Auflistung von Events und Incidents ist eine View, die durch die Darstellung der Infrastruktur nicht abgedeckt ist. Zusätzlich wird im Rahmen des Capacity Managements nach einer Sicht, in der QoS-Parameter über einen zeitlichen Verlauf dargestellt werden, verlangt (siehe Tabelle 1.21).
Auch wenn sich keine Anforderungen auf Basis von spezifischen Sichten definieren lassen, wird nachfolgend eine Beschreibung der jeweiligen Sichten gegeben, sodass die Konzeption der Oberfläche auf Basis der zuvor eruierten allgemeinen Anforderungen auf die hier genannten Sichten angewendet werden kann.

Objektansicht

Die Objektansicht ist essentieller Bestandteil jeder Netzmanagementplattform. Informationen, die ein Objekt (z.B ein Host oder Service) betreffen, können über diese

Ansicht eingesehen werden. Neben der Anzeige von für die Verfügbarkeit spezifischen Parametern, wie der IP-Adresse und einer Schnittstellenbeschreibung, werden häufig auch die dazu relevanten Performancedaten angezeigt. Der Einsatzzweck dieser Ansicht besteht hauptsächlich in der Fehleranalyse. Durch den Ausfall eines Webservers wird beispielsweise in aller Regel in einem ersten Schritt eine Analyse über die sogenannte Objektansicht durchgeführt um sicherzustellen, dass die für den Service benötigten Hosts auch erreichbar sind und die Antwortzeit in einem angemessenen Rahmen liegt. Falls in dieser Ansicht kein Fehler gefunden werden kann werden weitere Ansichten hinzugezogen. Sollte es sich um den Ausfall eines Servers handeln kann dieser durch einen fehlgeschlagenen Ping in der Objektansicht erkannt werden.
Folgende Elemente finden sich somit in einer typischen Objektansicht innerhalb eines Netzmanagementtools wieder:

- Unique Identifier (Name)
- Status
- Gruppenzugehörigkeit
- Parents (Abhängigkeiten)
- Adressinformationen

Auch wenn eine Sicht wie die Objektansicht von Plattform zu Plattform unterschiedlich bezeichnet wird, lässt sie sich in der Regel über die hier aufgelisteten Elemente identifizieren.

Netzansicht

Die Objektansicht befasst sich mit gekapselten Instanzen eines Netzes. Die Betrachtung einer solchen Instanz in Form eines einzelnen Hosts oder Services ist wichtiger Bestandteil einer Fehleranalyse. Nichtsdestotrotz ist eine Ansicht über ein gesamtes Netz oder definierte Netzabschnitte von essentieller Wichtigkeit. So können Abhängigkeiten zwischen Hosts auf eine übersichtliche Weise dargestellt werden. Dabei ist nicht nur die Fehleranalyse ein typischer Anwendungsfall für die Nutzung einer Netzansicht. Zusätzlich kann diese Ansicht genutzt werden um sich einen Überblick über den derzeitigen Status des Netzes zu verschaffen oder den Netzaufbau und die darin enthaltenen Abhängigkeiten zwischen Hosts zu untersuchen. Häufig können diese Maps mit Hintergrundgrafiken hinterlegt werden, um ein besseres räumliches Verständnis für den Standort der Hosts zu schaffen. Die Darstellung der Netze in Form von Darstellungstypen (Baummodell, Schichtenmodell etc.) wird in jedem Tool anders umgesetzt und spielt für die Darstellung von Dual-Stack-Umgebungen nur eine untergeordnete Rolle.
Für die oben genannten Anwendungsfälle ist es wichtig, dass der Status und wenn gewünscht auch weitere Informationen den Hosts zugeordnet und angezeigt werden.

Eine Netzansicht ohne Statusinformationen würde innerhalb des Netzmanagements keine nennenswerte Verwendung finden. Weitergehend sollen nicht nur ganze Netze angezeigt werden können, sondern auch vordefinierte Gruppen. So kann die Komplexität von großen Netzen in kleine Teile aufgetrennt werden und die Effektivität bei der Fehleranalyse gesteigert werden. [HAN99, S. 283] Folgende Elemente sind somit typische Bestandteile einer Netzansicht:

- Gruppendarstellung
- Abhängigkeiten
- Status der Objekte
- Weitergehende Objektinformationen

Eventansicht

Trotz, dass ein Netzmanagementtool nicht nur für das Aufdecken und Analysieren von Fehlern verwendet werden kann, wird meist ein auf Fehlern basierendes reaktives Verhalten ausgeübt. Die Eventübersicht bietet mit einer Art Auflistung von Events und Incidents ein Einstiegspunkt für die Analyse von Fehlern. Synonyme für eine solche Ansicht sind Problemansicht, Incidentansicht und die hier verwendete Bezeichnung als Eventansicht. [Bei08]
Die Hauptaufgabe dieser Ansicht ist der mit einem Fehlerbericht zu vergleichen. Alle zurzeit im Netz auftretenden Fehler oder Statusänderungen müssen aggregiert dargestellt werden und bereits erste Informationen in Form einer Fehlerbeschreibung enthalten. Von hier aus muss der Event- oder Incidentmanager über Verlinkungen zu den betroffenen Komponenten gelangen können. Zusätzlich wird in vielen Fällen eine Filteroption, für eine übersichtlichere Darstellung der Fehler, angeboten.
Folgende Komponenten werden somit für eine vollständige Eventansicht vorausgesetzt:

- Zuordnung von Host und Service
- Status (Host, Service)
- Statusinformationen (Host, Service)
- Filteroptionen

Performanceansicht

Das Sammeln und Darstellen von Performancedaten ist ein sehr individueller Prozess. Einer der Hauptaufgaben im Rahmen des Capacity Managements ist die Auswahl von geeigneten Parametern für die jeweiligen Services. Nach der Auswahl von relevanten Parametern werden aus diesen Graphen generiert. Graphen beziehen sich zumeist nur auf einen Parameter. Beispiele für solche Parameter sind die Anzeige des Traffics, Portstatistiken oder auch die Zahl der eingeloggten Benutzer auf einem System. Graphen werden meist aus zwei zusammenhängenden Parametern definiert. Internettraffic wird dadurch z.B. in "inbound" und "outbound"-Traffic aufgegliedert. Die Darstellung dieser Daten in Graphen hilft dem Capacity Management Über- und Unterkapazität zu lokalisieren.

1.4 Zusammenfassung

Für eine möglichst vollständige Analyse von Anforderungen an das Netzmanagement von Dual-Stack-Umgebungen wurden verschiedene Quellen herangezogen. Eine Gegenüberstellung von IPv4 und IPv6 hat dabei bereits erste grundlegende Anforderungen auf Basis der IPv6-Spezifikation aufgedeckt. Durch die Analyse von Services konnten in einem weiteren Schritt Anforderungen, die durch das Service-Management entstehen, eruiert wurden. Die Betrachtung unterschiedlicher Services hat dabei gezeigt, dass es neben charakteristischen Anforderungen auch Service-spezifische Anforderungen gibt. Weitere Anforderungen, die durch den Aufbau einer Netzmanagementplattform entstehen, wurden in Kapitel 1.3 berücksichtigt.
Für eine Betrachtung innerhalb der Konzeption werden Anforderungen mit ähnlicher oder identischer Ausprägung in Tabelle 1.22 kumuliert dargestellt.

Kumulierte Anforderung	Detaillierte Anforderung
Adressnotation	- Unterstützung von IPv6-Adressen - Syntaktische Prüfung von Adresseingaben
Portfamilie	- Zusätzliches Monitoring über Portbereich *AF_INET6*
Methoden-Support	- Anpassung von Methoden, die Broadcast-Kommunikation verwenden - Anpassung von Methoden auf die für IPv6 angepassten Hilfsprotokolle - Neukonzeption von Methoden
Methoden-Integration	- Integration von Methoden für IPv6 in vorhandene Methoden
Adressierung	- Parametrisierung von Objekten mit relevanten IPv6-Adressen in Dual-Stack-Umgebungen
SNMP-Support	- Unterstützung von RFC 4292 und 4293 für das Abfragen von IPv6-Informationen
Integrative Darstellung	- Integration von IPv6-Informationen in die grafische Oberfläche
Separierte Darstellung	- Separate Darstellung von IPv4- und IPv6-Informationen - Erweiterte Filtermöglichkeiten für die Darstellung von IP-spezifischen Informationen
Trigger-Korrelation	- Zusätzliche Definition von Triggern für IPv6 - Korrelation von Triggern und den daraus resultierenden Events

Tabelle 1.22: Anforderung an das Netzmanagement von Dual-Stack-Umgebungen

Literaturverzeichnis

[adl12] *ADLON IT Service Management nach ITIL.* www.adlon.de. http://www.adlon.de/loesungen/service-management/. Version: Juli 2012

[Bar12] Barth, Wolfgang: *Nagios - System- und Netzwerk-Monitoring.* 3. aktualisierte und erweiterte Auflage. München : No Starch Press, 2012. – ISBN 978–3–937–51446–8

[Bei08] Beims, Martin: *IT Service Management in der Praxis mit ITIL 3.* 1. Auflage. München, Wien : Hanser Verlag, 2008. – ISBN 978–3–446–41320–7

[Cac12a] *Cacti - thold Plugin.* http://docs.cacti.net/plugin:thold. Version: Juni 2012

[Cac12b] *Offizielle Webseite der Monitoringsoftware Cacti.* www.nagios.org. Version: Januar 2012

[CH09] Chesterfield, J. ; Haberman, B.: *Multicast Group Membership Discovery MIB.* RFC 5519 (Proposed Standard). http://www.ietf.org/rfc/rfc5519.txt. Version: April 2009 (Request for Comments)

[Che06] Chen, C.: Computer Network Management: Best Practices. (2006)

[cis12] *SNMP MIBs and IPv6.* www.cisco.com. http://www.cisco.com/web/about/security/intelligence/ipv6_mib.html. Version: juni 2012

[DBV+03] Droms, R. ; Bound, J. ; Volz, B. ; Lemon, T. ; Perkins, C. ; Carney, M.: *Dynamic Host Configuration Protocol for IPv6 (DHCPv6).* RFC 3315 (Proposed Standard). http://www.ietf.org/rfc/rfc3315.txt. Version: Juli 2003 (Request for Comments). – Updated by RFCs 4361, 5494, 6221, 6422

[DDWL11] Durand, A. ; Droms, R. ; Woodyatt, J. ; Lee, Y.: *Dual-Stack Lite Broadband Deployments Following IPv4 Exhaustion.* RFC 6333 (Proposed Standard). http://www.ietf.org/rfc/rfc6333.txt. Version: August 2011 (Request for Comments)

[DH98] Deering, S. ; Hinden, R.: *Internet Protocol, Version 6 (IPv6) Specification*. RFC 2460 (Draft Standard). `http://www.ietf.org/rfc/rfc2460.txt`. Version: Dezember 1998 (Request for Comments). – Updated by RFCs 5095, 5722, 5871, 6437

[DM05] Durand, J. ; Muyal, S.: IPv6 network management. (2005)

[Dra03] Draves, R.: *Default Address Selection for Internet Protocol version 6 (IPv6)*. RFC 3484 (Informational). `http://www.ietf.org/rfc/rfc3484.txt`. Version: Februar 2003 (Request for Comments)

[End12] Enders, J.: IPv6 im (G)UI - Was ist eine IPv6-Adresse? In: *IPv6-Kongress*, 2012

[FB11] Fleischhauer, K. ; Bonness, O.: On demand IPv4 address provisioning in Dual-Stack PPP deployment scenarios. (2011)

[FF05] Fenner, B. ; Flick, J.: *Management Information Base for the User Datagram Protocol (UDP)*. RFC 4113 (Proposed Standard). `http://www.ietf.org/rfc/rfc4113.txt`. Version: Juni 2005 (Request for Comments)

[FH04] Fink, R. ; Hinden, R.: *6bone (IPv6 Testing Address Allocation) Phaseout*. RFC 3701 (Informational). `http://www.ietf.org/rfc/rfc3701.txt`. Version: März 2004 (Request for Comments)

[Güt10] Gütter, Dr. D.: *Netzwerkmanagement*. Technische Universität Dresden, Februar 2010

[Gua00] Guardini, I.: Migrating from IPv4 to IPv6: planning an effective IPv6 transition. In: *Telecom Lab ITALIA* 24 (2000)

[Hab06] Haberman, B.: *IP Forwarding Table MIB*. RFC 4292 (Proposed Standard). `http://www.ietf.org/rfc/rfc4292.txt`. Version: April 2006 (Request for Comments)

[Hag06] Hagen, Silvia: *IPv6 essentials*. 2nd ed. Sebastopol, CA : O'Reilly Media, Inc., 2006. – ISBN 0596100582

[HAN99] Hegering, Heinz-Gerd ; Abeck, Sebastian ; Neumair, Bernhard: *Integriertes Management vernetzter Systeme - Konzepte, Architekturen und deren betrieblicher Einsatz*. Heidelberg : dpunkt-Verl., 1999. – ISBN 3932588169

[HD06] Hinden, R. ; Deering, S.: *IP Version 6 Addressing Architecture*. RFC 4291 (Draft Standard). `http://www.ietf.org/rfc/rfc4291.txt`. Version: Februar 2006 (Request for Comments). – Updated by RFCs 5952, 6052

[hei12] *World IPv6 Launch Day: Inhalteanbieter schalten IPv6 dazu.* heise.de. `http://heise.de/-1590409`. Version: Juni 2012

[HH05] Hinden, R. ; Haberman, B.: *Unique Local IPv6 Unicast Addresses.* RFC 4193 (Proposed Standard). `http://www.ietf.org/rfc/rfc4193.txt`. Version: Oktober 2005 (Request for Comments)

[HK05] Hsieh, I.P. ; Kao, S.J.: Managing the co-existing network of IPv6 and IPv4 under various transition mechanisms. In: *Information Technology and Applications, 2005. ICITA 2005. Third International Conference on* Bd. 2 IEEE, 2005, S. 765–771

[Hog12] Hogg, Scott: *Networkworld.com - IPv6: Dual Stack where you can; tunnel where you must.* `http://www.networkworld.com/news/tech/2007/090507-tech-uodate.html`. Version: Mai 2012

[HY06] Hirorai, R. ; Yoshifuji, H.: Problems on IPv4-IPv6 network transition. In: *Applications and the Internet Workshops, 2006. SAINT Workshops 2006. International Symposium on* IEEE, 2006, S. 5–pp

[ian12] *IPv6 Multicast Address Space Registry.* `http://www.iana.org/assignments/ipv6-multicast-addresses/ipv6-multicast-addresses.xml`. Version: Juni 2012

[IBM12] *Comparison of IPv4 and IPv6.* `http://publib.boulder.ibm.com/infocenter/iseries/v5r4/index.jsp?topic=%2Frzai2%2Frzai2compipv4ipv6.htm`. Version: März 2012

[Ici12] *Offizielle Webseite der Monitoringsoftware Icinga.* `www.icinga.org`. Version: Mai 2012

[IN07] Iqbal, Majid ; Nieves, Michael: *ITIL Service Strategy.* The Stationery Office, 2007. – ISBN 978–0–113–31045–6

[Jar11] Jarzyna, Dirk: *IPv6 - Das Praxisbuch.* 2011. Aufl. Heidelberg : Hï¿œthig Jehle Rehm, 2011. – ISBN 3826691172

[Kra12] *Kratos Networks - Five Considerations to Ensuring Your Network Management Software is IPv6 Ready.* `http://www.kratosnetworks.com/networkzone/post/five_considerations_to_ensuring_your_network_management_software_is_ip/`. Version: Januar 2012

[mat12] *Aktuelle MATERNA-Befragung: ITIL® kommt in Fahrt.* www.materna.de. `http://www.materna.de/DE/Pages/Presse/Pressemitteilungen/2010/BUI/Aktuelle%`

20MATERNA-Befragung%20ITIL%20kommt%20in%20Fahrt%20aber%20nur%20teilweise.html. Version: Juli 2012

[mic08] *TCP/IP Fundamentals for Microsoft Windows*. Bd. 2. http://www.microsoft.com/en-us/download/details.aspx?id=8781 : Microsoft, 2008. – ISBN 3932588169

[Myp12] *My-Plugin.de*. www.my-plugin.de. Version: Mai 2012

[Nag12a] *Nagios Core Dokumentation*. http://nagios.frank4dd.com/docs/de/plugins.html. Version: Juni 2012

[Nag12b] *Offizielle Webseite der Monitoringsoftware Nagios*. www.nagios.org. Version: Januar 2012

[Nag12c] *Offizielle Webseite der Nagios Plugins*. www.nagiosplugins.org. Version: Mai 2012

[Net12] *Offizielle Webseite der Netzlabore der Hochschule Bonn-Rhein-Sieg*. www.netlab.inf.h-brs.de. Version: Mai 2012

[Oec10] *Internet Addressing: Measuring Deployment of IPv6*. OECD, April 2010

[Ope12a] *Offizielle Webseite der Monitoringsoftware OpenNMS*. www.opennms.org. Version: Mai 2012

[Ope12b] *OpenNMS.org - IPv6 Support*. http://www.opennms.org/wiki/IPv6_Support. Version: Mai 2012

[PD06] Popoviciu, C. ; Dini, P.: IPv6 as a Practical Solution to Network Management Challenges. In: *Computing in the Global Information Technology, 2006. ICCGI'06. International Multi-Conference on* IEEE, 2006, S. 5–5

[pnp12] *PNP4Nagios*. http://www.pnp4nagios.org/. Version: Juni 2012

[Por11] Portmann, S.: *Es gibt keine Adressen mehr im Internet! Wie weiter?* Netcloud AG - Advisory-Team, September 2011

[Rag05] Raghunarayan, R.: *Management Information Base for the Transmission Control Protocol (TCP)*. RFC 4022 (Proposed Standard). http://www.ietf.org/rfc/rfc4022.txt. Version: März 2005 (Request for Comments)

[Ram98] Raman, L.: OSI systems and network management. In: *Communications Magazine, IEEE* 36 (1998), Nr. 3, S. 46–53

[Roo11a] Rooney, T.: *IP Address Management Principles and Practice*. Bd. 16. Wiley-IEEE Press, 2011

[Roo11b] Rooney, T.: *Service Provider IPv6 Deployment Strategies*. BT Diamond IP, 2011

[Rou06] Routhier, S.: *Management Information Base for the Internet Protocol (IP)*. RFC 4293 (Proposed Standard). `http://www.ietf.org/rfc/rfc4293.txt`. Version: April 2006 (Request for Comments)

[SYH+02] Samad, M. ; Yusuf, F. ; Hashim, H. ; Mahfudz, M. ; Zan, M.: Deploying internet protocol version 6 (ipv6) over internet protocol version 4 (ipv4) tunnel. In: *Research and Development, 2002. SCOReD 2002. Student Conference on* IEEE, 2002, S. 109–112

[Tel12] *Deutsche Telekom bietet anonymes Surfen mit IPv6*. `http://www.telekom.com/medien/konzern/93240`. Version: April 2012

[Ver09] Verma, Dinesh C.: *Principles of Computer Systems and Network Management* -. 2nd Printing. Berlin : Springer, 2009. – ISBN 0387890084

[Weg11] Wegener, C.: Netzwerküberwachung: Nagios und Co unter IPv6. In: *IPv6-Kongress*, 2011

[WY12] Wing, D. ; Yourtchenko, A.: *Happy Eyeballs: Success with Dual-Stack Hosts*. RFC 6555. `http://www.ietf.org/rfc/rfc6555.txt`. Version: April 2012 (Request for Comments)

[Zab12] *Offizielle Webseite der Monitoringsoftware Zabbix*. `www.zabbix.com`. Version: Mai 2012

[Zen05] Zengwei, Shen: *Computers Communications and Signal Processing International Conference - Research of the topology auto-discovery approach in the IPv6 access network*. Ieee Press Books, 2005. – ISBN 978—1–4–24–40–0