Copyright and Reference Information: This material (preprint, accepted manuscript, or other author-distributable version) is provided to ensure timely dissemination of scholarly work. Copyright and all rights therein are retained by the author(s) and/or other copyright holders. All persons copying this work are expected to adhere to the terms and constraints invoked by these copyrights. This work is for personal use only and may not be redistributed without the explicit permission of the copyright holder. The definite version of this work is published as
[·] Andreas Berl, Andreas Fischer and Hermann De Meer. Virtualisierung im Future Internet - Virtualisierungmethoden und Anwendungen. *Informatik-Spektrum*, Volume 33, Number 2, pages 186–194, April 2010. The original publication is available at www.springerlink.com (2010).
See http://www.net.fim.uni-passau.de/papers/Berl2010b for full reference details (BibTeX, XML).

Noname manuscript No.
(will be inserted by the editor)

Virtualisierung im Future Internet

Virtualisierungsmethoden und Anwendungen

Andreas Berl · Andreas Fischer · Hermann de Meer

Received: date / Accepted: date

Abstract The Future Internet architecture has to overcome ossification and shortcomings of the current Internet. It has to be robust, reliable, and fault tolerant, for instance, and it has to provide services in energy efficient ways. Furthermore, it is necessary to anticipate demands made by future services and networks, in order to enable the development of new services and protocols. Such goals require a highly flexible and reconfigurable network architecture, including simple and autonomous network management. Virtualization of host and network resources are among the key technologies in this context to achieve the needed flexibility. Virtualization is able to hide the complexity of physical network infrastructures and to provide homogenous, flexible, and dynamically reconfigurable virtual resources instead. This paper gives an overview on different methods of host and network virtualization. It illustrates (based on several examples) how challenges and requirements of today's Internet as well as those of the Future Internet can be approached.

Zusammenfassung Das Future Internet stellt sich der Herausforderung, die Verknöcherung und die Unzulänglichkeiten des heutigen Internets zu überwinden. Es soll beispielsweise robust, zuverlässig und fehlertolerant sein und dabei Dienste auf energieeffiziente Weise erbringen. Zusätzlich müssen auch neue Anforderungen antizipiert werden, die zukünftige Dienste und Netze stellen, um der Entwicklung von neuen Diensten und Protokollen nicht im Wege zu stehen. Erforderlich ist hierbei die Entwicklung einer äußerst variablen und rekonfigurierbaren Netzwerkarchitektur, die eine möglichst einfache und autonome Netzwerkverwaltung mit einschließt. Die Virtualisierung von Host- und Netzwerkressourcen stellt in diesem Zusammenhang eine der Schlüsseltechnologien dar, mit der diese notwendige Flexibilität erreicht werden kann. Virtualisierung verbirgt die Komplexität von physikalischen Netzwerkinfrastrukturen und stellt homogene, flexible und dynamisch rekonfigurierbare virtuelle Ressourcen zur

Universität Passau
Innstr. 43, 94032 Passau
Tel.: +49-851-5093050
Fax: +49-851-5093052
E-Mail: {berl, andreas.fischer, demeer}@uni-passau.de

Verfügung. Dieser Artikel gibt einen Überblick über verschiedene Host- und Netzwerk-Virtualisierungsmethoden. An mehreren Beispielen wird aufgezeigt, wie verschiedene Herausforderungen angegangen werden können, die sowohl im heutigen Internet als auch im Internet der Zukunft eine Rolle spielen.

Schlüsselwörter Future Internet, Virtualisierung, virtuelle Netzwerke, autonomes Management, Widerstandsfähigkeit, Energieeffizienz

1 Das Future Internet und seine Herausforderungen

Es stellt sich die Frage, ob das heutige Internet seinen Anforderungen noch gewachsen ist. Beispielsweise ist die Verknappung von IP-Adressen ein offensichtliches Problem, das sich eigentlich durch die Einführung von IPv6 lösen ließe. Dies wurde bislang nur unzureichend umgesetzt, was zeigt, wie schwierig es inzwischen ist, Unzulänglichkeiten eingefahrener Protokolle anzugehen. Diese und weitere Schwächen (z.B. mangelnde Dienstequalität für Voice over IP oder aufwändige Netzwerkadministration) des heutigen Internets führen dazu, dass sich die Wissenschaft verstärkt mit der Entwicklung eines zukünftigen Internet, dem Future Internet, auseinander setzt. Bei dessen Entwicklung müssen aber nicht nur Schwächen und Grenzen des heutigen Internet berücksichtigt werden. Es sind auch mögliche zukünftige Herausforderungen, die von neuen Diensten, Protokollen und Infrastrukturen gestellt werden, zu beachten. Einige der erwarteten Anforderungen an das Future Internet sind z.B. Zuverlässigkeit, Fehlertoleranz, Sicherheit, Dienstequalität, Mobilität, Anpassungsfähigkeit, Widerstandsfähigkeit oder Energieeffizienz.

Einige dieser Anforderungen können mit Hilfe von Host- und Netzwerkvirtualisierung angegangen werden. Die dabei eingesetzten Methoden abstrahieren von den physikalischen Eigenschaften des Netzwerkes und stellen virtuelle Ressourcen zur Verfügung. Durch diese Virtualisierungsebene erhöht sich zwar zunächst die Komplexität, weil zusätzlich zu den physikalischen Ressourcen auch die virtuellen Ressourcen verwaltet werden müssen. Die neue Abstraktionsebene bringt aber auch Vorteile.

- Reduktion der Verwaltungsaufwands: Virtuelle Ressourcen sind homogen – obwohl sie flexibel konfiguriert werden können, bieten sie vereinheitlichte Hardwareschnittstellen. Damit sind sie leichter zu verwalten als physikalische Ressourcen.
- Dynamische Rekonfigurierbarkeit: Virtuelle Ressourcen können zur Laufzeit erzeugt, bewegt, suspendiert oder verworfen werden. Darüber hinaus können ihre zugewiesenen Eigenschaften (z.B. Arbeitsspeicher, Speicherplatz, Bandbreite, ...) in einem gewissen Rahmen dynamisch verändert werden.
- Unterstützung unterschiedlicher Netzwerkarchitekturen: Mehrere virtuelle Netze mit unterschiedlichen Protokollschichten können parallel zueinander auf dem physikalischen Netzwerk betrieben werden. Dabei sorgt die Virtualisierungsebene für eine saubere Trennung der einzelnen virtuellen Netze.

Diese Vorteile bieten Lösungsansätze für einige der oben genannten Probleme. So wird beispielsweise die oben geforderte Anpassungsfähigkeit des Future Internet unterstützt. Die Netzwerkkonfiguration im heutigen Internet gilt als komplex und fehleranfällig. Trotzdem ist es nicht ohne weiteres möglich neue Protokolle in der Netzwerkschicht oder Transportschicht einzuführen. So wartet etwa der IPv4-Ersatz IPv6 – trotz der

dringenden Notwendigkeit – seit Jahren auf einen flächendeckenden Einsatz. Das Future Internet muss daher nicht nur Unterstützung für heutige Protokolle anbieten, sondern generell Mechanismen bieten, die es erlauben, neue Protokolle sanft einzuführen und veraltete Protokolle ebenso sanft außer Betrieb zu nehmen. Durch den Einsatz von Netzwerkvirtualisierung können verschiedene virtuelle Netze parallel zueinander betrieben werden, was das Erproben und Einführen neuer Dienste und Protokolle erheblich vereinfacht. Virtuelle Netze können auf bestimmte Dienste spezialisiert sein, um diese so gut wie möglich zu unterstützen. Weiterhin erleichtert die Gleichartigkeit und Flexibilität von virtuellen Ressourcen die Netzwerkkonfiguration und vereinfacht die Entwicklung von softwaregestützten Verwaltungsmechanismen. Eine adaptive Zuteilung von Netzwerkressourcen zu Diensten und Protokollen kann durchgeführt werden. Netze, die auf virtuellen Ressourcen basieren, werden dadurch in die Lage versetzt, sich an aktuelle Gegebenheiten anzupassen.

Die Widerstandsfähigkeit gegen äußere Einflüsse (z.B Katastrophen, Fehlfunktionen oder Angriffe) muss im Future Internet ebenfalls berücksichtigt werden. Die (in Zeiten des kalten Krieges entstandene) Kernfunktionalität des heutigen Internet bietet zwar bereits grundlegende Resistenz gegenüber Ausfällen von Hosts oder Leitungsunterbrechungen; jedoch beschränkt sich diese auf die Netzwerkschicht. Widerstandsfähigkeit von Diensten in der Anwendungsschicht zu ermöglichen, verursacht bislang hohen Aufwand. Im Future Internet soll die Widerstandsfähigkeit von Diensten durch Virtualisierung zusätzlich unterstützt werden, indem virtuelle Netze bei Bedarf dynamisch restrukturiert werden. Durch die rechtzeitige Verlagerung von virtuellen Ressourcen kann beispielsweise dem Ausfall kritischer Hardware entgegengewirkt oder Angriffen begegnet werden.

Eine weitere wichtige Anforderung des Future Internet ist seine Energieeffizienz. Das Future Internet muss den energieeffizienten Betrieb von IT- und Kommunikationsinfrastrukturen als wesentlichen Bestandteil beinhalten. Zurzeit kann man eine Verschiebung des Kosten-Engpasses für IT-Ausstattung beobachten. Während Hardware günstiger wird, verteuert sich die Energie, die zum Betrieb dieser Hardware notwendig ist. Die ansteigenden Energiekosten und die weltweit beabsichtigte Reduktion der CO_2 Emissionen sind heute treibende Kräfte für die Entwicklung zukünftiger Technologien. Virtualisierung bietet ein flexibles Ressourcenmanagement, das um die Randbedingung der Energieeffizienz erweitert werden kann. So kann der Energieverbrauch durch ein energiebewusstes Management reduziert werden. Beispielsweise können verschiedene Dienste konsolidiert werden, um genutzte Hardware stärker auszulasten und ungenutzte Hardware abzuschalten.

Die genannten Beispiele zeigen, dass Virtualisierung dazu geeignet ist, Anforderungen des Future Internet umzusetzen. In Kapitel 2 werden darum zunächst grundlegende Virtualisierungstechnologien vorgestellt. Kapitel 3 diskutiert die Einführung eines autonomen Managements von virtuellen Ressourcen und Netzwerken im zukünftigen Internet. In den Kapiteln 4 und 5 wird der Einsatz von Virtualisierung im Future Internet anhand zweier Beispiele – der Widerstandsfähigkeit von Diensten und der Energieeffizienz von zukünftigen Infrastrukturen – aufgezeigt.

2 Virtualisierung von Host- und Netzwerkressourcen

In diesem Abschnitt werden grundlegende Methoden der Virtualisierung beschrieben, die als Basis für ein zukünftiges Internet geeignet sind.

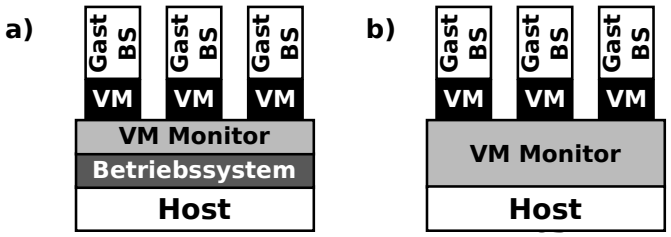

Abb. 1 Systemvirtualisierung mit und ohne Host-Betriebssystem

2.1 Virtualisierung von Hostressourcen

Es gibt zwei grundsätzliche Arten der Virtualisierung, die *Aggregation von Ressourcen* und das *Aufsplitten von Ressourcen*. Beide Varianten werden genutzt, um eine optimierte Nutzung von Ressourcen zu ermöglichen. Wenn Ressourcen aggregiert werden, wird eine *virtuelle Umgebung* auf mehrere Geräte abgebildet. Diese Art der Virtualisierung wird im Grid-Computing-Bereich eingesetzt. Wenn Ressourcen gesplittet werden, wird ein Gerät in mehrere virtuelle Umgebungen aufgeteilt, die unabhängig voneinander genutzt werden können. *Systemvirtualisierung* ist eine Ausprägung dieser Virtualisierungsart und wird häufig in Rechenzentren zur Servicevirtualisierung eingesetzt. Mit dieser Technik wird eine so genannte *Virtual Machine (VM)* erzeugt, bestehend aus virtueller Hardware (Prozessor, Hauptspeicher, Netzwerkkarte, etc.), einschließlich eines BIOS. Dabei erfolgt die Virtualisierung transparent bis auf Kernelebene, so dass gängige Betriebssysteme ohne Änderung in der virtuellen Umgebung lauffähig sind. Die Erzeugung einer VM sowie die Zuteilung von Ressourcen geschieht durch einen *VM Monitor* [29]. Ein VM Monitor kann mehrere virtuelle Maschinen gleichzeitig und unabhängig voneinander bereitstellen. Ein in einer VM laufendes Betriebssystem bezeichnet man auch als Gast-Betriebssystem (Gast-BS). Im Sinne der Netzwerkvirtualisierung lässt sich ein derartig virtualisiertes Gast-BS mit Routing-Funktionalität als virtueller Router betrachten. Es gibt eine Menge von Managementfunktionen, die den Umgang mit den virtuellen Ressourcen einer VM erleichtern, z.B. create VM, destroy VM, start VM, stop VM, move VM, copy VM und pause VM [8]. Es ist sogar möglich, einen Service der in einer VM eingeschlossen ist, zu einem anderen Host zu migrieren, ohne ihn zu unterbrechen [18].

In Abbildung 1 ist ein VM Monitor dargestellt, der jeweils 3 virtuelle Maschinen bereitstellt, jede mit einem eigenen Gast-BS. In Abb. a) läuft der VM Monitor als Anwendung innerhalb eines Host-BS. Dies ist aus Sicht des VM Monitors die einfachere Variante, weil er nicht alle Treiber für die Hardware selbst bereitstellen muss. Andererseits erzeugt die zusätzliche Softwareschicht zusätzlichen Rechenaufwand. Im Gegensatz dazu wird der VM Monitor in Abb. b) direkt auf der Hardware ausgeführt. Eine Übersicht über Hostvirtualisierungstechniken findet sich in [10] und [13].

2.2 Virtualisierung von Netzwerkressourcen

Netzwerkvirtualisierung [16][20] konzentriert sich auf die Virtualisierung von Links und Routern. Diese werden miteinander kombiniert und erzeugen zusammen virtuelle Netzwerke.

Die Abstraktion von Netzwerklinks kann (ähnlich wie bei der Hostvirtualisierung) auf zwei Arten stattfinden: es können sowohl mehrere virtuelle Links innerhalb eines physikalischen Links erzeugt werden, als auch mehrere physikalische Links zu einem virtuellen Link aggregiert werden.

Zwei Formen der *Linkvirtualisierung* sind heute populär: *Virtual Local Area Networks (VLAN)* und *Virtual Private Networks (VPN)*. VLAN, wie etwa IEEE 802.1Q [9], ermöglichen eine logische Segmentierung lokaler Netzwerke auf der Verbindungsschicht. VPN, wie IPSec [23], erstellen verschlüsselte Tunnel und verbinden damit entweder einzelne Rechner untereinander, einzelne Rechner mit einem Netzwerk, oder sogar mehrere Netzwerke untereinander über das öffentliche Internet.

Die Virtualisierung von Routern wurde in [20] untersucht und ist bereits in kommerziellen Produkten verfügbar [5]. Cisco beschreibt zwei Konzepte zur Routervirtualisierung: Software-Isolated Virtual Router (SVR) und Hardware-Isolated Virtual Router (HVR) [7]. In beiden Konzepten werden Ressourcen per Software oder Hardware voneinander isoliert. Es gibt verschiedene SVR-Ansätze: Die Virtualisierung im Router kann parallele Betriebssysteme erzeugen, oder im Betriebssystem-Kern durchgeführt werden. Beide Methoden reduzieren die Leistungsfähigkeit des Routers und nutzen die zur Verfügung stehenden Ressourcen nicht optimal aus. Alternativ kann SVR auch auf der Applikationsebene durchgeführt werden. Diese Methode erzeugt weniger Overhead, erhöht aber auch die Komplexität der Anwendungen, die an die Virtualisierung angepasst werden müssen. Im Gegensatz dazu weist der hardwarebasierte HVR-Ansatz jeder virtuellen Instanz eigene Control-Plane- und Data-Plane-Ressourcen zu. Diese Vorgehensweise hat den Vorteil, dass softwareseitig keinerlei Modifikationen durchgeführt werden müssen, der Kernel und seine Anwendungen laufen wie gewohnt. Allerdings wird hier kein echtes Teilen von Ressourcen durchgeführt, da die Hardwareressourcen der einzelnen Instanzen vollständig voneinander getrennt sind.

Wang et al. [33] haben die Migrierbarkeit von virtuellen Routern in optischen Netzen diskutiert, um die logische und physische Konfiguration von Routern zu entkoppeln.

In [19] und [27] wurde die Leistungsfähigkeit von Systemvirtualisierungssoftware im Bezug auf Routervirtualisierung untersucht. Das Aufteilen von Ressourcen eines physischen Routers auf mehrere virtuelle Router erzeugt dabei eine Konkurrenzsituation bezüglich des Ressourcenbedarfs der einzelnen virtuellen Router. Durch häufige kostenintensive Kontextwechsel bei der Verarbeitung von Paketen, kann es daher insbesondere beim Paket-Forwarding zu Leistungseinbrüchen kommen. Zwar lässt sich dieses Problem durch die großzügige Vergabe von Ressourcen für virtuelle Router teilweise kompensieren, allerdings ist dies im Widerspruch mit bestimmten Zielen der Virtualisierung – die Optimierung von Ressourcenaufwand und die Reduzierung ungenutzter Ressourcen kann so nicht mehr erreicht werden. Dedizierte Hochleistungsrouter aus dem professionellen Umfeld verwenden spezielle Forwarding-Hardware, um Leistungsengpässen entgegenzuwirken. Hier bleibt zu untersuchen, inwieweit solche Hardwaremechanismen für Virtualisierung nutzbar gemacht werden können.

Wenn Router mit Hilfe von Systemvirtualisierung virtualisiert werden, entsteht eine bestimmte Art von virtuellen Netzen, wie sie in [11] beschrieben ist. Aus virtuellen Routern und virtuellen Links ergibt sich ein virtualisiertes Netzwerk, in dem mehrere virtuelle Netze gleichzeitig und unabhängig voneinander betrieben werden können. Diese Netze können unterschiedlich konfiguriert sein und parallel unterschiedliche Protokolle benutzen, z.B. IPv4 und IPv6. Die Virtualisierung erfolgt dabei für die einzelnen Netze vollkommen transparent ohne Änderung der Protokolle.

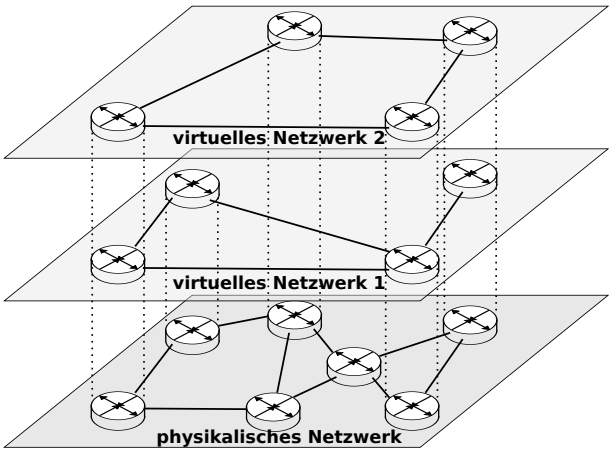

Abb. 2 Zwei unabhängige virtuelle Netzwerke auf einem physikalischen Netzwerk

Abbildung 2 zeigt zwei virtuelle Netze (virtuelles Netzwerk 1 und virtuelles Netzwerk 2) mit verschiedenen Topologien. Sieben physikalische Router bilden das zugrundeliegende Netzwerk. Die virtuellen Ressourcen werden dabei in geeigneter Weise auf die physikalischen Ressourcen abgebildet. Eine der herausragenden Eigenschaften einer solchen virtuellen Umgebung ist, dass virtuelle Netzwerke beeinflusst werden können, in dem man sie als Black Box betrachtet und von außen die zur Verfügung stehenden virtuellen Ressourcen modifiziert.

Ein weiterer Ansatz zur Virtualisierung von Netzwerken sind *Peer-to-Peer* (P2P) Netzwerke, wie z.B. Chord, Pastry, eDonkey oder Skype [31]. In P2P Netzen werden logische Links auf Applikationsebene erzeugt. Ein einzelner logischer Hop kann sich dabei über mehrere physikalische Hops erstrecken. Man klassifiziert P2P Netze unter anderem nach der Ausprägung der Peers. In so genannten *reinen* P2P Overlays (z.B. Chord) haben alle Peers die gleichen Aufgaben, wohingegen in *hybriden* P2P Overlays (z.B. eDonkey) unterschiedliche Arten von Peers unterschiedliche Aufgaben erfüllen. Man nennt P2P Overlays *strukturiert*, wenn die Erzeugung des Overlays einem bestimmten Muster folgt (etwa einem Ring), sonst nennt man sie *unstrukturiert*. Im Gegensatz zu vorher genannten Netzwerkvirtualisierungsformen, ermöglichen P2P Netze zusätzlich über ihr Addressierungsschema das effiziente Auffinden von Hosts und Ressourcen. So können beispielsweise in File-Sharing Netzen (wie eDonkey) Dateien gefunden werden, wohingegen in VoIP Netzen (wie Skype) Benutzer gefunden und adressiert werden können.

Forschungs-Plattformen wie PlanetLab [17], GENI[4] oder G-Lab[3] nutzen bereits heute die Möglichkeiten der Netzwerkvirtualisierung, um flexible Testumgebungen zur Forschung am Future Internet bereitzustellen.

3 Autonomes Netzwerk-Management

Die in Abschnitt 2 genannten Technologien bieten eine hohe Flexibilität in Bezug auf Organisation und Management von Netzwerkressourcen. Die neu gewonnene Freiheit, physische Ressourcen beliebig zu virtuellen Netzwerken zusammenzuschließen,

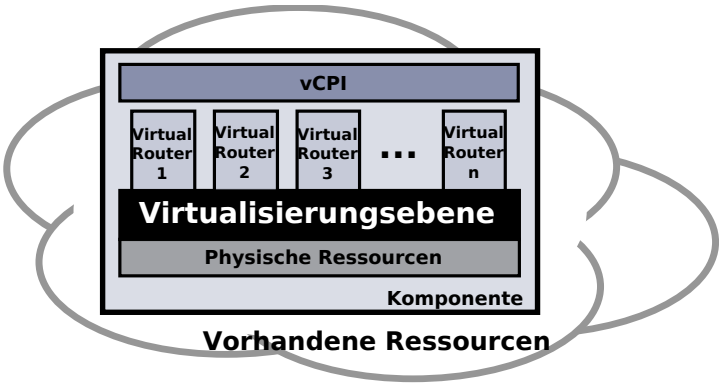

Abb. 3 Verwaltung virtueller Ressourcen durch die Virtualisierungsebene

eröffnet weitaus agilere Nutzungsmöglichkeiten als sie das bisherige Internet bieten kann. So können beispielsweise neue Netzwerktechnologien gefahrlos Seite an Seite mit bewährten Architekturen auf realer Infrastruktur getestet werden, ohne sich gegenseitig zu beeinflussen oder voneinander zu wissen. Weitere Möglichkeiten ergeben sich aus der Option, ganze Netzwerkzustände einzufrieren oder auf einen vordefinierten Zustand zurückzusetzen, was eine flexible Form der Entwicklung von Netzwerktechnologien erlaubt. Die Umsetzung und Implementierung dieser Technologien in die Kernkomponenten des Internet ermöglicht eine graduelle Inbetriebnahme neuer Technologien und ein sanftes Ausblenden veralteter Technologien – eine Funktion, die wir heutzutage beim Umstieg von IPv4 auf IPv6 vermissen. Schließlich bieten Virtualisierungsmethoden einen Ansatz, um unterschiedliche Kommunikationspfade auch im Netz logisch voneinander zu trennen und dadurch zusätzliche Sicherheit zu gewährleisten – eine Tatsache, der bereits heutzutage durch den vermehrten Einsatz von VPN Rechnung getragen wird.

Diese neu gewonnene Flexibilität, mit all ihren Vorteilen, stellt allerdings zunächst neue Anforderungen an das Management von Netzwerkressourcen. Zusätzlich zu physikalischen Ressourcen müssen jetzt virtuelle Ressourcen verwaltet werden. Dabei sollte dieses Management so autonom wie möglich erfolgen; das heißt, diese neue Komplexität soll weitgehend ohne Interaktion mit Netzwerkadministratoren automatisch vom System gehandhabt werden. Forschungsprojekte wie beispielsweise das Autonomic Internet Projekt [1][21], aber auch andere Projekte [30][14], widmen sich dieser Herausforderung und suchen nach Möglichkeiten, Netzwerkadministratoren die Verwaltung virtueller Netze zu erleichtern. Die grundlegende Idee dabei ist es, eine neue Abstraktionsebene zu schaffen. So wird die Virtualisierung von physikalischen Ressourcen (und die Abbildung auf virtuelle Ressourcen) in einer eigens geschaffenen *Virtualisierungsebene* durchgeführt (siehe Abb. 3). Die im Netzwerk vorhandenen Ressourcen werden dabei zunächst einer logischen Einheit – der Komponente – als physische Ressourcen zugeordnet. Diese Komponente repräsentiert eine physische Hardwareeinheit (beispielsweise einen Router). Innerhalb dieser Komponente erstellt die Virtualisierungsebene virtuelle Ressourcen und gruppiert diese wiederum zu einer virtuellen Einheit – beispielsweise einem oder mehreren virtuellen Routern. Eine standardisierte Schnittstelle – das ,,virtual Component Programming Interface" (vCPI) stellt dabei Funktionalität bereit, die es anderen Softwarekomponenten erlaubt darüber virtuelle Netze zu erstellen

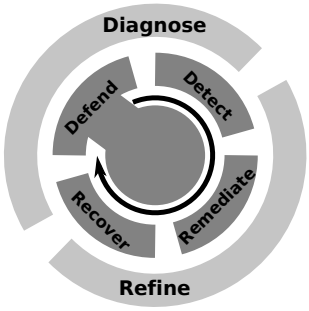

Abb. 4 Die $D^2R^2 + DR$ Strategie

und zu verwalten. Die Kapselung dieser Funktionalität innerhalb der Virtualisierungsebene ermöglicht es einem umfassenden Netzwerkmanagement von der eigentlichen Beschaffenheit der physikalischen Ressourcen zu abstrahieren und ausschließlich mit virtuellen Ressourcen zu arbeiten. Durch die Virtualisierungsebene stehen auf diese Weise äußerst flexible und homogene virtuelle Ressourcen zur Verfügung, die wesentlich einfacher und dynamischer zu verwalten sind als die ursprünglichen physikalische Ressourcen. So unterstützt die Virtualisierungsebene beispielsweise eine logische Aufgabentrennung durch entsprechende Gruppierung virtueller Resourcen in einem virtuellen Netzwerk. Zudem kann durch Hinzufügen oder Wegnehmen virtueller Ressourcen auch während der Laufzeit dynamisch die Topologie eines virtuellen Netzwerks geändert und angepasst werden. Dies ermöglicht eine optimierte Verwaltung der Netzstruktur unter Berücksichtigung der Anforderungen netzwerkbasierter Dienste.

4 Widerstandsfähigkeit durch Virtualisierung

Ein wichtiges Ziel zukünftiger Internetarchitekturen ist es, die Widerstandsfähigkeit netzwerkbasierter Dienste zu stärken. Der Begriff der Widerstandsfähigkeit versteht sich hierbei als eine Kombination von Fehlertoleranz im Sinne der funktionalen Sicherheit und Zuverlässigkeit im Sinne der Informationssicherheit. Durch die zunehmende Ausweitung der Internetnutzung auf kritische Bereiche (wie beispielsweise Notfalldienste) steigen die Anforderungen bezüglich der Ausfallsicherheit drastisch an. Dabei müssen viele potentielle Fehlerquellen berücksichtigt werden: mutwillige Angriffe auf das Netzwerk, fehlerhafte Softwareimplementierungen, die Auswirkungen von Naturkatastrophen, oder auch der Ausfall kritischer Hardware. Auch das Interagieren unterschiedlicher Dienste kann zu unerwarteten Engpässen führen, welche es im Vorhinein zu erkennen und vermeiden gilt [28]. Im Hinblick auf zukünftige Netzwerke ist besondere Aufmerksamkeit geboten – so erfordern beispielsweise Abhängigkeiten zwischen einzelnen Netzdiensten eine weitergehende, holistische Betrachtung bezüglich der Widerstandsfähigkeit eines kombinierten Dienstes [15]. In diesem Fall muss, um das Problem zu diagnostizieren, nicht nur der konkrete, fehlerhafte Dienst betrachtet werden – die Fehleranalyse muss auch die Systemumgebung und Abhängigkeiten dieses Dienstes berücksichtigen, um bei der Wiederherstellung die Situation nicht etwa zu verschlechtern.

Ein Projekt, das sich mit der Widerstandsfähigkeit des zukünftigen Internet auseinandersetzt, ist das ResumeNet Projekt [6]. Virtualisierungstechniken spielen hier eine

wichtige Rolle. Wenn Probleme im Netzwerk auftreten, können Problembereiche durch die Virtualisierung isoliert werden. Dies ermöglicht eine für darüber liegende Dienste transparente Behandlung von Problemen. Das ResumeNet Projekt propagiert dabei die $D^2R^2 + DR$ Strategie (siehe Abb. 4 als Designschablone für ein widerstandsfähiges Netz [22]. Hierbei werden zwei einander überlagerte Rückkopplungsschleifen als wesentliche Teile einer widerstandsfähigen Architektur identifiziert: eine innere (kurzfristige) Schleife "Defend, Detect, Remediate, Recover" sowie eine äußere (langfristige) Schleife "Diagnose, Refine". Netzwerkvirtualisierung kann hierbei vor allem in den Bereichen "Defense", "Remediate" und "Recover" eine wichtige Rolle spielen, indem Problembereiche durch Abstraktion für die Netzwerkdienste transparent behandelt werden. So kann etwa ein VPN benutzt werden, um Einschränkungen durch Firewalls zu umgehen, indem Netzwerkverkehr durch einen virtuellen Link hindurch getunnelt wird. Diese Einführung von virtuellen Links bleibt für Dienste transparent. P2P Overlays können genutzt werden, um die Netzwerkstruktur eines Dienstes resistent gegen eine hohe Fluktuation von Netzteilnehmern zu machen [26]. Es ist möglich, trotz erheblicher Störeinflüsse auf das Netz, die Netzstruktur zu erhalten und die Kommunikation zwischen den verbleibenden Nutzern sicherzustellen. Das dynamische Erstellen von neuen virtuellen Netzwerken ermöglicht es, Fehler in einem Netz in einer sicheren Umgebung aufzuspüren und zu diagnostizieren [34]. Dadurch kann die Fehleranalyse ohne nennenswerte Beeinträchtigung des Produktionsnetzwerks erfolgen.

Systemvirtualisierung bietet die Möglichkeit, einen Netzwerkdienst in eine VM zu kapseln. Hier erlaubt die Abstraktion, Dienste im Netzwerk von einer Hardwarekomponente auf eine andere zu migrieren. So kann beispielsweise auf den Ausfall von Hardwarekomponenten reagiert werden. Solange genug Zeit bleibt, um die Migration durchzuführen, kann so der Dienst trotz Hardwareausfalls weiter im Betrieb gehalten werden. Dies wäre beispielsweise denkbar als Reaktion auf herannahende Naturkatastrophen, geplante Wartungszeiten von Hardware, oder bei Stromausfällen, bei denen üblicherweise Hardware noch für kurze Zeit über eine unabhängige Stromversorgung mit Strom versorgt wird.

5 Energieeffizienz

Der Stromverbrauch von IT- und Kommunikationsinfrastrukturen steigt dramatisch an. Koomey [25] berichtet von einer Verdopplung des Energieverbrauchs zwischen 2000 und 2005 von kleinen, mittleren und High-End Servern in den USA und weltweit. Für das Jahr 2010 rechnet das Bundesministerium für Wirtschaft und Arbeit mit 55 Milliarden kWh Stromverbrauch für die IT- und Telekommunikationsinfrastruktur in Deutschland [32]. All dies legt nahe, dass die Energieeffizienz des Future Internet von höchster Bedeutung ist.

Heutzutage ermöglichen stromsparende Technologien die Reduzierung des Energieverbrauchs von Geräten in Abhängigkeit vom Lastprofil. Techniken wie SpeedStep, PowerNow, Cool'n'Quiet oder Demand Based Switching vermindern die CPU-Frequenz (Clock Gating), wodurch die Stromaufnahme und Hitzeentwicklung abnimmt. Auch können einzelne Bestandteile von Prozessoren deaktiviert werden (Power Gating). Solche Techniken konzentrieren sich auf den Energieverbrauch einzelner Geräte oder Komponenten. Um eine umfassende Energieeffizienz im zukünftigen Internet zu erreichen, muss ein grundlegender Paradigmenwechsel erfolgen. Im Ressourcenmanagement von Infrastrukturen wird heutzutage im Allgemeinen das ökonomische Maximumprinzip

(vorgegebener Input, maximaler Output) angewendet. Die vorgegebenen Ressourcen (verfügbare Hardware und Energie) werden so genutzt, dass das Ergebnis (z.B. Datendurchsatz oder Rechenleistung) maximiert wird. Will man aber einen energieeffizienten Betrieb der verfügbaren Hardware erreichen, so muss das komplementäre Minimumprinzip (vorgegebener Output, minimaler Input) angewendet werden. Bei diesem Ansatz wird ein im Voraus definiertes Ergebnis (z.B. ein Dienst mit einem bestimmten Grad an Dienstqualität oder Sicherheit) durch den Einsatz einer minimalen Menge von Ressourcen erbracht.

Virtualisierung kann genutzt werden, um das Minimumprinzip zu unterstützen. Sie entkoppelt auszuführende Aufgaben von der zugrunde liegenden Hardware. So können Dienste, die auf virtuellen Ressourcen laufen dynamisch auf physikalische Ressourcen abgebildet werden. Allgemein sollten Dienste auf derjenigen Hardware ausgeführt werden, auf der sie am energieeffizientesten erbracht werden können. Virtualisierung partitioniert physikalische Ressourcen und ermöglicht es, Hardware für mehrere Aufgaben gleichzeitig zu nutzen. Diese Konsolidierung von Diensten [24] ist ein Ansatz zur Steigerung der Energieeffizienz. Häufig besitzen Dienste nur geringe Ressourcen-Anforderungen an Hardware, verursachen aber dennoch relativ hohen Stromverbrauch. Abhängig von der beanspruchten Leistung können mehrere virtualisierte Dienste auf einer einzelnen Hardware-Instanz zusammengeführt werden. Unbenutzte Server werden dann abgeschaltet oder in einen Standby-Modus versetzt.

Virtualisierung ermöglicht zwar einerseits ein flexibles Management von Ressourcen, fügt aber andererseits dem System Overhead hinzu. Die zusätzliche Virtualisierungsschicht verbraucht Rechenleistung und erzeugt Kommunikation. Deshalb ist die Überwachung und ein ausgewogenes Management von physikalischen und virtuellen Ressourcen notwendig, um energieeffiziente Virtualisierung und Konsolidierung zu ermöglichen. Daten über die Auslastung von virtuellen und physischen Ressourcen, sowie aktuelle Temperaturen physikalischer Geräte müssen erfasst werden, um eine energiebasierte Sicht auf eine Infrastruktur zu erlangen. Zusätzlich muss ein Hitzemanagement durchgeführt werden, da die Kühlung von Hardware einen erheblichen Teil zu den Energiekosten beiträgt. Dabei müssen energiebezogene Probleme in Einklang mit definierten Richtlinien gelöst werden ohne dabei menschliche Interaktion zu benötigen. Anwender im Future Internet müssen in der Lage sein, energieeffiziente IT-Infrastrukturen zu nutzen, ohne sich mit dem zugrunde liegenden Management auseinander zu setzen. Maschinenlesbare Beschreibungen der Eigenschaften und Fähigkeiten von Diensten, Servern und Netzwerken müssen verfügbar sein, um das Ziel dieses autonomen, energieeffizienten Ressourcenmanagements zu ermöglichen. Die Energieeffizienz des Future Internet wird in [12] diskutiert und unter anderem im G-Lab_Ener-G Projekt [3, 2] untersucht.

6 Zusammenfassung und Ausblick

Das Future Internet soll die Herausforderungen des heutigen Internet meistern und auch für zukünftige Dienste und Protokolle geeignet sein. Dieser Artikel hat einige dieser Herausforderungen diskutiert und gezeigt, wie man sie im Future Internet mit Hilfe der Schlüsseltechnologie Virtualisierung angehen kann. Die Virtualisierung von Host- und Netzwerkressourcen abstrahiert von der Komplexität des physikalischen Netzwerks und erzeugt einen Pool gleichartiger, flexibler, rekonfigurierbarer und einfach zu verwaltender virtueller Ressourcen. Diese Eigenschaften ermöglichen die Ent-

wicklung eines autonomen Netwerkmanagements, das Protokolle, Dienste und Netzwerke im zukünftigen Internet unterstützt und bestimmte Randbedingungen (wie etwa Widerstandsfähigkeit oder Energieeffizienz) erfüllen kann. Der Artikel hat verschiedene Virtualisierungstechniken im Detail diskutiert und gezeigt, wie mit virtuellen Ressourcen ein autonomes Netzwerkmanagement aufgebaut werden kann. Weiterhin wurden Ansätze vorgestellt, welche die Widerstandsfähigkeit von Diensten und Netzen im Future Internet unterstützen und den energieeffizienten Betrieb des Future Internet ermöglichen.

Danksagung The research leading to these results has received funding from the European Community's Seventh Framework Programme ([FP7/2007-2013] [FP7/2007-2011]) in the context of the ResumeNet project, grant agreement n° 224619.

Literatur

1. Autonomic Internet Project (AUTOI), STREP, FP7, grant no. ICT-2007-1-216404. http://www.ist-autoi.eu. Letzter Zugriff am 09.01.2010.
2. G-Lab_Ener-G. www.net.fim.uni-passau.de/ener-g. Letzter Zugriff am 09.01.2010.
3. German Lab. www.german-lab.de. Letzter Zugriff am 09.01.2010.
4. Global Environment for Networking Innovations. www.geni.net. Letzter Zugriff am 09.01.2010.
5. Logical Routers Commands on Cisco IOS XR Software. www.cisco.com/en/US/docs/ios_xr_sw/iosxr_r3.2/interfaces/command/reference/hr32lr.html. Letzter Zugriff am 09.01.2010.
6. ResumeNet (Resilience and Survivability for future networking: framework, mechanisms and experimental evaluation), STREP, FP7 Call2 (ICT-2007-2) Grant 224619. http://www.resumenet.eu. Letzter Zugriff am 09.01.2010.
7. Router Virtualization in Service Providers. www.cisco.com/en/US/solutions/collateral/ns341/ns524/ns562/ns573/white_paper_c11-512753_ns573_Networking_Solutions_White_Paper.html. Letzter Zugriff am 09.01.2010.
8. DMTF Standard DSP 1057. Virtual System Profile. http://www.dmtf.org/standards/published_documents/DSP1057.pdf, May 2007. Letzter Zugriff am 09.01.2010.
9. IEEE Standard 802.1Q. IEEE Standards for Local and Metropolitan Area Networks: Virtual Bridged Local Area Networks. http://standardsieee.org/getieee802/download/802.1Q-2003.pdf, May 2003. Letzter Zugriff am 09.01.2010.
10. C. Baun, M. Kunze, and T. Ludwig. Servervirtualisierung. *Informatik-Spektrum*, 32(3):197–205, 2009.
11. A. Berl, A. Fischer, and H. De Meer. Using System Virtualization to Create Virtualized Networks. In *Workshops der Wissenschaftlichen Konferenz Kommunikation in Verteilten Systemen (WowKiVS2009), Kassel, Germany, March 2-6, 2009*, volume 17 of *Electronic Communications of the EASST*. EASST, March 2009.
12. A. Berl, E. Gelenbe, M. di Girolamo, G. Giuliani, H. De Meer, M. Q. Dang, and K. Pentikousis. Energy-Efficient Cloud Computing. *The Computer Journal*, August 2009.
13. J.-C. Brendel. Schöner Schein? *Linux Magazin: Technical Review 01 - Virtualisierung Ressourcenmanagement auf neuem Level*, 2006.
14. J. Carapinha and J. Jiménez. Network virtualisation – a view from the bottom. pages 73–80, Barcelona, Spain, 2009. ACM.
15. P. Cholda, A. Mykkeltveit, B. E. Helvik, O. J. Wittner, and A. Jajszczyk. A survey of resilience differentiation frameworks in communication networks. *Communications Surveys & Tutorials, IEEE*, 9(4):32–55, 2007.
16. N. M. M. K. Chowdhury and R. Boutaba. A Survey of Network Virtualization. Technical report, University of Waterloo, Oct. 2008.
17. B. Chun, D. Culler, T. Roscoe, A. Bavier, L. Peterson, M. Wawrzoniak, and M. Bowman. PlanetLab: an overlay testbed for broad-coverage services. *SIGCOMM Comput. Commun. Rev.*, 33(3):3–12, 2003.

18. C. Clark, K. Fraser, S. Hand, J. G. Hansen, E. Jul, C. Limpach, I. Pratt, and A. Warfield. Live Migration of Virtual Machines. In *2nd conference on Symposium on Networked Systems Design & Implementation (NSDI'05)*, pages 273–286, Berkeley, CA, USA, 2005. USENIX Association.
19. N. Egi, A. Greenhalgh, M. Handley, M. Hoerdt, L. Mathy, and T. Schooley. Evaluating XEN for Router Virtualization. In *16th Int. Conf. on Comp. Commun. and Networks - ICCCN 2007*, pages 1256–1261, Aug. 2007.
20. N. Feamster, L. Gao, and J. Rexford. How to lease the internet in your spare time. *SIGCOMM Comput. Commun. Rev.*, 37(1):61–64, 2007.
21. A. Galis, S. Denazis, A. Bassi, P. Giacomin, A. Berl, A. Fischer, H. de Meer, J. Strassner, S. Davy, D. Macedo, G. Pujolle, J. Rubio-Loyola, J. Serrat, L. Lefevre, and A. Cheniour. *Management Architecture and Systems for Future Internet Networks*, pages 112–122. IOS Press, 2009.
22. D. Hutchison and J. P. G. Sterbenz. ResiliNets: Resilient and Survivable Networks. In *ERCIM News 77*, April 2009.
23. S. Kent and K. Seo. IETF RFC 4301: Security Architecture for the Internet Protocol. http://tools.ietf.org/html/rfc4301, December 2005.
24. J. Koomey. Energystar server energy measurement protocol version 1.0. *SIGCOMM Comput. Commun. Rev.*, March 2006.
25. J. Koomey. Estimating total power consumption by servers in the us and the world, technical report. Technical report, Lawrence Berkeley National Laboratory Stanford University, February 2007.
26. D. Liben-Nowell, H. Balakrishnan, and D. Karger. Analysis of the evolution of peer-to-peer systems. In *PODC '02: Proceedings of the twenty-first annual symposium on Principles of distributed computing*, pages 233–242, New York, NY, USA, 2002. ACM.
27. A. Menon, A. L. Cox, and W. Zwaenepoel. Optimizing Network Virtualization in Xen. In *USENIX Annual Technical Conference*, pages 15–28, May 2006.
28. M. Menth, M. Duelli, R. Martin, and J. Milbrandt. Resilience Analysis of Packet-Switched Communication Networks. in IEEE/ACM Transactions on Networking, accepted for publication, IEEE.
29. G. J. Popek and R. P. Goldberg. Formal Requirements for Virtualizable third Generation Architectures. *Commun. ACM*, 17(7):412–421, 1974.
30. G. Schaffrath, C. Werle, P. Papadimitriou, A. Feldmann, R. Bless, A. Greenhalgh, M. Kind, O. Maennel, and L. Mathy. Network Virtualization Architecture: Proposal and Initial Prototype. pages 63–71, Barcelona, Spain, 2009. ACM.
31. R. Steinmetz and K. Wehrle. *Peer-to-Peer Systems and Applications (Lecture Notes in Computer Science)*. Springer-Verlag New York, Secaucus, NJ, USA, 2005.
32. Bundesverband Informationswirtschaft Telekommunikation und neue Medien e.V. Energieeffizienz im Rechenzentrum. *Telekommunikation und neue Medien*, 2:10, 2008.
33. Y. Wang, E. Keller, B. Biskeborn, J. van der Merwe, and J. Rexford. Virtual routers on the move: live router migration as a network-management primitive. *SIGCOMM Comput. Commun. Rev.*, 38(4):231–242, 2008.
34. A. Wundsam, A. Mehmood, A. Feldmann, and O. Maennel. Improving Network Troubleshooting using Virtualization. Technical Report 2009-12, TU Berlin, Fak IV, 2009.