

Infrastruktur

MWN, DFN, GÉANT – München weltweit vernetzt

Das „Netz“ ist heute unverzichtbar für Wissenschaftler und Studierende. Und genau so wird es auch wahrgenommen: Es ist einfach da, es funktioniert immer und (am besten) überall. Dass dafür hochkomplexe kooperative Infrastrukturen etabliert, betrieben und ausgebaut werden müssen, erschließt sich oft erst auf den zweiten Blick.

Und ja – der Wissenschaftsstandort München ist nicht nur fachlich, sondern auch technisch weltweit hervorragend vernetzt. Grundlage dieser Vernetzung ist das Münchner Wissenschaftsnetz.

VON HELMUT REISER



Abb. 1: Von Ingolstadt bis zur Zugspitze, von Augsburg bis zum Wendelstein: das Münchner Wissenschaftsnetz (MWN).

DAS MÜNCHNER Wissenschaftsnetz (MWN) hat nur wenig mit Universitätsnetzen in anderen Städten gemein. Es versorgt nicht nur eine Universität, sondern alle Münchner Universitäten, Hochschulen und viele Forschungseinrichtungen; es wird nicht von einer Uni für die Uni, sondern vom Leibniz-Rechenzentrum der Bayerischen Akademie der Wissenschaften für alle diese Einrichtungen betrieben. Dadurch lassen sich Synergie- und Skaleneffekte nutzen, gleichzeitig stehen modernste und fortschrittlichste Technologien zur Verfügung.

Das Netz wird zwar als Münchner Wissenschaftsnetz bezeichnet, geht aber weit über die Stadt München hinaus (Abb. 1). Derzeit werden gut 120.000 Nutzer in mehr als 540 Gebäudekomplexen über das MWN erschlossen. Es bildet die Grundlage für die verschiedensten Dienste wie VPNs, Koppelung von Telefonanlagen, Voice over IP, WLAN usw. Neben einer hohen Bandbreite (derzeit 10 Gbit/s im Backbone und zum DFN/Internet) und einer flächendeckenden Versorgung wird der ausfallsichere Betrieb immer wichtiger. Dies spiegelt sich auch in Redundanzmechanismen bei den Netzkomponenten sowie in der Backbone-Struktur wider (Abb. 2). Große Standorte sind über mehrere Leitungen erschlossen; innerhalb des Backbones gibt es mehrere Ringe, damit es selbst bei Ausfall einer Backbone-Leitung alternative Wege gibt. Neben dem primären Internetzugang über das Deutsche Forschungsnetz (DFN) gibt es einen redundanten Anschluss an den lokalen Provider M-net mit

reduzierter Bandbreite und volumenabhängiger Tarifierung. Auch auf Seiten der Netzdienste werden große Anstrengungen unternommen, um wichtige Dienste ausfallsicher betreiben zu können. Der DNS-Dienst zur Namensauflösung wird z. B. durch vier Server an verschiedenen Standorten im MWN erbracht. Die Server sind alle über die gleiche IP-Adresse (Anycast) erreichbar und können so zur Lastverteilung genutzt werden. Selbst beim Ausfall von drei Servern ist der Dienst noch verfügbar.

Mobile Nutzung

Das Backbone-Netz wird von zwölf Routern gebildet, an denen die Nutzer über kaskadierte Switches und über eine strukturierte Verkabelung angebunden sind. Gegenwärtig betreibt das LRZ 1.250 Switches mit rund 77.000 Ports. Daneben wird die mobile Internetnutzung immer wichtiger, die das LRZ derzeit mehr als 1.900 WLAN Access Points in gut 350 Gebäuden gewährleistet. Während des Semesters sind auf den Access Points mehr als 7.000 Nutzer gleichzeitig aktiv (zum Vergleich: 2009 waren es nur 3.000). Auch bei den Geräten zeigt sich ein massiver Zuwachs: Während des Semesters sind innerhalb einer Woche mehr als 40.000 verschiedene Geräte im WLAN aktiv. Damit auch reisende Wissenschaftler und Studenten das MWN nutzen können, unterstützt das LRZ flächendeckend die europäische Roaming-Infrastruktur eduroam. So können sich Gäste in München mit ihrer Heimatkennung am Netz anmelden und dieses nutzen. Das gilt auch für Münchner Nutzer, die andere Universitäten im In- und Ausland besuchen.



Sicherheit

Das LRZ ist für den Betrieb des MWN bis zur Dose verantwortlich. Die Art des Gerätes, das dort angeschlossen wird, liegt in der Verantwortung der entsprechenden Einrichtung. Daher ist das MWN im Hinblick auf die versorgten Systeme sehr heterogen.

Ein derart großes, heterogenes Netz erfordert umfangreiche Sicherheitsmechanismen. So betreibt das LRZ u. a. mandantenfähige Firewalls, Monitoring-, Intrusion Detection- und Intrusion Prevention-Systeme (IDS/IPS). Im Gegensatz z. B. zu Firmennetzen sind im MWN auch Verfahren im Einsatz, die Angriffe aus dem MWN heraus verhindern können. Hier ist das vom LRZ entwickelte System Secomat zu nennen: Es ist in der Lage, auf Basis verschiedener Heuristiken Angriffe zu erkennen. Verkehr aus privaten Netzen (z. B. WLAN, Wohnheime usw.) wird über den Secomat geleitet und dort analysiert. Werden Angriffe erkannt, wird das verursachende System vollautomatisch gesperrt und der Nutzer informiert. In den meisten Fällen ist das betroffene System ohne Wissen des Nutzers mit Schadsoftware infiziert worden.

Entwicklung

Das MWN hat sich seit den 1980er Jahren von einem Datenfernverarbeitungsnetz zu einer universellen Kommunikations-, Basis- und damit auch kritischen Infrastruktur entwickelt, die für die tägliche Arbeit von Wissenschaftlern und Studierenden unverzichtbar ist. Es bedarf daher einer konstanten Weiter- und Fortentwicklung sowie kontinuierlicher Innovation. Durch die Skaleneffekte können modernste Kommunikationstechniken genutzt und allen versorgten Einrichtungen modernste Netzdienste zur Verfügung gestellt werden. Derzeit wird z. B. die Ersetzung der Router-Plattform geplant, um das Backbone zukunftsfähig für die nächsten Bandbreitenklassen von 40 Gbit/s bzw. sogar 100 Gbit/s zu machen.

DFN und GÉANT

Das MWN ist über das Deutsche Forschungsnetz (DFN) deutschlandweit mit allen Universitäten, Hochschulen, Forschungseinrichtungen, aber auch mit kommerziellen Providern vernetzt. Das DFN wird in der Rechtsform eines Vereins aller angeschlossenen Universitäten und Forschungseinrichtungen betrieben. Das LRZ bringt sich als Mitglied in diversen Gremien ein. Das DFN als nationales Forschungsnetz ist selbst wieder in den Verbund von europäischen Forschungsnetzen (GÉANT) eingebunden und bietet über den GÉANT-Backbone die Verbindungen nach Europa. Ein international wichtiger Austauschpunkt, genutzt sowohl vom DFN als auch GÉANT, ist Frankfurt. Dort befinden sich auch viele Übergänge in internationale Netze.

Die kooperative Infrastruktur aus MWN, DFN und GÉANT bietet viele sehr innovative Möglichkeiten, damit Wissenschaftler auch international kooperieren können. Exemplarisch seien hier nur sog. Optical Private Networks (OPN) genannt, die relativ schnell europaweit oder auch international aufgebaut werden können. OPN sind private Hochgeschwindigkeitsnetze, die etwa für einen Forschungsverbund wie das Large Hadron Collider Grid (LHCG) genutzt werden, um die Daten, die am Beschleuniger am CERN anfallen, an Physiker weltweit zu verteilen. Ein weiteres OPN ist ein Verbund der größten europäischen Zentren im Rahmen der „Partnership for Advanced Computing in Europe“ (PRACE) zur engen Kopplung ihrer Höchstleistungsrechner.

Ohne die sehr gute und enge Zusammenarbeit zwischen MWN, DFN und GÉANT wären solche speziellen Dienste für die Münchner Wissenschaft, wenn überhaupt, nur äußerst schwer zu realisieren, aber vermutlich nicht zu bezahlen.

DER AUTOR

PD Dr. Helmut Reiser leitet die *Abteilung Kommunikationsnetze am Leibniz-Rechenzentrum der Bayerischen Akademie der Wissenschaften.*

Abb. 2: Das Münchner Wissenschaftsnetz ist mehrfach gegen Ausfälle gesichert.

