Leibniz-Rechenzentrum
der Bayerischen Akademie der Wissenschaften

Das Münchner Wissenschaftsnetz (MWN)

Konzepte, Dienste, Infrastruktur und Management

Januar 2019

Helmut Reiser, Stefan Metzger

Direktorium:
Prof. Dr. D. Kranzlmüller
(Vorsitzender)
Prof. Dr. M. Schulz
Prof. Dr. H.-J. Bungartz
Prof. Dr. T. Seidl

Leibniz-Rechenzentrum

Boltzmannstaße 1
85748 Garching
E-Mail:
UST-ID Nr. DE811335517

Telefon +49-89-35831-8000
Telefax +49-89-35831-9700
lrzpost@lrz.de
Internet: www.lrz.de

Inhaltsverzeichnis

1 Grundsätze

Das Münchner Wissenschaftsnetz (MWN) verbindet die Gebäude der Münchner Universitäten und Hochschulen; darüberhinaus sind viele außeruniversitäre Einrichtungen angeschlossen. Das MWN ist als flächendeckendes Netz kontinuierlich auf dem jeweils aktuellen Stand der Technik zu halten, um bedarfsorientiert Kapazitäten bereitzustellen. Jeder Mitarbeiter und jeder Student der an diesem Netz angeschlossenen Institutionen soll an seinem Arbeitsplatz und bei Bedarf auch von zu Hause oder unterwegs aus komfortablen und uneingeschränkten Zugang zu allen Netzdiensten haben, die er für seine Arbeit in Forschung, Lehre und Studium benötigt. Das Netz vermittelt den Zugang zu Servern bzw. zu Netzdiensten innerhalb des MWN, zu nationalen und internationalen Wissenschaftsnetzen und zum allgemeinen Internet. Bei Planung, Ausbau und Betrieb des MWN wirken Leibniz-Rechenzentrum (LRZ), zuständige Bauämter und angeschlossene Institutionen eng zusammen.

2 Bedarfsbegründende Grunddaten

Das Leibniz-Rechenzentrum der Bayerischen Akademie der Wissenschaften ist gemeinsames Rechenzentrum der

- Bayerischen Akademie der Wissenschaften (BAdW)
- Ludwig-Maximilians-Universität München (LMU)
- Technischen Universität München (TUM)

Es bedient auch die

- Akademie der Bildenden Künste (ADBK)
- Hochschule München (HM)
- Hochschule Weihenstephan-Triesdorf (HSWT)

Zudem wird das MWN mitgenutzt von:

- Ägyptische Staatssammlung
- AFK - Ausbildungs- und Fortbildungskanäle Bayern
- Archäologische Staatssammlung
- Bauamt 2 München
- Bayerisches Armeemuseum Ingolstadt
- Bayerisches Forschungs- und Technologiezentrum für Sportwissenschaft
- Bayerische Staatsbibliothek
- Bayerische Staatsbrauerei

- Bayerische Staatsgemäldesammlung
- Bayerische Theaterakademie August Everding
- Bayerisches Nationalmuseum
- Bayerisches Zentrum für angewandte Energieforschung (ZAE)
- Botanischer Garten
- Deutscher Wetterdienst
- Deutsches Herzzentrum
- Deutsches Theatermuseum
- Die Neue Sammlung
- Dörner Institut
- Fraunhofer Institut für angewandte und integrierte Sicherheit (AISEC)
- Fraunhofer Institut BioCAT in Straubing
- Fraunhofer Institut für Verfahrenstechnik und Verpackungen in Weihenstephan
- Garchinger Technologie- und Gründerzentrum (GATE)
- General Electric Global Research
- Generaldirektion der Staatlichen Naturwissenschaftlichen Sammlungen
- Gesellschaft für Anlagen und Reaktorsicherheit (GRS)
- Hochschule für Fernsehen und Film
- Hochschule für Musik und Theater
- Hochschule für Philosophie
- Hochschule für Politik
- Innovations- und Gründerzentrum Biotechnologie (IZB) in Martinsried und Weihenstephan
- Isotopen Technologie München (itm)
- Kath. Stiftungsfachhochschule München
- Kompetenzzentrum Nachwachsende Rohstoffe
- Max-Planck-Gesellschaft, Zentralverwaltung
- Max-Planck-Institut für Biochemie
- Max-Planck-Institut für Neurobiologie
- Max-Planck-Institut für Physik
- Max-Planck-Institut für Plasmaphysik
- Max-Planck-Institut für Sozialrecht und Sozialpolitik
- Max-Planck-Institut für Psychatrie

- Monumenta Germaniae Historica
- Munich Creative Networks (MCN) Verein
- Museum Brandhorst
- Museum Fünf Kontinente
- Museum für Abgüsse klassischer Bildwerke
- Neues Museum Nürnberg
- Pinakotheken
- Prähistorische Staatssammlung
- Schack-Galerie
- Schülerforschungszentrum Berchtesgaden
- Staatliche Antikensammlung
- Staatliche Graphische Sammlung
- Staatliches Museum für Ägyptische Kunst
- Staatsinstitut für Hochschulforschung und Hochschulplanung
- Staatsinstitut für Schulpädagogik und Bildungsforschung
- Studentenwerk München (und dessen Studentenwohnheime)
- Studentenwohnheime anderer Träger
- Umweltforschungsstation Schneefernerhaus
- Wissenschaftszentrum Straubing
- Zentralinstitut für Kunstgeschichte
- Zentrum für Arbeitsbeziehungen und Arbeitsrecht (ZAAR)
- Zoologische Staatssammlung

2.1 Allgemeine Angaben zur Ludwig-Maximilians-Universität München

- Fakultäten:
  - Evangelisch-Theologische Fakultät
  - Fakultät für Betriebswirtschaft
  - Fakultät für Biologie
  - Fakultät für Chemie und Pharmazie
  - Fakultät für Geowissenschaften
  - Fakultät für Geschichts- und Kunstwissenschaften
  - Fakultät für Kulturwissenschaften
  - Fakultät für Mathematik, Informatik und Statistik
  - Fakultät für Philosophie, Wissenschaftstheorie und Religionswissenschaft

  - Fakultät für Physik
  - Fakultät für Psychologie und Pädagogik
  - Fakultät für Sprach- und Literaturwissenschaften
  - Juristische Fakultät
  - Katholisch-Theologische Fakultät
  - Medizinische Fakultät
  - Sozialwissenschaftliche Fakultät
  - Tierärztliche Fakultät
  - Volkswirtschaftliche Fakultät
- Studierende (im WS 2017/2018): 50.918
- Personal (ohne Kliniken): 762 Professoren, 3.308 Wissenschaftler, 2422 Angestellte
- Räume (ohne Kliniken): 14.522 Räume auf 430.056 m^2 Hauptnutzfläche

2.2 Allgemeine Angaben zur Technischen Universität München

- Fakultäten:
  - Architektur
  - Chemie
  - Elektrotechnik und Informationstechnik
  - Informatik
  - Ingenieurfakultät Bau Geo Umwelt
  - Luftfahrt, Raumfahrt und Geodäsie
  - Maschinenwesen
  - Mathematik
  - Medizin
  - Physik
  - Sport- und Gesundheitswissenschaften
  - TUM School of Education
  - TUM School of Governance
  - Wirtschaftswissenschaften
  - Wissenschaftszentrum Weihenstephan für Ernährung, Landnutzung und Umwelt
- Studierende (im WS 2018/2019): 41.375
- Personal: 566 Professoren, 6.459 sonstige Wissenschaftler, 3.276 Nicht-Wissenschaftler
- Räume (ohne Kliniken): 15.989 Räume auf 550.790 m^2 Hauptnutzfläche

2.3 Allgemeine Angaben zur Hochschule München

- Fakultäten:
  - Angewandte Naturwissenschaften und Mechatronik
  - Angewandte Sozialwissenschaften
  - Architektur
  - Bauingenieurwesen
  - Betriebswirtschaft
  - Design
  - Elektrotechnik und Informationstechnik
  - Geoinformation
  - Informatik und Mathematik
  - Maschinenbau, Fahrzeugtechnik, Flugzeugtechnik
  - Studium Generale und interdisziplinäre Studien
  - Tourismus
  - Versorgungs- und Gebäudetechnik, Verfahrenstechnik Papier und Verpackung, Druck- und Medientechnik
  - Wirtschaftsingenieurwesen
- Studierende (im WS 2018/2019): 18.400
- Personal: ca. 2.000, davon 463 Professoren
- Räume: 2.292 Räume auf 106.555 m^2 Hauptnutzfläche

2.4 Allgemeine Angaben zur Hochschule Weihenstephan-Triesdorf

- Fakultäten:
  - Bioingenieurwissenschaften
  - Gartenbau und Lebensmitteltechnologie
  - Landschaftsarchitektur
  - Landwirtschaft, Lebensmittel und Ernährung
  - Nachhaltige Agrar- und Energiesysteme
  - Wald und Forstwirtschaft
  - Umweltingenieurwesen (Triesdorf)
- Studierende (im WS 2018/2019): 6.150
- Personal: 942, davon 461 Professoren und Lehrbeauftragte
- Räume: 1.246 Räume auf 52.202 m^2 Hauptnutzfläche

2.5 Standorte

Das Münchner Wissenschaftsnetz (MWN) verbindet vor allem Standorte der Ludwig-Maximilians-Universität München (LMU), der Technischen Universität München (TUM), der Bayerischen Akademie der Wissenschaften (BAdW), der Hochschule München (HM) und der Hochschule Weihenstephan-Triesdorf miteinander. Diese Standorte sind insbesondere über die gesamte Münchner Region (i. W. Münchner Stadtgebiet, Garching, Großhadern/Martinsried und Weihenstephan) verteilt, umfassen aber auch weitere Standorte in Bayern. Die zu versorgenden Universitäten stellen von ihrer Ausprägung her keine reinen Campus-Universitäten dar, auch wenn Bestrebungen erkennbar sind, dies in einzelnen Bereichen zu forcieren. Beide Universitäten sind aufgrund der räumlichen Enge der Münchner Innenstadt über viele Gebäudeareale verteilt. Erst in den letzten 20 Jahren erfolgte eine gewisse räumliche Konzentration (TUM in Garching und Weihenstephan, LMU in Großhadern/Martinsried).

Derzeit sind an das MWN mehr als 600 als Unterbezirke bezeichnete Gebäudegruppen in mehr als 60 Arealen angebunden (siehe Abbildung 1). Die Lage von Standorten, die außerhalb des Münchner Stadtgebietes liegen, ist in der Abbildung nicht maßstabsgetreu dargestellt, sondern lediglich schematisch (Himmelsrichtung) angedeutet. Die Größe der zu versorgenden Areale ist sehr unterschiedlich; sie reicht von einem einzelnen Gebäude bis zu einem gesamten Campusbereich (z. B. Garching, Weihenstephan) mit mehr als 30 Gebäuden und mehr als 13.000 angeschlossenen Endgeräten. Derzeit sind bereits 52 Studentenwohnheime mit insgesamt rund 12.500 Wohnheimplätzen am MWN angeschlossen. Die Abbildungen 2 und 3 zeigen die einzelnen Standorte und ihre Verbindungen im Detail.

Die Areale des MWN werden zu Dokumentationszwecken auch mit Kürzeln aus einem oder zwei Zeichen (sog. Unterbezirke) benannt. Siehe hierzu den Anhang *Liste aller Unterbezirke des Münchner Wissenschaftsnetzes* ab Seite 64 oder `www.lrz.de/services/netz/ubezliste/`.

Die folgende Liste gibt einen ungefähren Eindruck über die wichtigsten an das MWN derzeit angeschlossenen Standorte sowie über die dort an vom LRZ verwaltete Netzkomponenten angeschlossenen Endgeräte. Die Sortierung erfolgt nach der Anzahl der angeschlossenen Endgeräte:

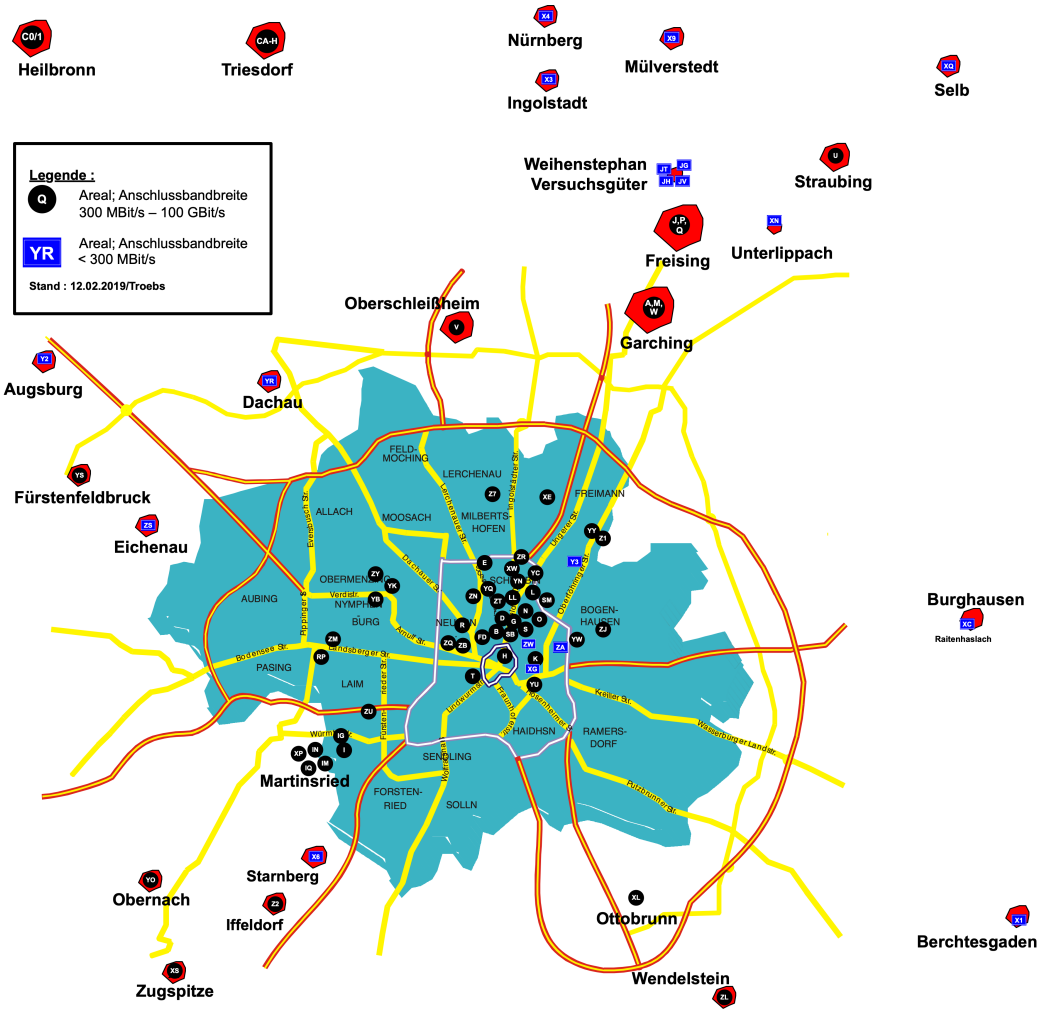


Abbildung 1: Lage der Standorte im MWN (außerhalb Münchens nicht maßstabsgetreu)

Standort	Standortkürzel	Kabelgebundenen Endgeräte	Drahtlose Endgeräte	Summe Endgeräte
LMU Stammgelände	G,S	5421	7775	13196
Campus Garching	A,M,W	10230	2909	13139
TUM Stammgelände	B	5657	6047	11704
HS München	R	7802	5145	12947
Campus Weihenstephan, HSWT, TUM	J,Q,P	5101	3097	8198
Großhadern	I	3506	2129	5635
LRZ Garching	WL,WR,WZ,WC	2382	117	2499
LMU, Leopoldstr.	L	1628	2184	3812
Königsplatz, LMU, TUM, HfMT	F	2183	1086	3269
TUM, Medizin	K	5000		5000
HSWT Triesdorf	C	515	867	1382
LMU Theresienstraße 39-43 , Museen	D	1675	1210	2885
LMU Oettingenstr. 67	O	1525	838	2363
Studentenwerk, Wohnheim Freimann	Z1	2440		2440
Studentenwerk, Wohnheim Olypiadorf	EO	1853		1853
TUM Sportmedizin	E	381	531	912
LMU Königinenstr.	N	931	589	1520
Staatsbibliothek	SB, SX	221	388	609
Deutsches Museum	YU	116	71	187
TUM Marsstr. 20-22	ZB	522	475	997
BAdW, Marstallplatz	H	369	57	426
LMU, Oberschleißheim	V	449	151	600
LMU, Sternwarte	ZJ	193	109	302
Akademie der Bildenden Künste	YJ	404	68	472
TUM, Baumbachstr	ZM	263	110	373
TUM, Straubing	U	436	229	665
LMU, Edmund-Rumpler-Str.	XE, XR	330	240	570
LMU, Winzerstr. 45	YQ	159	83	242
TUM, Schragenhofstr.	ZY	149	30	179
LMU, Medizin Innestadt und Medieninformatik	T	233	222	455
TUM Obernach	YO	59	23	82
LMU Fürstenfeldbruck	YS	52	6	58
LMU Iffeldorf	Z2	23	15	38
LMU Wendelstein	ZL	84	1	85
Summe		**62292**	**36802**	**99094**

Die Anzahl tatsächlich ans MWN angeschlossener Endgeräte ist höher als die Summe der oben angegebenen Werte. Der Grund hierfür ist, dass in die obige Aufstellung die an nicht vom LRZ verwalteten Netzkomponenten angeschlossenen Endgeräte nicht einfließen. Beispielsweise werden in der Medizin und in der Informatik der TUM sowie in der Hochschule München und mehreren Studentenwohnheimen die Campusnetze selbst verwaltet. Unter

Berücksichtigung entsprechender Rückmeldungen dieser nicht direkt erfassten Standorte beträgt die Gesamtzahl der im MWN versorgten Endgeräte derzeit über 200.000.

2.6 Mengengerüst zur Netznutzung

- Nutzungsberechtigte: Alle Mitglieder und Angehörigen der angeschlossenen Hochschulen sowie die Mitarbeiter der angeschlossenen Institutionen sind berechtigt, das MWN zu benutzen. Die Fakultäten der Medizin (LMU, TUM), der Informatik (TUM) sowie der Hochschule München betreiben die in ihren Räumen gelegenen Netzstrukturen selbst. Dies ist begründet u. a. in den geänderten Anforderungen an Medizinnetze und dem speziellen Lehr- und Forschungscharakter von Informatiknetzen. Der Anschluss zum Internet (X-WiN und Backup über M-net) wird jedoch gemeinsam genutzt.
- Eingetragene Nutzer: Die LRZ-Benutzerverwaltung wird von den Campus-Management-Systemen der beiden Münchner Universitäten und der Hochschule München gespeist und durch überwiegend manuelle Eintragung aller anderen Benutzer – dies umfasst sowohl Benutzer innerhalb des MWN als auch High-Performance-Computing-Nutzer aus dem deutschen und internationalen Umfeld – ergänzt. Insgesamt nutzen derzeit mehr als 200.000 Kennungen Dienste am LRZ.
- Versorgte Systeme: In der Spitze sind über 222.000 Geräte (MAC-Adressen) innerhalb von 7 Tagen am MWN angebunden. Im Mittel sind knapp 175.000 Geräte pro Woche im Netz. Abbildung 4 zeigt die Anzahl der verschiedenen im MWN angemeldeten Geräte innerhalb der jeweils letzten 7 Tage über das Jahr 2018.
- Netzdienste: Charakteristische Daten für die wichtigsten Netzdienste sind:
  - Durchschnittlicher Durchsatz X-WiN ca. 2,8 PByte/Monat empfangene und ca. 1,3 PByte/Monat gesendete Daten.
  - Etwa 6.900.000 E-Mails, die pro Monat über das Mail-Relay des LRZ zugestellt werden; dabei werden fast doppelt so viele weitere E-Mails gar nicht erst angenommen, weil sie durch Greylisting und andere Verfahren als Spam identifiziert werden.
  - Etwa 140 TByte werden täglich für Backup und Archiv über das MWN zum Archiv-Server im LRZ transportiert.
  - Etwa 12.000 verschiedene Benutzer pro Woche verbinden sich zu den VPN-Servern.
  - Etwa 4.000 WLAN-Accesspoints.

2.7 Rechenzentrumsnetz

Das zur Erbringung dieser Dienste eingesetzte Rechenzentrums-Kernnetz ist in Abbildung 5 dargestellt. Hier erfolgte im Jahr 2018 ein grundlegender Umbau, als Vorbereitung des aktuellen Höchstleistungsrechner SuperMUC-NG. Bisher waren alle Komponenten über zwei zentrale Switching- bzw. Routing-Systeme mit dem Backbone verbunden. Wegen steigender Bandbreitenanforderungen, einer stark zunehmenden Anzahl von Ports sowie der Verteilung der Systeme über 6 Brandabschnitte, die beim zentralen Ansatz einen erheblichen Nachverkabelungsaufwand erfordert hätten, wurde der zentrale Ansatz zu Gunsten einer Leaf & Spine Architektur aufgegeben.

Münchner Wissenschaftsnetz

Teil 1

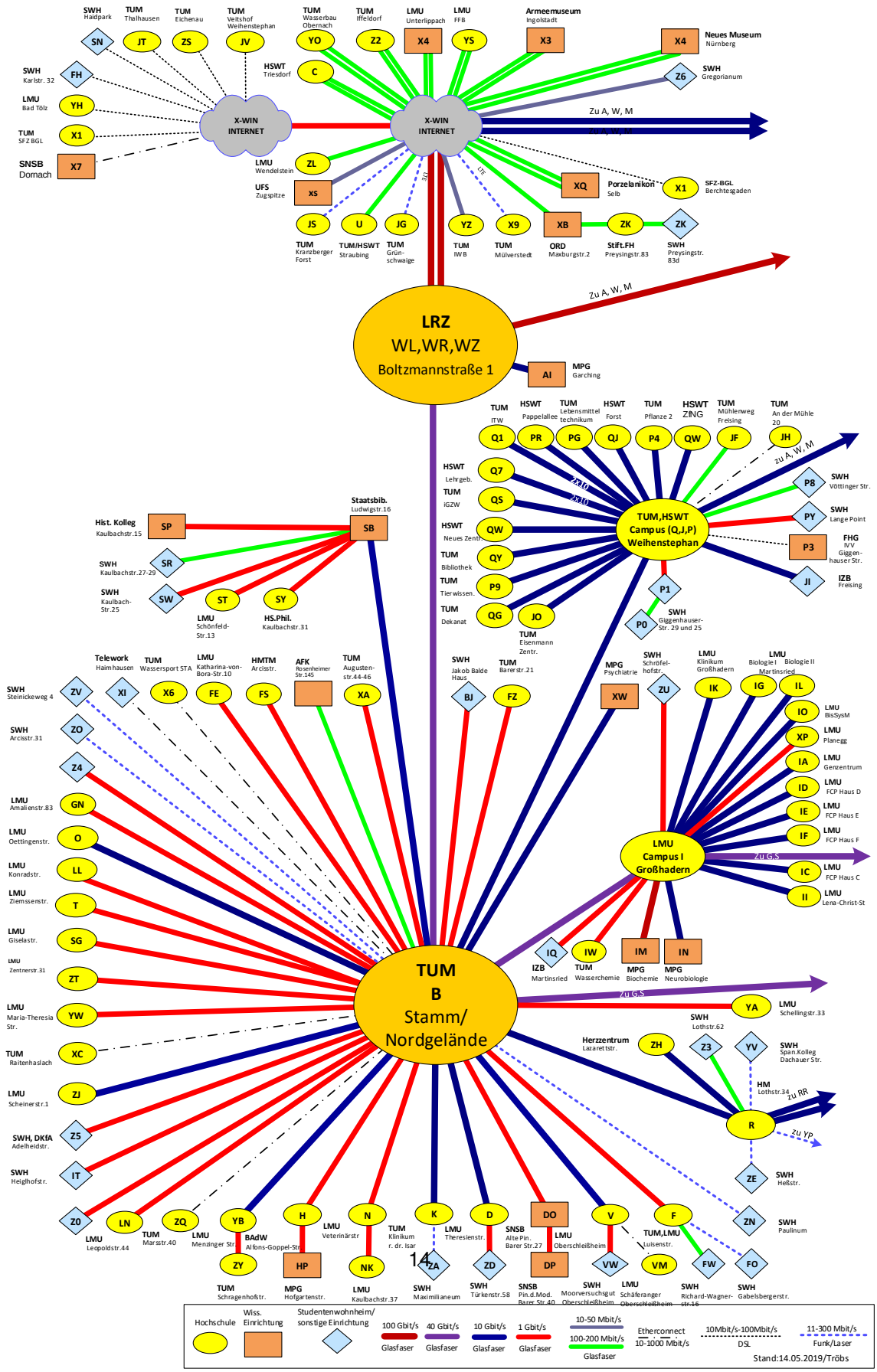
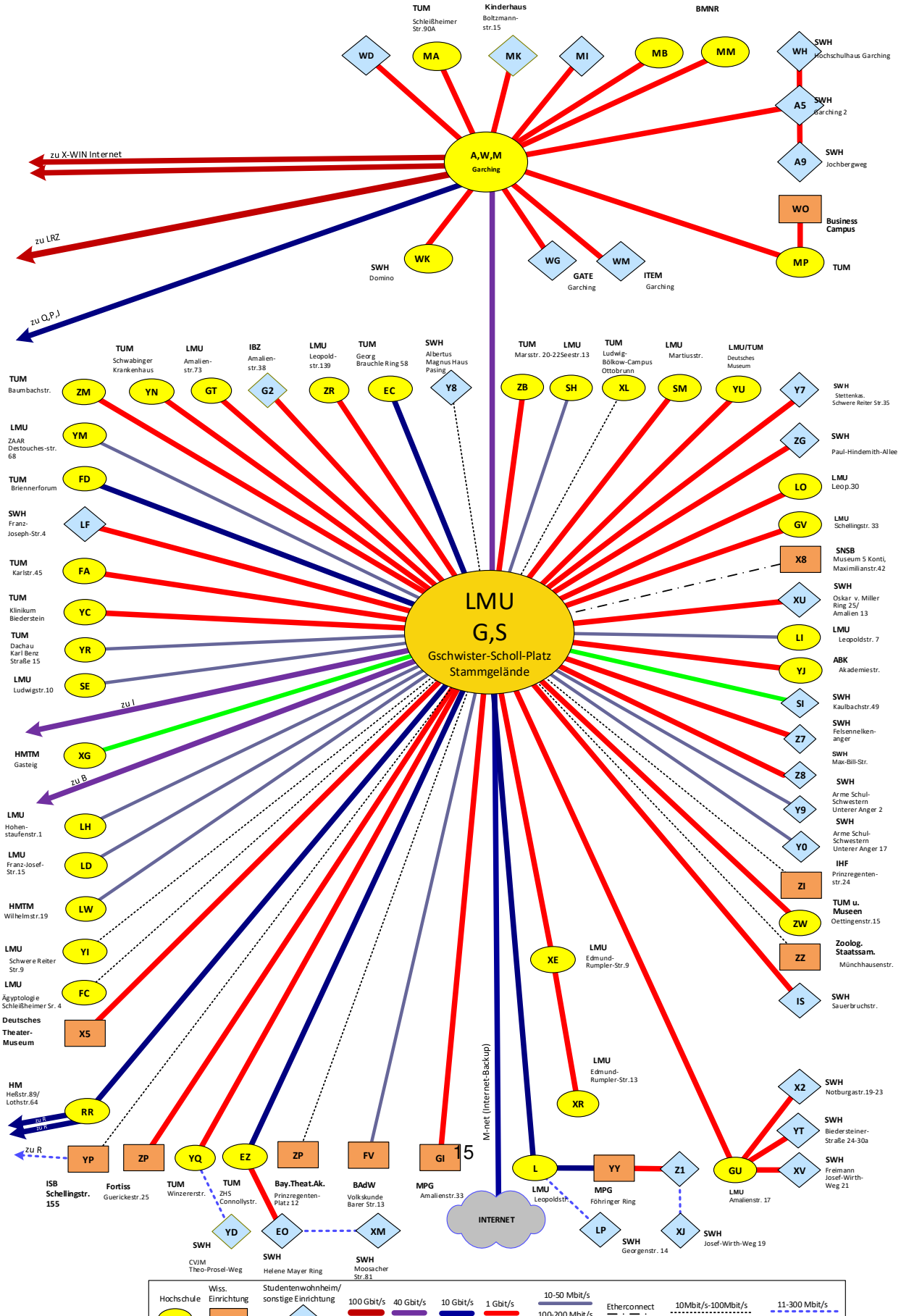


Abbildung 2: Standorte und Verbindungen im MWN, Teil 1/2

Münchner Wissenschaftsnetz

Teil 2



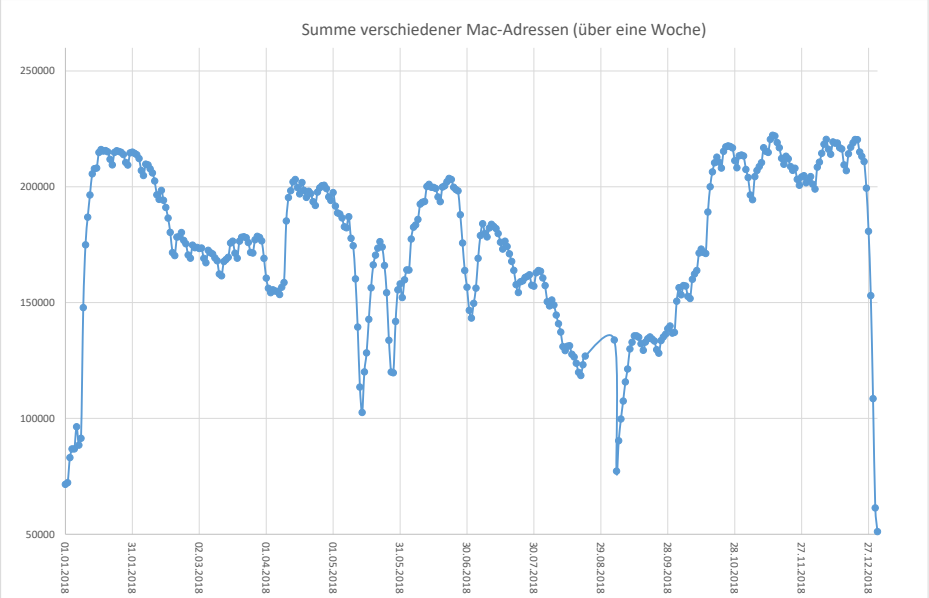


Abbildung 4: Anzahl der verschiedenen im MWN angemeldeten Geräte innerhalb der letzten 7 Tage

Die Idee dabei ist, möglichst nahe an den Endsystemen Leaf-Switches zu platzieren und dort die Endgeräte anzuschließen. Jeder Leaf-Switch hat eine oder mehrere Verbindungen in die Spine-Schicht. Durch die Nähe von Leaf-Switches und Endgeräten, bleibt der Nachverkablelungsaufwand auch lokal auf den jeweiligen Brandabschnitt beschränkt und ist deutlich wirtschaftlicher. Ein weiterer großer Vorteil, ist die hohe Skalierbarkeit. Werden weitere Endsysteme in Betrieb genommen, kann über zusätzliche Leaf- und ggf. Spine-Switches skaliert werden. Werden höhere Bandbreiten nötig, kann über zusätzliche Verbindungen skaliert werden. Diese Vorteile werden allerdings durch einen höheren Grad an Komplexität erkauft. Insgesamt hat sich die Design-Entscheidung als sehr positiv, effizient und effektiv herausgestellt.

3 Netzdienste

Im Folgenden werden der Stand der Netzdienste, die Entwicklung des Dienstspektrums und die Zielsetzung bezüglich der Dienstqualität beschrieben.

3.1 Stand der Netzdienste

Aufgrund des insgesamt sehr hohen Datenvolumens wird der Backup- und Archivdienst von den übrigen Diensten getrennt behandelt.

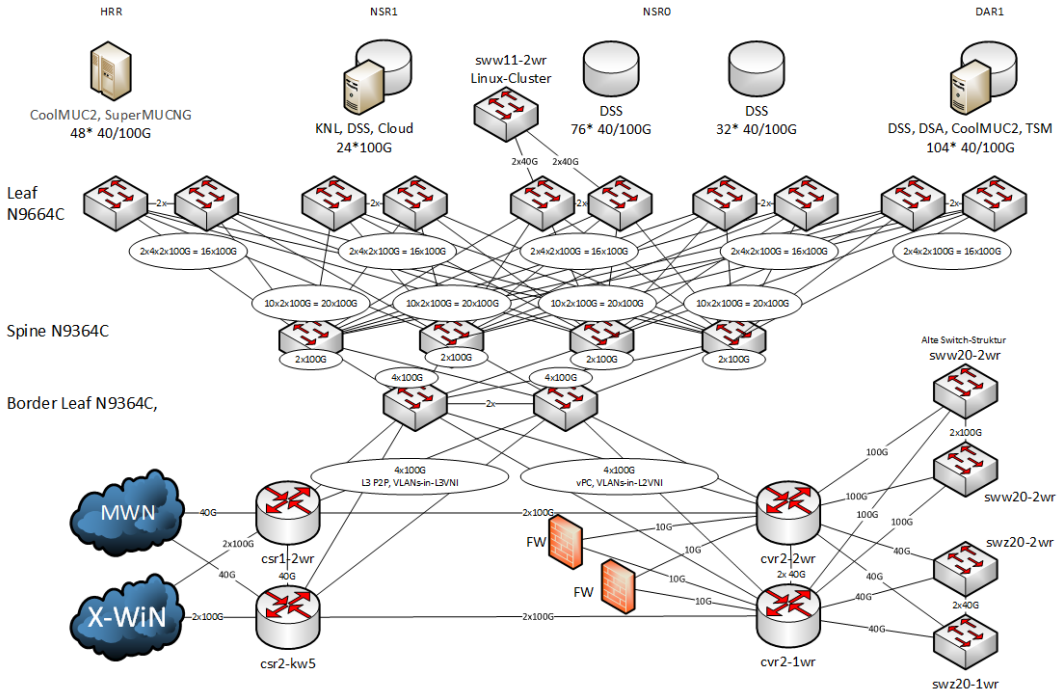


Abbildung 5: Struktur des Kernnetzes im Rechenzentrum

3.1.1 Standarddienste

Die vom LRZ betriebenen Dienste wie Webhosting, E-Mail, Datenbanken, Sync & Share, Onlinespeicher, Zugang zu Online-Medien, Compute- und Cloud-Services usw. stehen allen Berechtigten auf der Basis von Servern und systemnahen Diensten (DNS, NTP, DHCP u. a.) zur Verfügung. Es werden jedoch auch von den Institutionen selbst solche Dienste betrieben.

Als Protokolle werden flächendeckend IPv4 und IPv6 eingesetzt. Nur wenige Dutzend der insgesamt über 8.000 Subnetze sind auf Wunsch der Benutzer noch von der IPv4-/IPv6-Dual-Stack-Umgebung ausgenommen und werden nur mit IPv4 versorgt. Bis auf wenige Legacy-Systeme sind alle vom LRZ angebotenen Dienste ebenfalls bereits über IPv6 erreichbar.

3.1.2 Backup und Archiv

Das LRZ betreibt seit 1996 einen zentralen Service für Backup und Archivierung, für dessen Nutzung rund 10.000 Rechner (größtenteils Server, die mehrere Arbeitsplatzrechner bedienen) aus über 450 Einrichtungen der Münchner Hochschulen registriert sind. Die Hardware-Komponenten des Systems (Server, Plattenspeicher, Bandbibliotheken und Bandlaufwerke) wurden seit damals kontinuierlich erneuert und erweitert. Dabei wurden die Daten jeweils auf das neue System übernommen. Eine der letzten großen Neuinstallationen mit zwei Bandbibliotheken im Jahre 2012 war das Hochleistungsarchiv, das primär den SuperMUC bedient. Dieses Archiv ist inzwischen mit 35 PB fast voll belegt. Es wird 2019/20 durch ein neues Archiv mit einer Kapazität von 200 PB abgelöst. Derzeit sind rund 80 PetaBytes Daten auf über 46.000 Bandkasetten gespeichert. Etwa 130 Terabyte werden pro Tag für Backup und Archiv über das MWN auf die Speichersysteme im LRZ transportiert.

3.2 Entwicklung des Dienstspektrums

Auch bei der Entwicklung des Dienstspektrums wird nach Standarddiensten und den Backup- und Archivdiensten differenziert; zudem werden die Verzeichnisdienste betrachtet, die eine einrichtungsübergreifend konsistente Benutzerverwaltung im MWN ermöglichen.

3.2.1 Standarddienste

Die Standarddienste müssen so weiterentwickelt werden, dass

- die rasch (derzeit ca. Faktor 1,5 pro Jahr) ansteigenden Volumina bewältigt werden,
- weitgehende Ausfallsicherheit (Hochverfügbarkeit) erreicht wird,
- Quality of Service (QoS) einführbar wird und
- die Sicherung gegen Angriffe und Missbrauch verbessert wird (Vertraulichkeit, Integrität, Verfügbarkeit).

3.2.2 Daten- und Speicherverwaltung

Die Anzahl der Teilnehmer an Backup und Archivierung nimmt seit Jahren kontinuierlich zu. Dabei werden in aller Regel nicht einzelne Arbeitsplatzrechner, sondern lokale Server gesichert, die wiederum ihre Daten den Arbeitsplatzrechnern zur Verfügung stellen.

Im Rahmen des DFG-geförderten Projekts IntegraTUM ist eine hochschulweit nutzbare Datenspeicherplattform, die über Datensicherungs- und Archivierungsfunktionen verfügt und eng mit einem zentralen Verzeichnisdienst gekoppelt ist, etabliert worden. Dazu ist eine Fileserver-Konfiguration implementiert, die auf Network Attached Storage aufbaut.

Seit 2004 besteht eine Kooperation zwischen der Bayerischen Staatsbibliothek (BSB) und dem LRZ, die inzwischen durch drei DFG-geförderte Projekte (BABS, BABS2 und vd16-digital), die BSB-Google Partnerschaft und die Einführung des Langzeitarchivierungsmanagementsystems Rosetta der Firma Ex-Libris an der BSB ausgeweitet wurde. Außerdem betreibt das Münchner Digitalisierungszentrum der BSB auch das bayerische Kulturportal bavarikon (`www.bavarikon.de`) und die Verkündungsplattform Bayern. Dabei tritt das LRZ für die BSB als Dienstleister für die Langzeitarchivierung, das Bereitstellen von Onlinespeicher, das Attended Housing von Clusterknoten und Hosting von virtuellen Servern auf. Bisher wurden von der BSB mehr als 2 Milliarden Objekte mit einem Datenvolumen von 1.000 TB am LRZ archiviert.

BayernShare ermöglicht Wissenschaftlern und Studenten die Synchronisierung von Daten auf verschiedenen Endgeräten und den unkomplizierten Austausch dieser Daten mit Kollegen und Kommilitonen weltweit. Im Oktober 2015 ging der Dienst im Rahmen von Bayern-Digital in Betrieb. BayernShare wird gebildet aus drei Instanzen von Diensten, die am Regionalen Rechenzentrum in Erlangen, an der Universität der Bundeswehr und am LRZ betrieben werden. Im LRZ firmiert der entsprechende Dienst unter der Bezeichnung LRZ Sync & Share.

Die Nachfrage war von Anfang an groß. Der Dienst wird intensiv genutzt mit enormen Zuwachsraten von bis zu 1.000 Neuregistrierungen pro Woche (s. Abbildung 6). Neben den

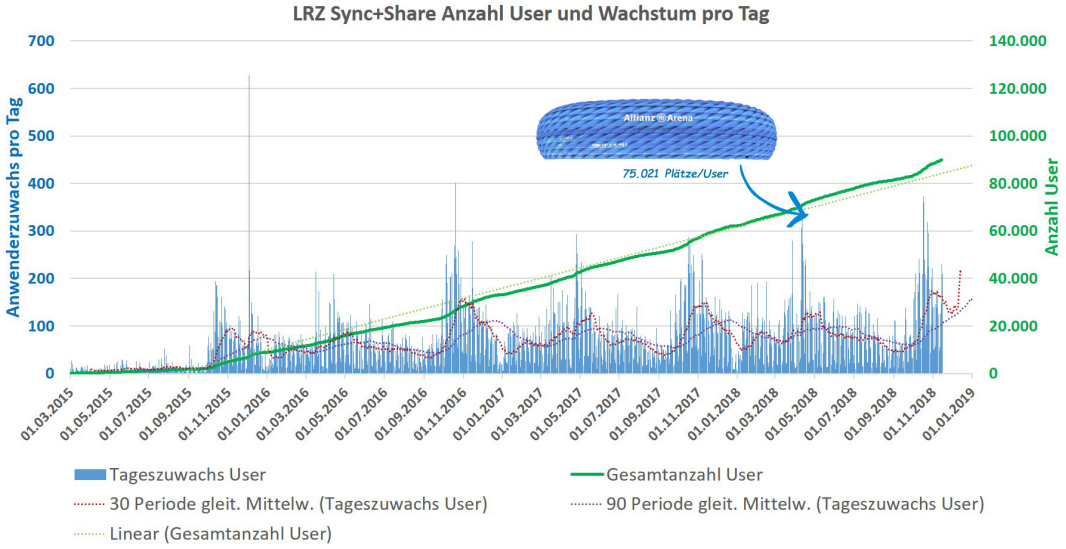


Abbildung 6: Entwicklung der Nutzerzahlen bei Sync & Share 2018

Münchner Universitäten steht der Dienst allen bayerischen Hochschulen und Universitäten zur Verfügung.

Data Science Storage (DSS) ist ein Speicher für sehr große Datenmengen. Den Service gibt es erst seit wenigen Jahren. Er erlaubt das schnelle Verarbeiten großer Datenmengen an den HPC-Systemen des LRZ. Das Basissystem von 2016 hat eine Plattenkapazität von 2 Petabyte und wird von handverlesenen Projekten genutzt. Bereits 2017 wurde im Auftrag der TUM ein weiteres DSS-System beschafft. Es wird am LRZ betrieben und ging 2018 in den Produktionsbetrieb. Auch die LMU hat in diesem Jahr ein eigenes System bestellt, das am LRZ installiert und betrieben werden wird. Für die neue Generation des Höchstleistungsrechners wurde der DSS um 2 x 10 Petabyte erweitert. Ein wichtiger Aspekt dabei ist der Zugriff bzw. die Austauschmöglichkeit der Daten mit anderen Rechenzentren.

Inzwischen fest an den Universitäten etabliert in Form von Projekt- und persönlichen Verzeichnissen, die MWN-weit abrufbar sind, ist der sogenannte MWN-Speicher aka Cloud Storage. Während beim DSS der hohe Durchsatz großer Datenmengen von wenigen Nutzern im Vordergrund steht, wird der **MWN-Speicher** von einer breiten Nutzerschaft verwendet. Täglich greifen tausende von Rechnern parallel auf den Speicher zu. Höchste Verfügbarkeit ist hier unerlässlich. Sie wird durch den Einsatz redundanter NAS-Speicher erreicht.

3.2.3 Verzeichnisdienste

Beide Münchner Universitäten betreiben bereits seit einigen Jahren LDAP-basierte Verzeichnisdienste, mit denen die Verwaltung der Benutzer der Hochschulportale CampusLMU bzw. TUMonline und der damit integrierten Dienste erfolgt.

Im Rahmen des Projekts LRZ-SIM (Secure Identity Management) wurde 2008 die in die Jahre gekommene zentrale Benutzerverwaltung des LRZ durch eine Migration auf aktuelle LDAP-Technik vollständig erneuert. Durch die seither weiterentwickelte direkte Kopplung mit den Verzeichnisdienstsystemen der beiden Universitäten werden die Datenerfassungs- und Verwaltungsprozesse wesentlich vereinfacht und somit die Qualität sowohl der verarbeiteten Daten als auch der darauf basierenden Dienste deutlich verbessert.

Im Rahmen der beiden Projekte IntegraTUM und LRZ-SIM wurde darüber hinaus der Betrieb eines MWN-weiten Verzeichnisdienstes auf Basis von Microsoft Active Directory pilotiert, um hochschulweite Systemadministrationskonzepte für die Plattform Microsoft Windows umzusetzen, Groupware-Lösungen wie Microsoft Exchange und Sharepoint Server anbieten zu können und die zentrale, NAS-Filer-basierte Speicherlösung zu unterstützen; seit 2009 befindet sich dieser Dienst im Produktivbetrieb.

Ferner betreibt das LRZ seit 2007 die zur Teilnahme an der vom Deutschen Forschungsnetz (DFN) betriebenen deutschlandweiten Authentifizierungs- und Autorisierungs-infrastruktur (DFN-AAI) notwendigen Komponenten für die beiden Münchner Universitäten; die auf der Software Shibboleth basierende Infrastruktur ermöglicht eine hochschulübergreifende Dienstnutzung, die bereits in den Bereichen E-Learning, Verteilung lizenzierter Software und im Umfeld elektronischer Bibliotheksangebote mit kontinuierlich steigenden Nutzerzahlen sehr erfolgreich eingesetzt wird.

3.2.4 Managed Hosting für Hochschulstart

Die am LRZ für die Stiftung für Hochschulzulassung als Managed Hosting betriebene Plattform für das so genannte *Dialogorientierte Serviceverfahren* befindet sich seit 2010 im Wirkbetrieb. Über die Plattform wird deutschlandweit die Studienplatzvergabe koordiniert.

Der Dienst inklusive seiner webbasierten Schnittstellen zu den Endanwendern und den Verwaltungen der teilnehmenden Hochschulen und Universitäten wird aufgrund der Sensibilität der verarbeiteten personenbezogenen Daten auf dedizierten Servern betrieben, nutzt jedoch weite Teile der Netzinfrastruktur des LRZ mit, u. a. Service Load Balancer und Firewalls. Die Verfügbarkeit des Dienstes ist über mehrere Wochen jedes Jahres, die mit wichtigen Phasen der Bewerbungs- und Zuteilungsverfahren korrespondieren, kritisch, woraus sich einige so genannte *Frozen Zones* ergeben, in denen außer dringenden Security-Patches keine Konfigurationsänderungen an unmittelbar relevanten Netzkomponenten durchgeführt werden. Zudem stellt in dieser Zeit eine Rufbereitschaft rund um die Uhr sicher, dass auf mögliche Störungen unmittelbar reagiert wird.

3.3 Dienstqualität

Wichtigstes Ziel ist die möglichst hohe Verfügbarkeit des Netzes und der Dienste, besonders der Basisdienste DHCP, DNS, E-Mail, LDAP, Storage und WWW. Das soll vor allem durch redundante Auslegung von wichtigen Teilen der aktiven Komponenten im Backbone und im Rechenzentrumsnetz des LRZ sowie durch Steigerung der Qualität des Netzmanagements (z.B. Einsatz von Monitoring-, Steuerungs- und Reportingwerkzeugen) erreicht werden. Operateurbetrieb für die zentralen Systeme und Komponenten besteht durchgängig in drei Schichten. Damit bezüglich des Datenverkehrs keine Engpässe entstehen, ist beim Ausbau auf ein ausgewogenes Verhältnis von Primär-, Sekundär- und Tertiärnetz in Bezug auf Bandbreiten und Auslegung der aktiven Komponenten zu achten. Um dieses Ziel zu erreichen, werden proaktiv die Anschlussleitungen der Institute sowie die Leitungen im Backbone auf ihre Auslastung überwacht. Übersteigt die durchschnittliche Auslastung eines Interfaces tagsüber mehrfach die Marke von 30% im Mittelwert für 15 Minuten, so werden entsprechende Schritte für eine Hochrüstung der Bandbreite eingeleitet. Dieser Grenzwert hat sich im Rahmen der steigenden Nutzung von zeitkritischen Multimediaanwendungen (Videokonferenzen und Vorlesungsübertragungen) als signifikant erwiesen. Nur unterhalb dieses Werts ist eine qualitativ hochwertige, zeitkritische Multimediaanwendung i. A. möglich. Damit müssen die weitergehenden Kriterien für Class of Service (CoS, Paketverluste, Verzögerung, Jitter) im lokalen Netz nicht zusätzlich betrachtet werden.

4 Netzstruktur

Nachfolgend werden der aktuelle Stand der Netzstruktur, die fortlaufende Entwicklung und die strategischen Netztechnologien vorgestellt.

4.1 Aktueller Stand

Das MWN verbindet die einzelnen (Sub-)Netze der Hochschuleinrichtungen an den verschiedenen Standorten. Zur Anbindung der einzelnen Standorte sind langfristig (jeweils für 5–10 Jahre) Dark-Fibre-Leitungen (Monomode-Lichtwellenleiter mit exklusiver Nutzung durch das LRZ) von der Telekom, dem Münchner Provider M-net, von Colt und von Gasline angemietet. Derzeit werden 43 Leitungen von der Telekom, 34 von M-net, vier von Colt, sowie eine von Gasline zum Aufbau des Backbonenetzes genutzt. Das damit geschaffene Backbonenetz hatte seit dem Umzug des LRZ nach Garching 2006 die Hauptknotenpunkte LRZ, LMU-Stammgelände, Campus Großhadern und TUM-Nordgelände, Campus Weihenstephan sowei der Hochschule München an denen sternförmig alle Leitungen zu den externen Standorten angeschlossen sind. Netze mit einer geringeren Anzahl von Endgeräten werden mit SDSL-Verbindungen (bis zu 25 Mbit/s für Institute und Studentenwohnheime) von M-net, Fibre-DSL von M-net (10–50 Mbit/s), in Einzelfällen auch VDSL (bis 100 MBit/s) oder WLAN-Verbindungen an die Backbone-Router angeschlossen.

Alle Leitungen für den Backbone sind redundant realisiert, d. h. bei einem Ausfall einer Leitung im Backbone kommt es zu keinen Einbußen bei der Konnektivität. Allerdings führt ein Ausfall einer Leitung von einem Hauptknoten des Backbone zu einem externen Standort dazu, dass der gesamte Standort keine Konnektivität zum Rest des MWN besitzt. Ausgenommen davon sind die meisten Gebäude im Campus Garching für die jeweils zwei unabhängige Glasfaser Anbindungen existieren. Ferner ist die Anbindung des MWN an das Internet seit Anfang 2003 redundant ausgelegt (2x X-WiN Anschluss und Backup über M-net, siehe Abbildung 7).

An den externen Campus-Standorten sind die anzubindenden Gebäude in der Regel ebenfalls sternförmig gemäß EN 50173 mittels in eigener Regie verlegter Glasfaserkabel an einen zentralen Standortverteiler angebunden. Hierzu wurden in der Vergangenheit anfänglich Mischkabel mit mindestens 8 Fasern Multimode-LWL (Lichtwellenleiter) und 4 Fasern Monomode-LWL verlegt. Dann wurde die Anzahl der Fasern auf 16 Multimode und 8 Monomode danach auf 12 Multimode und 12 Monomode erhöht. Die Bedeutung von Multimode nimmt bei der Anbindung von Gebäuden immer mehr ab, da die damit erreichbaren Bandbreiten (bei Verbindungen über 300 m) stark beschränkt sind. Deshalb haben wir uns 2014 dazu entschieden künftig Gebäude nur noch mit 12 bzw. 24 Fasern Monomode anzubinden. Zum Teil müssen in Zukunft Monomode-Strecken nachgerüstet werden, um Gebäude mit ausreichender Bandbreite versorgen zu können.

Bis auf ganz wenige Ausnahmen besteht flächendeckend eine strukturiert Verkabelung gemäß EN 50173. Dies wurde in den letzten Jahrzenten durch das bayerischen Netz-Investitions-Programms (NIP) erreicht mittels dem ältere Gebäude Netztechnisch saniert wurden.

Die Verkabelungsstruktur des MWN ist in Abbildung 8 schematisch dargestellt.

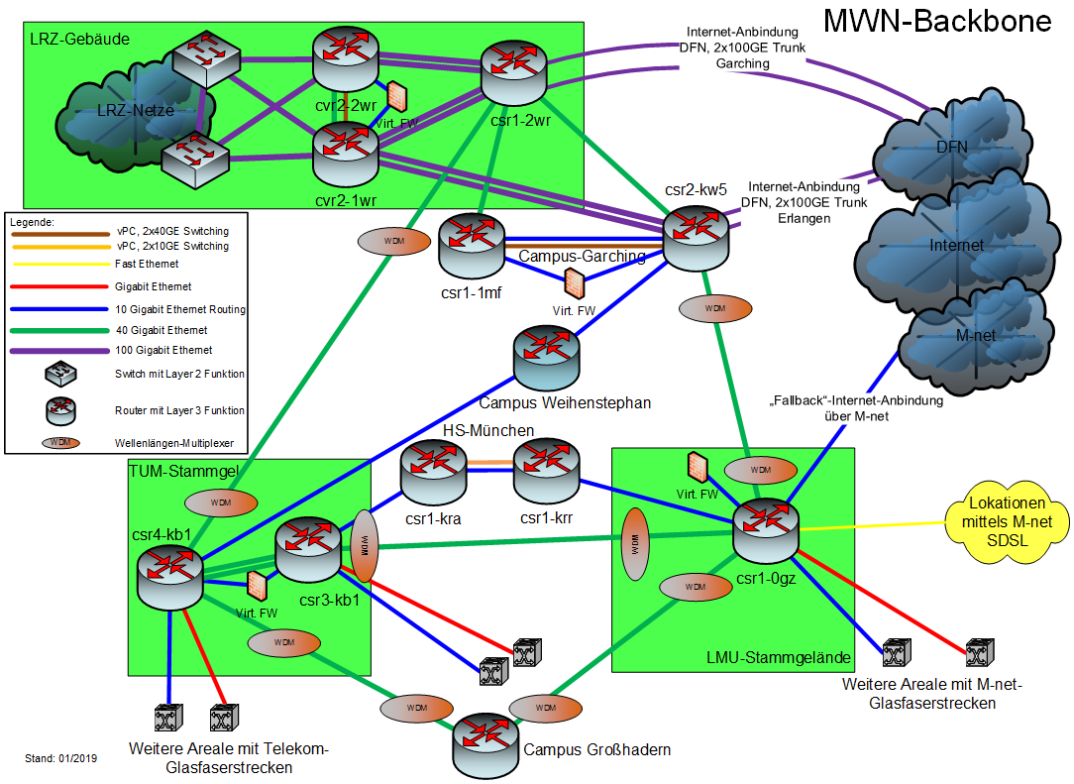


Abbildung 7: Backbonenetz des MWN

4.1.1 Erhöhung der Redundanz für Campusbereiche

Seit 2012 wird versucht auch die Redundanz für große Campusbereiche zu erhöhen. Mit einer Umsetzung diese Konzeptes wurde für den Campus Garching begonnen. Dort wurden 2016 die Gebäudeareale Chemie, Catalysis Research Center (CRC), Physikdepartment und Maschinenwesen redundant an das MWN-Backbone angeschlossen. Dazu wurden in jedem der o.g. Areale zwei neue Zentral-Switches installiert, die jeweils mit 2 x 40 Gbit/s an die beiden zentralen Backbone-Router im CRC sowie im Maschinenwesen angeschlossen (s. Abbildung 9). An die neuen Zentral-Switches wurde jeder einzelne Switch in den Etagenverteiler ebenfalls redundant mit 2 x 10 Gbit/s angebunden. Alle neuen Gebäude im Campus Garching werden mit mindestens 2x 10 GBit/s an die beiden Router-Standorte geführt.

Am Campus Weihenstephan konnte ein Standort für einen zweiten redundanten Knoten gefunden werden. In den letzten beiden Jahren wurden von der TUM für Gebäudebereiche LWL zu diesem zweiten Knoten nachinstalliert. Im diesem Jahr wird der zweite Knoten mit einer USV-Anlage sowie einem Router ertüchtigt und dann sukzessive das Redundanzkonzept auch in Weihenstephan umgesetzt.

4.1.2 Netzstrukturierung und Komponenten

Auf der vorgenannten Infrastruktur wird das MWN betrieben. Es besteht im Wesentlichen aus einem Backbonenetz, an das über Router die einzelnen Areal- bzw. Gebäudenetze an den verschiedenen Standorten angeschlossen sind. Die Router sind untereinander derzeit

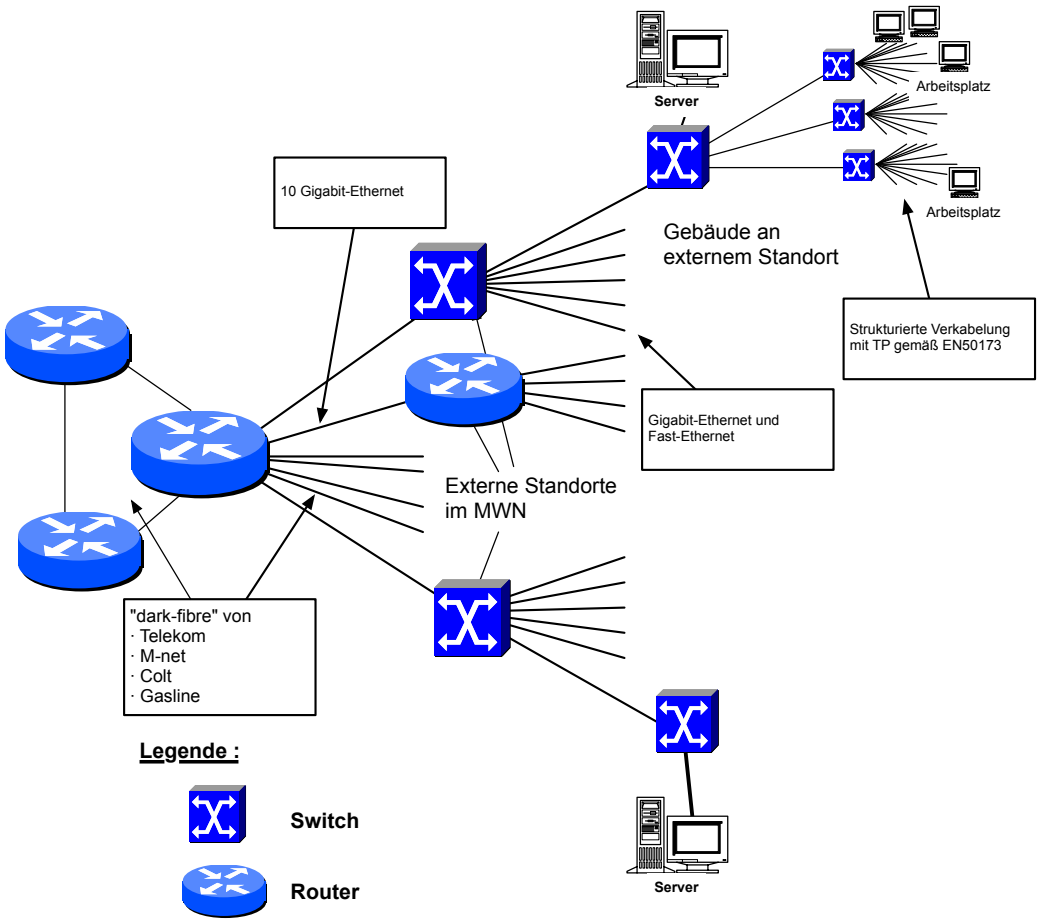


Abbildung 8: Schematische Verkabelungsstruktur

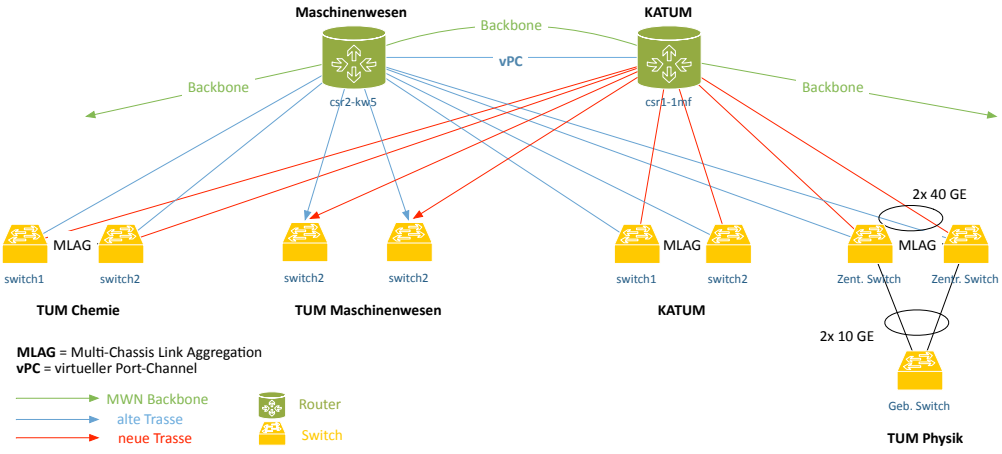


Abbildung 9: Redundante Anbindung großer Areale am Campus Garching

im Allgemeinen mit 40 bzw. mehrfach 10 Gigabit-Ethernet verbunden; das LRZ ist mit dem Backbone und dem Campus Garching mit mehrfach 100 Gigabit-Ethernet verbunden. Die Anschlussbandbreite an das Backbone des MWN richtet sich nach dem transferierten Datenvolumen und der Größe des jeweiligen Standortes (Anzahl angeschlossener Endgeräte). Diese wird aufgrund der Auslastungsdaten des Netzmanagementsystems sowie in Absprache mit den Nutzern bei Bedarf der jeweiligen Gegebenheit (Bandbreitenbedarf) angepasst.

An den Routern sind die einzelnen Instituts- bzw. Gebäude-LANs angebunden. Derzeit sind gebäudeseitig knapp 530 lokale Routerinterfaces konfiguriert. Abhängig von der verfügbaren Verkabelungsinfrastruktur wird mittels Switches i. d. R. ein komplett geswitchtes Netz bis zum Endgerät mit einer Anschlussgeschwindigkeit von typischerweise 1 Gbit/s, bei Server-Anbindungen i. d. R. 10 Gbit/s realisiert.

Zu diesem Zweck sind aktuell im Einsatz:

- 14 Backbone-Router Cisco Nexus C7010 bzw. Nexus C7710
- 18 Cisco-Router Nexus 9364C bzw 9336CFX2 für die Leaf-and-Spine Architektur im Rechenzentrumsnetz
- 61 Router Cisco 1921, ASR 1001-x bzw. C11128P zur Anbindung von abgesetzen Standorten
- 1.604 LAN-Switches der Firma HP und 334 LAN-Switches der Firma Microsens mit insgesamt ca. 100.000 aktivierten Ports.
- 504 WLAN-Accesspoints der Firma HP und 3.755 WLAN-Accesspoints der Firma Alcatel-Lucent (Aruba)

Aus Support-Gründen (Management, Konfiguration, Logistik) werden im MWN für die jeweiligen Aufgaben nur Produkte weniger Hersteller und wenige verschiedene Gerätetypen eingesetzt.

An den Hauptknotenpunkten sind Router vom Typ Cisco Nexus C7010 installiert, die die Verbindung zu den einzelnen Standorten des MWN realisieren. Größere Standorte werden mit 10 Gigabit vereinzelt auch bereits mit 40 Gigabit Ethernet angebunden. Aufgrund des Datenaufkommens kann dies dem aktuellem Bedarf kurzfristig angepasst werden (z. B. mittels Port-Trunking durch Nutzung redundanter Glasfasern bzw. Einsatz von WDM-Systemen).

Bei den größeren Arealen werden zur Anbindung ebenfalls Router dieses Typs eingesetzt. Die Geräte unterstützen alle gängigen Medien und Technologien und verfügen über 100, 40 und 10 Gigabit-Ethernet- (Backbone und dedizierte Server-Cluster), sowie Gigabit-Ethernet-Schnittstellen.

Zum Einsatz im Gebäudebereich kommen derzeit standardmäßig Switches der Firma Hewlett-Packard (HP) vom Typ ProCurve 5400R (auch mit 40 und 10 GE-Interfaces). Diese Geräte unterstützen alle gängigen Ethernet-Infrastrukturen.

4.1.3 Internetzugang und Redundanz

Die Anbindung des MWN an das Internet ist seit Anfang 2003 redundant ausgelegt (X-WiN-Anschlüsse und Backup-Leitung über M-net, s. Abbildung 10). Die Anbindung ans X-WiN erfolgt über zwei unabhängige Trunks mit je 2 * 100 Gbit/s an die Kernnetzknoten in Garching und Erlangen. Die nominelle Bandbreite für den Clusteranschluss liegt bei 229,2

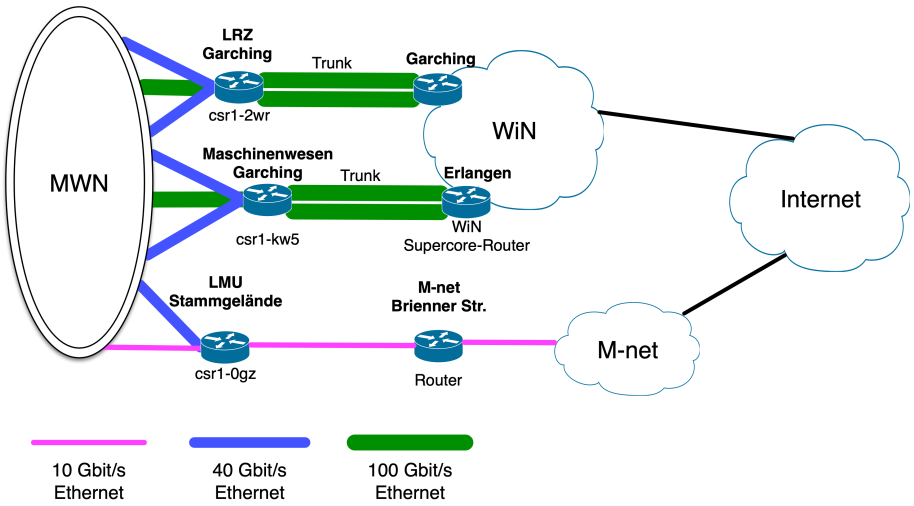


Abbildung 10: Redundante Internet-Anbindung über X-WiN und M-net

Gbit/s. Auf MWN-Seite sind dazu zwei unabhängige Router im LRZ sowie im Gebäude des Maschinenwesens im Einsatz. Zusätzlich dazu gibt es eine 10 Gbit/s Anbindung an M-net, um auch Ausfälle im X-WiN oder Routing-Probleme abfangen zu können.

Das Backbone hat eine vermaschte Struktur aus mehreren Ringen (vgl. Abbildung 7). Die zur Anbindung notwendigen Router sind größtenteils doppelt vorhanden. Durch die direkte Verbindung dieser Eckpunkte (Primärnetzknoten) wird somit eine Redundanz im Backbone-Netz des MWN erreicht. Im Rechenzentrum selbst sind alle kritischen Netzkomponenten mindestens doppelt vorhanden und auf zwei verschiedene Brandabschnitte verteilt. Damit bleibt selbst bei einem massiven Problem auf Basis der Gebäudeinfrastruktur die Netzkonnektivität über den zweiten Standort erhalten. Dieses Prinzip wird derzeit auch auf erste Campus-Bereiche ausgedehnt. So wurde der zentrale Campus-Router am Campus Garching auf zwei Geräte aufgeteilt, die mittels Virtual Path Channel (VPC) verbunden sind. Diese beiden Geräte sind auf zwei Gebäude (Maschinenwesen, Katalysezentrum) aufgeteilt. Damit ist auch hier eine deutlich höhere Sicherheit gegenüber Gebäudeausfällen gegeben, sowie die grundsätzliche Möglichkeit geschaffen, Gebäudeswitches redundant an das Router-Paar anzubinden. Außerdem wurden die Faserwege aus der Innenstadt (von der TUM bzw. LMU) am Campus Garching konsequent auf verschiedene Trassen verteilt, um auch bei Problemen in den Kabelwegen nicht beide Anbindungen in die Innenstadt zu gefährden.

4.1.4 WDM-Systeme

Die dem MWN zugrunde liegende Glasfaserinfrastruktur dient sowohl zur Kopplung der Ethernet-Infrastrukturen (wissenschaftliches Produktionsnetz) als auch zum Tunneln der Verbindungen zur Max-Planck-Gesellschaft. Die Max-Planck-Institute in Martinsried betreiben hochauflösende Rasterelektronenmikroskope, deren Daten vollständig ins Max-Planck

Computing & Data Facility (MPCDF) in Garching übertragen werden. Auf dem dortigen Hochleistungsrechner werden aus den Daten dreidimensionale Bilder berechnet. Um die Datenmenge in angemessener Zeit übertragen zu können, sind dedizierte Verbindungen mit 100 Gbit/s und eine entsprechende Ausfallsicherheit bzw. Redundanz erforderlich.

Aus diesem Grund wurden 2014 / 2015 Wellenlängenmultiplex-Systeme (DWDM) im Backbone aufgebaut und der zentrale Netzknoten am Campus Garching aufgeteilt, um die Ausfallsicherheit auch bei Schäden am Gebäude, zu erhöhen (vgl. Abbildung 7).

Derzeit werden WDM-Systeme von der Firma ADVA (FSP 3000 R7) im MWN auf den folgenden Strecken eingesetzt:

- Campus Garching; TUM-Katalysezentrum — TUM-Nordgelände (1x 100 Gigabit Ethernet; 1x 40 Gigabit-Ethernet)
- TUM-Nordgelände — Campus Großhadern (1x 100 Gbit-Ethernet, 1x 40 Gigabit-Ethernet)
- Campus Großhadern — LMU Stammgelände (1x 10 Gigabit-Ethernet, 1x 40 Gigabit-Ethernet)
- LMU-Stammgelände — Campus Garching; Maschinenwesen (1x 10 Gigabit-Ethernet, 1x 40 Gigabit-Ethernet)
- TUM-Stammgelände — LMU-Stammgelände (1x 40 Gigabit-Ethernet)

Die Institute in Martinsried sind mit wegeredundanten LWL-Strecken an je einem der beiden WDM-Systeme angebunden. Derzeit ist nur eine 100 Gbit/s Strecke, auf dem linken Ast über das TUM-Stammgelände, realisiert. Bei einem Ausfall kann die redundante Strecke auf dem rechten Ast, mit der reduzierten Bandbreite von 10 Gbit/s, genutzt werden. Mittelfristig ist geplant, auch den rechten Ast auf 100 Gbit/s zu heben. In Garching wird das Rechenzentrum der Max-Planck-Gesellschaft (MPCDF) über wegeredundante LWL-Verbindungen mit den WDM-Systemen im Maschinenwesen und dem Katalysezentrum (KaTUM) verbunden. D. h. selbst bei einem vollständigen Ausfall eines gesamten Gebäudes ist die Konnektivität zwischen RZG und Martinsried gegeben.

Zusätzlich sind Standorte der Hochschule München per WDM an den zentralen Standort in der Lothstraße angebunden. Hierbei kommen jeweils passive WDM-Komponenten zum Einsatz (z.B. für Wissenschaftsnetz, TK-Anlage, Verwaltungsnetz). Dabei werden pro Kanal unterschiedliche Wellenlängen verwendet (dazu sind entsprechende Transceiver in den aktiven Komponenten, Router und Switches, nötig).

4.1.5 Zugänge zum MWN von außerhalb

Das LRZ betreibt zwei VPN-Server, die für den gesicherten Zugang in das MWN genutzt werden können.

Die Anzahl der gleichzeitigen VPN-Nutzer blieb bei maximal 2.700 konstant, das maximale monatliche Datenvolumen über ein Jahr stieg von 73 TB auf 86 TB.

Die Validierung geschieht über die LRZ-Radius-Proxies an den zentralen Verzeichnisdiensten der Universitäten und einen Verbund von rund 70 RADIUS-Servern, die überwiegend dezentral bei den Instituten betriebenen werden.

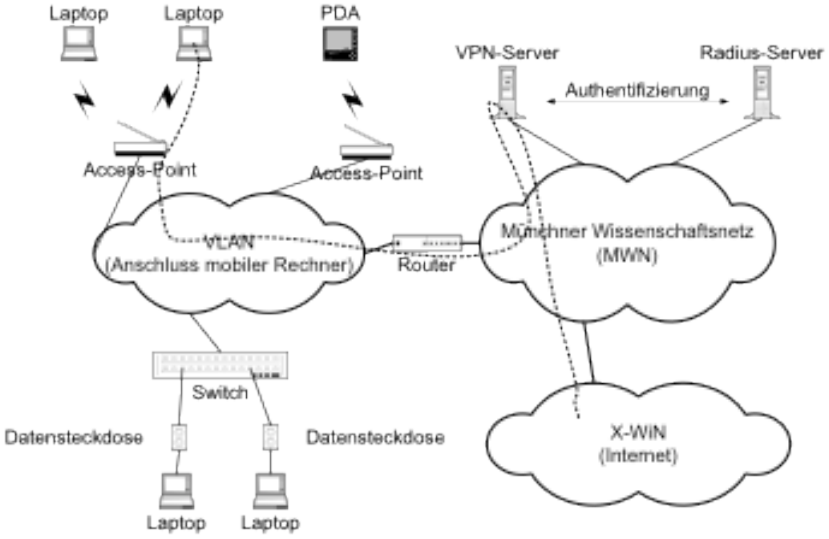


Abbildung 11: Zugang zum MWN über VPN-Server

4.1.6 Zugang zum MWN für mobile Endgeräte; WLAN

Für den Anschluss von mobilen Endgeräten stehen z. Z. im gesamten MWN über 4.200 Access-Points in rund 250 Gebäuden und ca. 350 vorkonfigurierte Datendosen an rund 30 Standorten zur Verfügung.

Der Zugang zum MWN per Mobiler Rechner kann über zwei Wege erfolgen. Über ein offenes WLAN mit der SSID ”lrzünd über den EDUROAM Zugang (SSID ëduroam”). Mit der SSID ”lrz”landet man in einem sparaten VLAN das man nur verlassen kann wenn man einen VPN-Client (im Regelfall Cisco AnyConnect Client) verwendet und sich über diesen authentifiziert. Genauso sind einige öffentlich zugängliche Datendosen geschützt. Der Zugang zum MWN über dieses Angebot ist entweder mit derselben Kennung möglich, mit der die anderen LRZ-Dienste genutzt werden können, oder mit einer institutseigenen Kennung, sofern diese in den RADIUS-Verbund aufgenommen ist.

Dadurch wird sowohl ein Schutz gegen den Missbrauch dieses Netzes erreicht, da der Internet-Anschluss des MWN nicht unbefugt genutzt werden kann, als auch der administrative Aufwand möglichst klein gehalten. Ohne Authentisierung kann keine Kommunikation mit Rechnern im MWN oder im Internet erfolgen. Abbildung 11 zeigt exemplarisch die notwendige Anmeldung und Nutzung mittels des VPN-Servers. Eine weitere Möglichkeit des Zugangs besteht über 802.1x (eduroam, siehe unten).

4.1.7 Rechenzentrumsnetz - Leaf & Spine

Seit 2018 wurde mit dem InHPC Projekt ein zusätzliches Hochgeschwindigkeits Netz (Leaf & Spine Technik) aufgebaut (vgl. Abschnitt 2.7). Mittlerweile sind viele LRZ-Server bereits hierauf migriert. Ziel des Leaf&Spine Netzes ist es ein rasch skalierbares Netz für HPC Dienste zur Verfügung zu stellen, das viele 40/100 Gigabit-Ethernet Ports bereitstellen kann. Die Bandbreite des Backbones kann durch Erhöhung der Spine-Switches skaliert werden. Zusätzliche HPC Server werden, falls nötig, durch weitere Leaf-Switches bedient.

4.2 Entwicklung der Netzstrukturen

Im Folgenden wird die Entwicklung bei der Verkabelung, bei der Netzstruktur und den eingesetzten Komponenten, bei den Zugängen zum MWN von außerhalb und beim Zugang für mobile Geräte skizziert.

4.2.1 Verkabelung

Mit NIP (Netzinvestitionsprogramm in Bayern) wurde zwar eine flächendeckende Vernetzung erreicht, diese ist jedoch an der TUM in München und Garching noch zu einem kleinen Teil in Koax ausgeführt. Die bis Ende 2009 gesetzte Aufgabe, diese Koax-Verkabelung durch eine strukturierte Verkabelung (Kupfer oder Glas) zu ersetzen, verzögert sich bei einigen wenigen Gebäuden noch durch das Warten auf deren Generalsanierung bzw. die Klärung der zukünftigen Nutzung.

TU München (ohne Weihenstephan) Im Bereich der TU München (ohne Weihenstephan) wurde 2009 eine Reihe von Gebäuden im Rahmen von NIP saniert. Seit dem Jahr 2013 wird in mehreren Bauabschnitten das Gebäude 0503 auf dem Stammgelände mit einer dem aktuellen Standard entsprechenden Datenverkabelung modernisiert. Im Gebäude des Maschinenwesens auf dem Campus Garching wurde ebenfalls im Jahr 2013 mit der Ersetzung der veralteten, strukturierten Datenverkabelung, die lediglich eine Übertragungsrate von maximal 100 Mbit/s (Cablesharing) bieten konnte, begonnen. Nach vierjähriger Unterbrechung wird diese Modernisierung seit 2017 fortgesetzt und voraussichtlich 2019 abgeschlossen. Die zum Maschinenwesen gehörenden Hallen sind jedoch nicht in der Modernisierungsmaßnahme enthalten. Auf dem Garchinger Campus bleibt damit nur noch der Gebäudeteil CH2 des Chemiegebäudes übrig, welcher zum Teil noch über eine Koax-Verkabelung betrieben werden muss. Auf dem Stamm- bzw. Nordgelände der TUM steht das Gebäude 0106 (N6) noch zur Koax-Ersetzung an.

LMU München Im Bereich der LMU München sind alle Gebäude mit einer strukturierten Verkabelung versehen. Es gab jedoch teilweise Defizite in der Verwendung der installierten Medien (nur vier-drahtiger Anschluss, d.h. Cable-Sharing, oder Installation von Kat5-Kabeln). Diese Gebäude (insgesamt 22) werden im Rahmen des 2. Bauabschnittes der NIP V-Maßnahme saniert. Die Sanierung des Datennetzes im FCP in Großhadern ist inzwischen abgeschlossen, eine weitere Gebäudegruppe zu der die Maria-Theresia-Straße 21, das Observatorium in Fürstenfeldbruck, der Standort Unterlippach sowie ein Gebäude der Tierklinik in Oberschleißheim gehört, wurde im Frühjahr 2018 zum Abschluss gebracht. Daran schließt sich nun eine letzte Gebäudegruppe mit 10 zu sanierenden Gebäuden an. Diese Gruppe wird ab Herbst 2017 neu verkabelt und soll im Frühjahr 2020 den Abschluss der NIP V-Maßnahme bilden.

Weihenstephan (TU München) Am Campus Weihenstephan der TU München sind alle Gebäude mit einer strukturierten Verkabelung versehen. In allen Bereichen wurden entweder Kupfer (Kat7-Kabel) oder Glas (Multimode) verwendet. Glasfaserkabel wurden verlegt, wo die Kabelwege für den Einsatz von Kupferkabeln zu lang sind, wobei pro Gebäude nur ein Medium im Tertiärbereich zum Einsatz kommt. Hier ist in den nächsten Jahren kein größerer Verkabelungsbedarf innerhalb von Gebäuden sichtbar. Viele Gebäude in Weihenstephan waren nur per Multimode-LWL angebunden. Damit war eine Anbindung mittels 10 Gbit/s nur über sehr kurze Strecken (maximal 300 m) möglich. Eine Optimierung der

Backboneverkabelung durch den Einzug von Singlemodefasern wurde inzwischen abgeschlossen. Zusätzlich wurden im Rahmen dieser Maßnahme erste redundante Kabelwege ertüchtigt und damit das vorliegende Redundanzkonzept der Backboneverkabelung auf dem Campus Weihenstephan z.T. umgesetzt. Aktuell erfolgt der Ausbau des redundanten Netzknotens im Bibliotheksgebäude 4220. Dieser Ausbau umfasst die Aufstellung eines Backbone-Routers, eine an den Standort dimensionierte unterbrechungsfreie Stromversorgung (USV) sowie die Verstärkung der Gebäudestromversorgung.

4.2.2 Netzstrukturierung und Komponenten

May

Netzstrukturierung Mit dem Umzug nach Garching wurde der Kern des Backbones leitungs- und komponentenmäßig redundant ausgelegt. Im Backbonebereich sind nun alle Verbindungen mit 10, 40 oder 100 Gbit/s, realisiert. Im Anschlussbereich sind deutlich mehr 10 Gbit/s als 1 Gbit/s Anschlüsse vorhanden.

An Funktionalität der Komponenten sind die Unterstützung von VLANs, von Class-of-Service (CoS) und eine Zugangskontrolle gefordert. Mittelfristig wird von einer komponenten- oder gebäudelokalen zu einer netzweiten, leicht managebaren VLAN-Strukturierung übergegangen. Eine durchgehende CoS-Unterstützung aller Komponenten kann für die Übertragung zeitkritischer Daten wie Video und Ton wichtig werden. Zugangskontrollen am Netzrand (IEEE 802.1x) werden zu einem wichtigen Sicherheits- und Kontrollinstrument. Der Stabilität und Ausfallsicherheit im Netz muss durch den Einsatz von USVs, redundanten Komponententeilen und (eventuell) doppelter Leitungsführung Rechnung getragen werden. In diesem Zusammenhang spielen auch Virtualisierungstechnologien, wie z.B. vPC (Virtual Port Channel) bei Cisco- und IRF (Intelligent Resilient Framework) bei HP-Switches, eine immer größere Rolle. Dies beschränkt sich nicht nur auf den Backbone-Bereich sondern wird mittlerweile auch im Distribution- und Edge-Bereich verwendet.

Flächendeckender Ausbau Bei der Erstplanung wurden aus Kostengründen nur wirklich aktiv benötigte Leitungen beschaltet; auf eine Vollversorgung aller vorhandenen Dosen mit aktiven Komponenten wurde verzichtet. Zurzeit sind knapp 80 % der vorhandenen Anschlüsse aktiv geschaltet. Bei einem Umzug oder Neuanschluss muss daher die Verbindung im Patchfeld (entfernt und) neu geschaltet werden. Eine Untersuchung, ob dieses personalaufwändige Änderungsmanagement durch eine (fast) volle Beschaltung aller Anschlüsse erheblich reduziert werden kann, stellte hierfür einen nicht vertretbaren finanziellen Mehraufwand fest. Aktuell wird bei einem Neubezug von Gebäuden (Neubau oder Sanierung) für zukünftige Erweiterungen in den Verteilerräumen ein Überhang von zusätzlich ca. 10% an aktiven Ports vorgehalten.

Flächendeckende Versorgung auf Switching-Basis Die Switch-Infrastruktur realisiert Geschwindigkeiten von 1, 10 und bis zu 40 Gbit/s in Richtung Backbone-Netz, in Richtung Nutzeranschluss 100/1000 Mbit/s autosensing Switched Ethernet Ports, in zahlreichen Fällen aber auch 10 Gigabit-Ethernet (Archivierungssystem, Compute-Cluster, Video-Server). Insbesondere für den Backbone-Bereich wird eine schrittweise Ausrüstung auf 40 bzw. 100 Gbit/s Komponenten konzipiert.

4.2.3 Zugänge zum MWN von außerhalb

Die Zugänge vom häuslichen Arbeitsplatz sowohl für Studenten als auch für Hochschulmitarbeiter z. B. im Rahmen von Telearbeit werden durch die DSL-Angebote der verschiedenen Provider unterstützt. Der Zugang zum MWN erfolgt über VPN-Dienste. Durch geeignete VPN-Server auf IPsec- und TLS-Basis können die häuslichen Arbeitsplätze an das MWN angebunden werden und alle Dienste des lokalen Netzes unter Berücksichtigung der geltenden Zugangsregelungen nutzen. Dazu wird nach dem Aufbau eines gesicherten Tunnels und der Authentifizierung eine MWN-weit gültige IP-Adresse vergeben. Für die von den Universitäten im Rahmen von BayKOM 2010 (Rahmenvertrag des Freistaates Bayern für Mobilfunk und Telefoniedienste) eingesetzten mobilen Geräte (Smartphones, PDAs), welche über Mobilfunk (UMTS, GSM, etc.) ins Netz gehen, wurde ein geregelter Zugang (Corporate Data Access, CDA) zum MWN geschaffen. Basierend auf der eindeutigen Rufnummer des Endgerätes wird eine MWN-weit gültige IP-Adresse zugewiesen, mit der die Nutzung aller MWN-relevanten Dienste möglich ist. Damit sind die Installation eines eigenen VPN-Clients sowie die Validierung nicht notwendig. Dieses Konzept wird auch im Rahmen der Nachfolgeausschreibung BayKOM 2017 weiter verfolgt.

4.2.4 WLAN; Zugang zum MWN für mobile Endgeräte

Der Zugang für mobile Endgeräte wird kontinuierlich weiter ausgebaut. Es werden sowohl drahtlose Verbindungen über IEEE 802.11g, 802.11n und 802.11ac als auch Kabelgebundene Anschlüsse mit 100 Mbit/s oder 1 Gbit/s Ethernet-Datendosen (RJ45) angeboten. Aktuell werden nur Accesspoints (APs) verbaut, die den Standard 802.11ac unterstützen.

Bei der Größe des zu versorgenden Bereiches ist an eine flächendeckende Versorgung aller Bereiche (auch Büros) mit WLAN weiterhin nicht zu denken. Es können daher nur öffentlich zugängliche Orte (z.B. Hörsaal, Seminarraum, Bibliothek, Mensa, Cafeteria, Foyer) mit Accesspoints versehen werden. Eine Vollversorgung all dieser Orte wird angestrebt, dies erfordert allerdings deutlich mehr als 8.000 Access-Points (z. Zt. 4.000). Bei Neuinstallationen wird eng mit den Hochschulen zusammengearbeitet, die federführend bei der Benennung der Örtlichkeiten sind.

Pro Jahr sollen mindestens 300 weitere Accesspoints im MWN installiert werden. Außerdem müssen noch viele veraltete Geräte (802.11g) durch Neuere ersetzt werden. Insbesondere in den letzten fünf Jahren macht sich eine massive Zunahme der Geräte- und Nutzerzahlen im WLAN bemerkbar. Im letzten Wintersemester erreichte die Anzahl der gleichzeitigen Nutzer im WLAN fast die Grenze von 44.000 (vgl. Abbildung 13). Es wird erwartet, dass dieses Wachstum noch einige Zeit anhalten wird.

Um die Nutzung der Funknetze für reisende Wissenschaftler auch in fremden Universitäten zu ermöglichen, wurde das weltweit nutzbare eduroam eingeführt. Die MWN-RADIUS-Serverstruktur wurde hierfür in den zentralen DFN-RADIUS/eduroam-Verbund integriert. Für die Validierung auswärtiger Gäste im MWN-WLAN steht ebenfalls der Zugang über eduroam zur Verfügung.

Der Zugang zum MWN erfolgt ebenfalls über den erwähnten VPN-Server auf IPsec- oder TLS-Basis. Für Veranstaltungen (Kongresse, Tagungen usw.) mit fremden Teilnehmern wurde die zusätzliche SSID *mwn-events* eingeführt. Benutzer müssen sich dabei analog zum eduroam-Zugang mit Benutzernamen und Passwort authentifizieren; die entsprechenden Informationen erhalten die lokalen Veranstalter nach einer Anmeldung über ein spezielles LRZ-Webportal.

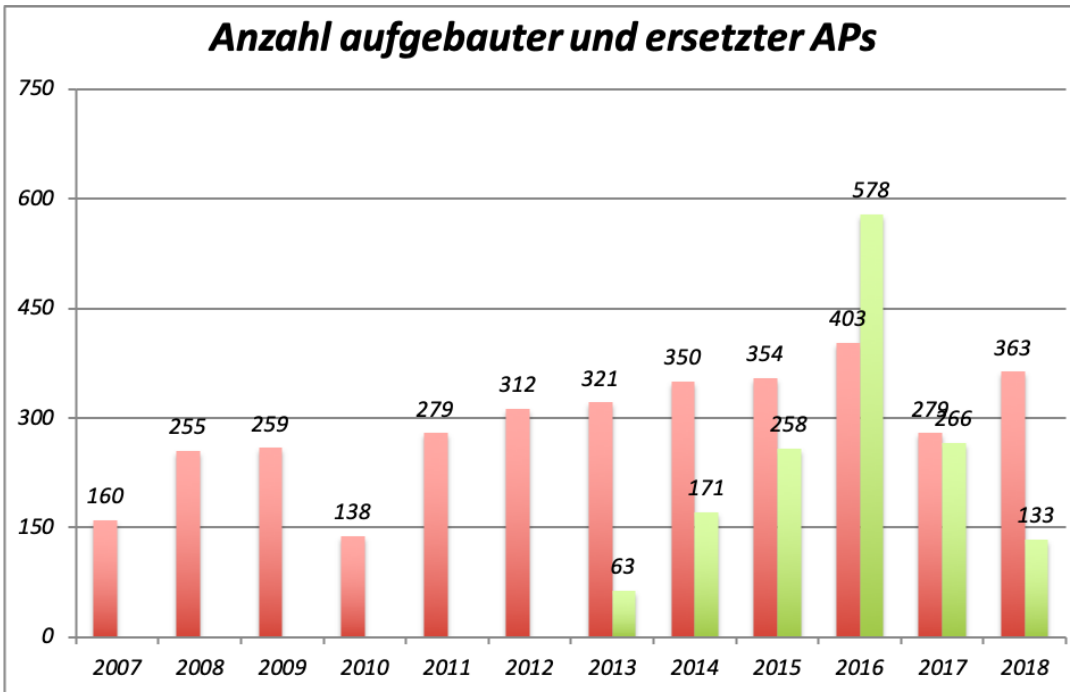
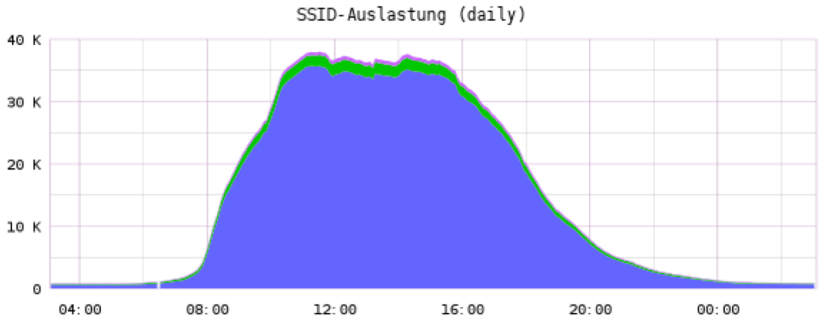


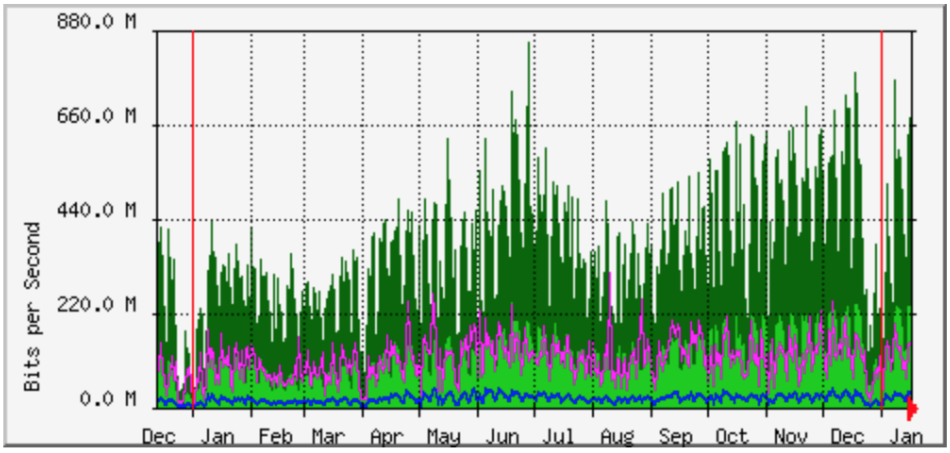
Abbildung 12: Anzahl der neu aufgebauten und der ersetzten Accesspoints



Auslastung (MWN) nach SSIDs in den letzten 3 Tagen	(max - aktuell - min - avg)
Gesamt:	(43823 - 1004 - 613 - 16712.81)
eduroam:	(37429 - 652 - 422 - 14110.61)
lrz:	(2156 - 122 - 88 - 829.77)
mwn-events:	(004 - 0 - 0 - 0.27)
@BayernWLAN:	(3554 - 142 - 36 - 1482.36)
Sonstige:	(680 - 88 - 67 - 289.80)

Abbildung 13: Anzahl der gleichzeitigen WLAN-Nutzer im Tagesverlauf (22.11.2018)

Jahresübersicht (Skalierung 1 Tag Mittel\)



	Maximal	Mittel	Aktuell
Herein	849.3 Mb/s (84.9%)	118.2 Mb/s (11.8%)	235.3 Mb/s (23.5%)
Hinaus	308.5 Mb/s (30.8%)	18.6 Mb/s (1.9%)	33.9 Mb/s (3.4%)

Abbildung 14: Jahresübersicht des BayernWLAN Verkehrs 2018

BayernWLAN Der Freistaat Bayern hat 2016 ein offenes WLAN (@BayernWLAN) ausgeschrieben. Die Ausschreibung ermöglicht es nachgeordneten Behörden sowie Kommunen und Landkreisen Hotspots zu beziehen, um Behördenstandorte, touristisch interessante Lokationen u.ä. mit freiem WLAN zu versorgen. Im Rahmen einer Kooperation mit den Universitäten konnte erreicht werden, dass auf allen @BayernWLAN Hotspots auch die SSID eduroam mit ausgestrahlt wird. Gleichzeitig können die Universitäten auf ihren APs die SSID @BayernWLAN ausstrahlen. Ende 2018 waren 17.000 @BayernWLAN Hotspots im Freistaat aktiv (s. `https://www.wlan-bayern.de`), von denen 12.000 von Universitäten oder Hochschulen betrieben werden.

Da der @BayernWLAN-Verkehr nicht über das X-WiN abgeführt werden darf, wird eine Anbindung zu einem kommerziellen Provider über das Finanzministerium finanziert. Innerhalb des MWN wird @BayernWLAN auf mehr als 3.400 APs ausgestrahlt und am Übergang zum kommerziellen Provider wurden in der Spitze bis zu 880 Mbit/s übertragen (s. Abbildung 14).

4.3 Netztechnologien

Im Backbone sind die, von verschiedenen Providern gemieteten, Dark-Fibers das begrenzende Element bei der Realisierung höherer Bandbreiten, bzw. für die Einrichtung von kunden- oder dienstspezifischen Kanälen. Aus diesem Grund wurden zu Beginn des Jahres 2015 Dense Wavelength Devision Multiplexer (DWDMs) im Backbone integriert (s. Abschnitt 4.1.4). Damit ist es einfach möglich mehrere 1 Gbit/s, 10 Gbit/s, 40 Gbit/s sowie 100 Gbit/s Kanäle über ein Faserpaar zu schalten. Die eingesetzte DWDM-Technologie ermöglicht bis zu 40 Kanäle auf einem Faserpaar zu schalten.

Funknetze werden als ergänzende Technologie angesehen und sind vor allem zur Anbindung von mobilen Rechnern gedacht; eine Ersetzung von festen Kabelstrukturen ist damit nach wie vor nicht zu erreichen und bis auf Weiteres auch nicht vorgesehen, obwohl der

Wunsch nach flächendeckender WLAN-Versorgung insbesondere bei Neubauten zunimmt und bei einer Kostenübernahme durch die jeweilige Einrichtung bzw. das Bauamt auch realisiert wird.

5 Netzintegration

Im Folgenden wird skizziert, wie die Telefonie, die Verwaltungsnetze und die Gebäudemanagement-Netze im MWN integriert sind.

5.1 Sprachkommunikation

Eine Integration der Sprach- und Datenkommunikation findet zurzeit bei der Nutzung von Datenleitungen für die Verbindung der TK-Anlagen der TUM (für rund 15 Standorte) und der bei der LMU (Großhadern und Oberschleißheim) über IP statt. Bei der TK-Anlage der Hochschule München (flächendeckend für alle ihre Standorte) werden auf angemieteten LWL-Leitungen mittels WDM-Systemen eigene Kanäle zur Verbindung geschaltet.

Da die TK-Anlagen der TUM und LMU relativ neu sind, ist eine allgemeine Zusammenführung von Sprache und Daten in einem einheitlichen IP-Netz (vorerst) nicht geplant. Es ist allerdings vorgesehen, Neubauten mit einer einzigen Verkabelungsstruktur auszustatten und VoIP-Telefone zu betreiben. Die beiden TK-Anlagen der TUM und LMU haben inzwischen integrierte VoIP-Server, die in steigendem Umfang bereits VoIP-Telefone bedienen.

Für die Sprachkommunikation am LRZ wurde mit dem Umzug nach Garching eine VoIP-Anlage installiert. Die ursprüngliche Separierung von Daten- und VoIP-Netz wurden im Jahr 2016 aufgehoben. In den letzten Jahren wurde konsequent die Verschlüsselung der Sprachdaten und dann auch der Signalisierungsdaten eingeführt. Damit entfällt der Grund für ein eigenes physisches VoIP-Netz. Im Jahr 2017 wurden alle Anbindungen nach außen von klassischem $S2_m$ auf All-IP in Form verschlüsselter SIP-Trunks umgestellt. Abbildung 15 zeigt die Systemarchitektur der LRZ-VoIP-Anlage.

5.2 Verwaltungsnetze

Die Verwaltungsnetze der LMU und TUM bilden in ihrem Stammbereich eigene physische Netze, die über Firewalls vom eigentlichen Hochschulnetz abgetrennt sind. Außenstellen der Verwaltung (z. B. in Weihenstephan oder Garching) werden jedoch mittels VLANs an die eigentlichen Verwaltungsnetze angebunden.

5.3 Facility-Management-Netze

Das MWN wird zurzeit an einigen Standorten bereits für Facility-Management (z. B. Gebäudesteuerung, Zugangskontrolle und Arbeitszeiterfassung) benutzt. Eine Ausweitung vor allem im Bereich der Gebäudesteuerung (Klima, Heizung) ist geplant. Sie ist Bestandteil von Neubauplanungen und erfolgt darüber hinaus bei der Sanierung alter Gebäudetechnik.

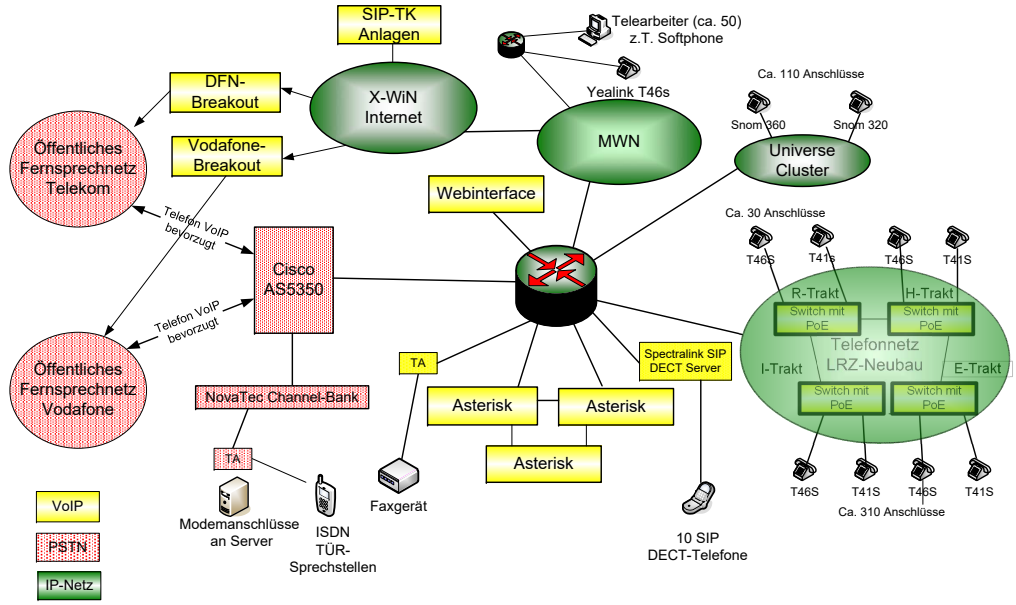


Abbildung 15: VoIP-TK-Anlage am LRZ

6 Verantwortungs- und Zuständigkeitsverteilung

Das LRZ ist als Dienstleister für die Münchner Hochschulen grundsätzlich für Planung, Betrieb und Management des Münchner Wissenschaftsnetzes (MWN) bis zur Datendose im Arbeitsraum zuständig. Dies geschieht in enger Zusammenarbeit mit über 1.300 Netzverantwortlichen in den Fachbereichen und Instituten der angeschlossenen Einrichtungen. Mit der Einführung von Netzbenutzungsrichtlinien durch das LRZ wurde die bis dahin informelle Zusammenarbeit institutionalisiert und geregelt. Insbesondere wird hierin von Instituten die Benennung von Netzverantwortlichen zwingend gefordert. (Siehe dazu: `https://www.lrz.de/wir/regelwerk/richtlinien_mwn/`)

Der Netzverantwortliche hat folgende Aufgaben in seinem Zuständigkeitsbereich wahrzunehmen:

- Verwaltung der zugeteilten Namens- und Adressräume
- Führung einer Dokumentation über die ans MWN angeschlossenen Endgeräte bzw. Netze
- Zusammenarbeit mit dem LRZ bei der Planung und Inbetriebnahme von Erweiterungen der Gebäudenetze (neue Anschlusspunkte, neue Netzstrukturen)
- Mitarbeit bei der Fehlerbehebung (z. B. Durchführen von mit dem LRZ abgestimmten Tests zur Fehlereingrenzung)
- Zusammenarbeit mit dem LRZ bei der Eindämmung missbräuchlicher Netznutzung

Um jeweils aktuelle Daten der Netzverantwortlichen in den Instituten zur Verfügung zu haben, hat sich eine jährliche Überprüfung bewährt. Die Aktualität ist zwingend erforderlich, da Informationen zu Netzwartungen, Hinweise zum Netzmissbrauch usw. per E-Mail an diese Personengruppe geschickt werden. Als Gegenpart im LRZ steht der Servicedesk zur

Verfügung, der Service Requests und Störungsmeldungen an die entsprechenden Teams im Netzbetrieb weitergibt.

Falls es gewünscht wird, können einzelne Fakultäten und Institute in Absprache mit dem LRZ mehr oder weniger weitgehende Teilaufgaben der Netzadministration auch selbständig wahrnehmen. Derzeit ist dies lediglich für die Netze der medizinischen Fakultäten (TUM und LMU), der Informatik der TUM und der Hochschule München der Fall. Hier sind eigene Betriebsgruppen vorhanden, die aber mit dem LRZ zusammenarbeiten.

Die medizinischen Fakultäten planen, bauen und betreiben ihre internen Netze (Patienten-Netz und Wissenschaftsnetz) selbständig. Die Übergänge aus den Netzen der medizinischen Fakultäten in das MWN und darüber hinaus ins Internet (X-WiN oder M-net) werden vom LRZ betrieben.

6.1 Planung

An der Planung der Netzinfrastruktur des MWN sind neben den zuständigen Bauämtern (Staatliches Bauamt München 2, Staatliches Bauamt Freising, ...) die Verwaltungsinstanzen der beteiligten Institutionen, die Fachbereiche und Institute der Hochschulen in der Form von sog. DV-Beauftragten und, federführend, das Leibniz-Rechenzentrum beteiligt. In Zusammenarbeit mit den einzelnen Instanzen der Hochschulen (Verwaltung, CIOs und DV-Beauftragte der Fakultäten, Netzverantwortliche usw.) sowie der späteren Nutzer ermittelt das LRZ den Bedarf und entwickelt eine Planung für die mittelfristige Entwicklung in qualitativer und quantitativer Hinsicht unter besonderer Berücksichtigung der Nutzung innovativer Netztechniken.

Diese Planung ist Grundlage für die Umsetzung in konkrete Anträge, Bau- und Beschaffungsmaßnahmen, für die insbesondere auch die Verwaltungen und Bauämter im Rahmen ihrer Zuständigkeiten Verantwortung tragen. Durch geeignete Abstimmungsprozesse wird sichergestellt, dass die Intentionen der Planung tatsächlich umgesetzt werden.

6.2 Betrieb

Die grundsätzliche Zuständigkeit für den Betrieb des MWN liegt beim LRZ. Soweit im Einzelfall andere Regelungen vereinbart sind, wird im Folgenden darauf eingegangen.

6.2.1 Verkabelungsinfrastruktur

Zur Verkabelungsinfrastruktur gehören Kabelwege, Verteilerräume, Primär-, Sekundär-, Tertiärverkabelung und Funkstrecken. Die technischen Betriebsinstanzen der am MWN angeschlossenen Institutionen sind zuständig für die Bereitstellung und den Betrieb von Kabelwegen und Verteilerräumen. Alle Messungen, sofern diese nicht Bestandteil der Ersterstellung sind, die Beschaltung der Verteilerschränke samt zugehöriger Dokumentation und die Beseitigung von Störungen obliegen dem LRZ.

6.2.2 Netzkomponenten

Zu den Netzkomponenten gehören Switches, Router, Access Points, WDMs, Medienkonverter usw. Die Konfiguration, die Überwachung und die Beseitigung von Störungen sind grundsätzlich Aufgabe des LRZ. Die Netzkomponenten sind in den Verteilerräumen untergebracht. Sofern sie zum Betrieb lokaler, fachbereichseigener Infrastrukturen dienen (CIP und WAP-Cluster), können sie auch in den Räumen der Fachbereiche aufgestellt und von diesen betreut werden. In der Informatik der TUM, zu deren Forschungsaufgaben auch der Betrieb von Netzen zählt, werden Subnetze selbständig betrieben, die sich über mehrere Etagen und sogar über ganze Gebäude erstrecken. Darüber hinaus ist der Betrieb der Intranets der medizinischen Fakultäten (Patienten- und Wissenschaftsnetz) und der Hochschule München komplett in der Hand eigenständiger Betriebsabteilungen.

6.2.3 Netzdienste

Das LRZ betreibt das MWN und zentrale Services für die am MWN angeschlossenen Institutionen. Zur Sicherstellung eines reibungslosen Betriebs geht dies nicht ohne gewisse administrative Vorgaben und Einschränkungen. Diese sind unter `www.lrz.de/services/netz/einschraenkung/` festgehalten und werden bei Bedarf fortgeschrieben. Viele der in der Folge aufgelisteten zentralen Netzdienste werden sowohl vom LRZ als auch dezentral in den Instituten und Fachbereichen erbracht. Ähnlich wie auch bei anderen zentralen Netzdiensten (z. B. Mail-, DHCP-, WWW-Server) ist hier derzeit eine Rezentralisierung festzustellen, die sowohl im Sinne des LRZ als auch im Sinne der einzelnen an das MWN angeschlossenen Hochschulen liegt.

6.2.4 Verfügbarkeit der angebotenen zentralen Netzdienste

Die tägliche Arbeit der Mitarbeiter in den Hochschulen hängt mittlerweile essentiell von der Verfügbarkeit zentraler Netzdienste ab. Um Ausfälle zu vermeiden, wurden in den letzten Jahren immer mehr Dienste redundant und ausfallsicher hinter Server-Load-Balancern (SLB) implementiert. Mit dieser Technik lassen sich Dienste auf mehreren unabhängigen Maschinen aufsetzen, zum Nutzer werden sie jedoch quasi transparent unter einer IP-Adresse oder einem DNS-Namen angeboten. Die Last verteilt sich gleichmäßig auf alle Systeme. Im Falle eines Ausfalls eines Teils der Server-Hardware, bei Software-Updates usw. übernehmen die verbleibenden Maschinen die Last bzw. Anfragen; die Verfügbarkeit des Dienstes ist damit gesichert. Folgende Dienste werden redundant und für den Benutzer transparent über SLB angeboten:

- PAC-Server (automatische Proxy-Konfiguration)
- Zugriff auf die elektronischen Zeitschriften der TUM und LMU
- RADIUS-Server
- Öffentliche und interne WWW-Server des LRZ
- Virtuelle WWW-Server und E-Learning-Systeme von Hochschulinstituten
- SSH-Server
- LDAP-Server (Benutzerverwaltung)
- LRZ Sync & Share

- Weitere Dienste für unsere Kunden, wie z.B. Hochschulstart, Bayerische Staatsbibliothek, zentraler OPAC, Suchmaschinen, Digitalisate, Kulturportal des Freistaates Bayern (`www.bavarikon.de`), etc.

Eine andere Möglichkeit, Dienste hochverfügbar zu halten, ist die Installation einer HA-(High Availability)-Lösung. Dabei werden gleich konfigurierte Server miteinander gekoppelt. Mit Hilfe der HA-Software wird der Ausfall einer Anwendung automatisch festgestellt und ihre Übernahme auf einen anderen Server eingeleitet – mit dem Ziel, dass der Benutzer nicht oder nur geringfügig in seinen Arbeiten gestört wird. Folgende Server sind über eine HA-Lösung hochverfügbar:

- DHCP-Server
- Mailserver
- Sicherheits-/NAT-Gateway Secomat

Die Redundanz bei den DNS-Servern ist über IP-Anycast realisiert. Dabei sind jeweils zwei reale Server unter der gleichen IP-Adresse erreichbar.

Zudem werden alle Zugangswege zu den Systemen im Rechnergebäude des LRZ doppelt (Leitungen, Switches, Router) gehalten (vgl. Abbildung 5). Insbesondere sind die wichtigen Server und Höchstleistungsrechner im LRZ-Gebäude über zwei getrennte Router angebunden, welche wiederum an zwei unabhängige Backbone-Router am Campus Garching angebunden sind. Diese beiden Backbone-Router sind mit jeweils einem 2 * 100 Gbit/s Trunk direkt an den Kernnetzknoten des X-WiN in Erlangen und Frankfurt angeschlossen.

Um auch gegenüber Bränden abgesichert zu sein, wurden alle zentralen Netzkomponenten im LRZ im Jahr 2012 auf zwei unterschiedliche Brandabschnitte in zwei unterschiedlichen Stockwerken verteilt (Raum DAR1 im Erweiterungs- und Raum NSR0 im Bestandsbau des LRZ-Rechnergebäudes).

6.2.5 Verwaltung von IP-Adressen

Die Verwaltung einzelner (Teil-)Bereiche ist an die Netzverantwortlichen in den Instituten im Rahmen der von ihnen zu leistenden Tätigkeiten unter Koordination des LRZ delegiert. Neben offiziellen, weltweit gültigen IP-Adressen koordiniert das LRZ im MWN auch die Nutzung von privaten IP-Adressen gemäß RFC 1918. Zum Schutz vor Angriffen, zur Abschottung institutslokaler Infrastrukturen usw. werden bevorzugt private IP-Adressen im MWN vergeben, die auch im MWN geroutet werden und somit die Nutzung zentraler Dienste (Mail, Zugang zu Online-Medien usw.) ermöglichen, die vom LRZ oder anderen Einrichtungen (z.B. Bibliotheken) im MWN angeboten und betrieben werden. Das LRZ empfiehlt, nur für Server, die auch über das Internet erreichbar sein müssen, öffentliche IP-Adressen zu verwenden. Für IPv6, das private IP-Adressen nicht mehr in derselben Form wie IPv4 vorsieht, werden zur Einrichtung privater Subnetze äquivalente Sicherheitsmaßnahmen ergriffen. Für die Adressumsetzung (NAT) bietet das LRZ das System `Secomat` an, das neben der IPv4-Adressumsetzung zugleich auch als IPS (Intrusion Prevention System) eingesetzt wird und damit auffällige Rechner aufgrund ihres Verkehrsverhaltens, wie es z. B. für Botnetze bzw. Malware-Infektionen typisch ist, erkennt.

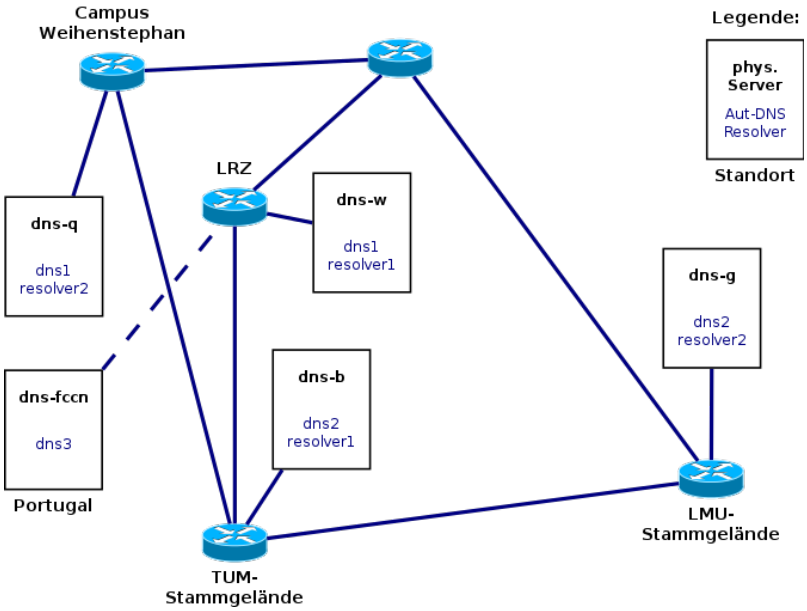


Abbildung 16: Standortübergreifende Verteilung der DNS-Server

6.2.6 Betrieb des Domain-Name-Systems (DNS und DNSSEC)

Mit der Verwaltung von IP-Adressen müssen aber nicht unbedingt auch die primären DNS-Dienste für die Teiladressbereiche von den Fachbereichen selbst erbracht werden. Das LRZ bietet als allgemeinen Dienst den Betrieb zentraler DNS-Server an. Er kann aber auch von den Instituten selbst erbracht werden, siehe `www.lrz.de/services/netzdienste/dns/`. Zudem wird eine web-basierte, mandantenfähige Schnittstelle am zentralen DNS des LRZ (webdns) angeboten, mit welcher der Netzverantwortliche des Instituts seine Bereiche selbst konfigurieren kann. Derzeit werden 2.995 Zonen verwaltet.

Die DNS-Server stehen wie in Abbildung 16 dargestellt verteilt im LRZ, im Stammgelände der LMU, im Stammgelände der TUM und in Weihenstephan. Die Dienste sind getrennt in den autoritativen Nameservice und den rekursiven Resolverdienst redundant konfiguriert. Durch die Konfiguration über Anycast sind die Dienste auf den verschiedenen Systemen unter jeweils der gleichen IP-Adresse erreichbar.

Über einen Domain-Reseller bietet das LRZ seinen Kunden die Möglichkeit, Second-Level-Domains zu registrieren (siehe Abschnitt 7.1). Die dabei anfallenden Kosten werden den Kunden in Rechnung gestellt.

DNSSEC Der Ausbau des optionalen Sicherheitsmechanismus DNSSEC (Domain Name System Security Extensions), welcher die Korrektheit von im DNS hinterlegten Informationen validierbar macht, wurde deutlich forciert. Alle unsere Resolver validieren nun DNSSEC Signaturen.

Seit 2014 ist der DNSSEC-Signing-Proxy des LRZ störungsfrei in Betrieb, auch nach der Aktivierung von DNSSEC für die prominenten Domains lmu.de, lrz.de und tum.de gab es keine Probleme. Die Domain für den Netzbetrieb, netz.lrz.de, wurde ebenfalls sicher delegiert, was unter Anderem für das Hinterlegen der SSH-Fingerprints von Netzkomponenten genutzt wird. Seit 2016 ist DNSSEC Standard für neue Domains, wenn die darüberliegende

Domain gesichert ist, also insbesondere bei allen Second-Level-Domains. Aktuell sind 229 Zonen (2016 waren 85) signiert und sicher delegiert.

Im Rahmen des BHN (Zusammenschluß von 30 Universitäten und Hochschulen) unterstützt das Bayerische Wissenschaftsministerium den Beschluß der bayerischen Universitäten und Hochschulen ihre Nameserver mit DNSSEC abzusichern. Auf der durch DNSSEC garantierten Authentizität der DNS-Antworten sollen auch die Mailserverkommunikation zwischen den beteiligten Universitäten durch DANE authentizitierte TLS-Zertifikate verschlüsselt werden.

Das LRZ unterstützt die lokalen Netzadministratoren an den bayerischen Universitäten und Hochschulen bei der Einführung von DNSSEC und DANE und stellt seine Expertise, eine Informationsaustauschplattform, Kurse mit praktischen Übungen und Förderung des Austausches der Systemadministratoren untereinander, sowie ganz praktische Unterstützung, zur Verfügung.

Ab 2019 wird das LRZ für kleinere Hochschulen, die personell nicht in der Lage sind DNSSEC zu betreiben, den Dienst DNSSEC as a Service (DNSSECaaS) anbieten. Der LRZ Signing Proxy wird damit nicht nur Zonen aus dem MWN sondern auch für externe Domains signieren.

6.2.7 DHCP

Das LRZ betreibt einen zentralen DHCP-Dienst für das gesamte MWN. Dieser Service kann auch von den Fachbereichen selbst erbracht werden. Aufgrund häufiger Betriebsprobleme mit falsch konfigurierten institutslokalen DHCP-Servern bietet das LRZ jedoch diesen Service verstärkt auch den einzelnen Instituten an. Er wird von 301 Instituten in rund 1.150 Subnetzen mit über 452.000 Adressen, genutzt. Der Zugang mobiler Endgeräte zum MWN (WLAN und VPN) setzt ebenfalls auf diesem Dienst auf. Der DHCP-Dienst ist IPv6-fähig (stateless) und mittels eines Failover-Protokolls (HA-Lösung) redundant ausgelegt, so dass selbst im Fehler- bzw. Wartungsfall für die Nutzer kein Ausfall eintritt.

6.2.8 Firewall

Eine einzige zentrale äußere Firewall (zum Wissenschaftsnetz) würde nur einen kleinen Teil der Sicherheitsprobleme der am MWN angeschlossenen Institutionen und Institute lösen. Die Heterogenität der Nutzerschaft und ihre sehr unterschiedlichen Kommunikationsinteressen machen es zudem ausgesprochen schwierig, eine Firewall so zu konfigurieren, dass sie einerseits ihre Schutzfunktion möglichst wirksam ausübt, andererseits aber nicht zu viele sinnvolle Kommunikationsformen verhindert oder erschwert. Es ist deshalb sinnvoll, den Zugriffsschutz möglichst nahe an kleineren Bereichen mit homogeneren Kommunikationsinteressen einzurichten.

Seit Frühjahr 2007 wird den Instituten die Möglichkeit geboten, über mandantenfähige virtuelle Firewalls selbst den Schutz zu realisieren. Somit besteht für die Institute die Möglichkeit, eigene Firewalls auf LRZ-Hardware zu betreiben und über das in Abbildung 17 dargestellte Managementfrontend zu verwalten.

Der Firewall-Dienst betreibt zur Zeit 174 virtuelle Firewalls für Institutionen; darüber hinaus werden weitere 40 Firewalls für LRZ-Dienste betrieben. Als Firewall-Plattform wird pfsense genutzt. Jeder Kunde erhält zwei virtualisierte Instanzen von pfsense, die ein hochverfügbares Pärchen pro Kunde bilden. Die Firewalls laufen als virtuelle Maschinen unter

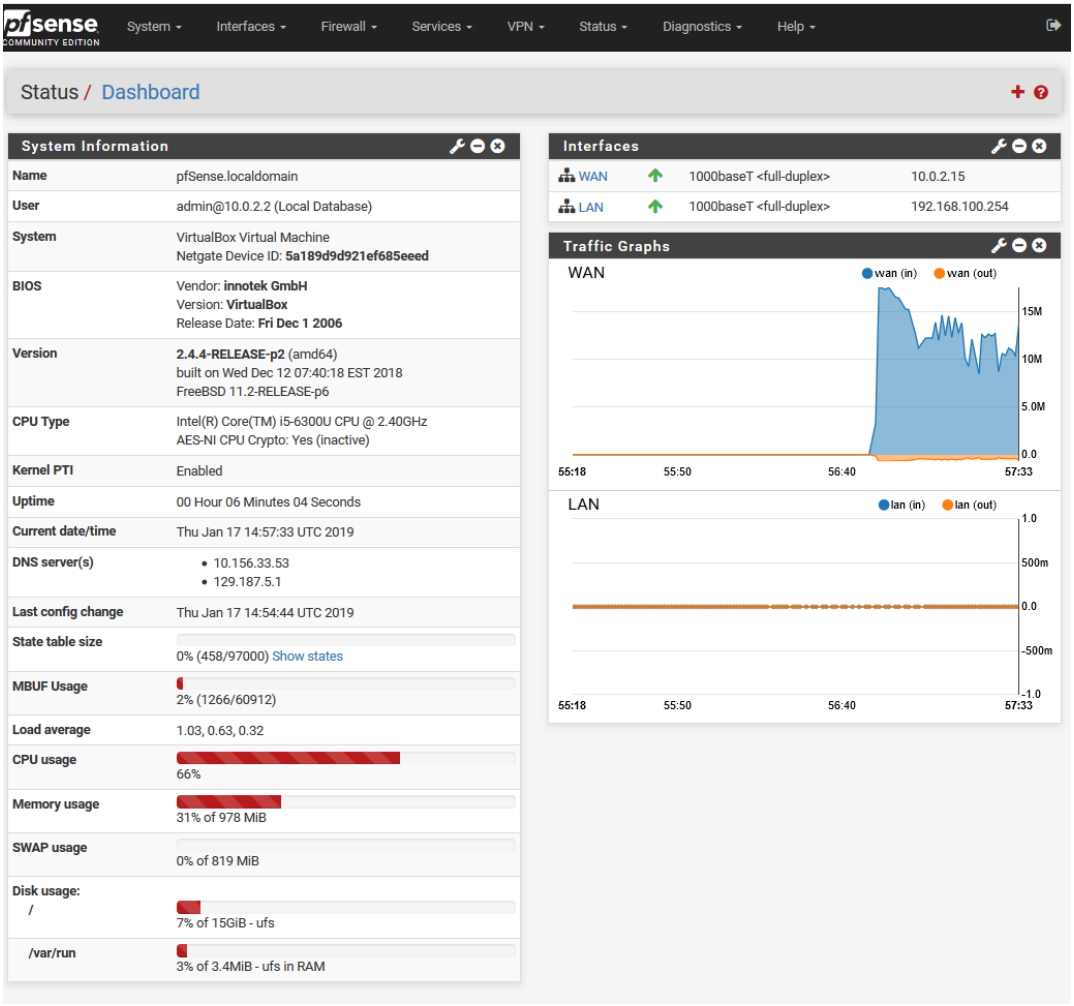


Abbildung 17: Managementoberfläche für die mandantenfähigen, virtuellen Firewalls

einer Virtualisierungslösung auf entsprechender Serverhardware (HP DL380 gen9 / DELL R740)) die in den Kernnetzknoten (Großhadern, LMU, TUM, Garching, Weihenstephan) nahe beim Kunden betrieben werden. An besonders stark belasteten Standorten (TUM, Garching) wurden zusätzliche Serverpaare (Dell R740) installiert. Die Plattform bietet neben HA-Features und VPN, auch die Möglichkeit zur Erweiterung mittels Zusatzpaketen.

6.2.9 Internet-Anschluss

Das MWN ist seit Anfang 2003 redundant an das Internet angebunden. Derzeit stehen zwei 200 Gbit/s-Ethernet-Anschlüsse (gedrosselt auf 115 Gbit/s) zum X-WiN (Uplinks nach Garching und Erlangen) und eine 10 Gbit/s Backup-Leitung über M-net zur Verfügung (vgl. Abbildung 10).

Um beim Ausfall des primären Internet-Zugangs den Verkehr automatisch umlenken zu können, betreibt das LRZ ein eigenes Autonomes System (AS 12816). Der Betrieb des X-WiN-Anschlusses liegt in der vollen Verantwortung des LRZ. An den Routerinterfaces, die den Übergang ins Internet darstellen (X-WiN und M-net), sind einige Filter installiert, die z. B. das IP-Address-Spoofing unterbinden, die Anzahl der von außen erreichbaren Mail-

und DNS-Server beschränken und einige Anwendungen mit bestimmten Ports aufgrund damit verbundener häufiger Sicherheitslücken verbieten.

6.2.10 InHPC-DE

Die drei nationalen Höchstleistungsrechner sind im Rahmen des Gauss Center for Supercomputing (GCS) eng gekoppelt und bieten den Forschern, aus allen wissenschaftlichen Bereichen, die mit Abstand leistungsfähigste Systeminfrastruktur in ganz Europa. GCS setzt sich zusammen aus dem High Performance Computing Center Stuttgart (HLRS), dem Jülich Supercomputing Centre (JSC) sowie dem Leibniz Rechenzentrum in Garching bei München (LRZ). Neben dem Infrastrukturprojekt zur Finanzierung der Supercomputer wird von Oktober 2017 bis Dezember 2021 das Projekt „Integration der nationalen Höchstleistungsrechenzentren Deutschland (InHPC-DE)“ gefördert.

Mit InHPC-DE wird die Integration der drei Standorte deutlich verstärkt und verbessert, um die Grundlage für ein ganzheitliches und gleichzeitig verteiltes Versorgungskonzept auf der Ebene Tier-0/1 zu bilden. Ein nationales, virtuelles Zentrum für Höchstleistungsrechnen, das technisch und organisatorisch eine einheitliche und nahtlose Nutzung der HPC-Services ermöglicht, ist das Ziel.

Im Rahmen des Projektes werden die dafür notwendigen Prozesse und Tools entwickelt. InHPC-DE gliedert sich in vier Arbeitspakete (AP). AP1 *Netzinfrastruktur* hat die Vernetzung der drei Zentren mit 100 Gbit/s zum Ziel und schafft damit die technischen Basis für die weiteren Forschungsaktivitäten. AP2 *Datenmanagement* entwickelt Lösungen für die stärkere Integration auf der Datenebene, untersucht Hochleistungsdatentransportmechanismen sowie die enge Koppelung der Storage-Systeme an den drei Zentren. AP3 *Workflows* unterstüzt die Wissenschaftler mit dem Ziel ihre Arbeitsabläufe und Berechnungen einfach zwischen den drei Systemen und Zentren zu migrieren. AP4 *Datenaufbereitung und Visualisierung* stärkt die Integration der Visualisierungsinfrastruktur zwischen den Zentren und ermöglicht komplexe Ergebnisdaten räumlich verteilt und kollaborativ zu visualisieren und an verschiedenen Standorten gemeinsam an der Visualisierung zu arbeiten und über beliebiege Distanzen die Ergebnisse der Forschung auszutauschen und gemeinsam zu bearbeiten.

Im Gegensatz zum DEISA Projekt, bei dem ein dediziertes Netz „nur“ für DEISA aufgebaut wurde, hat sich das Projekt dazu entschlossen, die Bandbreite über den „normalen“ X-WiN Anschluss der einzelnen Einrichtungen zu realisieren. Dies hat den Vorteil, dass die Bandbreite auch anderen Nutzern zur Verfügung steht, falls sie vom Projekt nicht gebraucht wird. Auch Nutzer aus anderen Universitäten und Zentren haben den Vorteil, dass sie ihre HPC-Daten schneller in eines der drei Zentren übertragen können, auch wenn sie nicht direkt an einem der Zentren angeschlossen sind.

6.2.11 Multicastdienst

Für eine effiziente Übertragung von Datenströmen, insbesondere Video- und Audiodaten, an mehrere Teilnehmer steht flächendeckend an den kabelgebundenen Standorten im MWN der vom LRZ betriebene Multicast-Dienst zur Verfügung; für WLAN-Verbindungen ist der Multicast-Dienst prinzipbedingt schlecht geeignet und wird nicht angeboten. Er basiert auf den Standardprotokollen IGMPv2 für IPv4 sowie MLDv2 für IPv6 und wird auf Anforderung durch den Netzverantwortlichen freigeschaltet.

Durch die Multicast-fähige Verbindung mit dem X-WiN ist auch ein Multicast-basierter Datenaustausch mit auswärtigen Institutionen möglich.

6.2.12 RADIUS-Server

Um eine einheitliche Authentifizierung der Nutzer beim Zugang zum MWN von öffentlichen Arbeitsplätzen und WLAN-Zugängen sicherzustellen, betreibt das LRZ einen zentralen RADIUS-Server. Bei Bedarf kann die Benutzerverwaltung auch in die einzelnen Institute delegiert werden. Derzeit ist die Verwaltung von ca. 50 der eingerichteten Radius-Zonen an Institute delegiert.

6.2.13 VPN-Server

Durch VPN-Server werden sichere Verbindungen über ein öffentliches, unsicheres Medium ermöglicht. Zu den unsicheren Medien gehören:

- Drahtlose Netzwerke (WLAN)
- Anschlussdosen für mobile Rechner in öffentlich zugänglichen Bereichen des MWN
- Zugang zu Diensten des MWN über das Internet (z.B. Telearbeitsplatz, reisende Wissenschaftler)

Das LRZ betreibt zur Absicherung fünf zentrale VPN-Server, die zu einem Cluster zusammengefasst sind. Als Schnittstelle zwischen VPN-Server und Benutzerverwaltung werden die RADIUS-Server des MWN verwendet. Damit kann auf die AAA-Möglichkeiten (Authentication, Authorization & Accounting) des RADIUS-Dienstes zurückgegriffen werden.

6.2.14 Mail-Server und Mailrelays

Das LRZ betreibt für die Institute des MWN zentrale Mailserver und Mailrelays. Einzelnen Instituten ist jedoch freigestellt, eigene Mailserver zu betreiben. Der Betrieb institutseigener Mailserver bedingt aber Betreuungsaufwand und Fachwissen, welche nicht jedes Institut aufbringen können. Aufgrund mangelnden Systemmanagements (Konfiguration, Einspielen von Sicherheitspatches usw.) wurde in der Vergangenheit eine Vielzahl von Institutsservern von externen Angreifern zu Spam-Zwecken missbraucht. Deshalb wird nur gut gepflegten, großen und spam-festen Mail-Servern der direkte Empfang von E-Mails erlaubt, die übrigen müssen ihre E-Mails über ausgezeichnete Mailserver (Mailrelays) des LRZ empfangen.

6.2.15 VideoConference (VC)-Dienst und Gatekeeper für das MWN

Das MWN ist am VC-Dienst des DFN beteiligt. Dieser Dienst setzt u.a. auf dem H.323-Standard auf und kann im MWN von jedem Nutzer verwendet werden. Um (weltweit) erreichbar zu sein, müssen die Clients an einem Gatekeeper registriert sein. Der Gatekeeper ist für die Auflösung der eindeutigen H.323-Adresse in die zugehörige IP-Adresse zuständig. Das LRZ betreibt zentral für das MWN einen entsprechenden Gatekeeper, der in den nationalen und weltweiten Verbund integriert ist. Das MWN hat die Vorwahl 0049 134 (vergleichbar mit der Vorwahl beim Telefon) zugeteilt bekommen. Die Struktur der Sub-Adressen im MWN orientiert sich an den im MWN genutzten Telefonnummern der angeschlossenen Institutionen.

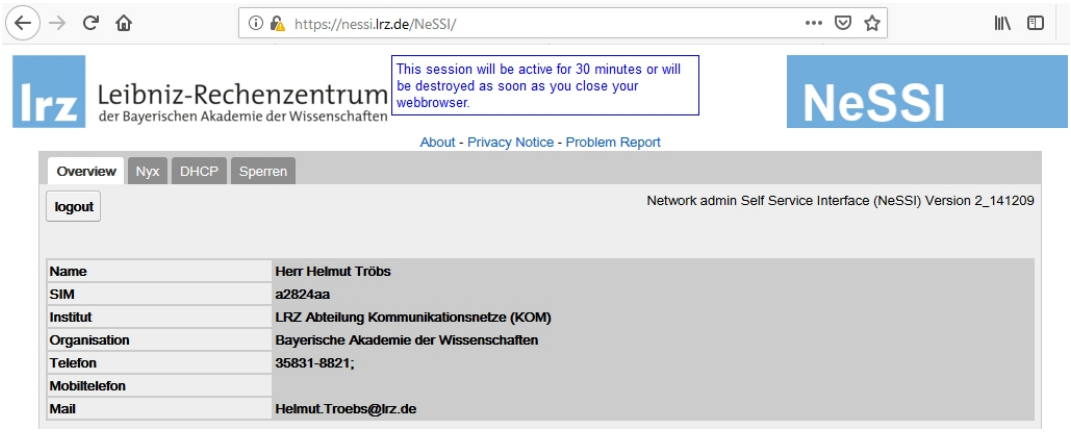


Abbildung 18: Das mandantenfähige Network Self Service Interface NeSSI

6.2.16 NTP-Dienst

Mit NTP (Network Time Protocol) können Rechner über das Internet (bzw ein TCP/IP-Netz) mit einer hochgenauen Zeit versorgt werden. Am LRZ werden drei Zeit-Server betrieben, die Servernamen lauten `ntp1.lrz.de`, `ntp2.lrz.de` und `ntp3.lrz.de`. `ntp1` und `ntp3` laufen auf Appliances der Firma Meinberg (Lantime M300/GLN), sie empfangen die Zeit direkt über GPS bzw. DCF77 (Stratum 1). `ntp2` ist durch ntp-Daemonen auf den DNS-Servermaschinen realisiert. Diese erhalten die Zeit von `ntp1` und `ntp3` sowie über die NTP-Server der PTB Braunschweig, der Freien Universität Berlin und der Friedrich-Alexander-Universität Erlangen-Nürnberg.

6.2.17 Nyx/Nessi

Nyx ist ein Sicherheits- und Netzmanagementwerkzeug, mit dem einzelne Rechner im MWN lokalisiert werden können. Nach Eingabe einer bestimmten MAC- oder IP-Adresse meldet Nyx den Switch, Port und die Dosenbezeichnung, wo der Rechner mit dieser Adresse angeschlossen ist. Zusätzlich wird in Eigenentwicklung mandatenfähige Plattformen für Netzverantwortliche bereitgestellt. Darüber können Netzverantwortliche auch selbst, wie in Abbildung 18 dargestellt, Nyx-Daten für die von ihnen verwalteten Adressbereiche abfragen.

7 Administration

Nachfolgend werden die Adress- und Namensräume, die das LRZ verwaltet, die Benutzerverwaltung und das Gerätemanagement beschrieben.

7.1 Adress- und Namensräume

Das LRZ betreibt im Zusammenhang mit der redundanten Anbindung an das Internet ein eigenes Autonomes System (AS 12816). Im Rahmen dieses Autonomen Systems werden alle in der nachfolgenden Tabelle in der ersten Spalte markierten IP-Netze geroutet. Bei den anderen IP-Netzen ist dies leider nicht möglich, da sie nicht Provider-unabhängig registriert sind. Im MWN werden derzeit folgende offizielle IP-Adressen (IPv4) benutzt:

- LRZ-IPv4-Netze (für LRZ registriert und vom LRZ verwaltet):
  - Class-B-Netze:

Netz	Zuordnung
129.187.0.0	TUM, LMU, BADW, LRZ
141.40.0.0	Campus Weihenstephan
141.84.0.0	LMU, LRZ
141.39.240.0– 141.39.255.255	Hochschule München

  - Class-C-Netze:

Netz	Zuordnung
192.68.211.0	Verschiedene Institute, z. B. Pinakotheken
192.68.212.0	Reserve
192.68.213.0	Gründerzentrum Garching
192.68.214.0	Kultusministerium
192.68.215.0	Akademie der Bildenden Künste
193.174.96.0– 193.174.99.0	Bayerische Staatsbibliothek
194.95.59.0	Bayerische Staatsbibliothek

- LRZ-IPv4-Netze, die außerhalb des MWN liegen und den X-WiN-Anschluss des LRZ nicht verwenden, aber z. B. die Mailserver verwenden dürfen:
  - (Max.) Class-C-Netze:

Netz	Zuordnung
193.175.201.0/24	Triesdorf
194.95.250.56/26	Limnologische Station Iffeldorf (TU)
195.37.11.0/26	Versuchsanstalt für Wasserbau in Obernach (TU)
195.37.68.0/24	Observatorium auf dem Wendelstein (LMU)
195.37.191.0/28	Schneefernerhaus auf der Zugspitze(LMU)

- IPv4-Institutsnetze, die über den X-WiN-Anschluss des LRZ geroutet werden:
  - Class-B-Netze:

Netz	Zuordnung
131.159.0.0	TUM Informatik
138.244.0.0	Patientenversorgungsnetz der LMU-Klinika (Großhadern und Innenstadt)
138.245.0.0	Forschungsnetz der LMU-Klinika (Großhadern und Innenstadt)
138.246.0.0- 138.246.128.255	Eduroam, Secomat, Externe Nutzer
138.246.128.0- 138.146.223.255	Forschungsnetze der LMU Klinika (Großhadern und Innenstadt)
138.246.224.0- 138.246.255.255	Eduroam, Secomat, Externe Nutzer
141.39.128.0- 141.39.191.255	Klinikum Rechts der Isar

  - Class-C-Netze:

Netz	Zuordnung
192.44.30.0/23	Fraunhofer AISEC
192.54.42.0	Beschleuniger-Labor Garching LMU
193.175.56.0– 193.175.63.0	Klinikum rechts der Isar
193.175.56-63.0	Klinikum Rechts der Isar
195.37.167.0	Zoologische Staatssammlung, München
195.37.7.0	PRACE (Europäisches HPC-Projekt)

Das LRZ hat sich im April 2005 durch seine Mitgliedschaft bei RIPE einen eigenen, global providerunabhängigen routebaren IPv6-Block, `2001:4ca0::/32`, gesichert. Adressen aus diesem Bereich wurden MWN-flächendeckend ausgerollt. Alle Router und wichtigen Netzdienste wie DNS, NTP, Web-Server, DHCP sind bereits IPv6-fähig und werden auch darüber angeboten. Eine IPv6-Anbindung nach außen ist sowohl über das X-WiN als auch über M-net gegeben.

Derzeit sind für Institutionen aus dem MWN und weitere wissenschaftliche Einrichtungen aus Bayern mehr als 900 Namensräume (Domains) vom LRZ registriert. Das LRZ bietet auch einen DNSSec Service an. Die wichtigsten Institutionen und die Anzahl der registrierten sowie gesicherten Domains sind in der folgenden Tabelle zusammengefasst.

Institution	**Anzahl registrierter Domains**	**Anzahl DNSSEC-gesicherter Domains**
Bayerische Staatsbibliothek	220	36
Bayerische Akademie der Wissenschaften	37	8
Hochschule Amberg-Weiden	8	1
Hochschule Coburg	28	27
Hochschule München	7	0
Hochschule Weihenstephan-Triesdorf	13	8
Leibniz-Rechenzentrum	65	15
Ludwig-Maximilians-Universität München	198	40
Otto-Friedrich-Universität Bamberg	10	1
Studentenwerk München	42	41
Technische Universität München	175	35
Sonstige	127	82
Summe	**930**	279

Die Strukturierung der Sub-Domains folgt den Strukturen auf der Ebene der Institute, Lehrstühle und Arbeitsgruppen. Die expliziten Regelungen sind unter `www.lrz.de/services/netzdienste/dns` dokumentiert.

Daneben existieren unter Kenntnis und Genehmigung der zuständigen Stellen weitere Second-Level-Domains, die von einzelnen Instituten, Lehrstühlen und Arbeitsgruppen nicht über das LRZ beantragt und anderweitig gepflegt werden.

Das LRZ hat einen MWN-weiten Active Directory Dienst (ADS, Windows) eingerichtet. Die Namensgebung der ADS-Domänen im MWN und der Subdomänen folgt den Konventionen des DNS-Namensraums.

7.2 Benutzerverwaltung

Für die vom LRZ angebotenen Ressourcen (Zentrale Server, WLAN, öffentliche Arbeitsplätze) ist eine einheitliche Nutzerverwaltung eingerichtet. In den einzelnen Institutionen wie z. B. der Verwaltung, der Bibliothek und in einigen Fachbereichen existieren eigene, davon unabhängige Nutzerverwaltungen. Sofern diese Nutzer auf Netz-Ressourcen des LRZ wie

z. B. WLAN-Zugang oder Zugriff auf öffentliche Netz-Anschlussdosen, kann dies über die von den Instituten selbständig verwalteten RADIUS-Zonen geschehen.

7.3 Geräte

Aufgrund der großen Anzahl angeschlossener Endgeräte, der verteilten Zuständigkeit und der Vielzahl beteiligter Institutionen besteht das LRZ derzeit nicht auf einer expliziten, vorab durchgeführten Anmeldung der ans Datennetz angeschlossenen und anzuschließenden Geräte. Dies ist und wird im Hinblick auf die zunehmende Anzahl mobiler Geräte und zukünftig evtl. auch IP-Telefone immer schwieriger realisierbar. Die entsprechende Dokumentation ist aufgrund der Delegation der IP-Adressverwaltung von den Netzverantwortlichen zu erbringen. Das LRZ hat bei Bedarf Zugriff auf diese Informationen. Lediglich die Information über netzrelevante Geräte (Router, Switches, Firewalls, Server für Netzdienste u. dgl.) — auch diejenigen in der Zuständigkeit der Institute — werden vom LRZ in einer Netzdokumentation gepflegt. Endgeräte werden hiervon explizit ausgenommen. Grund sind der hohe Verwaltungsaufwand und die große Änderungshäufigkeit.

8 Sicherheit

Nachfolgend werden die eingesetzten Schutzmechanismen gegen missbräuchliche Verwendung und Angriffe, für den sicheren Datenverkehr über unsichere Netze, zur Sicherung von Endgeräten und deren Netzzugang sowie zum sicheren Betrieb des Netzes beschrieben.

Seit Mitte 2001 hat die Aktivität der Hacker und der Autoren elektronischer Schädlinge weltweit dramatisch und kontinuierlich zugenommen. Damit steigt leider auch die Anzahl der Abuse-Fälle (d. h. der echten oder vermeintlichen Missbrauchsfälle) im MWN. Nach den Erfahrungen des LRZ hat dies folgende Gründe:

- Durch die zunehmende Kriminalisierung des Internet werden die Tools der Hacker, Schadprogramm-Bastler und Spammer inzwischen überwiegend von Profis und (teilweise hoch qualifizierten) Spezialisten entwickelt. Dementsprechend nahm die Qualität dieser Angriffswerkzeuge kontinuierlich zu.
- Die Zahl der elektronischen Schädlinge (Viren, Würmer, trojanische Pferde, Ransomware, usw.) nahm drastisch zu; oft tauchen an einem Tag mehr als 1.000 neue Schädlinge bzw. Varianten/Modifikationen schon existierender Schädlinge auf. Außerdem versuchen die Schädlinge immer intensiver, sich vor einer Entdeckung zu schützen. Als Folge nahm die Erkennungsrate installierter Viren-Scanner ab.
- Leider ist das Sicherheitsbewusstsein bzw. -verhalten zu vieler Benutzer nach wie vor unzureichend. Diesem setzt das LRZ diverse sicherheitsrelevante Dienste entgegen, wobei klar sein muss, dass die Sicherheitsprobleme nicht alleine durch technische Maßnahmen gelöst werden können.

8.1 Schutz gegen Missbrauch und Angriffe

Durch den Einsatz von leistungsfähigen Switches sind die Möglichkeiten zur unbefugten Kenntnisnahme von für andere bestimmtem Netzverkehr bis auf den für die verwendeten

Protokollwelten unvermeidlichen Broadcastverkehr eingeschränkt worden. Zudem gibt es die Möglichkeit der Bildung von VLANs. Diese werden konfiguriert, um homogene Nutzergruppen zu bilden, die dann zusätzlich durch einen Firewall geschützt werden können, oder um eigene Managementnetze für Netzkomponenten zu bilden. Es sind z. Z. rund 1.700 lokale (bis zum nächsten Router) VLANs für Nutzer, rund 350 lokale VLANs für das Management von Netzkomponenten und rund 20 MWN-weite VLANs für globale Nutzergruppen (z. B. TUM- und LMU-Verwaltung, Gebäudemanagement, Bibliothek, Bauamt) realisiert.

Aufgrund der Ergebnisse, die durch die Einführung einer Monitor-Station am X-WiN-Zugang gewonnen wurden (`www.lrz.de/services/security/sec-brief/`), setzt das LRZ in Absprache mit den Administratoren in den Instituten Werkzeuge zur Überprüfung der Konfiguration der Rechner in auffälligen Teilnetzen unter Sicherheitsgesichtspunkten ein. Diese Monitorstationen (Signatur-basiertes Intrusion Detection auf der Basis der Software Suricata und eine Anomalie-Erkennung auf Basis von Flow-Daten) werden derzeit zur Aufdeckung von Missbrauchsfällen wie z. B. Portscans, Denial-of-Service-Angriffe auf Ziele außerhalb des MWN und direkter Mailversand (Spamming) eingesetzt. Diese Aktivitäten sind i. d. R. ein Hinweis auf einen Malware-Befall bzw. auf ein anderweitig kompromittiertes System. Der eingesetzte Mechanismus ist mittlerweile so ausgereift, dass er im Falle des Auftretens etwa von SSH-Brute-Force-Angriffen und -Scans zu einer automatischen Sperre des betreffenden MWN-Rechners am X-WiN-Zugang führt.

Als zusätzliche Maßnahme zur Eingrenzung von missbräuchlicher Nutzung und Erkennung von kompromittierten Rechnern wurde das System Secomat eingeführt. Rechner mit privaten IPv4-Adressen sowie Verbindungen, die über WLAN oder VPN-Server in das MWN aufgebaut werden, müssen (zwangsweise) dieses System nutzen. Dabei werden, falls notwendig, die privaten in öffentliche IP-Adressen umgewandelt (NAT-Funktion) sowie das Kommunikationsverhalten der Rechner untersucht und bewertet. Bei Auffälligkeiten (z. B. hohe Anzahl von versendeten E-Mails, viele Portscans) wird die IP-Adresse des Rechners für eine bestimmte Zeit automatisch gesperrt.

Erkennung von Auffälligkeiten im Kommunikationsverhalten sowie die zentrale Auswertung der Sicherheitsmeldungen des Intrusion Detection Systems Suricata gehen Hand in Hand. Auf Basis eines zu diesem Zweck eingesetzten Security Information und Event Management (SIEM) Werkzeugs können insbesondere auch die Sicherheitsmeldungen von verschiedenen Sensoren zeitlich in Beziehung gesetzt, mit vorhandenen Schwachstellen auf dem jeweiligen System korreliert und entsprechende Informations- und Eskalationswege umgesetzt werden. Zusätzlich wird das LRZ vom DFN-CERT und CERT-Bund über Sicherheitsvorfälle informiert. Somit wird eine zeitnahe Reaktion sichergestellt.

Das LRZ berät die Systemverwalter der Institute in der Nutzung von Werkzeugen, die es den Endnutzern ermöglichen, die Sicherheit ihrer Rechner selbst zu überprüfen.

8.2 Proaktives Port- und Schwachstellenscanning

Sicherheit im MWN beginnt bereits damit, ein möglichst genaues Bild davon zu haben, welche Systeme vorhanden und welche Dienste dort betrieben werden. Ein einfaches aber probates Mittel dies in Erfahrung zu bringen ist das Scannen nach offenen Ports. Aus den hieraus gewonnenen Informationen lässt sich in vielen Fällen erkennen, ob der dokumentierte Soll-Zustand mit dem ermittelten Ist-Zustand übereinstimmt. Daneben lassen sich auch Lücken und Schwachstellen aufdecken. Dies schließt beispielsweise ein, dass durch eine zu weit gefasste Firewall-Regel der Zugang zu einem Institutsnetz offener ist als gewünscht.
Systeme im LRZ und aus einigen Bereichen im MWN werden täglich sowohl von einer im

LRZ als auch außerhalb des MWN platzierten Scan-Maschinen überprüft und die Scanergebnisse automatisch ausgewertet. Die Scanmaschinen werden aber auch dazu verwendet gezielt Schwächen in der System- oder Dienstkonfiguration aufzudecken, um den verantwortlichen Personen die Möglichkeit zu bieten, diese zu beheben, bevor sie aktiv für Angriffe ausgenutzt werden.

8.3 Sicherer Verkehr über unsichere Netze

Wissenschaftler und Studenten äußern immer häufiger den Wunsch, von einem beliebigen Ort aus gesicherten Zugang zu Daten zu erhalten, die auf Rechnern ihrer Arbeitsgruppe im MWN gespeichert sind. Hierzu benötigen sie einen Zugang aus öffentlichen Netzen ins MWN und darüber zum Institutsnetz, dem diese Rechner angehören. Derzeit ist ein Cluster von fünf VPN-Servern im Betrieb, die den Zugang über öffentliche Netze absichern. Dem Stand der Technik entsprechend sollte der Zugang zu an einem Hochschulinstitut gespeicherten Daten oder der administrative Zugang zu einem System im MWN abgesichert und verschlüsselt erfolgen.

8.4 Sicherung der Endgeräte und Zugangskontrollstrategien

Hierbei ist zwischen berechtigten Geräten und berechtigten Nutzern zu unterscheiden.

8.4.1 Berechtigte Geräte

Nur die vom LRZ den Netzverantwortlichen zugewiesenen IP-Adressen dürfen verwendet werden. An den Switches könnte zwar sichergestellt werden, dass nur Geräte mit registrierten MAC-Adressen einen Netzwerkzugang erhalten, dies wird jedoch wegen des hohen Verwaltungsaufwandes derzeit nur in sehr begrenztem Umfang (öffentliche Räume mit freien Netzdosen) durchgeführt. Hierdurch könnte lediglich sichergestellt werden, dass nur berechtigte Geräte, nicht aber berechtigte Nutzer die Infrastruktur verwenden. Eine Überprüfung der zugewiesenen IP-Adressbereiche geschieht an unseren Routern (Adress-Spoofing). Hier werden nicht zugewiesene IP-Adressen festgestellt und verfolgt.

8.4.2 Berechtigte Nutzer

Mittelfristig soll sichergestellt werden, dass nur authentifizierte Nutzer Zugriff auf Endgeräte und insbesondere Netzdienste erhalten. Eine anonyme Nutzung des Netzes sollte es jetzt bereits nicht geben.

Bei Geräten, die im Institutsbereich stehen und dort lokal verwaltet werden, hat der Netzverantwortliche bzw. der Systemverwalter dafür Sorge zu tragen, dass die Geräte nur von berechtigten Nutzern benutzt werden und für den Fall eines Missbrauchs auch identifizierbar sind. In öffentlichen PC-Räumen ist dies auf Basis der zwingend erforderlichen Nutzerverwaltung mittels Nutzerkennung und Passwort bereits geregelt. Bei der Nutzung von WLAN-Zugängen und beim Zugang über öffentliche Netze, erfolgt eine Authentifizierung der Nutzer über einen RADIUS-Server. Mit Verfügbarkeit von Netzkomponenten mit 802.1x-Authentifizierung (realisiert z.B. auf Basis von Radius) kann auch ein benutzerspezifischer Netzzugang realisiert werden, wie derzeit schon bei WLAN. Die vom LRZ aktuell eingesetzte Switch-Generation HP ProCurve unterstützt diese Funktionalität ebenso wie Systeme mit Windows Vista/7/8/8.1/10, Windows Server, Mac OS X und Linux.

8.5 Maßnahmen zum sicheren Betrieb des Netzes

Zur Sicherung des Netzbetriebs werden sowohl physische als auch Management-Software-seitige Maßnahmen ergriffen, die im Folgenden skizziert werden.

8.5.1 Sicherung der Verteilerräume

Durch die Art der Schließung hat nur technisches Personal Zugang zu den Verteilerräumen. Dem Stand der Technik folgend wird sukzessive im MWN eine Verbesserung der Zugangskontrolle in solche Räumlichkeiten angestrebt. Die Zugangskontrolle flächendeckend, d.h. MWN-weit durch automatische Zugangskontrollsysteme zu verschärfen und zu personalisieren ist jedoch nicht vorgesehen.

8.5.2 Stromversorgung der Verteilerräume, Klimatisierung und Brandschutz

Alle für einen größeren Bereich wichtigen Verteilerräume sind mit einer unterbrechungsfreien Stromversorgung (USV) zur Überbrückung kurzer Unterbrechungen versehen. Je nach Relevanz der abzusichernden Komponenten können hierdurch Überbrückungszeiten bis zu zwei Stunden gewährleistet werden. Die Knotenpunkte des MWN-Backbones sind mit leistungsfähigeren USVs ausgestattet, die 12 Stunden überbrücken können; der Eckpunkt W (LRZ Garching) ist an ein durch dynamische USVs und einen Dieselgenerator abgesichertes, unterbrechungsfreies Notstromnetz im LRZ angeschlossen. Mittelfristig muss erreicht werden, dass die entsprechende Versorgung auf alle Verteilerräume ausgedehnt wird. Zudem ist der punktuelle Anschluss an Notstromversorgungen zu realisieren, so dass auch längere Unterbrechungen keinen Schaden anrichten können. Die USVs werden durch das zentrale Netzmanagement überwacht und damit in den Störungsdienst einbezogen. Ein regelmäßiger Test der Funktionsfähigkeit wird im 14-tägigen Abstand von der USV selbst durchgeführt. Zur Verbesserung des Brandschutzes sollen die Verteilerräume mit Rauchmeldern ausgerüstet werden. Hierzu laufen Abstimmungen mit den Hochschulen, die für die jeweiligen Verteilerräume die Hausherren sind.

8.5.3 Ausfallsicherheit durch Redundanz

Um Ausfälle im Backbone soweit als möglich zu minimieren werden die in Abschnitt 4.1.3 dargestellten Maßnahmen umgesetzt.

Die Verteiler des Sekundärnetzes könnten bei Bedarf redundant an die Primärnetzknoten angeschlossen werden. Alle zum Betrieb des Backbones notwendigen Netzkomponenten sind mit einem redundanten Netzteil ausgestattet. Darüber hinaus verfügen alle eingesetzten Backbone-Router über redundante Managementmodule (notwendig für Routing). Bei der Auswahl der Netzkomponenten (Router und Switches) wurde großer Wert darauf gelegt, dass bei den eingesetzten chassis-basierten Systemen hot-swap-fähige Module zum Einsatz kommen. Hierdurch werden unnötige Ausfallzeiten bei Upgrades (Erweiterungen) und beim Austausch im Fehlerfalle vermieden.

8.5.4 Managementnetz

Aus Sicherheitsgründen ist zum Management aller Netzkomponenten ein eigenes Management-Netz auf der Basis eines im MWN gerouteten privaten Netzes realisiert. Dieses wird zudem durch eigene VLANs separiert. Über dieses Netz können alle Netzkomponenten von den Managementsystemen erreicht werden. In Zukunft könnte dieses Netz auch zu Accounting-Zwecken benutzt werden. Der Zugang zu den Routern und Switches ist nach Möglichkeit auf wenige Systeme, sog. Managementstationen beschränkt. Dem Stand der Technik entsprechend erfolgt der Zugang ausschließlich über gesicherte Protokolle, etwa SSH/SSL. Zum Zugriff auf die Managementinformationen der Netzkomponenten kommt SNMPv3 zum Einsatz. Bei Störungen müssen wichtige Netzkomponenten zusätzlich über ein Out-of-band-Management erreichbar sein (Modem, etc.). Dies ist derzeit für alle Backbone-Router realisiert, wobei die modembasierte Einwahl größtenteils durch kleine LTE-Router abgelöst wurde.

Für das zentrale Netz- und Systemmanagement wird als Plattform IBM Tivoli Netcool eingesetzt. Für das Management der HP-Switches kommt seit 2016 außerdem die Software IMC (Intelligent Management Center) in der Enterprise-Version zum Einsatz. Diese ergänzt Netcool um komponentenspezifische Funktionen, wie beispielsweise Configuration- und Asset-Management. Außerdem ist in IMC ein Modul enthalten, das eine Verkehrsanalyse auf Basis von sFlow ermöglicht. Für das Incident- und Change-Management wird ein IT-Service Management Werkzeug (iET ITSM Toolsuite) eingesetzt. Außerdem werden ein Tool für SLA-Reporting (InfoVista) und das Customer Service Management (CSM) für das MWN für spezifische Views auf die gesammelten Managementdaten verwendet.

9 Datenschutz

Hier wird nur der wissenschaftliche Bereich behandelt, ohne auf die an anderer Stelle geregelten besonderen Belange der Verwaltung bzw. der medizinischen Netze einzugehen. Der vorliegende Abschnitt gibt auch nur Auskunft über Daten, die im Zuständigkeitsbereich des LRZ beim Betrieb des Netzes und zentraler Server anfallen. Die angeschlossenen Institutionen regeln den Umgang mit diesen Daten in eigener Verantwortung. Es ist hierbei zwischen Nutzerdaten und Betriebs- bzw. Verkehrsdaten zu differenzieren.

Unter den Betriebs- bzw. Verkehrsdaten werden die Daten verstanden, die im LRZ beim Betrieb des Netzes und zentraler Server anfallen. Im LRZ existiert eine Auflistung aller dieser Daten. Für alle Daten ist der betriebliche Zweck, z. B. Erkennung von Störungen und Missbrauchsfällen aufgeführt, zu dem sie gespeichert werden, und daraus abgeleitet der Zeitraum (i. d. R. sieben Tage), nach dem sie wieder gelöscht werden.

Die Nutzerdaten, die im LRZ auf den zentralen Servern (z. B. Compute-, Mail-, WWW-Server) und im Backup- und Archivservice gespeichert sind, sind mit den üblichen Mechanismen durch Nutzerkennung und Passwort geschützt. Hier kommt es darauf an, Nutzerkennung und Passwort gegen unbefugte Kenntnisnahme zu schützen, und zwar sowohl an den Orten, an denen sie gespeichert sind, als auch auf dem Weg über das Netz. Soweit sie im LRZ gespeichert sind, sind sie mit den gängigen Mechanismen der verschlüsselten Speicherung in Linux- und Windowssystemen geschützt. Es muss vermieden werden, dass Nutzerkennungen und Passwörter im Klartext übermittelt werden. Deshalb sind z. B. die Server des LRZ schon lange nicht mehr über Telnet, sondern nur noch über SSH (secure shell) erreichbar. Für WWW-Zugriffe wird durchgängig HTTPS angeboten. Auch auf E-Mail und andere Dienste kann nur noch über sichere, meist SSL- bzw. TLS-basierte Verfahren zugegriffen werden.

Beim Backup- und Archivierungsdienst (am LRZ eingesetzt: TSM von IBM/Tivoli) ist sowohl eine verschlüsselte Client/Server-Übertragung als auch eine automatische Verschlüsselung bei der Speicherung konfigurierbar.

Für alle vom LRZ angebotenen Dienste und damit verbundenen Verarbeitungstätigkeiten existieren Beschreibungen gemäß den Vorgaben der Europäischen Datenschutzgrundverordnung (EU-DSGVO) und dem Bayerischen Datenschutzgesetz (BayDSG). Da das LRZ im rechtlichen Sinne Dienstleister und somit Auftragsverarbeiter ist, wurden mit den Kundeneinrichtungen, insbesondere LMU, TUM, HM, BSB, ... Auftragsdatenverarbeitungsverträge geschlossen.

10 Accounting

Beim Accounting wird zwischen Nutzerstatistiken zu Informations- bzw. Planungszwecken und Accounting zu Abrechnungszwecken unterschieden.

10.1 Nutzungsstatistik zu Informations- und Planungszwecken

Für die externe Nutzung der Netzdienste über den X-WiN-Anschluss wird eine Statistik erstellt. Sie ist in unterschiedlicher Detailtiefe vorhanden. Ein nennenswertes Beispiel solch einer Statistik ist die Auskunft über die Nutzung auf Basis der Rechner-IP-Adresse (Top-Talker). Das Security-Team entwickelt die zur Erkennung von Verkehrsanomalien eingesetzten Mechanismen stetig weiter.

Für Planungszwecke sind netzstrukturbezogene Daten über den internen (und auch den externen) Verkehr wichtig. Diese Verkehrsdaten werden derzeit regelmäßig nur auf der Ebene der Routerinterfaces gesammelt; Abbildung 19 zeigt dies am Beispiel der Entwicklung des Internet-Traffics am X-WiN-Übergang. Bei den Switches wird dies aufgrund des großen Aufwands nur für bestimmte Teilbereiche durchgeführt (zentrale Switchkomponenten in Campusbereichen). Endgeräteanschlüsse werden wegen des erheblichen Aufwands nicht in Erwägung gezogen. Dennoch hat man hiermit ein mächtiges Werkzeug in der Hand, um auf Veränderungen der Netznutzung rechtzeitig, d. h. proaktiv reagieren zu können. Diese Daten fallen im Rahmen eines eingesetzten Service-Level-Agreement-Tools (InfoVista) an.

10.2 Accounting zu Abrechnungszwecken

Zurzeit werden den satzungsgemäßen Nutzern bzw. den angeschlossenen Institutionen für die Nutzung des MWN keine Gebühren berechnet. Deshalb findet auch kein nutzerbezogenes Accounting statt. Allgemein dürfte es mit den derzeit zur Verfügung stehenden Möglichkeiten auch sehr schwer, wenn nicht unmöglich sein, aufgrund der äußerst heterogenen Struktur und der verteilten Zuständigkeiten im MWN ein halbwegs zuverlässiges, nutzerbezogenes Accounting zu realisieren.

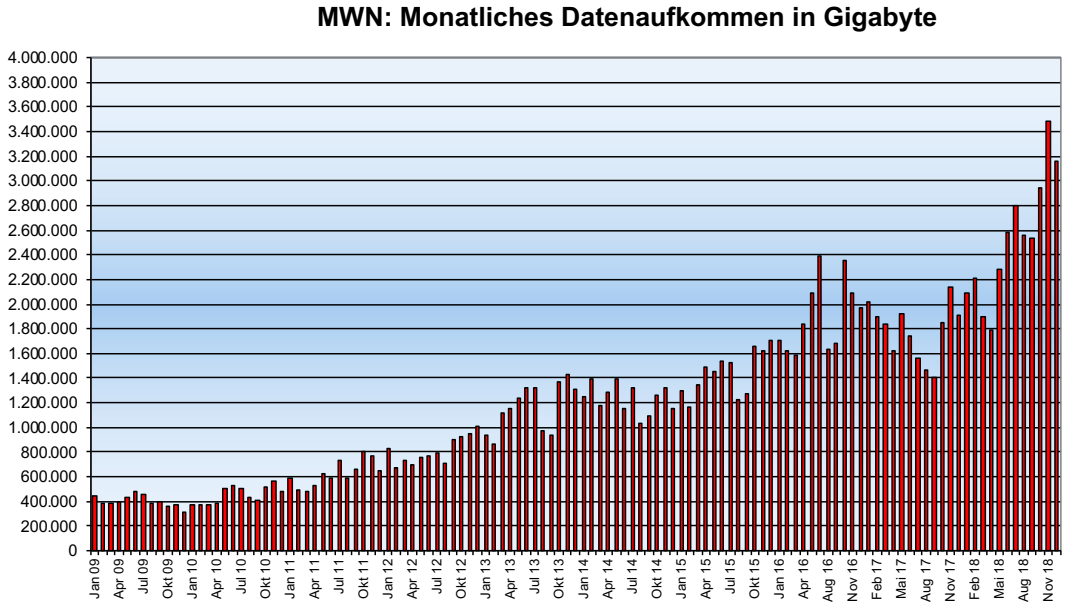


Abbildung 19: Entwicklung des Internet-Datenverkehrs in den vergangenen Jahren

11 Betriebs- und Nutzungsregelungen

Eine Übersicht über das Regelwerk des Leibniz-Rechenzentrums findet sich in

`www.lrz.de/wir/regelwerk/`

Dies umfasst alle für die Nutzung der vom LRZ angebotenen Dienste (zentrale Server, MWN, ...) geltenden Regelungen und Hinweise.

Die jeweils gültigen Betriebs- und Benutzungsregeln für die Nutzung der zentralen Server des LRZ („Benutzungsrichtlinien für die Informationssysteme des Leibniz-Rechenzentrums der Bayerischen Akademie der Wissenschaften“) finden sich in

`www.lrz.de/wir/regelwerk/benutzungsrichtlinien.pdf`

Die für die Nutzung des MWN gültigen Richtlinien sind zu finden unter

`www.lrz.de/wir/regelwerk/richtlinien_mwn/`

Diese werden durch die Regeln für den Betrieb von institutseigenen WLANs unter

`www.lrz.de/services/netz/mobil/inst-funklans/`

ergänzt.

12 Unterstützung dezentraler Systeme und Dienste über das Netz

In diesem Abschnitt wird die Rolle des Netzes sowohl für dezentrale Systeme als auch für diverse über das Netz angebotene Dienste beschrieben.

12.1 Mail- und Groupware-Services

Das LRZ betreibt zentrale Mailrelay-Rechner, die den ankommenden und abgehenden Mail-Verkehr (derzeit durchschnittlich ca. 850.000 E-Mails pro Tag) an die Mailserver im LRZ und in Hochschulinstituten weiterleiten. Aus Sicherheitsgründen (Viren- und Spam-Mails) ist es neben den Mailrelays des LRZ nur einer kleinen Anzahl weiterer Mailserver einzelner Fakultäten gestattet, direkt E-Mails aus dem Internet zu empfangen. Für alle anderen gilt eine Sperre des SMTP-Ports 25. Ungefähr 70% aller E-Mails aus dem Internet laufen über die Mailrelays des LRZ. Dort ankommende Mails durchlaufen zunächst das so genannte Greylisting und können dieses nur passieren, wenn die Mailquelle bereits bekannt ist, und ein DNS-basiertes Blacklisting. Dadurch werden ca. 99% der Viren- und Spam-Mails, für die in der Regel nur ein Zustellversuch unternommen wird, an den Mailrelays gar nicht erst angenommen. E-Mails, die diese Hürde nehmen, werden anschließend auf weiteren Rechnern auf Infektionen mit Viren und Würmer überprüft (durch Sophos-Antivirus und Clam-Antivirus) sowie einer Spam-Bewertung unterzogen (durch SpamAssassin).

Neben den Mailrelays betreibt das LRZ einen Mailinglisten-Server und mehrere Message-Stores mit ca. 200 virtuellen Maildomains. Auf einem Message-Store sind die Mailservices für das Portale CampusLMU realisiert. Auf einem weiteren Message-Store befindet sich der größte Teil der virtuellen Domains für einzelne Lehrstühle, Institute und Fakultäten der beiden Universitäten sowie anderer Organisationen. Auf alle Mailboxen kann mit den Protokollen IMAP und POP zugegriffen werden. Außerdem existiert eine Webmail-Oberfläche, über die die Mailboxen weltweit auf einfache Weise erreicht werden können.

Schließlich betreibt das LRZ eine Exchange-Server-Farm als Groupware-Lösung, die für die TUM, Hochschule München (HM), Hochschule Weihenstephan-Triesdorf (HSWT), Katholische Stiftungsfachhochschule (KSH), staatliche Museen und sowie im Pilotbetrieb für ausgewählte LMU-Fakultäten eingesetzt wird und aufgrund der außerordentlich guten Akzeptanz die anderen Mailserver sukzessive ablösen könnte.

Insgesamt werden ca. 89.000 Exchange-Postfächer (mit 41 TByte) sowie ca. 77.000 POP bzw. IMAP Postfächer (mit 10 TByte) betrieben.

12.2 Verzeichnisdienst-Services

Vom LRZ werden mehrere Verzeichnisdienste betrieben, die die zentrale Rolle in der Benutzerverwaltung für die vom LRZ angebotenen Dienste spielen und darüber hinaus für die Anmeldung an hochschulübergreifenden Diensten eingesetzt werden.

12.2.1 LRZ Identity Management mit LDAP-Verzeichnisdiensten

Die LRZ-Verzeichnisdienstarchitektur basiert auf einem zentralen Meta-Directory, das die Benutzerdaten zwischen den übrigen Verzeichnisdiensten abgleicht. Es werden insgesamt

21 produktive Verzeichnisdienst-Server betrieben, die der Authentifizierung und Autorisierung von LRZ-Benutzern sowie zur direkten LDAP-Anbindung oder Provisonierung vieler LRZ-Dienste und -Systeme dienen. Der im Meta-Directory enthaltene Benutzerdatenbestand wird insbesondere auch an das MWN-weite Active Directory übertragen, das zur delegierten Administration von Windows-Arbeitsplatzrechnern eingesetzt werden kann und die Basis für Dienste wie die Groupware Microsoft Exchange und den zentralen NAS-Filer bildet.

Ein zentraler Aspekt der Verzeichnisdienstarchitektur sind die Schnittstellen zu den Identity-Management-Systemen der beiden Münchner Universitäten, der Hochschule München und der Hochschule Weihenstephan-Triesdorf. Über Konnektorprogramme werden aktuelle und für den LRZ-Dienstbetrieb nötige Benutzerinformationen aller Hochschulangehörigen (differenziert nach Personal, Studierenden und Gästen) automatisiert und ohne Verzögerung zum LRZ übertragen. Damit entfällt eine erneute manuelle, fehleranfällige und zu Inkonsistenzen führende Neuerfassung der Benutzer.

Zum 31.12.2018 waren am LRZ insgesamt 336.138 aktive Benutzerkennungen angelegt, mit je individuellen Berechtigungen für die verschiedenen LRZ-Dienste. 99.878 Kennungen dienen der lebenslangen Mailweiterleitung für TUM-Alumni. 4.721 Kennungen waren für den Höchstleistungsrechner SuperMUC eingerichtet. Bei den übrigen Kennung verteilen sich die Berechtigungen für die größten Dienste wie folgt: 196.156 VPN- und WLAN/eduroam, 193.781 Sync+Share, 108.564 Cloud Storage, 97.463 Standard-Mail und 39.599 Mail- und Groupware Exchange.

12.2.2 DFN-AAI: Authentifizierungs- und Autorisierungsinfrastruktur

Durch hochschulübergreifend gemeinsame Studiengänge, den Bolognaprozess und die Mobilität von Lehrenden und Lernenden hat die hochschulübergreifende Nutzung von IT-Diensten heute eine große Bedeutung. Über die durch Roaming mögliche WLAN-Nutzung an anderen Hochschulen deutlich hinausgehend bildet die vom Verein zur Förderung eines deutschen Forschungsnetzes (DFN) betriebene Authentifizierungs- und Autorisierungsinfrastruktur (DFN-AAI) die Basis für die deutschland -und mittlerweile weltweite, hochschulübergreifende Nutzung von web-basierten Diensten wie E-Learning-Systemen, Speicherdiensten und Forschungsdatenbanken wie auch für den Zugang zu digitalen Medien von akademischen Verlagen und für den Download lizenzierter Software zu Sonderkonditionen für Forschung und Lehre. Zur Teilnahme einer Hochschule an der DFN-AAI ist der Betrieb eines so genannten Shibboleth Identity Providers notwendig, der zur Authentifizierung der Hochschulmitglieder eingesetzt wird und den Dienstleistern selektiv Benutzerprofildaten zur Verfügung stellen kann. Das LRZ betreibt diese Infrastruktur produktiv für die beiden Münchner Universitäten sowie für die Mitarbeiter der Bayerischen Akademie der Wissenschaften inkl. des LRZ.

12.3 GitLab

Das LRZ bietet mit GitLab einen web-basierten Dienst zur Verwaltung von Git-Repositories. GitLab stellt neben den eigentlichen Repositories Werkzeuge wie Wikis und einen Issue-Tracker bereit, die die Zusammenarbeit in Gruppen und Teams und die gemeinsame Entwicklungsarbeit unterstützen. Mit „Merge Requests“ gibt es ein Mittel, mit dem Code-Reviews gemeinsam und transparent durchgeführt werden können.

Zum Ende des Jahres 2018 gibt es über 14.000 Nutzer mit mehr als 20.000 Projekten.

12.4 Webhosting

Das LRZ betreibt eine auf die Bedürfnisse der LRZ-Kunden abgstimmte Webhosting-Umgebung. Das Setup besteht aus mehr als 80 Linux-Maschinen (realisiert als virtuelle Maschinen) hinter einem Loadbalancer, wobei immer mehrere Maschinen mit gleichem Setup als Pool zusammengefasst und für eine bestimmte Zielgruppe optimiert sind. Hinzu kommen weitere Zugangs- und Gateway-Maschinen (für ssh-Zugang, Cronjobs usw.).

Die Pflege der Betriebsumgebung erfolgt durch das LRZ, der Kunde kann sich ganz auf seine Webanwendung konzentrieren. Es werden zahlreiche Webauftritte (Stand 2018/12 rund 1.200) realisiert, meist umgesetzt mit CMS-Systemen auf Basis PHP und MySQL, wie beispielsweise Typo3, Wordpress, Joomla, Drupal, Limesurvey usw. Statische Webseiten sind natürlich ebenfalls möglich.

Hinzu kommen weitere sehr Kunden-spezifische Dienste:

- Betriebsumgebung für das zentrale E-Learning-System ”Moodle”der TUM
- Betriebsumgebung für das zentrale E-Learning-System ”Moodle”der LMU
- Betriebsumgebung für das zentrale Content-Management-System Typo3 der TUM
- Betriebsumgebung für den Haupt-Webauftritt der TUM (www.tum.de)
- Betriebsumgebungen für LRZ-eigene Webauftritte und Content-Management-Systeme (Fiona, Typo3, Confluence)

Darüber hinaus betreiben im Bereich des MWN viele Institute und Einrichtungen eigene Webserver, insbesondere in den technisch-naturwissenschaftlich bzw. ingenieurwissenschaftlichen Fakultäten.

12.5 File-Service

Für die Bereitstellung zentraler Dateiablagebereiche werden hochverfügbare NAS-Filer eingesetzt. Aus Sicherheitsgründen wird der Speicher per NFS in der Regel nur rechenzentrumsintern exportiert. Über das CIFS-Protokoll kann jedoch auf die Speicherbereiche MWN-weit zugegriffen werden. Besonders die TUM nutzt die Möglichkeiten des Diensts seit vielen Jahren intensiv. Auch an der LMU nimmt die Verbreitung zu. An der Hochschule München wird er im Bundle mit dem MWN-PC angeboten. Auf die Dateien in den gemeinsamen Ablagebereichen sowie im eigenen Home-Directory können die Benutzer auch über ein webbasiertes, weltweit erreichbares Frontend zugreifen (`webdisk.ads.mwn.de/`). Seit 2015 ist der Sync&Share-Dienst auf der Basis von Powerfolder produktiv. Damit können Dateien auf verschiedenen Geräten synchronisiert und auch mit externen Kooperationspartnern, die keine eigene LRZ-Kennung habe, ausgetauscht werden. In allen diesen Fällen ist ein hochperformanter und unterbrechungsfreier Netzbetrieb Grundvoraussetzung.

12.6 Data Science Storage (DSS)

In vielen Forschungsbereichen zeichnet sich ein enormes Datenwachstum ab. Ein Beispiel für solch einen Forschungsbereich sind die Lebenswissenschaften, die mit Next-Generation-Sequencing und ultrahochauflösenden Mikroskopen innerhalb der nächsten 5 Jahre viele

Petabyte an Daten generieren werden. Für diese und ähnliche Benutzergruppen hat das LRZ in 2015 das Konzept des Data-Science-Storage (DSS) entwickelt. Ein Rahmenvertrag erlaubt es Großkunden, Software-defined-Storage zu beschaffen, der im und vom LRZ betrieben wird. Große Datenmengen im Petabyte-Bereich, die an Hochschulinstituten vor Ort erzeugt werden, können auf den modular aufgebauten Festplattensystemen des DSS im LRZ dauerhaft gespeichert und anschließend performant auf den HPC-, Cloud- und Visualisierungssystemen am LRZ analysiert werden. Die dazu nötige leistungsfähige, skalierbare und nachhaltige Speicherarchitektur wird gleichzeitig an die LRZ-HPC-Systeme (IBM Spectrum Scale Client Cluster) sowie an weitere Rechnerressourcen im Münchner Hochschulumfeld angebunden.

12.7 Backup/Archivierung

Das LRZ bietet seit 1996 einen zentralen Backup- und Archivierungsdienst auf der Basis von IBM Spectrum Protect, vormals Tivoli Storage Manager, an. Im Hinblick auf die Architektur kann zwischen drei Systemen unterschieden werden:

1. LABS — das LTO-Archiv- und Backupsystem für allgemeine Anwendungen.
2. HABS — das Hochleistungsarchiv- und Backupsystem für besonders datenintensive Anwendungen.
3. DRABS — der Spiegel für Archivdaten, der auf Desaster Recovery optimiert ist.

Die Systeme bestehen aus 19 Rechnern mit 668 Cores, 8.736 GB RAM, vier Fibre Channel Switches und zwei Fibre Channel Direktoren, 56 10GE-LAN Ports mit 100 Gbit/s Uplink zum LRZ-Backbone, vier Storage Servern mit 5.820 TB verteilt auf 748 Festplatten mit 48 GB/s Gesamtdurchsatz, fünf Tape-Libraries mit insgesamt 63.243 Slots und 170 Bandlaufwerken (LTO-4, LTO-5 und LTO-6 sowie LTO-7) mit 32 GB/s Gesamtdurchsatz.

Der Datenfluss wird durch die großen Ein-/Ausgabedatenmengen der HPC-Systeme, vor allem des Höchstleistungsrechners, einerseits und die Sicherung von MWN-weit rund 10.000 Systemen von 450 verschiedenen Einrichtungen geprägt. Eine weitere, sehr rasch wachsende Datenquelle sind die Digitalisate der Bibliotheken, die zur langfristigen Speicherung ans LRZ geschafft werden.

Diese Anwendungen nutzen naturgemäß das Kommunikationsnetz sehr intensiv: Täglich werden an den TSM-Servern rund 130 TB Daten entgegengenommen. Über eine 10 Gbit-Verbindung werden die Archivdaten zusätzlich an das Rechenzentrum der Max-Planck-Gesellschaft in Garching gespiegelt.

12.8 Storage Area Network

Das Storage Area Netzwerk (SAN) des LRZ bildet die Grundlage für die Vernetzung der Massenspeicherkomponenten. Das ursprüngliche SAN, dessen Anfänge auf das Jahr 2000 zurückgehen, wurde in den letzten Jahren stark ausgebaut und aus Gründen der höheren Verfügbarkeit in mehrere sogenannte Fabrics aufgeteilt. Es werden getrennte Fabrics für das Hochleistungsarchiv, das LTO-Archiv- und Backupsysten und das Filesystem des Höchstleistungsrechner betrieben. An die SAN-Fabrics sind Storageserver mit einer Kapazität von mehr als 5,8 PetaByte, alle Bandlaufwerke der Libraries und alle Serversysteme mit hohem Datenverkehr, insbesondere die File- und Backupserver angeschlossen.

12.9 Windows, MacOS und Linux-Netzdienste

Das lokale Netz wird im Windows, MacOS und Linux-Bereich für die klassischen Dienste genutzt: Zugriff auf Datei- und Druckdienste, Mail-Services, zentrale Authentifizierung usw. Das LRZ setzt sie in folgenden Gebieten ein:

- Arbeitsplätze in Kursräumen, in denen Windows-Applikations- und Unix-/Linux-Administrations- und Programmierschulungen angeboten werden. Die einzelnen Windows-Kurs-PCs werden über das Kommunikationsnetz installiert und über die zentralen Softwareverteilung versorgt. Linux wird als virtuelle Maschinen unter Windows genutzt.
- Windows-PCs und MACs in öffentlichen Pools, zur Nutzung durch Studenten und Hochschulangehörige. Diese Geräte sind mit einer breiten Softwarepalette von Büroanwendungen bis zu Spezialgrafikprogrammen ausgestattet und ergänzen die fachspezifischen Geräte in den CIP-Pools der Münchener Hochschulinstitute.
- Mitarbeiterarbeitsplätze des LRZ auf Basis von Linux, MacOS und Windows, sowohl in der wissenschaftlichen Betreuung als auch in der Verwaltung. Alle Arbeitsplätze sind an eine zentrale Nutzerverwaltung angebunden und greifen auf gemeinsame Datei- und Druckdienste zu. Die Systeme werden über zentrale Softwareverteilungen für die jeweiligen Betriebssysteme installiert und verwaltet.
- Verwaltete MacOS und Windows-Arbeitsplätze an der Bayerischen Akademie der Wissenschaften, der TUM (im Rahmen des gemeinsam erbrachten Dienstes TUM-PC mit inzwischen mehr als 5.000 versorgten Endgeräten), der LMU mit rund 1.000 Geräten, der Hochschule München und der Hochschule für Musik und Theater mit Datei- und Druckdiensten, Softwareverteilung und zentraler Authentifizierung. Das Angebot MWN-PC wird in letzter Zeit von der LMU stärker nachgefragt, mit ähnlich zu erwartenden Ausbauzahlen zur TUM, nachdem von der LMU der organisatorische Rahmen geklärt wurde.
- Betrieb eines zentralen Active Directory für rund 15.000 aktiv angebundene Clientsysteme im MWN und als LDAP-Server für weitere angeschlossene Systeme zur zentralen Benutzerauthentifizierung wie der zentralen Groupware Exchange oder der VMware Infrastruktur am LRZ.

Neben dem Einsatz von Linux, MacOS und Windows gibt es Windows-basierte Citrix Terminal Services, die es erlauben, Applikationen, die nicht an lokalen Arbeitsplätzen verfügbar sind, remote zu nutzen. Auf diese Terminal Services kann auch über Unix/Linux/MacOS zugegriffen werden, z. B. um für diese Systeme MS-Office-Produkte verfügbar zu machen. Dieses Angebot ist auch Voraussetzung für die Telearbeit am LRZ, um den Mitarbeitern einen definierten Arbeitsplatz zur Verfügung stellen zu können. Die dauernde Verfügbarkeit des Netzes und dessen hohe Leistungsfähigkeit ist in allen diesen Einsatzbereichen von essentieller Wichtigkeit.

WSUS-Server Das LRZ bietet für Windows-Rechner im MWN die Nutzung eines Microsoft Windows Software Update Service (WSUS) an; der entsprechende Server wird am LRZ betrieben. Der Dienst ermöglicht Betreibern von Windows-Rechnern, ihre Systeme automatisch auf dem aktuellen Patch-Stand zu halten. Der Software Update Service des LRZ ist Teil eines umfassenden Software-Sicherheitskonzepts.

Sophos-Anti-Virus Das LRZ hat für die Anti-Viren-Software Sophos schon seit mehreren Jahren eine Landeslizenz für die bayerischen Hochschulen, die es u. a. erlaubt, das Produkt im Münchner Hochschulbereich weiterzugeben. In diesem Umfeld wird im MWN auch ein Verfahren angeboten, mit dem die Installation und die regelmäßigen Updates sehr einfach über einen Remote-Update-Server, der am LRZ betrieben wird, zu bewerkstelligen sind. Hierdurch können auch Rechner mit privaten Adressen in einem automatischen Updateverfahren versorgt werden.

12.10 Softwareverteilung

Das LRZ betreibt FTP-serverbasierte Transferbereiche zum Austausch von Dateien, die aufgrund ihrer Größe nicht z.B. per E-Mail verschickt werden können. Free- and Shareware anzubieten. Der Schwerpunkt liegt derzeit aber auf einer Softwareverteilung mit Datenträgern. Längerfristig ist jedoch mit einer deutlichen Zunahme der Verteilung über das Netz zu rechnen. Im Bereich der Institute werden weitere FTP-Server betrieben, darunter auch Mirror für populäre Open Source Software, z. B. Linux-Distributionen wie Debian.

13 Netz- und Dienstmanagement

Das Netz- und Dienstmanagement umfasst Maßnahmen zur Dienstqualität, Wartung, Überwachung und Störungsbeseitigung.

13.1 Dienstqualität

Das LRZ berät Nutzer des MWN bei der Verwendung der angebotenen Netzdienste und bei der Aufklärung von Störungsursachen via Servicedesk, der mit in das Störungsmanagement eingebunden ist, und durch regelmäßig abgehaltene Schulungsveranstaltungen.

Darüber hinaus findet mit den Netzverantwortlichen, die als Ansprechpartner für das LRZ vor Ort in den Instituten fungieren, in Fragen der Planung und Einrichtung neuer Infrastrukturen ein regelmäßiger Austausch statt. Um das notwendige Know-How vor Ort sicher zu stellen, werden für die Netzverantwortlichen und Interessierte auch spezielle Schulungen angeboten.

13.2 Dienstgüte

Die Behandlung der Dienstgüte umfasst die Aspekte Verfügbarkeit, Traffic-Klassifizierung und Reporting.

13.2.1 Verfügbarkeit

Ziel des LRZ ist es, mit dem vorhandenen Personalbestand eine maximale Verfügbarkeit des Netzes zu gewährleisten. Es werden alle zur Verfügung stehenden Mechanismen genutzt, die eine möglichst rasche und automatische Umschaltung im Fehlerfall bewirken, damit Betriebsunterbrechungen möglichst vermieden oder zumindest sehr kurz gehalten

werden können. Zudem sinken die Wartungskosten, weil nur noch in sehr wenigen Fällen sehr kurze (teure) Reaktionszeiten mit den Dienste/Komponenten-Lieferanten zu vereinbaren sind.

Zu den Redundanz-Mechanismen zählen:

- Redundante Leitungswege im Backbone
- Mehrfache Internet-Anbindung (doppelt über X-WiN + Backup über M-net, vgl. Abbildung 10)
- OSPF im Backbone, BGP zu den Internetprovidern (zur automatischen Wege-Umschaltung)
- Redundanter Rechenzentrums-Router (ausgeführt als Virtual Path Channel (VPC))
- Spanning-Tree im Rechenzentrums-Backbone wurde 2015 konsequent durch Multi-Chassis Trunking ersetzt, damit hat sich die Fehlersuche vereinfacht und die Bandbreite erhöht
- Proaktives Management (z. B. Überwachung der Fehlerzähler an Router- und Switchports)

13.2.2 Class-of-Service / Quality-of-Service

Grundsatz ist, im Netz zu jedem Zeitpunkt ausreichende Kapazitäten zur Verfügung zu halten, um die nachgefragten Dienste in guter Qualität abwickeln zu können. Das erscheint mittel- und langfristig effizienter und wirtschaftlicher als eine aufwändige und mit dem vorhandenen Personal ohnehin nicht leistbare Mangelverwaltung zu betreiben. Andererseits sollen völlig bedarfsferne Überkapazitäten vermieden werden. Deshalb ist es notwendig, wesentliche Charakteristika der Verkehrsflüsse in ihrer zeitlichen Entwicklung sowie wichtige Dienstgüteparameter zu messen und als Planungsgrundlage auszuwerten. Im Rahmen dieser Tätigkeiten werden derzeit die Anschlussleitungen der Institute sowie die Leitungen im Backbone auf ihre Auslastung hin überwacht. Übersteigt die durchschnittliche Auslastung eines Interfaces mehrfach die Marke von 30% (Mittelwert für 15 Minuten), so werden entsprechende Schritte für eine Hochrüstung der Bandbreite dieses Anschlusses eingeleitet.

Es ist abzusehen, dass (Multimedia-)Dienste an Bedeutung zunehmen werden, die auf bestimmte Dienstgüteparameter (Paketverluste, Verzögerung, Jitter) besonders empfindlich reagieren. Zur Qualitätssicherung für solche Dienste wird man auf steuernde Eingriffe nicht verzichten können. Bei der Auswahl von Netzkomponenten (Router und Switches) wurde vom LRZ bereits seit 1999 darauf geachtet, dass sich hier CoS-Funktionen abhängig von unterschiedlichen Parametern (IP-Adresse, MAC-Adresse, Port, ...) einstellen lassen. Leider enden derzeit die Möglichkeiten der Steuerung von CoS bereits am Übergang ins Internet (X-WiN). Es fehlen noch immer Absprachen (auf interorganisationeller Ebene), um eine Ende-zu-Ende-Priorisierung entsprechender Datenströme zwischen deutschen Wissenschaftseinrichtungen angehen zu können. Ob dies notwendig wird, muss die Zukunft zeigen: Es kann auch sein, dass aufgrund der verfügbaren Bandbreite ein Priorisieren mittels CoS nicht notwendig wird.

13.2.3 Service-Level-Reporting

Die Nutzer des MWN erwarten vom LRZ als ihrem Dienstleister auch Informationen über den Zustand der Netzdienste. Die Informationspflicht wird derzeit mit folgenden Mechanismen erfüllt:

- Statistiken über die Auslastung ausgewählter Backbone-Interfaces (X-WiN-Anschluss, Backbone-Router), Nutzung der WLAN-Accesspoints und globale Verfügbarkeit des MWN-Backbones. Diese Statistiken sind allen Nutzern des MWN zugänglich (`wwwmwn.lrz.de`, `wlan.lrz.de/apstat/`).
- Das seit längerem intern eingesetzte Service-Level-Reporting-Tool (InfoVista) liefert aktuelle Reports über Verfügbarkeitszahlen diverser Router, Auslastungsstatistik u. ä. Es wurde ein gestuftes Zugriffskonzept erarbeitet, um den unterschiedlichen Nutzergruppen (Anwender, Netzverantwortlicher, LRZ-intern) entsprechende Sichten auf die gesammelten Informationen zur Verfügung stellen zu können. Die entsprechenden Berichte werden nach Absprache auch für einzelne Netzverantwortliche bereitgestellt.

13.3 Wartung

Im MWN ist derzeit aus Gründen der Kostenoptimierung folgendes Wartungskonzept realisiert:

- Redundante Netzteile bei allen wichtigen Netzwerkkomponenten (z. B. Router, Switches). In den zentralen Backbone-Routern zusätzlich ein redundantes Managementmodul. Bei den eingesetzten chassis-basierten Systemen (Router und Switches) sind die zum Einsatz kommenden Module hot-swap-fähig. Hierdurch werden unnötige Ausfallzeiten bei Upgrades (Erweiterungen) und beim Austausch im Fehlerfall vermieden.
- Identifikation von Störungen, Störungsbehebung einschließlich Ein- und Ausbau von Komponenten ausschließlich durch das LRZ (während der Dienstzeiten kann so eine Entstörzeit von weniger als zwei Stunden gewährleistet werden).
- Einheitliches Servicekonzept für alle Netzkomponenten mit den folgenden Anforderungen:
  - Vorhaltung von Ersatzteilen für alle zentralen Komponenten, so dass ein Austausch eines defekten Elements jederzeit möglich ist.
  - Bring-In-Service mit Tausch der defekten Hardwarekomponenten innerhalb von 48 Stunden.
  - Service für Beratung (Servicedesk und Fernwartung des Serviceanbieters).
  - Softwareservice (Updates, Problemdatenbank, . . .).

Dieses Konzept erfordert eine möglichst homogene Geräteausstattung. Abhängig von der Funktion im Netz werden i. d. R. nur bestimmte, durch das LRZ in regelmäßigen Zeitintervallen ausgewählte Produkte eingesetzt. Dadurch lässt sich auch eine zentrale Ersatzteilhaltung realisieren, ohne sehr restriktiven Zeitvorgaben beim Bring-in-Service zu unterliegen und ohne dass die Qualität und die Verfügbarkeit des Netzes darunter leidet.

Während der Netzwartung (regelmäßig dienstags ab 07:00 Uhr bis max. 09:00 Uhr) werden eventuell notwendige Updates an Netzkomponenten eingespielt, veraltete oder defekte Geräte ausgetauscht oder gewünschte Konfigurationsänderungen durchgeführt. Für

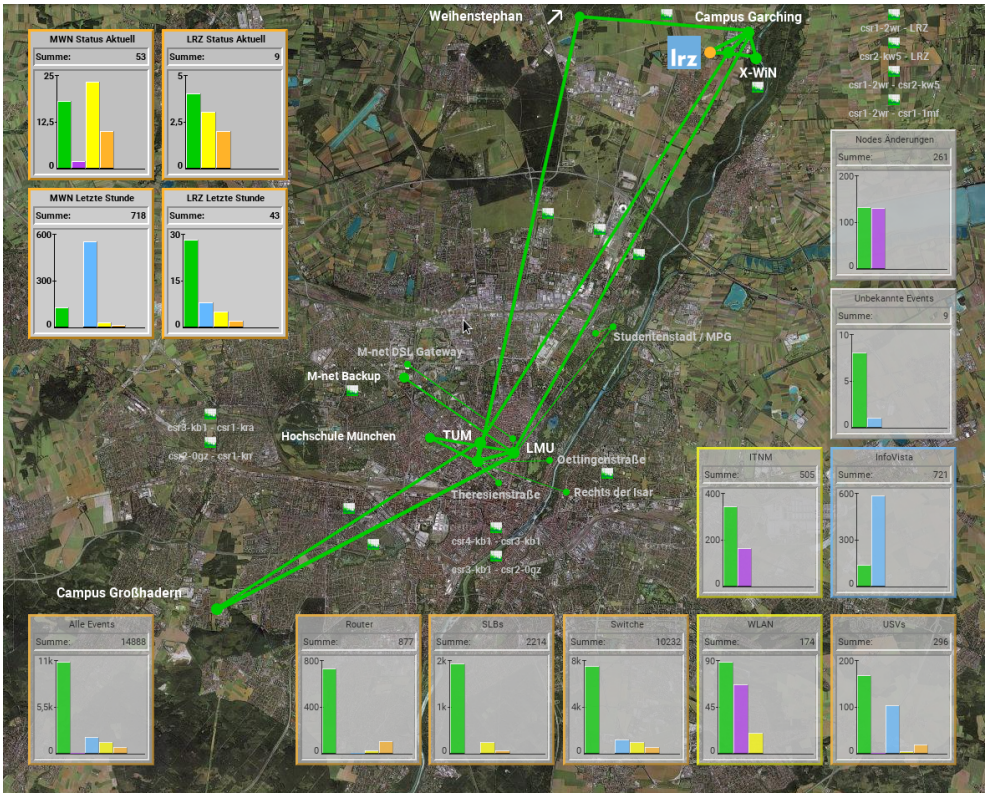


Abbildung 20: Darstellung des MWN-Monitoring in einer Gesamtübersicht

größere Wartungen oder umfangreichere Ersetzungsmaßnahmen werden an Donnerstagen bei Bedarf angekündigte Sonderwartungstermine angesetzt. Da die meisten Arbeiten aber nur lokale Teilnetze betreffen, ist meistens trotzdem der größte Teil des Netzes erreichbar. Die Unterbrechungen (wann ungefähr, wie lange und welche Bereiche oder Dienste betroffen sind) werden mindestens einen Tag vorher über die aktuellen Mitteilungen (ALI) des WWW-Servers des LRZ (`www.lrz.de/aktuell`) sowie per E-Mail an alle Netzverantwortliche bekannt gegeben. Größere Eingriffe oder Umbauten am Netz werden jeweils am Samstag durchgeführt. Die Ankündigungen hierzu erfolgen mindestens eine Woche im Voraus.

13.4 Netzüberwachung

Die Netzüberwachung und die Überwachung von Betriebsparametern erfolgt automatisiert und proaktiv durch die zentrale Netzmanagementplattform (IBM Tivoli Netcool); Abbildung 20 zeigt eine der Ansichten dieser Plattform. In regelmäßigen Abständen (5-Minuten-Intervall) werden sämtliche Netzkomponenten gepollt und der Status abgefragt. Fehler werden zusätzlich sofort dem für den Betrieb zuständigen Personal (Verteilerliste) per E-Mail und ggf. per SMS signalisiert. Da es bei größeren Störungen in diesem Umfeld aber zu einer erhöhten Flut von Fehlermeldungen kommen kann, wird mit einem Korrelationsverfahren gearbeitet, das eine Vorfilterung der Meldungen nach gewissen Regeln ermöglicht (Root Cause Analyse).

13.5 Incident und Change Management nach ISO/IEC 20000

Die Arbeitsfähigkeit sehr vieler Hochschulangehöriger hängt wesentlich von der Funktionsfähigkeit des Netzes und seiner Netzdienste ab. Störungen werden durch das Netzmanagementsystem (s. o.) und durch Meldungen der Nutzer erkannt. Fehlermeldungen der Nutzer können sowohl telefonisch an den LRZ-Servicedesk, wie auch per Web-Schnittstelle (Self-Service) gemeldet werden. Näheres ist beschrieben in `www.lrz.de/fragen/`.

Je nach Art der Störung werden vom LRZ (ggf. in Zusammenarbeit mit anderen, wie z. B. externen Providern, Netzverantwortlichen und Lieferanten) geeignete Maßnahmen eingeleitet. Um (besonders in komplexen Fällen) einen geordneten und koordinierten Verlauf sicherzustellen und zu dokumentieren, wird als zentrales Steuerungsinstrument ein Trouble-Ticket- und Incident-Management-System benutzt (iET ITSM-Suite). Durch entsprechende Vorkehrungen kann sich ein (berechtigter) Nutzer über den Bearbeitungszustand des von ihm initiierten Incident-Tickets (Störungsmeldung) per Web-Interface informieren; über wesentliche Lösungsschritte wird er zudem per E-Mail informiert. Bei der Klassifikation des Vorfalls wird nach Wichtigkeit (gering, mittel, kritisch) differenziert, wobei sich dieser Wert i. d. R. aus dem Umfang der betroffenen Nutzerschaft und den Service Level Agreements ableitet. Abhängig von dieser Klassifikation sind unterschiedliche Reaktionszeiten und Eskalationszeiträume hinterlegt.

Der Servicedesk des LRZ, der auch eine Telefon-Hotline betreibt, ist die Anlaufstelle, bei der alle Störungsmeldungen für den Verantwortungsbereich des LRZ auflaufen. Sie ist über eine einheitliche Rufnummer bzw. E-Mail-Adresse erreichbar und rund um die Uhr besetzt. Die zentrale Management-Station überwacht in regelmäßigen Abständen (5-Minuten-Intervall) per SNMP die Funktionsfähigkeit aller Netzkomponenten. Fehlersituationen generieren eine Meldung per E-Mail und bei wichtigen Netzkomponenten auch eine Nachricht per SMS.

Der zuverlässige Netzbetrieb ohne Unterbrechung sollte auch außerhalb der Dienstzeiten sichergestellt werden. Deshalb wurde die Möglichkeit der Einrichtung einer formellen Rufbereitschaft geprüft und für Netzkomponenten, die ausgewählte Dienste betreffen, eingeführt. Unabhängig davon liegt die Verfügbarkeit des zentralen Backbone-Netzes mit den entsprechenden Übergängen zu den Institutsinfrastrukturen fast immer bei mehr als 99,9%.

Im Rahmen der Ausrichtung der LRZ IT Service Management Prozesse nach ISO/IEC 20000 wurde auch das Management von Änderungen an den Netzdiensten und der Netzinfrastruktur formalisiert. Änderungsanträge werden in so genannten Change Requests (CRs) erfasst, priorisiert, auf Abhängigkeiten untersucht, bewertet und genehmigt. In den CRs werden auch der gesamte Bearbeitungsverlauf und der jeweils aktuelle Stand festgehalten. Die aktuell in Bearbeitung befindlichen CRs werden einem wöchentlichen Review unterzogen und stehen als Dokumentation über den Abschluss der Arbeiten hinaus zur Verfügung.

13.6 Zertifizierung nach ISO/IEC 20000 und ISO/IEC 27001

Das LRZ hat Anfang 2018 ein Projekt zur Einführung eines integrierten Informationssicherheits- und Servicemanagementsystems (I/SMS) gestartet. Das Projekt hat die Professionalisierung des IT-Managements und damit eine höhere Kundenzufriedenheit, eine höhere Flexibilität sowie eine größere Transparenz der IT-Prozesse zum Ziel. Mit dem Projekt werden klare Strukturen geschaffen, Aufgaben, Vorgaben und Verantwortlichkeiten sowie die dafür notwendigen Prozesse definiert und etabliert. Dabei ist es für den Erfolg essentiell die Umsetzung mit einem angemessenen Aufwand - Nutzenverhältnis zu erreichen. Ein Basiskonzept ist der kontinuierliche Verbesserungsprozess im I/SMS, der am LRZ gelebt wird.

Eine Organisationszertifizierung des prozessorientierten und integrierten Managementsystems nach den internationalen Standards ISO/IEC 20000 für das Servicemanagement und ISO/IEC 27001 für das Informationssicherheitsmanagement wird für Mitte 2019 angestrebt. Dementsprechend wurde als Projektkürzel ISO47k als Summe von ISO 20000 und ISO 27001 gewählt.

14 Personelle Zuordnung

Die Abteilung Kommunikationsnetze des LRZ ist für das MWN zuständig. Dies bedeutet die Planung, Inbetriebnahme und den laufenden Betrieb des Netzes bis zur Datendose am Arbeitplatz des einzelnen Hochschulangehörigen. Die Leitung der Abteilung liegt in den Händen von Herrn Prof. Dr. Helmut Reiser. Die Abteilung gliedert sich in drei Gruppen Planung, Betrieb und Wartung.

Die Gruppe *Planung Kommunikationsnetze* betreut die Netzmanagement-Plattformen und –Werkzeuge (Netzdoku-System, Reporting-Tools, Trouble-Ticket-System und ITSM-Suite, Accounting usw.), ist bei Produktauswahlen und -konsolidierungen aktiv, hält einen ständigen Marktüberblick und beteiligt sich aktiv bei Pilotprojekten und Beta-Tests von Netzkomponenten und Managementwerkzeugen. Sie überwacht und treibt den schrittweisen Ausbau der Netzinfrastruktur voran und ist bei der Auswahl und Dimensionierung der aktiven Komponenten in Absprache mit den Instituten beteiligt (Netzplanung). Neben der Erarbeitung von Einsatzkonzepten (z. B. Einsatz von Firewalls im MWN) beschäftigt sich die Gruppe mit der Integration von Managementwerkzeugen sowie der pilothaften Untersuchung und Installation neuer Dienste sowie Sicherheitssystemen (IDS, IPS, SIEM, Security-Reporting, Policy Management, Traffic Management usw.). Werden diese Dienste produktionsrelevant, dann gehen sie i. d. R. in den Zuständigkeitsbereich anderer Gruppen im LRZ über. In der Gruppe werden auch drittmittel-finanzierte Forschungsprojekte durchgeführt. Die europäische Union fördert wissenschaftliche Arbeiten beispielsweise zum Management, zur Visualisierung und zum Monitoring von GÉANT, dem Verbund der europäischen Forschungsnetze, sowie in den Bereichen Software Defined Networking und Federated Identity Management. Die Gruppe besteht aus Hochschul- und Fachhochschulabsolventen mit Schwerpunkt Informatik/Nachrichtentechnik. Die Leitung der Gruppe liegt in den Händen von Herrn Dipl.-Inf. (Univ.) Stefan Metzger.

Die Gruppe *Betrieb Kommunikationsnetze* betreut die aktiven Komponenten im MWN (Router, Switches, Accesspoints und netznahe Dienste wie z. B. DHCP, DNS, VPN, Firewall usw.). Zu den Aufgaben gehören die Konfiguration, die Dokumentation, das Monitoring der Netzinfrastruktur sowie die Fehlersuche (Layer 2 — Layer 7). Hinzu kommt die Unterstützung von Nutzern durch das Erstellen von Anleitungen und persönlichen Beratungen. Fremdfirmen werden bei diesen Prozessen nicht eingebunden. Wartungsverträge für die Netzkomponenten sehen nur einen Hotline-Support, Software-Update sowie einen Austausch defekter Teile per Paket vor; eine Präsenz vor Ort ist nicht vorgesehen. Die Gruppe besteht aus Hochschul- und Fachhochschulabsolventen mit Schwerpunkt Informatik bzw. Nachrichtentechnik sowie Mathematisch-Technischen Assistentinnen. Die Leitung der Gruppe liegt in den Händen von Herrn Dipl.-Ing. (Univ.) Helmut Tröbs.

Die Gruppe *Wartung Kommunikationsnetze* ist hauptsächlich mit der Inbetriebnahme neuer Infrastrukturen sowie mit der Fehlersuche und Fehlerbeseitigung vor Ort bei den Nutzern beschäftigt. Sie stellt die wesentliche Schnittstelle zu den Bauämtern und Planungsbüros bei der Realisierung neuer passiver Netzinfrastrukturen (Leitungswege, Verteilerstandorte usw.) dar. Eigene Leitungsinstallationen werden nicht durchgeführt; die Gruppe nimmt jedoch die Überwachung anstehender Installationen (Schnittstelle zum Installateur) sowie de-

ren Abnahme wahr. Die Gruppe besteht bis auf den Leiter aus Mitarbeitern, die als Informationselektroniker oder IT-Systemelektroniker ausgebildet wurden. Die Leitung der Gruppe liegt in den Händen von Herrn Dipl.-Ing. (FH) Christof Häfele.

15 Anlage: Liste aller MWN-Unterbezirke

- **A: Garchinger Hochschulgelände 1**
  - **A0**: TUM, Gebäude 5212, RCM-Hauptbau
  - **A1**: TUM, Gebäude 6101, Heizhaus
  - **A2**: TUM, Gebäude 6104, Feuerwehr
  - **A3**: TUM, Gebäude 5275, Bayerisches Zentrum für Angewandte Energieforschung e.V. (ZAE Bayern)
  - **A4**: TUM, Gebäude 5701, Munich School of BioEngineering (ehm.IMETUM)
  - **A5**: SWH, Wohnheim Enzianstraße (Garching II)
  - **A6**: TUM, Gebäude 5209, (alter) Reaktor-Betriebs- und Laborgebäude
  - **A7**: TUM, Gebäude 5210, (alter) Reaktor-Betriebszentrale
  - **A8**: TUM, Gebäude 6102, Betriebsgebäude I
  - **A9**: SWH, Wohnheim Jochbergweg (Garching I)
  - **AA**: Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) gGmbH
  - **AB**: TUM/LMU, Maier-Leibniz-Laboratorium
  - **AC**: TUM, Gebäude 5402, Chemiegebäude Bau Ch2
  - **AD**: TUM, Gebäude 5403, Chemiegebäude Bau Ch3
  - **AE**: TUM, Gebäude 5408, Hofgebäude I
  - **AF**: TUM, Gebäude 5401, Chemiegebäude Bau Ch1, Bibliothek, Hörsaal
  - **AG**: TUM, Gebäude 5406, Chemiegebäude Bau Ch6
  - **AH**: TUM, Gebäude 5407, Chemiegebäude Bau Ch7
  - **AI**: MPG, Institut für Plasmaphysik (IPP)
  - **AJ**: TUM, Gebäude 5204, Umformtechnik und Gießereiwesen
  - **AK**: TUM, Gebäude 5203, Bürogebäude (ehem. GRS)
  - **AL**: LMU, Gebäude 5109, Physikgebäude
  - **AM**: TUM, Gebäude 5202, Reaktorbereich, Zyklotron
  - **AN**: TUM, Gebäude 5302, Mensa, Raumfahrttechnik, Campus Cneipe
  - **AO**: TUM, Gebäude 5219, Verwaltungsstelle
  - **AP**: TUM, Gebäude 5215, Reaktorstation
  - **AQ**: TUM, Gebäude 5107, Physik II
  - **AS**: TUM, Gebäude 5201, Reaktorbereich
  - **AT**: TUM, Gebäude 5101, Physikgebäude
  - **AU**: WMI, Gebäude 5213, Tieftemperaturforschung
  - **AV**: TUM, Gebäude 5103, Betriebsgebäude II (Siemensbau)
  - **AW**: TUM, Gebäude 5111, Wassergütewirtschaft
  - **AX**: TUM, Gebäude 5108, Infra-Schall-Labor in Messbunker (im Gelände)
  - **AY**: WSI, Gebäude 5112, Walter-Schottky-Institut
  - **AZ**: TUM, Gebäude 5130, Neubau Telefonzentrale
- **B: TUM-Stammgelände, TUM-Nordgelände und nächste Umgebung**
  - **B1**: TUM, Gebäude 0101, (N1) Hörsäle (U-Trakt)
  - **B2**: TUM, Gebäude 0102, (N2) Hochvolthaus
  - **B3**: TUM, Gebäude 0103, (N3) El.Masch./Geräte
  - **B4**: TUM, Gebäude 0104, (N4) Elektro Physik
  - **B5**: TUM, Gebäude 0105, (N5) Elektrotechnik
  - **B6**: TUM, Gebäude 0106, (N6) Materialprüfamt
  - **B8**: TUM, Gebäude 0108, (N8) Verfügungsgebäude
  - **B9**: TUM, Gebäude 0109 RAR, (N9) Reflexionsarmer Raum
  - **BA**: TUM, Gebäude 0510 (Stammgelände), TU-Verwaltung

  - **BB**: TUM, Gebäude 0501 (Stammgelände)
  - **BC**: TUM, Gebäude 0502 (Stammgelände)
  - **BD**: TUM, Gebäude 0503 (Stammgelände)
  - **BE**: TUM, Gebäude 0504 (Stammgelände)
  - **BF**: TUM, Gebäude 0505 (Stammgelände)
  - **BG**: TUM, Gebäude 0506 (Stammgelände-Theresianum)
  - **BH**: TUM, Gebäude 0507 (Stammgelände)
  - **BI**: TUM, Gebäude 0508 (Stammgelände), im Kern
  - **BJ**: Jakob-Balde-Haus
  - **BL**: TUM, Gebäude 0205
  - **BM**: TUM, Gebäude 0509 (Stammgelände)
  - **BN**: TUM, Gebäude 0206, Mensa
  - **BS**: TUM, Gebäude 0202
  - **BT**: TUM, StudiTUM Gebäude 0201
  - **BU**: TUM, Gebäude 0204
  - **BV**: TUM, Gebäude 0203
  - **BW**: TUM, Gebäude 2920
- **C: HSWT Triesdorf (CA-CZ)**
  - **C0**: TUM, Gebäude L, Bildungscampus Heilbronn
  - **C1**: TUM, Gebäude D, Bildungscampus Heilbronn
  - **CA**: HSWT, Triesdorf Gebäude A (Altbau)
  - **CB**: HSWT, Triesdorf Gebäude B (HTE)
  - **CC**: HSWT, Triesdorf Gebäude C (Neubau)
  - **CD**: HSWT, Triesdorf Gebäude D (Steingruberhaus und Container)
  - **CE**: HSWT, Triesdorf Gebäude E
  - **CF**: HSWT, Triesdorf Gebäude F
  - **CG**: HSWT, Triesdorf Gebäude G
  - **CH**: HSWT, Triesdorf, Gasthaus Adler
- **D: Block Theresienstraße /Barer Straße /Gabelsbergerstraße /Türkenstraße**
  - **DA**: LMU, Block A
  - **DB**: LMU, Block B
  - **DC**: LMU, Block C
  - **DN**: Neue Pinakothek
  - **DO**: Alte Pinakothek
  - **DP**: Pinakothek der Moderne-Architekturmuseum
- **E: Oberwiesenfeld / ZHS**
  - **EC**: TUM, Gebäude 2940, Campus C, Sport Ausweichquartier O2
  - **ED**: TUM, Gebäude 2941, Campus D, Sport Ausweichquartier O2
  - **EF**: TUM, Gebäude 2315, ZHS, BFTS (Bayerisches Forschungs- und Technologiezentrum für Sportwissenschaft)
  - **EG**: TUM, Gebäude 2303, ZHS Kleine Halle
  - **EH**: TUM, Gebäude 2301, ZHS Spielhalle
  - **EK**: TUM, Gebäude 2303, ZHS
  - **EN**: TUM, Gebäude 2305-Zentralbau Nord
  - **EO**: Studentenviertel Olympisches Dorf
  - **ET**: TUM, Gebäude 2308, ZHS Tribüne
  - **EZ**: TUM, Gebäude 2306-Zentralbau Süd
- **F: Königsplatz**
  - **FA**: TUM, Gebäude 2906, Karlstraße 45
  - **FB**: Bau 5.2, Staatssammlung f. Anthropologie u. Paläoanatomie
  - **FC**: LMU Schleißheimer Straße 4
  - **FD**: TUM, Gebäude 2910-2911, Brienner Forum
  - **FE**: LMU, Haus der Kulturen, ZIKG

  - **FF**: HFF, Hochschule für Fernsehen und Film (HFF) Neubau
  - **FG**: LMU, Geologische und Geographische Institute
  - **FH**: TUM, Katholische Hochschulgemeinde an der TUM
  - **FI**:
  - **FJ**:
  - **FK**: Test Gebert, Gabelsbergerstraße 29
  - **FL**: TUM, Gebäude 0401, Verwaltung, Mathematik
  - **FM**: Musikhochschule, Luisenstraße 37a
  - **FN**: Gästeappartement Musikhochschule, Appartement 11
  - **FO**: Wohnheim K.St.V. Ottonia
  - **FP**: LMU, Paläontologie
  - **FR**: HMTM, Karolinenplatz 4 (ehem. Lotteriegebäude)
  - **FS**: HMTM, Musikhochschule
  - **FV**: Institut für Volkskunde
  - **FW**: Wohnheim der Ingeborg-van-Calker-Stiftung
  - **FY**: Ägyptische Staatssammlung (Neubau)
  - **FZ**: TUM, Gebäude 0305, (Südost 5) Block D (ehem. LRZ)

- **G: Westlich Ludwigstraße, südlich Akademiestraße, östlich Türkenstraße, nördlich Theresienstraße**
  - **G2**: IBZ, Amalienstraße 38
  - **GA**: LMU, Gebäude 0110, Akademiestraße 1
  - **GB**: LMU, Gebäude 0030, Hauptgebäude inkl. Turmgebäude, Bibliothek
  - **GC**: LMU, Fakultät für Geschichte (Historicum), Schellingstraße 12, Altbau in Amalienstraße 52
  - **GD**: LMU, Gebäude 0010, Hauptgebäude an der Adalbertstraße (Adalberttrakt)
  - **GE**: LMU, Gebäude 0000E, Hauptgebäude an der Amalienstraße (Amalientrakt)
  - **GF**: LMU, Gebäude 0090, Amalienstraße 54
  - **GG**: LMU, Gebäude 0252, Schellingstraße 7
  - **GH**: LMU, Fachbibliothek Philologicum
  - **GI**: MPG, Digital Library, MPI für Sozialrecht und Sozialpolitik (MPISOC)
  - **GJ**: LMU, Schellingstraße 5
  - **GK**: LMU, Gebäude 0020, Hauptgebäude/Kernbereich, Physik-Altbau, Salinenhof
  - **GL**: LMU, Schellingstraße 9
  - **GM**: LMU, Gebäude 0000M, Hauptgebäude/Mitteltrakt
  - **GN**: LMU, Amalienstraße 83
  - **GO**: LMU, Gebäude 0121, Vorder- und Rückgebäude, Philosophie
  - **GP**: LMU, Gebäude 0040, Philosophie
  - **GQ**: LMU, Gebäude 0122, Rechtsinformatik
  - **GR**: LMU, Gebäude 0200, Rückgebäude, Fak. für Kulturwissenschaften Bibliothek
  - **GS**: LMU, Gebäude 0203, Vordergebäude
  - **GT**: LMU, Amalienstraße 73
  - **GU**: LMU, Bioinformatik, Medieninformatik
  - **GV**: LMU, Gebäude 0120, Statistik, Ludwigstraße 33
  - **GW**: LMU, Gebäude 0000W, Hauptgebäude, Geschwister-Scholl-Platz 1, Nord
  - **GX**: LMU, Gebäude 0060, Schellingstraße 10
  - **GY**: LMU, Gebäude 0050, Schellingstraße 4
  - **GZ**: LMU, Gebäude 0000Z, Hauptgebäude, Telefonzentrale

- **H: Residenz und Umgebung**
  - **HA**: BAdW, Bau A (Turmbau), Akademiegebäude
  - **HC**: BAdW, Bau C, Akademiegebäude
  - **HK**: BAdW, Kapellenhof, Akademiegebäude
  - **HM**: Staatliche Münzsammlung München
  - **HP**: MPG, Hauptverwaltung
  - **HT**: LMU, Theaterwissenschaften, Bühne
  - **HZ**: BAdW, Bau B, Akademiegebäude

- **I: Campus Großhadern / Martinsried**
  - **IA**: LMU, FCP-A, Genzentrum, Molekularbiologie und Biochemie
  - **IB**: LMU, FCP-B, Pharmazeutische Biologie und Technologie
  - **IC**: LMU, Gebäude 2957, FCP-C, Pharmakologische Chemie
  - **ID**: LMU, FCP-D, Anorganische Chemie
  - **IE**: LMU, FCP-E, Physikalische Chemie
  - **IF**: LMU, FCP-F, Organische Chemie
  - **IG**: LMU, Neubau Bauabschnitt 2, Biologie I, Martinsried
  - **IH**: LMU, Jugendmedizin
  - **II**: LMU, Tiermedizin, Ausweichquartier in Planegg
  - **IJ**: Mensa Martinsried
  - **IK**: LMU, Gebäude 010-060, (Bettenhaus), Klinikum Großhadern, Rechenzentrum der Medizin
  - **IL**: LMU, Neubau Bauabschnitt 1, Biologie II, Martinsried
  - **IM**: MPG, Institut für Biochemie, Martinsried
  - **IN**: MPG, Institut für Neurobiologie, Martinsried
  - **IO**: LMU, Neubau BioSysM, Haus K (Erweiterung Genzentrum)
  - **IP**: Zentrum für Prionforschung
  - **IQ**: IZB, Gründerzentrum Biotechnologie, Martinsried
  - **IS**: Wohnheim Sauerbruchstraße
  - **IT**: Wohnheim Heiglhofstraße
  - **IU**: LMU, Bauamt
  - **IV**: Studentenbistro Martinsried
  - **IW**: TUM, Gebäude 2801, Wassergüte
  - **IZ**: LMU, Biomedizinisches Centrum (BMC)
- **J: Weihenstephan (inkl. Außenbezirke)**
  - **J0**: TUM, Gebäude 4321, TUM-Verwaltung (TBA)
  - **J1**: TUM, Gebäude 4320, Heizhaus
  - **J2**: HSWT, Zentrum für Angewandte Brau- und Getränketechnologie
  - **J3**: TUM, Gebäude 5403, Versuchsgut Dürnast, ehem. Rinderstall
  - **J4**: TUM, Gebäude 5401, Versuchsgut Dürnast, Gutshof
  - **J5**: TUM, Gebäude 4231, Versuchsgut Dürnast, LS Pflanzenernährung
  - **J6**: TUM, Gebäude 4232, Versuchsgut Dürnast, GHL 3
  - **J7**: TUM, Gebäude 4234 und 4235, Versuchsgut Dürnast, GHL 1 und 2
  - **JA**: HSWT, Gebäude 4199, Bioinformatik, (Altes Bauamt)
  - **JB**: TUM, Gebäude 4111, Versuchs- und Lehrbrauerei
  - **JC**: TUM, Gebäude 423/4224, (Neubau), Biowissenschaft/Gentechnik
  - **JD**: TUM, Gebäude 4225, Lebensmittelchemie u.Molekulare Sensorik
  - **JE**: Kinderkrippe Krabbelstube
  - **JF**: TUM, Gebäude 4129/4132, Aquatische Systembiologie 'Mühle'
  - **JG**: HSWT, Versuchsgut Grünschwaige
  - **JH**: TUM, Gebäude 4275, Stallgebäude
  - **JI**: IZB, Weihenstephan
  - **JJ**: TUM, Gebäude 4280, Servergebäude
  - **JK**: TUM, Gebäude 4384, Aufbereitungshalle für Gemüse
  - **JL**: TUM, Gebäude 4209, Landtechnik
  - **JM**: TUM, Gebäude 4211, Landtechnik
  - **JN**: TUM, Gebäude 4521-4524,Versuchsstation Viehhausen
  - **JO**: TUM, Gebäude 4318, Hans Eisenmann-Zentrum (Zentralinstitut für Agrarwissenschaften)
  - **JP**: TUM, Gebäude 4264, Protein Modelling
  - **JQ**: TUM, Gebäude 4103, Sammlungsbau
  - **JS**: TUM, Versuchsstation Kranzberger Forst
  - **JT**: TUM, Gebäude 4601-4620, Thalhausen
  - **JV**: TUM, Gebäude 4180-4192,Veitshof
- **K: Klinikum Rechts der Isar**

  - **K1**: TUM, Gebäude 561 — Chirurgische Klinik
  - **K2**: TUM, Gebäude 546
  - **K3**: TUM, Gebäude zwischen 523 und 507
  - **K4**: TUM, 2 kleine Gebäude zwischen 507 und 528
  - **K5**: TUM, Gebäude 1514, Interdisziplinäres Forschungsgebäude
  - **K6**: TUM, Gebäude 528, Ecke Troger- / Einsteinstraße
  - **K7**: TUM, Gebäude neben Gebäude 523
  - **K8**: TUM, Gebäude 541
  - **K9**: TUM, Gebäude 713, Lehr und Trainingszentrum (LUTZ)
  - **KA**: TUM, Gebäude 501, Hauptgebäude
  - **KB**: TUM, Gebäude 502
  - **KC**: TUM, Gebäude 503
  - **KD**: TUM, Gebäude 504
  - **KE**: TUM, Gebäude 507
  - **KF**: TUM, Gebäude 518, Psychosomatische Ambulanz
  - **KG**: TUM, Gebäude 523, Klinikum (ABCE-Fächer) (RZ)
  - **KH**: TUM, Gebäude 508
  - **KI**: TUM, Gebäude 509
  - **KJ**: TUM, Gebäude 510
  - **KK**: TUM, Gebäude 511
  - **KL**: TUM, Gebäude 505
  - **KM**: TUM, Gebäude 1536, Geschichte und Ethik der Medizin
  - **KN**: TUM, Gebäude 514
  - **KO**: TUM, Gebäude 716
  - **KP**: TUM, Gebäude 516
  - **KQ**: TUM, Gebäude 517
  - **KR**: TUM, Gebäude 512
  - **KS**: TUM, Trogerstraße 5
  - **KT**: TUM, Gebäude 513
  - **KU**: TUM, Gebäude 506
  - **KV**: TUM, Gebäude 520
  - **KW**: TUM, Gebäude 551, Hörsaalgebäude
  - **KX**: TUM, Gebäude 552
  - **KY**: TUM, Gebäude 557

- **L: Leopoldstraße vom Siegestor bis Münchner Freiheit mit Seitenstraßen**
  - **L1**: KHG, Studentencafe der Katholischen Hochschulgemeinde
  - **L3**: LMU, Gebäude 0601
  - **LA**: LMU, Gebäude 0602
  - **LB**: LMU, Gebäude 0603
  - **LC**: LMU, Leopoldstraße 11, 11a, 11b
  - **LD**: LMU, Center of Advanced Studies CAS
  - **LE**: LMU, Georgenstraße 11
  - **LF**: Studentinnenheim Sophie-Barat-Haus
  - **LG**: LMU, Georgenstraße 5
  - **LH**: LMU, Seniorenstudium
  - **LI**: frei
  - **LJ**: ABZ, Ausbildungszentrum für Pastoralreferenten
  - **LK**: LMU, Georgenstraße 7
  - **LL**: LMU, Soziologie
  - **LM**: Mensa, Leopoldstraße
  - **LN**: LMU, Leopoldstraße 44
  - **LO**: LMU Leopoldstraße 30
  - **LP**: Priesterseminar St. Johannes der Täufer
  - **LQ**: Studentenwohnheim Deutsche Burse e.V.

  - **LS**: LMU, Gebäude 0610
  - **LT**: LMU, Gebäude 0620
  - **LV**: LMU, Gebäude 0600
  - **LW**: HMTM Musikhochschule Außenstelle Wilhelmstraße
  - **LZ**: Staatsbibliothek

- **M: Garchinger Hochschulgelände 3**
  - **M7**: TUM, Garching, Gebäude 5142, Parkhaus 7
  - **MA**: TUM, Gebäude 8111, Schleißheimer Straße 90A
  - **MB**: TUM, Gebäude 5414, Neubau Zentrum Energie und Information (ZEI)
  - **MC**: TUM, Exzellenzcluster MIAPP (ehem. T1-Gebäude IPP)
  - **MD**: TUM, Gebäude 5622-Duschkontainer am Sportplatz
  - **ME**: TUM, Gebäude 5530-Exzellenzzentrum (vor Maschinenwesen)
  - **MF**: TUM, Gebäude 5410-Forschungszentrum für Katalyse CRC (Katum)
  - **MG**: Neubau Mensa Garching, Gebäude 5304
  - **MH**: TUM, Gebäude 5620, TUM Hall Interims Audimax I
  - **MI**: Metall-Innung München-Freising-Erding
  - **MJ**: TUM, Gebäude 5519, Leichtbauhalle (bei Imetum)
  - **MK**: Kinderhaus, Gebäude 5531 (hinter Maschinenwesen)
  - **ML**: LMU, Laboratory for Extreme Photonics (LEX), Center for Advanced Laser Applications (CALA)
  - **MM**: TUM, Gebäude 5413 BNMR (Bavarian Nuclear Magnetic Resonanz) Zentrum
  - **MN**: TUM, Gebäude 5116, ZNN Zentrum für Nanotechnologie und Nanomaterialien
  - **MO**: TUM, Garching, Gebäude 5416, Interims Audimax II
  - **MP**: TUM, Gebäude 8102, Business Campus Garching II
  - **MQ**: TUM, CPA
  - **MS**: TUM, Gebäude 5515, Zentrum für Softskills
  - **MT**: UnternehmerTUM Neubau + ECM Gebäude 5433
  - **MU**: TUM, Physik Untergrundlabor
  - **MV**: TUM, Garching, Gebäude 5532, StudiTUM
  - **MZ**: TUM, MaiTUM 2018, Festzelt

- **N: LMU, Tierärztliche Fakultät und Nano Institut, Schwabing**
  - **NA**: LMU, Gebäude C (früher 0802), Anatomie
  - **NB**: LMU, Gebäude J (früher 0828), Chirurgie der Schweine
  - **NC**: LMU, Gebäude G (früher 0824), Chirurgie
  - **ND**: LMU, Gebäude N (früher 0825), Chirurgie
  - **NF**: LMU, Gebäude P (früher 0823), Gynäkologie
  - **NG**: LMU, Gebäude E/F (früher 0820/0822), Gynäkologie
  - **NH**: LMU, Gebäude R (früher 0840), Hygiene
  - **NK**: LMU, Gebäude 0310, Zoologie Fischkrankheiten
  - **NL**: LMU, Gebäude L (früher 0827) Pharmazie
  - **NM**: LMU, Gebäude S (früher 0850), Mikrobiologie+Pathologie
  - **NN**: LMU, Gebäude T (früher 0851), Mikrobiologie
  - **NO**: LMU, Gebäude Q (früher 0835), Rechnerbetriebsgruppe
  - **NP**: LMU, Gebäude H (früher 0826), Pharmazie
  - **NQ**: LMU, Gebäude K (früher 0830), Pharmazie
  - **NS**: LMU, Gebäude V (früher 0860), Stallung
  - **NT**: LMU, Gebäude B (früher 0801), Tierzucht
  - **NY**: LMU, Gebäude A (früher 0800), Physiologie
  - **NZ**: LMU, Neubau Nano-Institut

- **O: LMU, Oettingenstraße 67**
  - **OK**: LMU, Baracke auf Parkplatz
  - **OZ**: LMU, Gebäudeteil Z, Hauptgebäude, Mitte

- **P: Campus Weihenstephan 1**

  - **P0**: Wohnheim Giggenhauserstraße (Weihenstephan II)
  - **P1**: Wohnheim Giggenhauserstraße (Weihenstephan IV)
  - **P2**: TUM, Gebäude 4323, Kfz-Mechanikwerkstatt
  - **P3**: FHG/IVV, Fraunhofer Gesellschaft
  - **P4**: TUM, Gebäude 4218, Zierpflanzenbau, Botanik, Mikrobiologie
  - **P5**: TUM, Gebäude 4153, Teilverwaltung TUM (früheres Verwaltungsgebäude der Molkerei)
  - **P6**: TUM, Gebäude 4307, Tierernährung Versuchsanlage
  - **P7**: Bayerische Staatsbrauerei Weihenstephan
  - **P8**: SWH Vöttinger Straße (Weihenstephan I)
  - **P9**: TUM, Gebäude 4317, Neubau Tierwissenschaften
  - **PA**: TUM, Gebäude 4378, Heizhaus
  - **PB**: HSWT, Gebäude 4375, SVA Lehrstuhl für Bodenkunde und Pflanzen
  - **PC**: HSWT, Gebäude 4376, SVA Lehrstuhl für Obstbau und Baumschulung
  - **PD**: TUM, Gebäude 4231/4232/4234/4235, Versuchsgut Dürnast
  - **PE**: HSWT, Gebäude 4383, Fachbereich Gartenbau, Technische Landwirtschaft
  - **PF**: HSWT, Gebäude 4379, SVA Lehrstuhl für Zierpflanzenbau
  - **PG**: TUM, Gebäude 4213, Lebensmitteltechnikum
  - **PH**: HSWT, Gebäude 4372, Hörsäle L-P, Staatliche Versuchsanstalt, Lehrstuhl für Obstverwertung
  - **PI**: TUM, Gebäude 4306, Tierernährung-Hauptgebäude
  - **PJ**: HSWT, Gebäude 4373, Hörsäle Lange Point, SVA Info-Stelle
  - **PK**: HSWT, Gebäude 4374, Hörsaal L-P, SVA Institut für Gemüsebau, Stauden und Gehölze
  - **PL**: HSWT, Gebäude 4386
  - **PM**: TUM, Gebäude 4304, Pflanzenbau
  - **PN**: HSWT, Gebäude 4377
  - **PO**: TUM, Gebäude 4308, Tierernährung-Institutsgebäude
  - **PP**: TUM, Gebäude 4309, Wirtschaftslehre des Gartenbaus
  - **PQ**: TUM, Gebäude 4313, Zierpflanzenbau
  - **PR**: HSWT, Gebäude 4179, Pappelallee
  - **PS**: TUM, Gebäude 4311, Zierpflanzenbau
  - **PT**: TUM, Gebäude 4108
  - **PU**: HSWT Gebäude 4123 (von HSWT freigegeben)
  - **PV**: HSWT, Gebäude 4171, Alte Baumschule (A10)
  - **PW**: HSWT, Gebäude 4173, Institutsgebäude (A4)
  - **PX**: HSWT, Gebäude 4174, Bibliothek (A8)
  - **PY**: Wohnheim Lange Point (Weihenstephan III)
  - **PZ**: TUM, Gebäude 4223, Anbau an Gebäude 4219, Genetik

- **Q: Campus Weihenstephan 2**
  - **Q0**: TUM, Gebäude 4219, Landpflege und Botanik
  - **Q1**: TUM, Gebäude 4221, Telefonzentrale
  - **Q2**: TUM, Gebäude 4277, Forstwissenschaft, FVA-Forstwissenschaftliche Versuchsanstalt
  - **Q3**: TUM, Gebäude 4238, Werksfeuerwehr
  - **Q4**: TUM, Gebäude 4106, Wirtschaftslehre des Landbaus
  - **Q5**: TUM, Gebäude 4107, Ernährungslehre
  - **Q6**: Dienstleister / Eltern-Kind, Gebäude 4254
  - **Q7**: HSWT, Gebäude 4176, Lehrgebäude (A1)
  - **Q8**: TUM, Gebäude 4212, Physik, Chemie, Zentrallaboratorium
  - **Q9**: HSWT, Gebäude 4125, Löwentorgebäude (A3)
  - **QA**: TUM, Gebäude 4124, FML neu-Zentrum für Milch- und Lebensmittel
  - **QB**: TUM, Gebäude 4130, ehemalige Datenverarbeitung
  - **QC**: TUM, Gebäude 4117, Grünlandlehre
  - **QD**: TUM, Gebäude 4109, Studierendenservice, LS f. Lebensmittelverpackungstechnik
  - **QE**: TUM, Gebäude 4101
  - **QF**: HSWT, Gebäude 4172, Stammgebäude (A5), Verwaltung (A6) und Salettl (A7)
  - **QG**: TUM, Gebäude 4102, Bibliothek und Dekanatsgebäude

  - **QH**: TUM, Gebäude 4105, Ökologischer Landbau, Grünlandlehre
  - **QI**: TUM, Gebäude 4214, Zentrales Hörsaalgebäude
  - **QJ**: HSWT, Gebäude 4276, Wald und Forstwirtschaft
  - **QK**: TUM, Gebäude 4210 Landtechnik
  - **QL**: TUM, Gebäude 4215, Zentrales Praktikagebäude
  - **QM**: TUM, Gebäude 4110, Brauerei I
  - **QN**: TUM, Gebäude 4119 / 4120
  - **QO**: TUM, Gebäude 4126, Lebensmittelverfahrenstechnik
  - **QP**: TUM, Gebäude 4114, Betriebshof
  - **QQ**: TUM, Gebäude 4115, Senger-Wohnhaus
  - **QR**: HSWT, Gebäude 4178, Kleine Kustermannhalle (A9)
  - **QS**: TUM, Gebäude 4226, Internationales Getränkewissenschaftliches Zentrum (iGZW)
  - **QT**: TUM, Gebäude 4217, Bodenkunde
  - **QU**: TUM, Gebäude 4113, Versuchs- und Lehrbrennerei, Mikrobiologie
  - **QV**: TUM, Gebäude 4116, Kinderkrippe "Kindervilla"
  - **QW**: TUM/HSWT Weihenstephan, Gebäude 4281, Zentrum für Naturwissenschaftliche Grundlagen, Gebäude D1
  - **QX**: TUM, Server Gebäuder WZW (Neubau)
  - **QY**: TUM, Gebäude 4220, Bibliothek Neubau
  - **QZ**: TUM, Gebäude 4216, Mensa
- **R: Hochschule München**
  - **RA**: HM, Gebäude A
  - **RB**: HM, Gebäude B
  - **RC**: HM, Gebäude C
  - **RD**: HM, Gebäude D
  - **RE**: HM, Gebäude E
  - **RF**: HM, Gebäude F
  - **RG**: HM, Gebäude G
  - **RH**: HM, Gebäude H
  - **RI**: HM, Erweiterungsbau Bibliothek
  - **RK**: HM, Gebäude K, Altbau
  - **RL**: HM, Gebäude L, Pasing, Neubau
  - **RM**: HM, Gebäude M
  - **RN**: HM, Gebäude N
  - **RR**: HM, Gebäude R1, R2, R3
  - **RS**: HM, Gebäude S
  - **RT**: HM, Gebäude T, Neubau
  - **RV**: HM, Lazarettstraße 67
  - **RW**: HM, Gebäude W
  - **RX**: HM, Gebäude 2201/2202, Vorder und Rückgebäude
  - **RY**: HM, Gebäude Y
  - **RZ**: HM, Gebäude Z, Kita Herzerl
- **S: LMU, östlich Ludwigstraße, nördlich Adalbertstraße**
  - **SA**: LMU, Bauamt
  - **SB**: Staatsbibliothek
  - **SC**: LMU, Schackstraße 4
  - **SD**: LMU, Ludwigstraße 14
  - **SE**: Hochschule für Philosophie (Medienethik, Philosophie und Leadership)
  - **SF**: LMU, Vestibülbau
  - **SG**: LMU Giselastraße 10
  - **SH**: LMU, Seestraße 13
  - **SI**: Wohnheim Kaulbachstraße, Marie-Antonie Haus
  - **SJ**: LMU, Juristisches Seminargebäude
  - **SK**: LMU, Gebäude 0407, Rückgebäude
  - **SL**: LMU, Gebäude 0410, Vordergebäude

  - **SM**: LMU Martiusstraße 4
  - **SN**: Wohnheim Georgianum
  - **SO**: LMU, Ostasieninstitut
  - **SP**: Historisches Kolleg
  - **SQ**: LMU, Kaulbachstraße 45
  - **SR**: SWH Newman-Haus
  - **ST**: LMU, (DAF, MCG) Schönfeldstraße 13
  - **SU**: LMU, Jura, Veterinärstraße 1
  - **SV**: LMU, Jura, Veterinärstraße 5
  - **SW**: Johannes-Hanselmann-Haus
  - **SX**: Bayerische Staatsbibliothek
  - **SY**: Hochschule für Philosophie, Institut für Gesellschaftspolitik

- **T: LMU, Innenstadtkliniken**
  - **TA**: LMU, Augenklinik
  - **TB**: LMU, Zahnklinik
  - **TC**: LMU, Chirurgische Klinik
  - **TD**: LMU, Frauenlobstraße 7a
  - **TE**: LMU, Schillerstraße 42-46
  - **TF**: LMU, Innenstadtkliniken, Bavariaring 19
  - **TG**: LMU, Gebäudekomplex Bereich Physiologie
  - **TH**: LMU, Medizinische Lesehalle
  - **TL**: LMU, Gebäudekomplex Nervenklinik
  - **TM**: LMU, Frauenklinik
  - **TP**: LMU, Kreislaufprophylaxe + Bauamt
  - **TQ**: LMU, Theoretische Institute, Pettenkoferstraße 12
  - **TR**: LMU, Theoretische Institute, Pettenkoferstraße 14
  - **TS**: LMU, Rechtsmedizin
  - **TW**: LMU Klinikum, Campus Innenstadt
  - **TZ**: LMU, Klinikum, Ziemssenstraße 1

- **U: Wissenschaftszentrum Straubing (TUM+HSWT)**
  - **U0**: TUM, Geb 76C, für Luftfahrt, Raumfahrt und Geodäsie, Ludwig-Bölkow-Campus
  - **U1**: TUM, Algentechnikum, Gebäude 78, Ludwig-Bölkow-Campus
  - **U2**: TUM, Gebäude 90B, Lehrstuhl LCC, Ludwig-Bölkow-Campus
  - **U3**: TUM, Gebäude 91.12, Lehrstuhl LCC, Ludwig-Bölkow-Campus Lageplan
  - **UA**: TUM/WZS, Gebäude 2929, Straubing Neubau
  - **UB**: WZS, Kompetenzzentrum Nachwachsende Rohstoffe
  - **UC**: TUM/WZS, Gebäude 2927, Straubing Klostertrakte
  - **UD**: TUM/WZS, Gebäude 3501, Straubing Fraunhofer Institut Projektgruppe BioCat
  - **UE**: TUM/WZS, Gebäude 3502, ehemalige VHS
  - **UF**: TUM/WZS, Gebäude 3503, ehem. Jugendamt
  - **UG**: TUM/WZS, Am Essigberg
  - **UH**: TUM/WZS, Nachhaltige Chemie
  - **UI**: TUM/WZS, Gebäude ?, Interimsgebäude

- **V: LMU, Oberschleißheim**
  - **VA**: LMU, Tiermedizin, Klinik für Pferde
  - **VC**: LMU Oberschleißheim Container, Gebäude 4924
  - **VH**: LMU, Versuchsgut St. Hubertus
  - **VM**: LMU, Moorversuchsgut Badersfeld
  - **VP**: LMU, Reptilienklinik Oberscheißheim, Gebäude 4052
  - **VR**: LMU, Klauentierklinik, Gebäude 4070
  - **VS**: LMU, Schleicherbau, Gebäude 4925
  - **VV**: LMU, Geflügelkrankheiten (Vogelklinik), Gebäude 4050
  - **VW**: Wohnheim Oberschleißheim

  - **VZ**: LMU, Tiermedizin, Gebäude 4057, Zentrale Einrichtungen

- **W: Garchinger Hochschulgelände 2**
  - **W0**: TUM, Gebäude 5500 (Bauteil 0 5510), Maschinenwesen
  - **W1**: TUM, Gebäude 5500 (Bauteil 1 5501), Maschinenwesen
  - **W2**: TUM, Gebäude 5500 (Bauteil 2 5502), Maschinenwesen
  - **W3**: TUM, Gebäude 5500 (Bauteil 3 5503), Maschinenwesen
  - **W4**: TUM, Gebäude 5500 (Bauteil 4 5504), Maschinenwesen
  - **W5**: TUM, Gebäude 5500 (Bauteil 5 5505), Maschinenwesen
  - **W6**: TUM, Gebäude 5500 (Bauteil 6 5506), Maschinenwesen
  - **W7**: TUM, Gebäude 5500 (Bauteil 7 5507), Maschinenwesen
  - **W8**: TUM, Gebäude 5500 (Bauteil 8 5508), Maschinenwesen
  - **W9**: TUM, Gebäude 5500 (Bauteil 9 5509), Maschinenwesen
  - **WA**: TUM, Gebäude 5222, FRM II, Zugangshalle
  - **WB**: TUM, Gebäude 5220, FRM II, Neutronenleiterhalle
  - **WC**: LRZ, Institutsgebäude 2
  - **WD**: Studentenhaus DOMINO
  - **WE**: Gebäude 7901, Speicherbibliothek der Bayerischen Staatsbibliothek
  - **WF**: Schotterparkplatz Garching
  - **WG**: GATE, Gründerzentrum
  - **WH**: Hochschulhaus Garching
  - **WI**: TUM, Gebäude 5600, Informatik / Mathematik
  - **WJ**: GALILEO
  - **WK**: TUM, Exzellenz-Cluster Universe (ehem. ITER-Gebäude)
  - **WL**: LRZ, Institutstrakt
  - **WN**: TUM, Gebäude 5131, FRM-Poststelle
  - **WO**: TUM, Gebäude 8101, Business Campus Garching I
  - **WQ**: TUM, Gebäude 5301, IAS-Gebäude
  - **WR**: LRZ, Rechnerwürfel
  - **WS**: TUM, Gebäude 5517, Halle 17, Maschinenwesen
  - **WU**: Garching U-Bahnhof Forschungsgelände
  - **WV**: Campus Garching, GE Global Research
  - **WX**: TUM, Gebäude 7910-Oskar-von-Miller-Turm (Wetterturm)
  - **WY**: TUM; Gebäude 5160, UCN-Testanlage (Tritron Hütte)
  - **WZ**: LRZ, Hörsaaltrakt

- **X: Kleinere Unterbezirke 1**
  - **X0**: Regionales Rechenzentrum Universität Erlangen
  - **X1**: Schülerforschungszentrum Berchtesgaden
  - **X2**: SWH, Studentenwohnheim Frauendorfer-Haus
  - **X3**: SMSB, Bayerisches Armeemuseum
  - **X4**: SMSB, Neues Museum Nürnberg
  - **X5**: SMSB, Deutsches Theatermuseum
  - **X6**: TUM, Gebäude 3901-3902 & 3904,Wassersportzentrum
  - **X7**: Dornach, Staatssammlung f. Anthropologie u. Paläoanatomie, Archiv
  - **X8**: SMSB, Museum ”Fünf Kontinente”
  - **X9**: TUM, Gebäude 3100, Feldstation Mülverstedt-Projektbüro Hainich
  - **XA**: TUM, Gebäude 2903, TU-Verwaltung-Haus Soller
  - **XB**: Erzbischöfliches Ordinariat München
  - **XC**: TUM, Gebäude 9001, Science & Study Centre, Kloster Raitenhaslach
  - **XD**: Fortiss-Institut, UCC
  - **XE**: LMU, Universitätsarchiv + Physik
  - **XF**: Landesfachstelle für das öffentliche Bibliothekswesen
  - **XG**: HMTM, Gasteig, Hochschule für Musik und Theater
  - **XH**: TUM Forschungsstation Berchtesgaden
  - **XI**: Teleworker Haimhausen

  - **XJ**: SWH, Wohnheim Josef-Wirth-Weg 19
  - **XK**: MPG Halbleiterlabor
  - **XL**: frei (früher Ludwig Bölkow Campus)
  - **XM**: TUM, Geriatronik-Forschungszentrum
  - **XN**: LMU, Geophysik Außenstelle Unterlippach
  - **XO**: Oberste Baubehörde
  - **XP**: LMU, Planegg
  - **XQ**: Porzellanikon, Staatliches Museum für Porzellan Hohenberg a. d. Eger / Selb
  - **XR**: LMU, Edmund-Rumpler-Straße 13
  - **XS**: TUM/LMU, Schneefernerhaus Zugspitze
  - **XT**: Test Unterbezirk
  - **XU**: Wohnheim Oskar-von-Miller-Forum (Haus der Bay. Bauwirtschaft)
  - **XV**: Studentenwohnheim Freimann
  - **XW**: MPI für Psychiatrie
  - **XX**: Ort unbekannt, bzw. LRZ ist nicht zuständig
  - **XY**: Heimarbeitsplätze der LRZ-Mitarbeiter
  - **XZ**: M-net Vermittlungsstelle
- **Y: Kleinere Unterbezirke 2**
  - **Y0**: Studentinnenheim Arme Schulschwestern Unterer Anger 17
  - **Y1**: Wohnheim Ludwigskolleg
  - **Y2**: Staatliches Textil- und Industriemuseum (TIM)
  - **Y3**: Sammlung Goetz
  - **Y4**: IFP, Staatsinstitut für Frühpädagogik
  - **Y5**: Museum für Franken
  - **Y6**: Glasmuseum Frauenau
  - **Y7**: Wohnheim Schwere-Reiter-Straße
  - **Y8**: St-Albertus-Magnus-Haus
  - **Y9**: Studentinnenheim Arme Schulschwestern Unterer Anger 2
  - **YA**: LMU Geisteswissenschaften
  - **YB**: LMU, Gebäude 3102 / 3103, Botanik
  - **YC**: TUM, Gebäude 0602 / 0603, Klinikum Biederstein
  - **YD**: John-Mott-Haus
  - **YE**: LMU, Schwere Reiter Straße 9 Nord
  - **YF**: BSB Landesfachstelle für das öffentliche Bibliothekswesen Außenstelle Würzburg
  - **YG**: AFK, Rosenheimer Straße 145
  - **YI**: LMU, Tiermedizin, Schwere-Reiter-Straße 9 Süd
  - **YJ**: ADBK, Akademie der Bildenden Künste
  - **YK**: BIOTOPIA, Maria-Ward-Straße 1a
  - **YM**: Stiftung für Arbeitsrecht (ZAAR)
  - **YN**: TUM, Klinikum Schwabing
  - **YO**: TUM, Gebäude 3101-3121, Versuchsanstalt für Wasserbau Obernach
  - **YP**: ISB und IFP
  - **YQ**: TUM, Gebäude 2401
  - **YR**: TUM, Gebäude 2805, Bauklimatik und Haustechnik
  - **YS**: LMU, Ludwigshöhe 8
  - **YT**: Wohnheim Biedersteiner Straße
  - **YU**: TUM/LMU, Gebäude 2804, Deutsches Museum
  - **YV**: Spanisches Kolleg
  - **YW**: LMU, CAP
  - **YY**: MPG Physik
  - **YZ**: frei
- **Z: Kleinere Unterbezirke 3**
  - **Z0**: Wohnheim Chiemgaustraße
  - **Z1**: Studentenstadt Freimann, SWH

- **Z2**: TUM, Gebäude 4401-4405, Limnologische Station, Iffeldorf
- **Z3**: Studentenwohnheim Lothstraße 62
- **Z4**: Wohnheim Kreittmayrstraße 14
- **Z5**: Wohnheim Agnes-/Adelheidstraße und Internationales Haus, DKFA
- **Z6**: Studentenwohnheim Haidpark
- **Z7**: Studentenwohnheim Felsennelkenanger (FNA, Panzerwiese)
- **Z8**: SWH Max-Bill-Straße
- **Z9**: Studienkolleg bei den Universitäten des Freistaates Bayern
- **ZA**: Stiftung Maximilianeum
- **ZB**: TUM, Gebäude 2907, Marsstraße 20-22
- **ZC**: TUM, Roboterwissenschaften und Systemintelligenz & Bayerische Staatsgemäldesammlungen BStGS
- **ZD**: Wohnheim Türkenstraße
- **ZE**: Massmannwohnheim
- **ZG**: Wohnheim Heidemannstraße
- **ZH**: DHM, Deutsches Herzzentrum
- **ZI**: IHF, Institut für Hochschulforschung
- **ZJ**: LMU, Sternwarte
- **ZK**: Johann-Michael-Sailer-Haus (Kath. SFH)
- **ZL**: LMU, Observatorium Wendelstein
- **ZM**: TUM, Gebäude 2601-2607, Pasing
- **ZN**: frei
- **ZO**: Hugo-Maser-Haus (Arcisheim)
- **ZP**: Bayerische Theaterakademie August Everding im Prinzregententheater
- **ZQ**: TUM, Gebäude 2908 Marsstraße 40; Denisstraße 1b, Gebäude 2909
- **ZR**: TUM, Gebäude 2926, Betriebswirtschaftslehre
- **ZS**: TUM, Gebäude 3201, Geodäsie, Außenstelle Eichenau
- **ZT**: LMU, Zentnerstraße 31
- **ZU**: Wohnheim Stiftsbogen
- **ZV**: Oekumenisches Studentenwohnheim, Oek-Heim
- **ZW**: TUM, Gebäude 2806, Lst. Restaurierung, Nationalmuseum, Archäologische Staatssammlung
- **ZX**: Telekom Vermittlungsstelle
- **ZY**: TUM, Gebäude 2103-2109, Verbrennungskraftmaschinen
- **ZZ**: ZSM, Zoologische Staatssammlung