Informationsveranstaltung für Netzverantwortliche im MWN

http://www.lrz.de/services/schulung/unterlagen/netzverantwortliche/

Agenda

- Aufgaben eines NV (Reiser)
- Neues im MWN (Reiser)
- Dienste im MWN (Tröbs)
- Sicherheitsmonitoring (Hommel)

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**)
- Firewall-Konfiguration

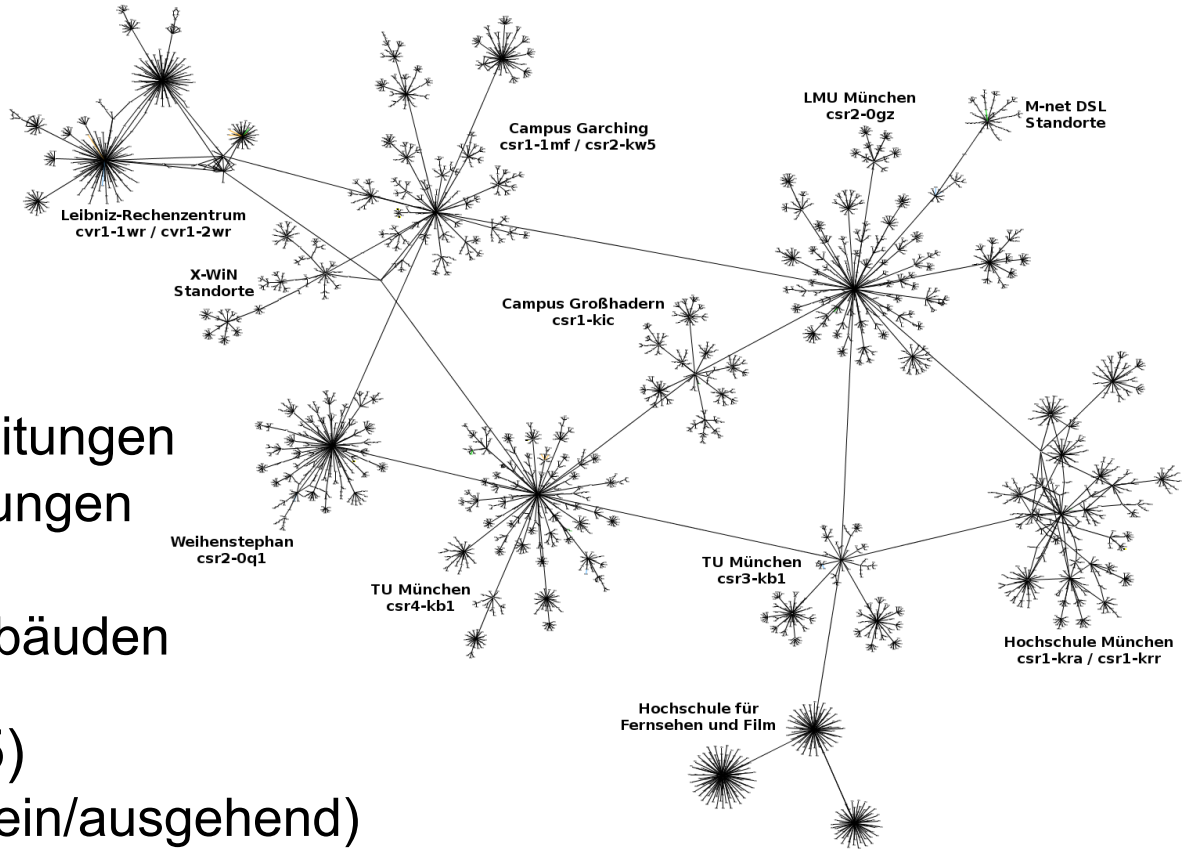
- Nützliche Informationen und Werkzeuge für NV:
  https://www.lrz.de/services/schulung/unterlagen/netzverantwortliche/nv-einfuehrung-2014.pdf

Agenda

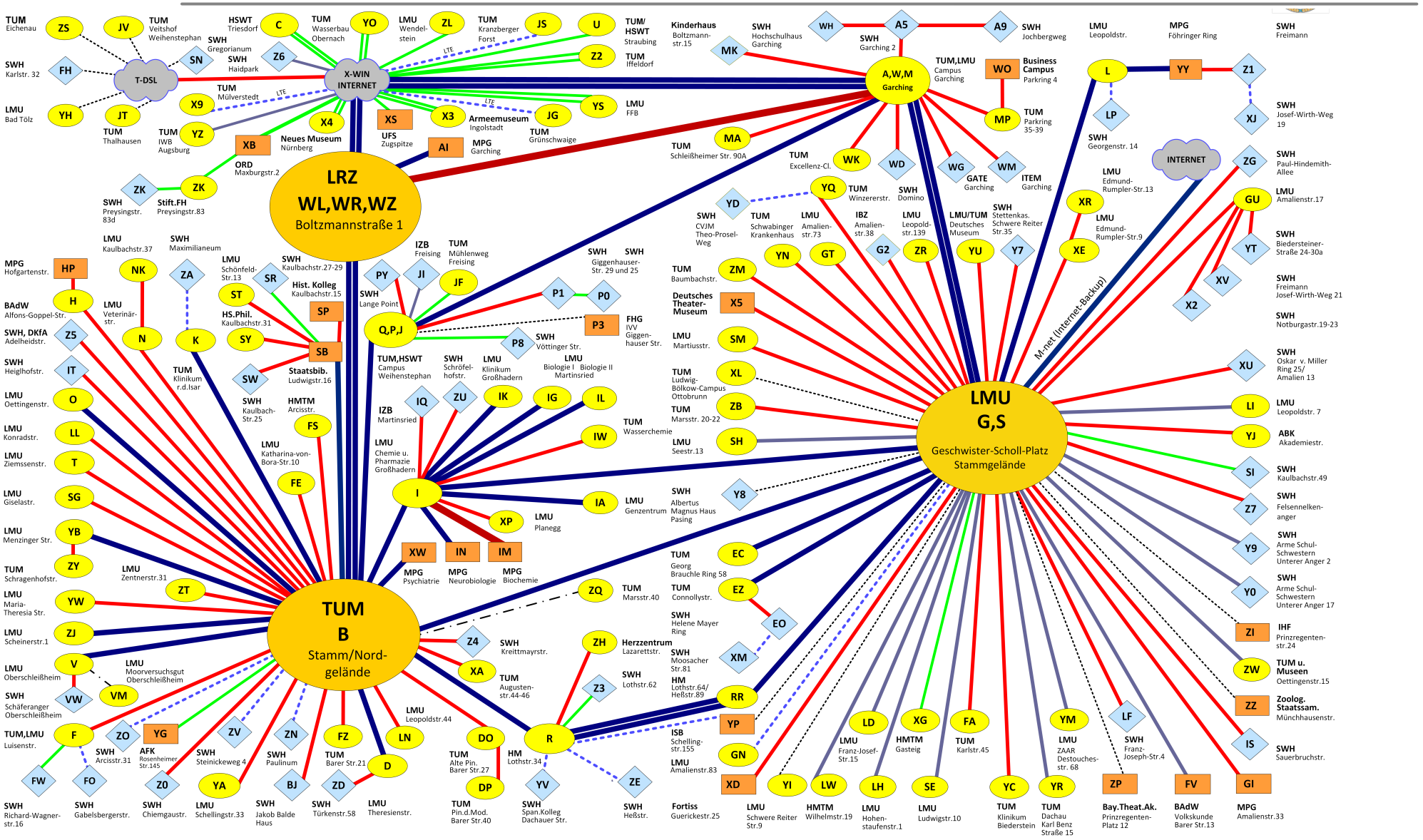
- Aufgaben eines NV
- Neues im MWN (Reiser)
  - Backbone (WDM, Ausfallsicherheit, Redundanz)
  - NIP
  - WLAN, Eduroam of Campus, @BayernWLAN
- Dienste im MWN (Tröbs)
- Sicherheitsmonitoring (Hommel)

MWN - Überblick

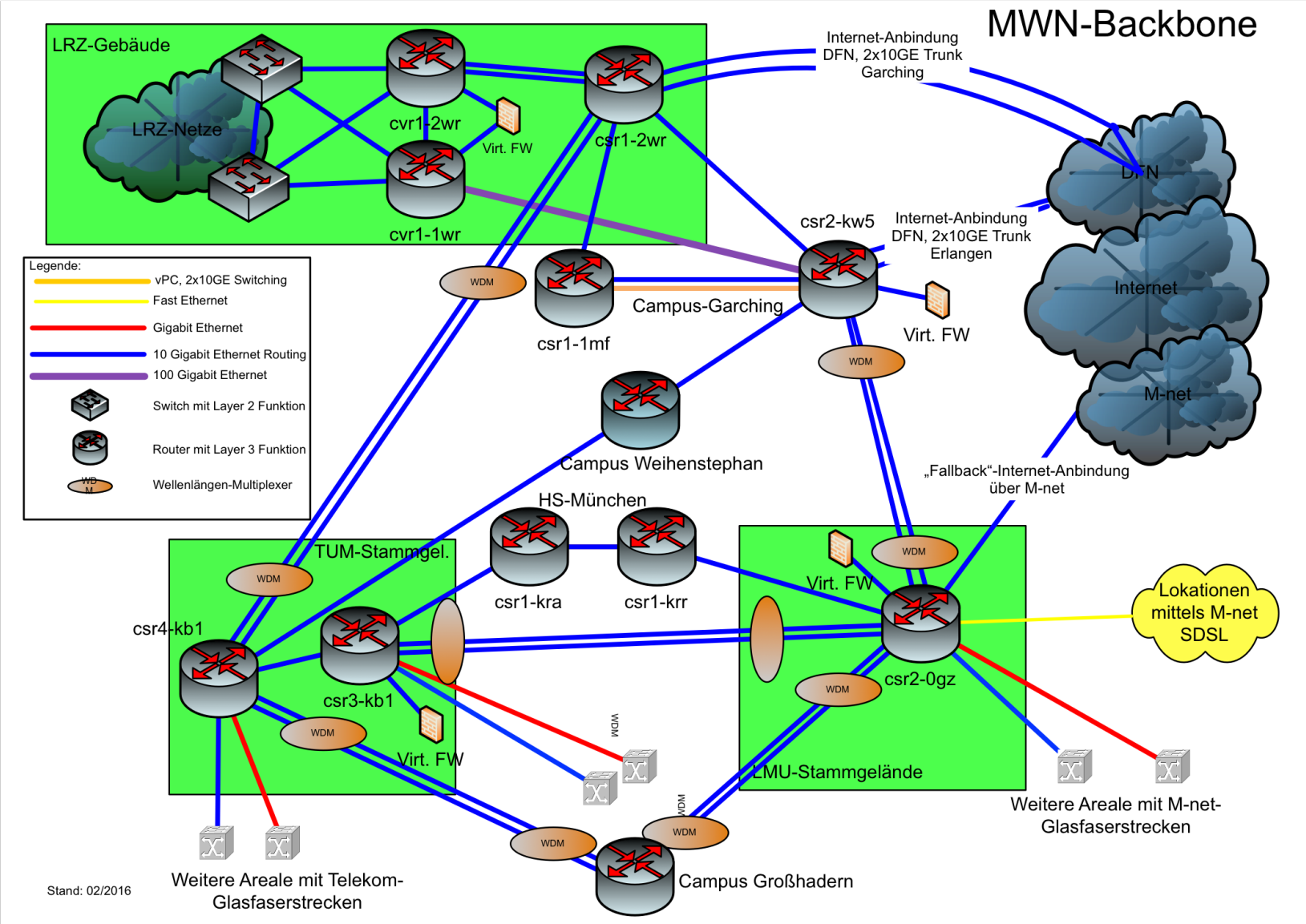
- Kommunikationsnetz für Münchner Hochschulen
  - 110.000 Studenten
  - 30.000 Mitarbeiter
- Kennzahlen
  - 16 Router
  - 1.500 Switches
  - > 3.000 Access points
  - 76 gemietete dark fibre Leitungen
  - 40+ private dark fibre Leitungen
  - > 150.000 Endgeräte
  - 50 Lokationen mit 540 Gebäuden
- Übertragene Daten (Mai 2015)
  - 1.100 / 800 Tbyte/Monat (ein/ausgehend)
  - 22 PByte/Monat über Backbone

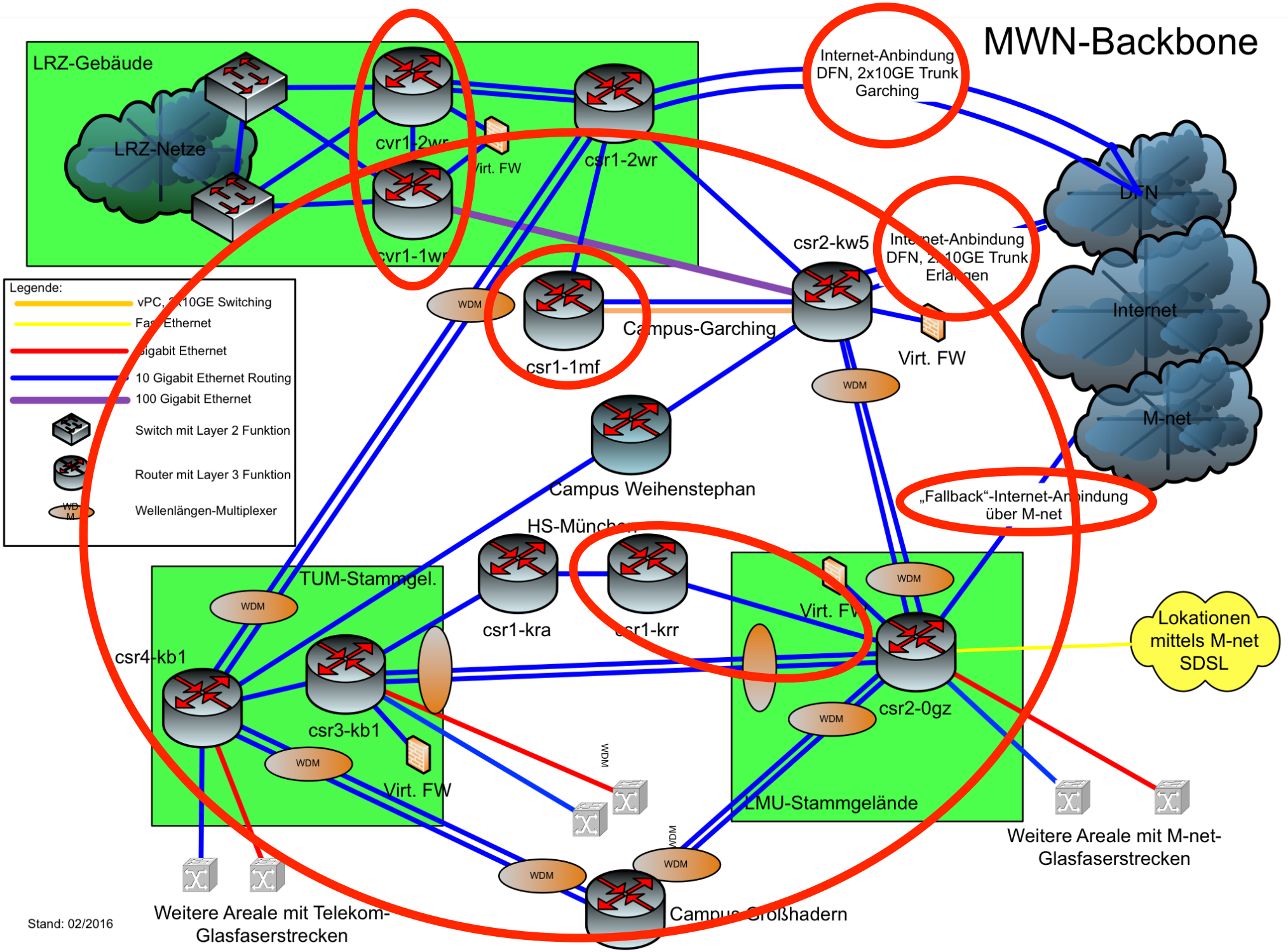


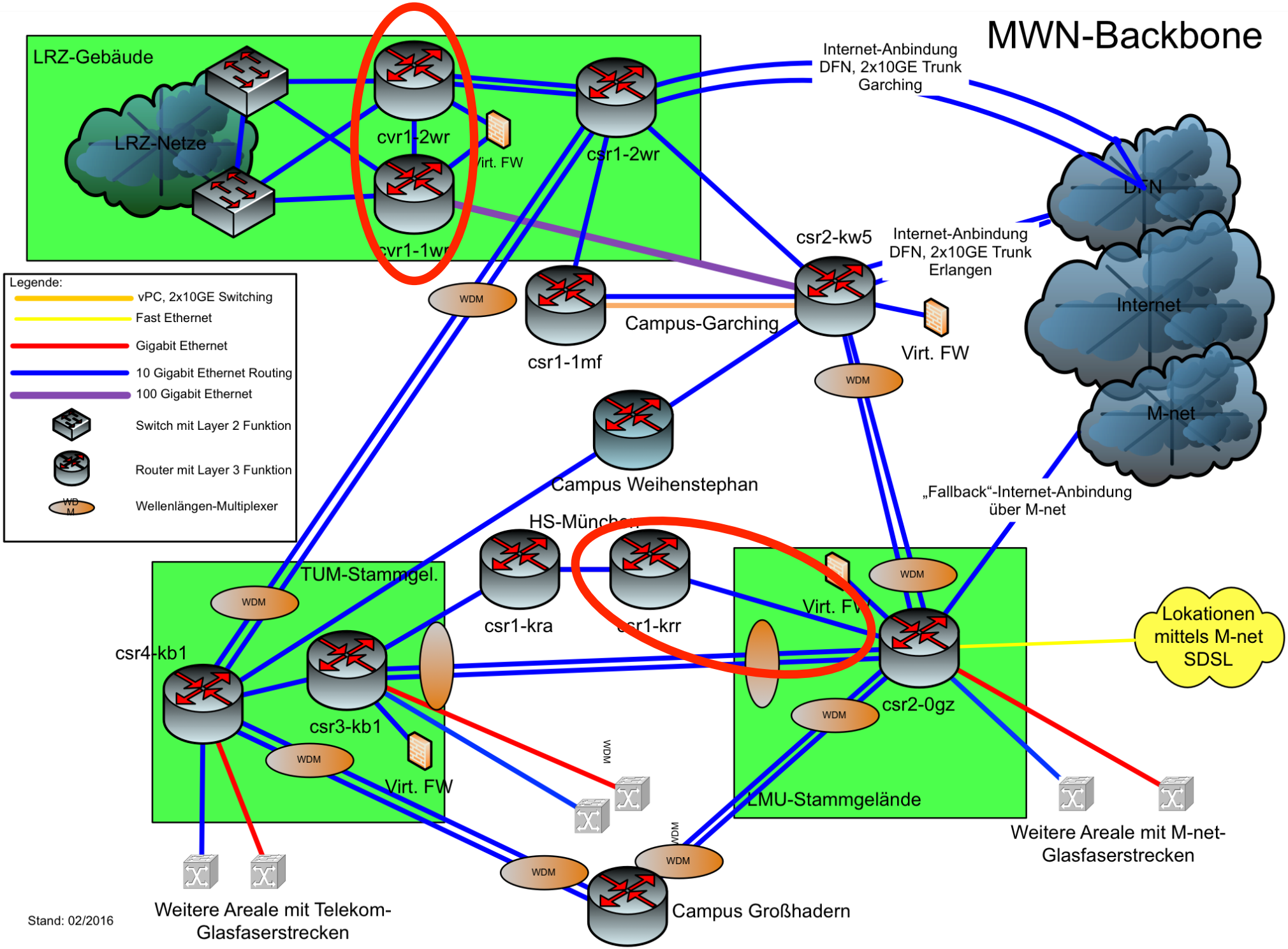
MWN Ende 2015

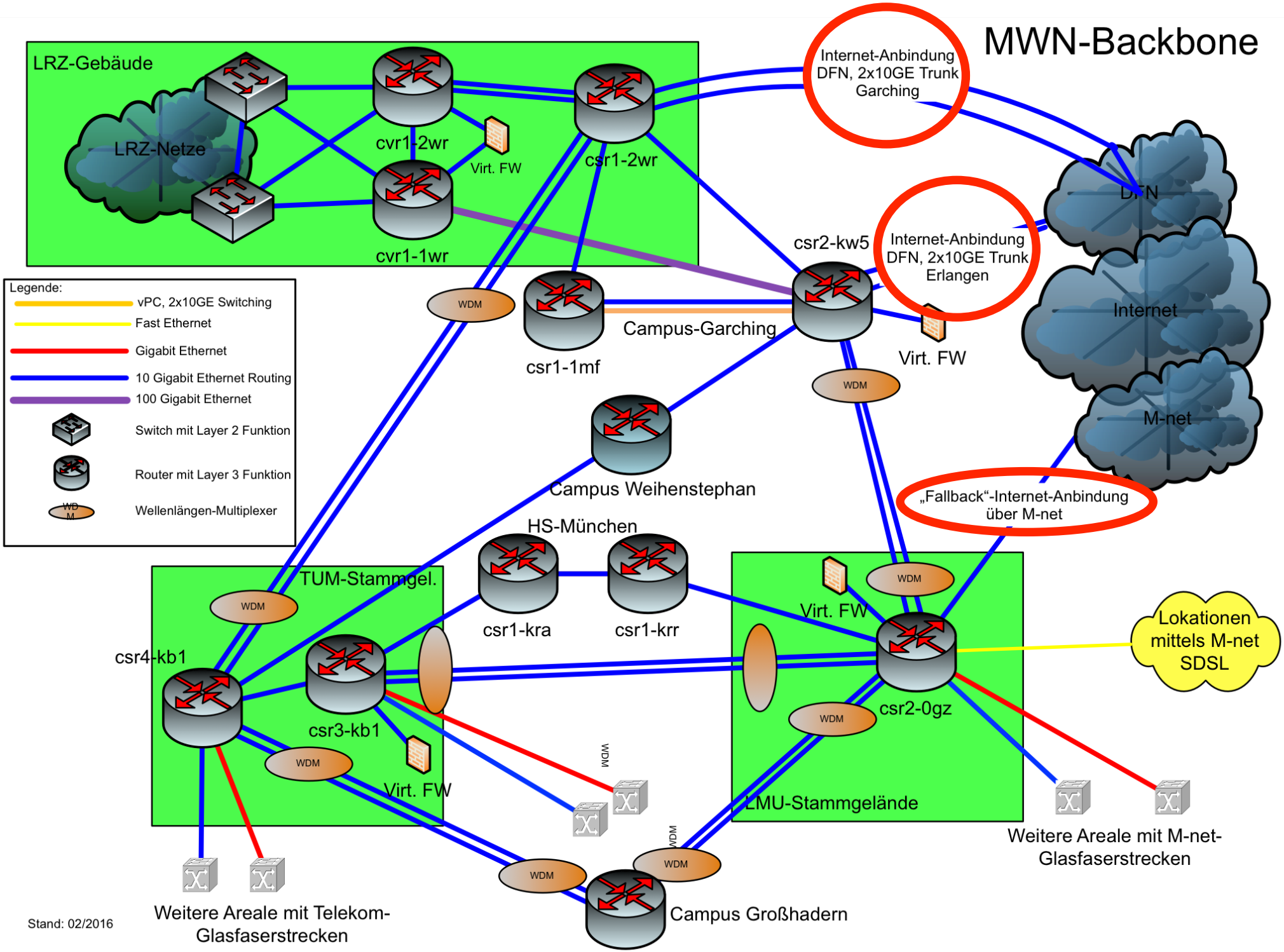


MWN Backbone



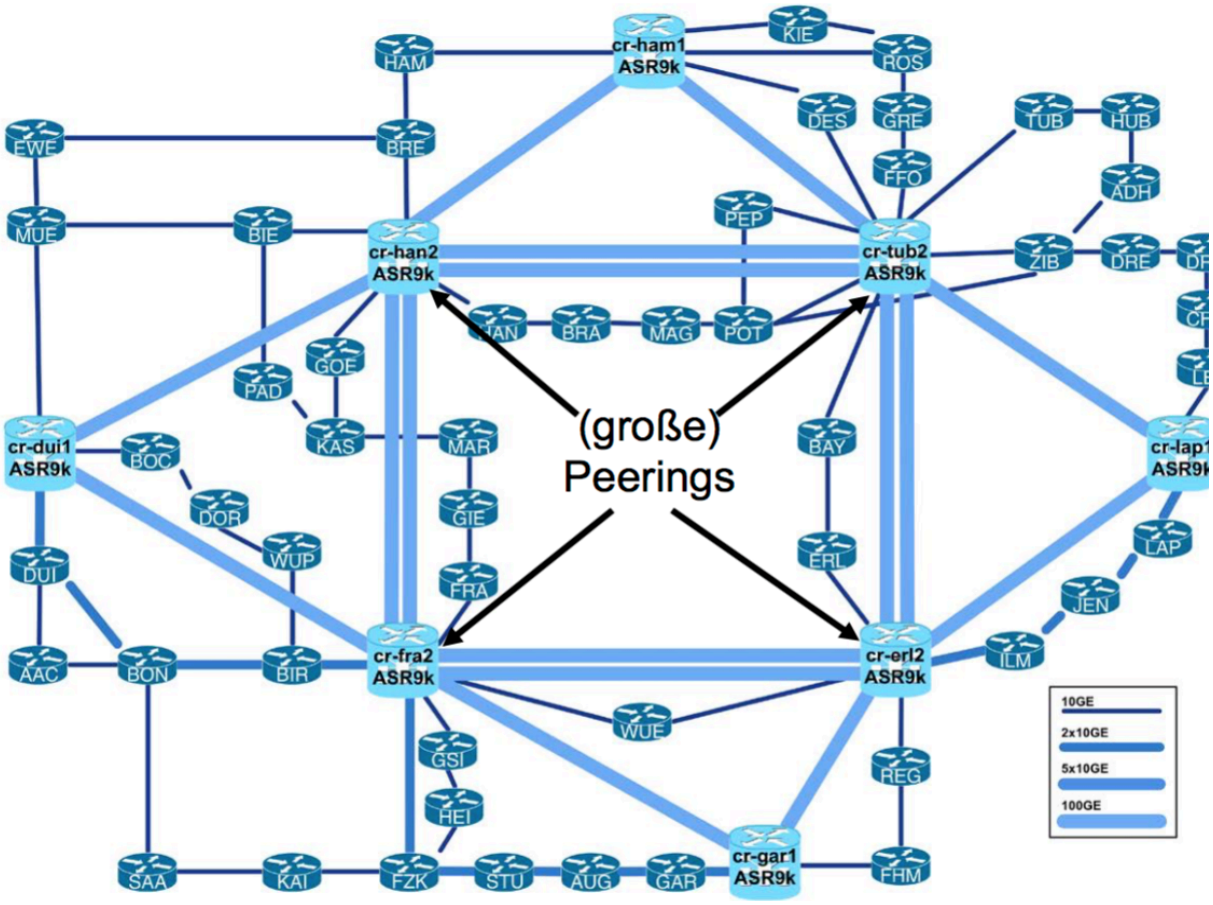

MWN-Backbone
LRZ-Gebäude
LRZ-Netze
cvr1-2wr
cvr1-1wr
Virt. FW
csr1-2wr
Internet-Anbindung DFN, 2x10GE Trunk Garching
DFN
Internet
M-net
csr2-kw5
Internet-Anbindung DFN, 2x10GE Trunk Erlangen
Legende:
vPC, 2x10GE Switching
Fast Ethernet
Gigabit Ethernet
10 Gigabit Ethernet Routing
100 Gigabit Ethernet
Switch mit Layer 2 Funktion
Router mit Layer 3 Funktion
Wellenlängen-Multiplexer
WDM
csr1-1mf
Campus-Garching
Virt. FW
Campus Weihenstephan
„Fallback"-Internet-Anbindung über M-net
HS-München
csr1-kra
csr1-krr
TUM-Stammgel.
csr4-kb1
csr3-kb1
Virt. FW
LMU-Stammgelände
csr2-0gz
Lokationen mittels M-net SDSL
Weitere Areale mit M-net-Glasfaserstrecken
Weitere Areale mit Telekom-Glasfaserstrecken
Campus Großhadern
Stand: 02/2016

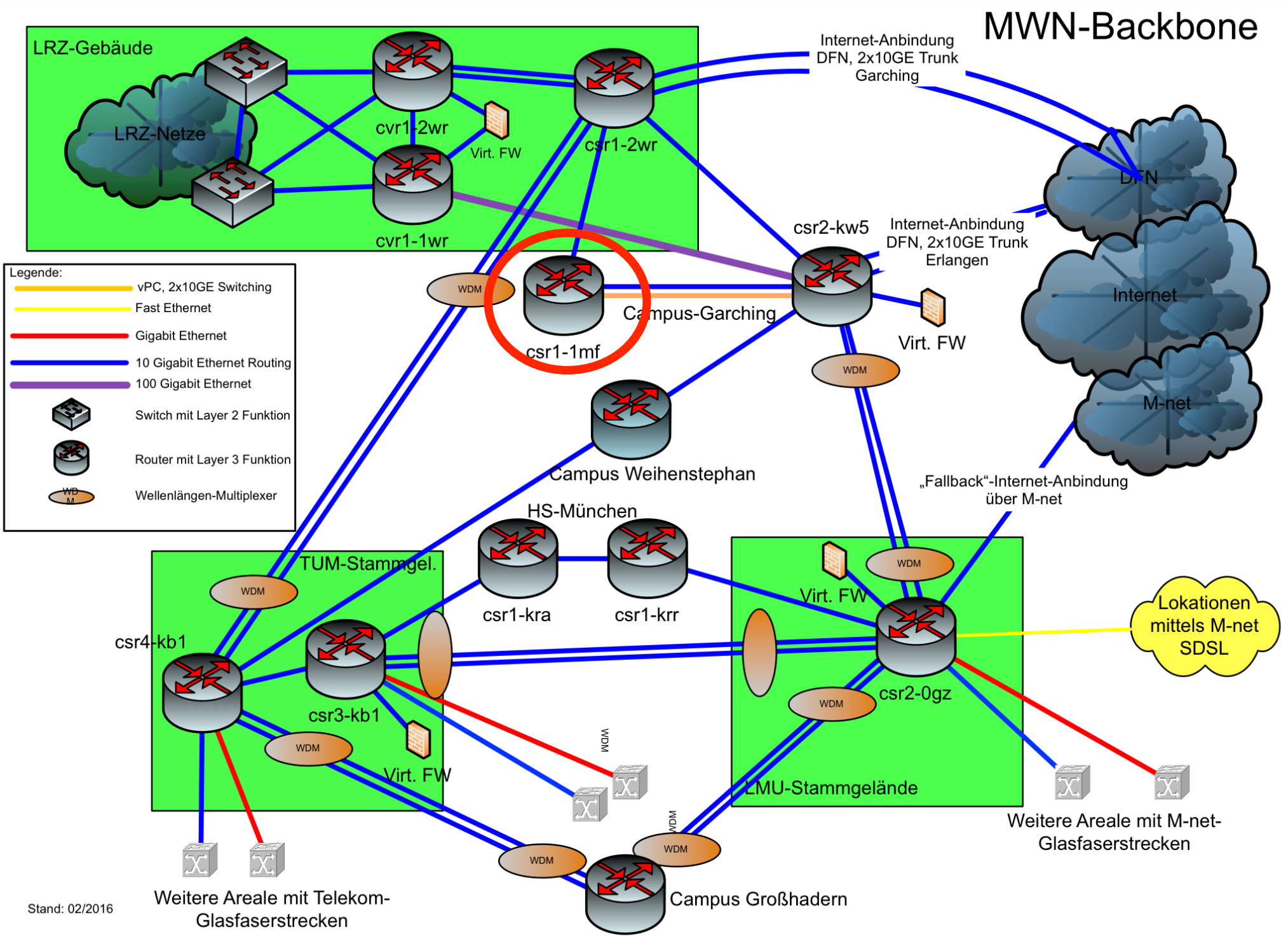

MWN-Backbone
LRZ-Gebäude
LRZ-Netze
cvr1-2wr
cvr1-1wr
Virt. FW
csr1-2wr
Internet-Anbindung
DFN, 2x10GE Trunk
Garching
DFN
Internet
M-net
csr2-kw5
Internet-Anbindung
DFN, 2x10GE Trunk
Erlangen
WDM
csr1-1mf
Campus-Garching
Virt. FW
WDM
Campus Weihenstephan
„Fallback“-Internet-Anbindung
über M-net
Legende:
vPC, 2x10GE Switching
Fast Ethernet
Gigabit Ethernet
10 Gigabit Ethernet Routing
100 Gigabit Ethernet
Switch mit Layer 2 Funktion
Router mit Layer 3 Funktion
Wellenlängen-Multiplexer
HS-München
csr1-kra
csr1-krr
TUM-Stammgel.
csr4-kb1
csr3-kb1
WDM
Virt. FW
Virt. FW
WDM
csr2-0gz
WDM
LMU-Stammgelände
Lokationen
mittels M-net
SDSL
WDM
WDM
WDM
WDM
Campus Großhadern
Weitere Areale mit M-net-
Glasfaserstrecken
Weitere Areale mit Telekom-
Glasfaserstrecken
Stand: 02/2016


MWN-Backbone
LRZ-Gebäude
LRZ-Netze
cvr1-2wr
cvr1-1wr
Virt. FW
csr1-2wr
Internet-Anbindung DFN, 2x10GE Trunk Garching
DFN
Internet
M-net
Internet-Anbindung DFN, 2x10GE Trunk Erlangen
csr2-kw5
Virt. FW
WDM
csr1-1mf
Campus-Garching
Campus Weihenstephan
„Fallback"-Internet-Anbindung über M-net
HS-München
csr1-kra
csr1-krr
TUM-Stammgel.
csr4-kb1
csr3-kb1
Virt. FW
LMU-Stammgelände
csr2-0gz
Lokationen mittels M-net SDSL
Weitere Areale mit M-net-Glasfaserstrecken
Weitere Areale mit Telekom-Glasfaserstrecken
Campus Großhadern
Stand: 02/2016
Legende:
vPC, 2x10GE Switching
Fast Ethernet
Gigabit Ethernet
10 Gigabit Ethernet Routing
100 Gigabit Ethernet
Switch mit Layer 2 Funktion
Router mit Layer 3 Funktion
Wellenlängen-Multiplexer

Internet Anbindung

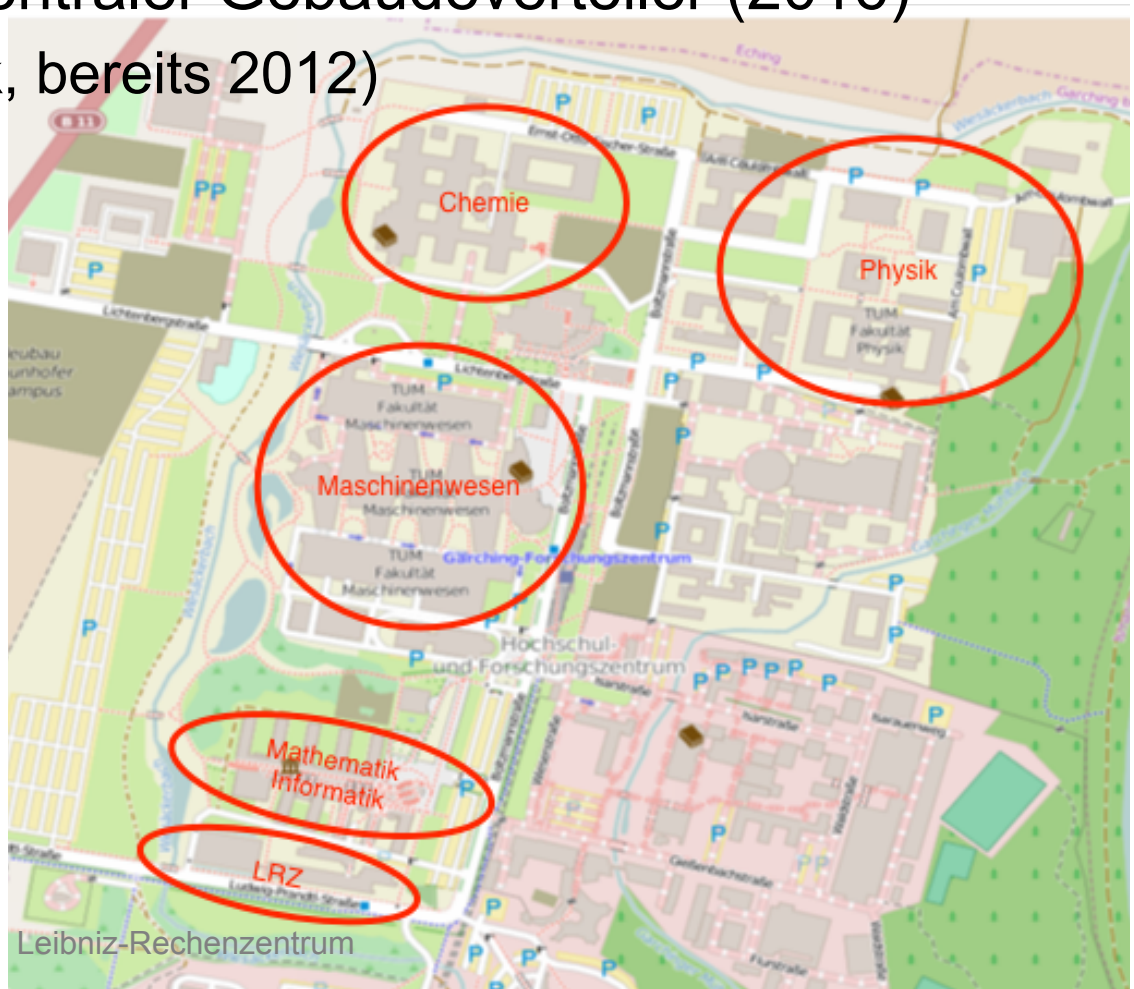
- Anbindung ans X-WiN
  - 2 Trunks mit je 2 x 10 GE
  - Direkt an den Super Core des DFN angebunden:
    - Erlangen
    - Garching
- Anbindung über M-net
  - Erhöhung auf 10 GE
  - Volumenbasierte Tarifierun



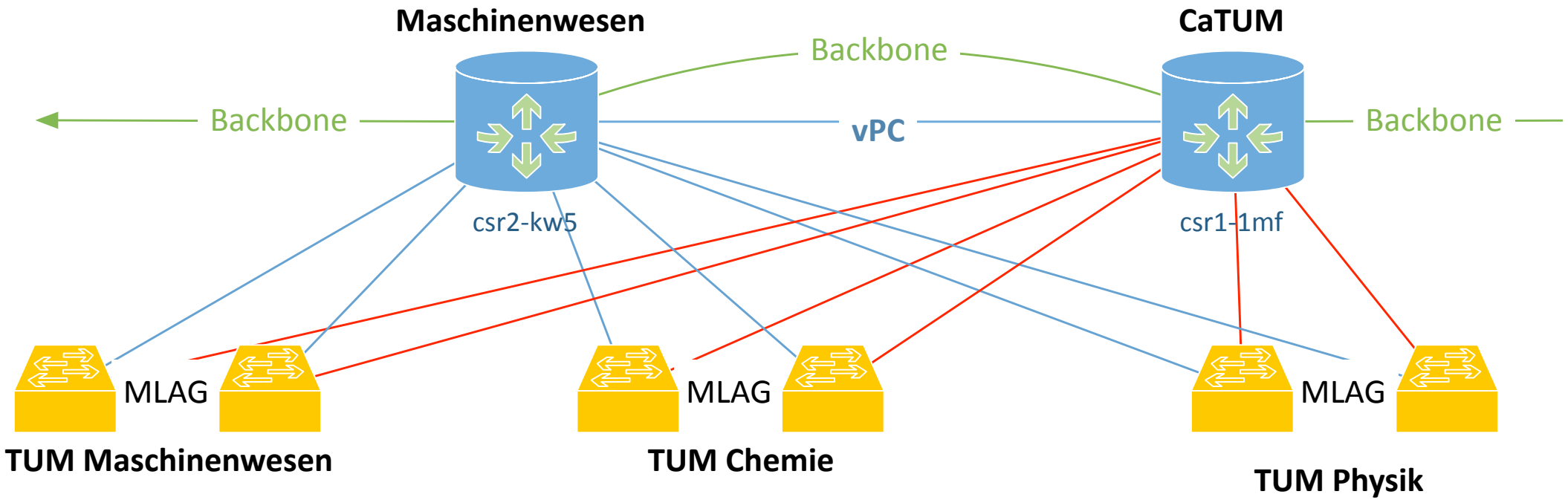

MWN-Backbone
LRZ-Gebäude
LRZ-Netze
cvr1-2wr
cvr1-1wr
Virt. FW
csr1-2wr
Internet-Anbindung
DFN, 2x10GE Trunk
Garching
DFN
Internet
M-net
csr2-kw5
Internet-Anbindung
DFN, 2x10GE Trunk
Erlangen
WDM
csr1-1mf
Campus-Garching
Virt. FW
WDM
Campus Weihenstephan
„Fallback"-Internet-Anbindung
über M-net
Legende:
vPC, 2x10GE Switching
Fast Ethernet
Gigabit Ethernet
10 Gigabit Ethernet Routing
100 Gigabit Ethernet
Switch mit Layer 2 Funktion
Router mit Layer 3 Funktion
Wellenlängen-Multiplexer
HS-München
csr1-kra
csr1-krr
TUM-Stammgel.
csr4-kb1
csr3-kb1
WDM
Virt. FW
Virt. FW
WDM
csr2-0gz
WDM
LMU-Stammgelände
Lokationen
mittels M-net
SDSL
Weitere Areale mit M-net-
Glasfaserstrecken
Weitere Areale mit Telekom-
Glasfaserstrecken
Campus Großhadern
Stand: 02/2016

Erhöhung der Redundanz am Campus Garching

- Gebäudebereiche über redundante LWLs erschlossen (2013)
- 2. zentraler Netzknoten im Katalysezentrum CaTUM (2015)
- Redundante Anbindung zentraler Gebäudeverteiler (2016)
  - (Mathematik / Informatik, bereits 2012)
  - Chemie
  - Physik
  - Maschinenwesen



Redundante Versorgung von Gebäuden



Legende

neuer Switch

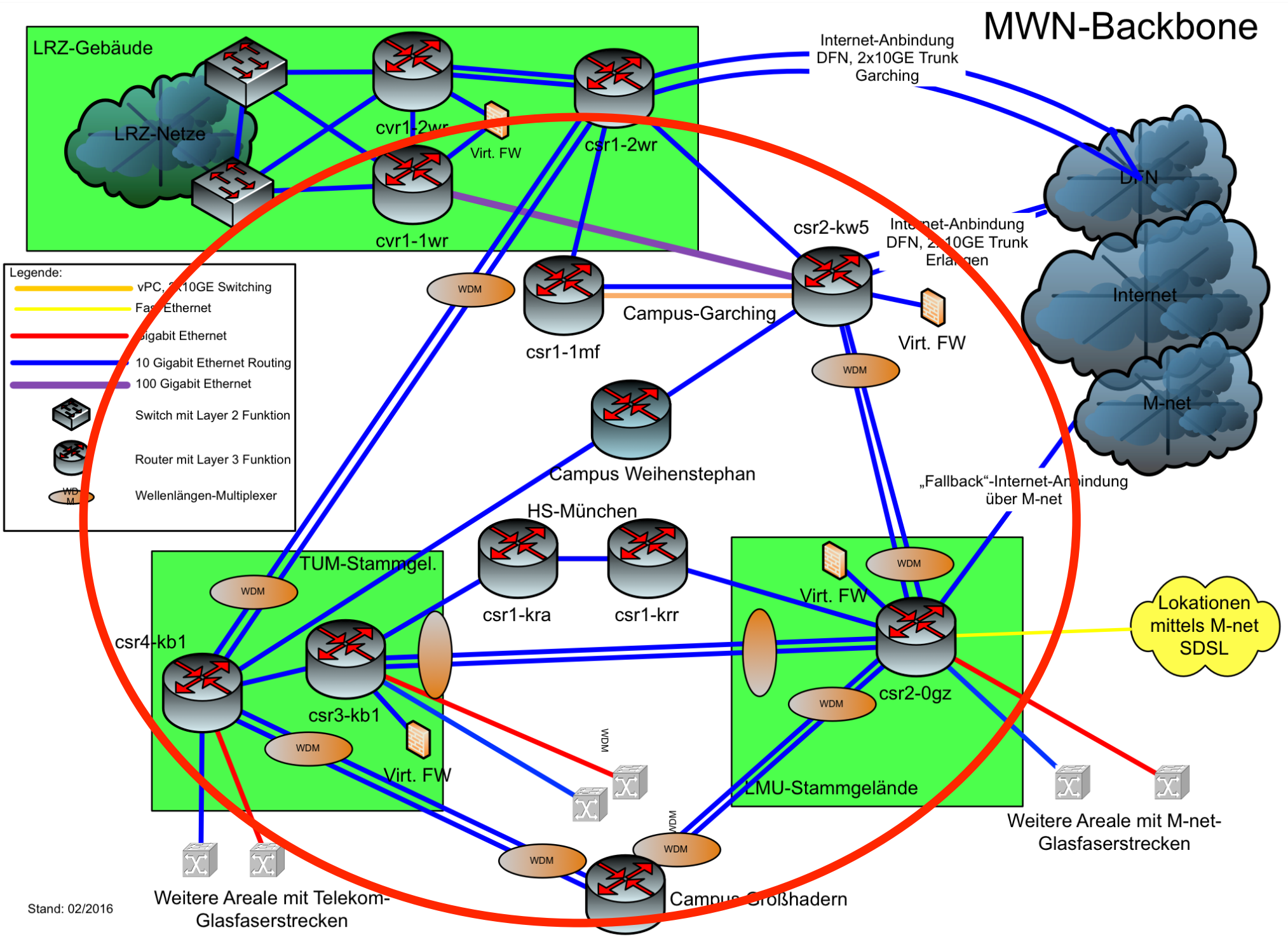
Router Bestand

MLAG = Multi-Chassis Link Aggregation

vPC = virtueller Port-Channel

alte Trasse

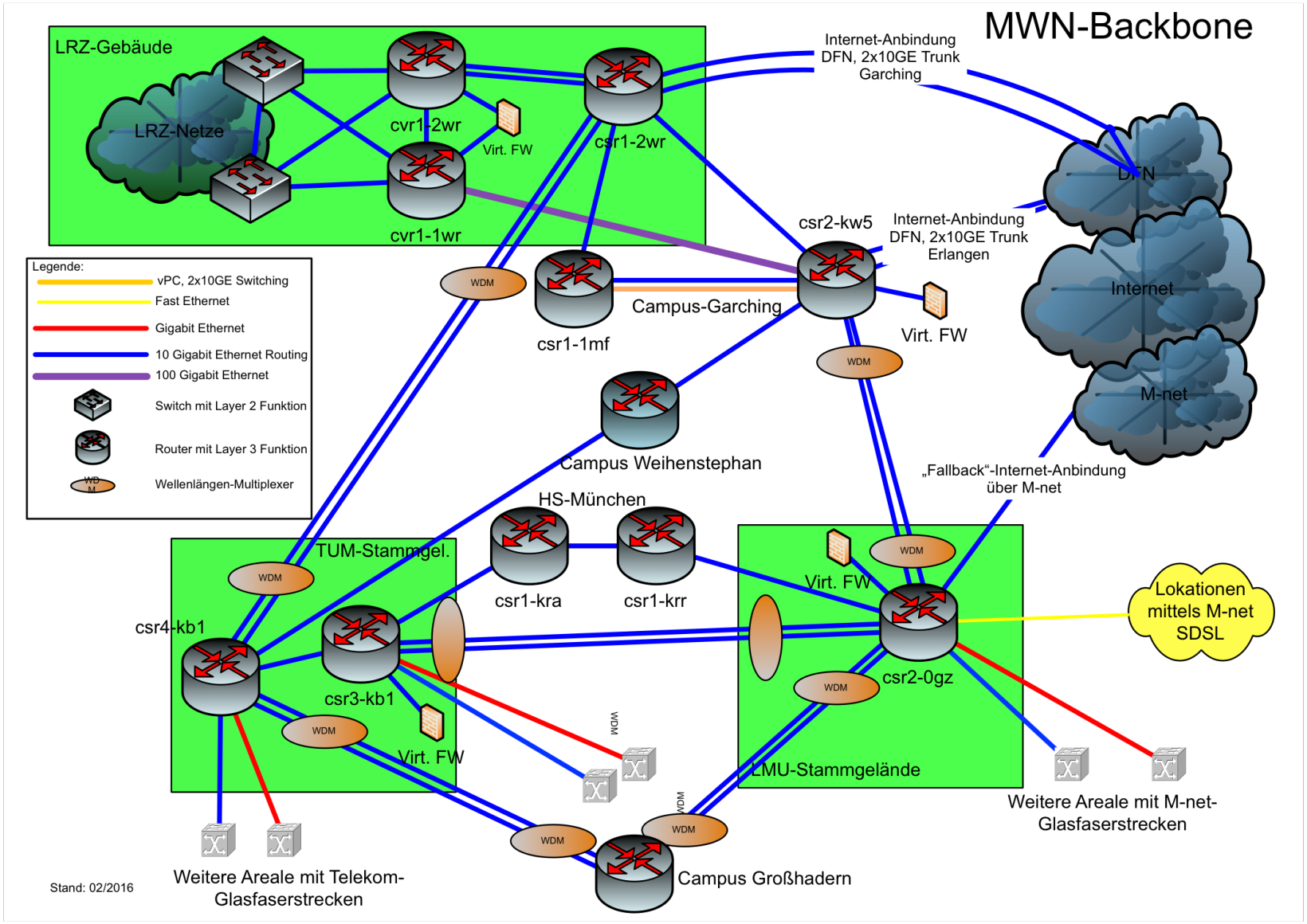
neue Trasse


MWN-Backbone
LRZ-Gebäude
LRZ-Netze
cvr1-2wr
cvr1-1wr
Virt. FW
csr1-2wr
Internet-Anbindung
DFN, 2x10GE Trunk
Garching
DFN
Internet
M-net
csr2-kw5
Internet-Anbindung
DFN, 2x10GE Trunk
Erlangen
WDM
csr1-1mf
Campus-Garching
Virt. FW
WDM
Campus Weihenstephan
„Fallback"-Internet-Anbindung
über M-net
HS-München
csr1-kra
csr1-krr
TUM-Stammgel.
WDM
csr4-kb1
csr3-kb1
WDM
Virt. FW
WDM
Virt. FW
WDM
csr2-0gz
WDM
LMU-Stammgelände
Lokationen
mittels M-net
SDSL
WDM
WDM
WDM
Weitere Areale mit M-net-
Glasfaserstrecken
Weitere Areale mit Telekom-
Glasfaserstrecken
Campus Großhadern
Legende:
vPC, 2x10GE Switching
Fast Ethernet
Gigabit Ethernet
10 Gigabit Ethernet Routing
100 Gigabit Ethernet
Switch mit Layer 2 Funktion
Router mit Layer 3 Funktion
WDM
Wellenlängen-Multiplexer
Stand: 02/2016

Erhöhung der Backbone-Bandbreite; WDM

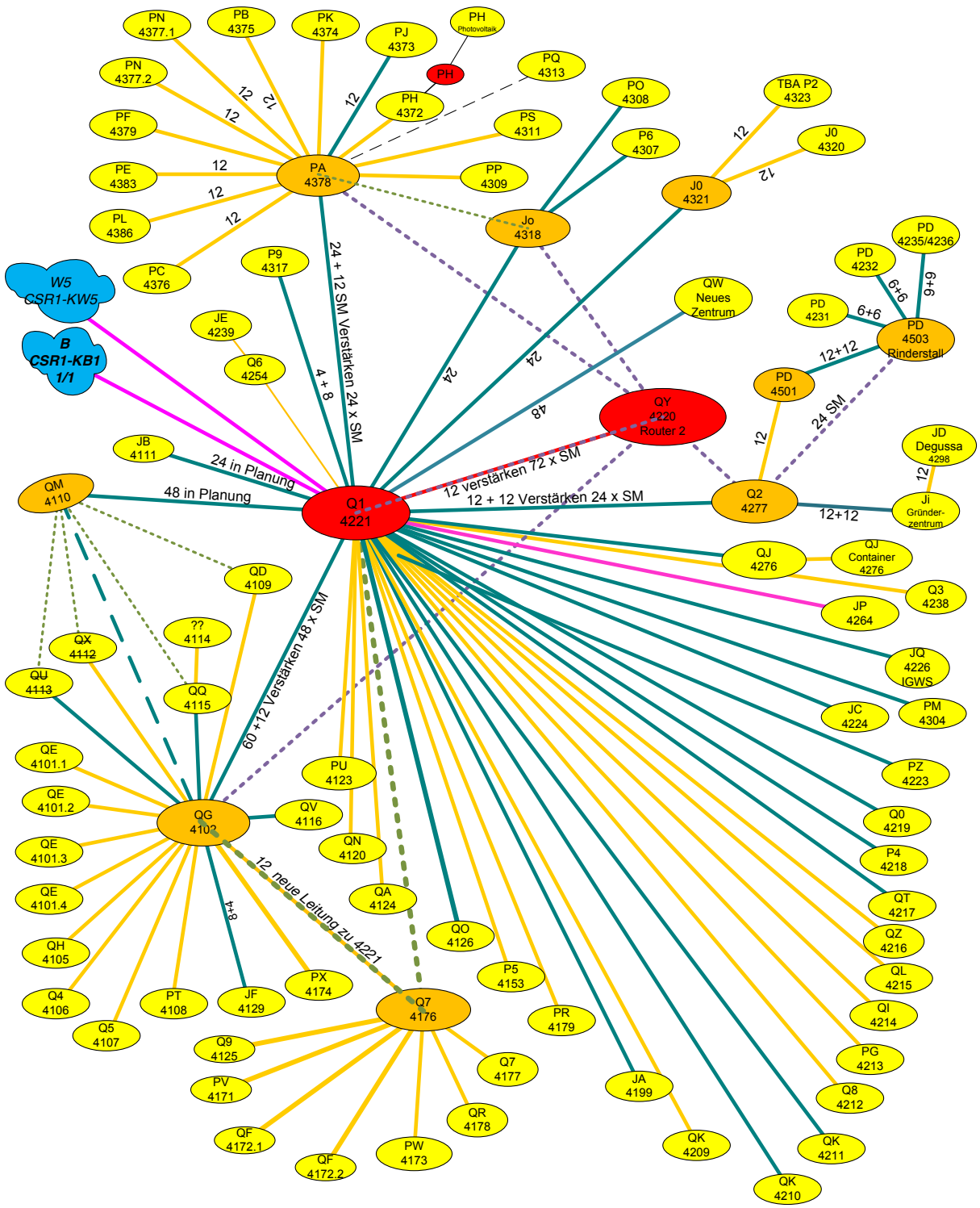
- Zwischen den Backbone-Standorten i.d.R. gemietete LWL (1 Faserpaar)
- WDM (Wave Division Multiplexer)
  - Übertragung mehrerer Wellenlängen (Kanäle) über 1 Faserpaar
  - Pro Wellenlänge Bandbreite (1, 10, 40, 100 GE) aktivierbar
  - Schaltung eigener Kanäle für die Max-Planck-Gesellschaft (MPG)
    - Martinsried zum Rechenzentrum der MPG in Garching
    - 1 x 100 Gbit/s, 1 x 10 Gbit/s
- Erhöhung der Bandbreite auf 2 x 10 GE im inneren Ring:
  - Großhadern – TUM, TUM-Garching, Garching-LMU, LMU-Großhadern, TUM-LMU

MWN Backbone: WDM



Erhöhung der Redundanz am Campus Weihenstephan

- LWL-Ertüchtigung (gestartet 2015)
  - Sehr viele Gebäude nur mit Multimode versorgt
  - Single-Mode-Nachrüstung
  - Anbindung der Gebäude über zwei Faserpaare (selbe Trasse, unterschiedliche Leerrohre) (2016)
- 2. Routerstandort
  - Auswahl eines zweiten Router-Standortes (Bibliothek)
  - Verstärkung der Querverbindung Bibliothek – Telefonzentrale (2015)



14.03.16

Leibniz-Rechenzentrum

Switch
Router
Multi / Mono
Multimode
10 GE SM
10 GE MuM

Agenda

- Aufgaben eines NV
- Neues im MWN (Reiser)
  - Backbone (WDM, Ausfallsicherheit, Redundanz)
  - NIP
  - WLAN, Eduroam of Campus, @BayernWLAN
- Dienste im MWN (Tröbs)
- Sicherheitsmonitoring (Hommel)

Netzinvestitionsprogramm II (NIP II)

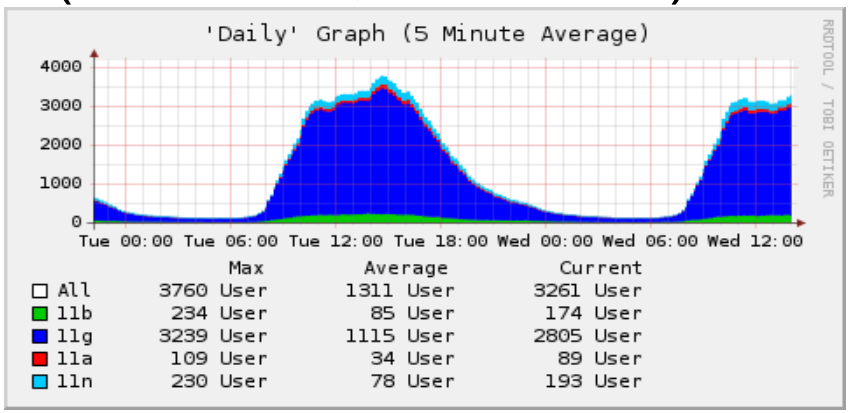
- Ertüchtigung der passiven Verkabelung an der LMU
- Aktuell in der Umsetzung
  - FCP: Gebäude B-F, Abschluss im Spätsommer 2016 geplant
  - Maria-Theresia-Straße 21
  - Observatorium Fürstenfeldbruck Ludwigshöhe 8 (ab April)
  - Schönleutner Str. 8 Oberschleißheim
  - Unterlippach
- Standorte 2016:
  - Kaulbachstr. 45
  - Leopoldstr. 30
  - Leopoldstr. 5
  - Schackstr. 4
- Standorte 2017
  - Leopoldstr. 15
  - Richard-Wagner-Str. 10
  - Akademiestr.1 / Ludwig 33
  - Schellingstr. 3
- Standorte 2018:
  - Schellingstr. 5, 7, 9, 10, 12
  - Amalienstr. 52, 83
  - Veterinästr. 13
  - Ludwig 33
  - Leo 3

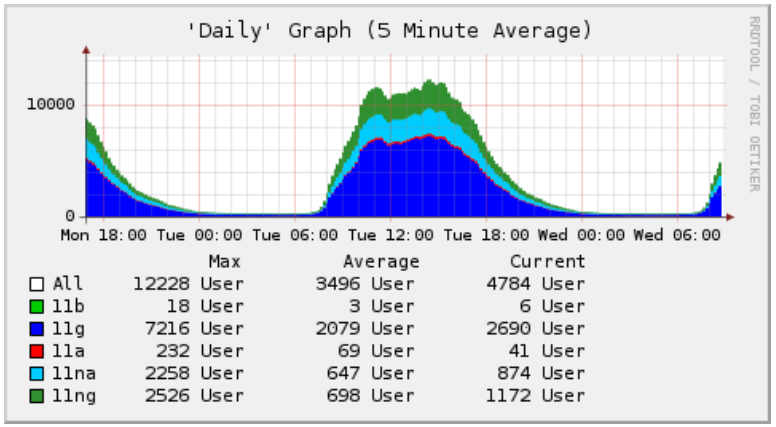
Agenda

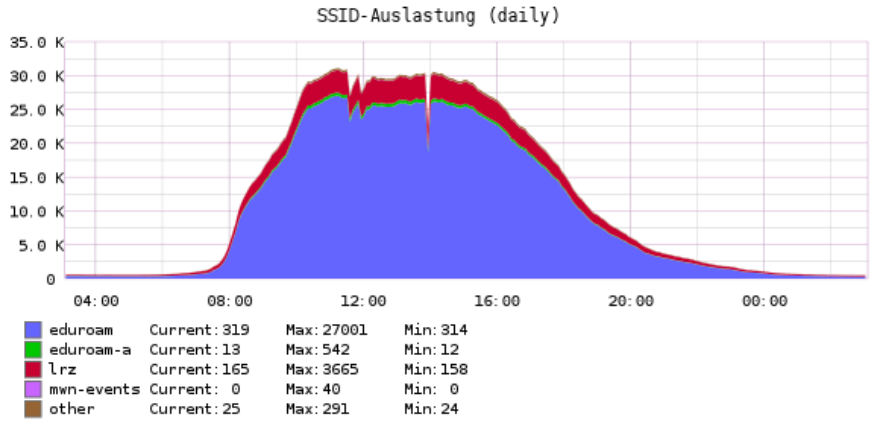
- Aufgaben eines NV
- Neues im MWN (Reiser)
  - Backbone (WDM, Ausfallsicherheit, Redundanz)
  - NIP
  - WLAN, Eduroam of Campus, @BayernWLAN
- Dienste im MWN (Tröbs)
- Sicherheitsmonitoring (Hommel)

Entwicklung WLAN im MWN

- Entwicklung seit letzten NV-Treffen (Okt. 2010, Jan. 2013)
- Anzahl der APs
  - 2010: 1.412 APs
  - 2013: 2.066 APs
  - 2016: 3.095 APs
- Anzahl der gleichzeitigen Nutzer
  - 2010: 3.760
  - 2013: 12.228
  - 2016: 33.184





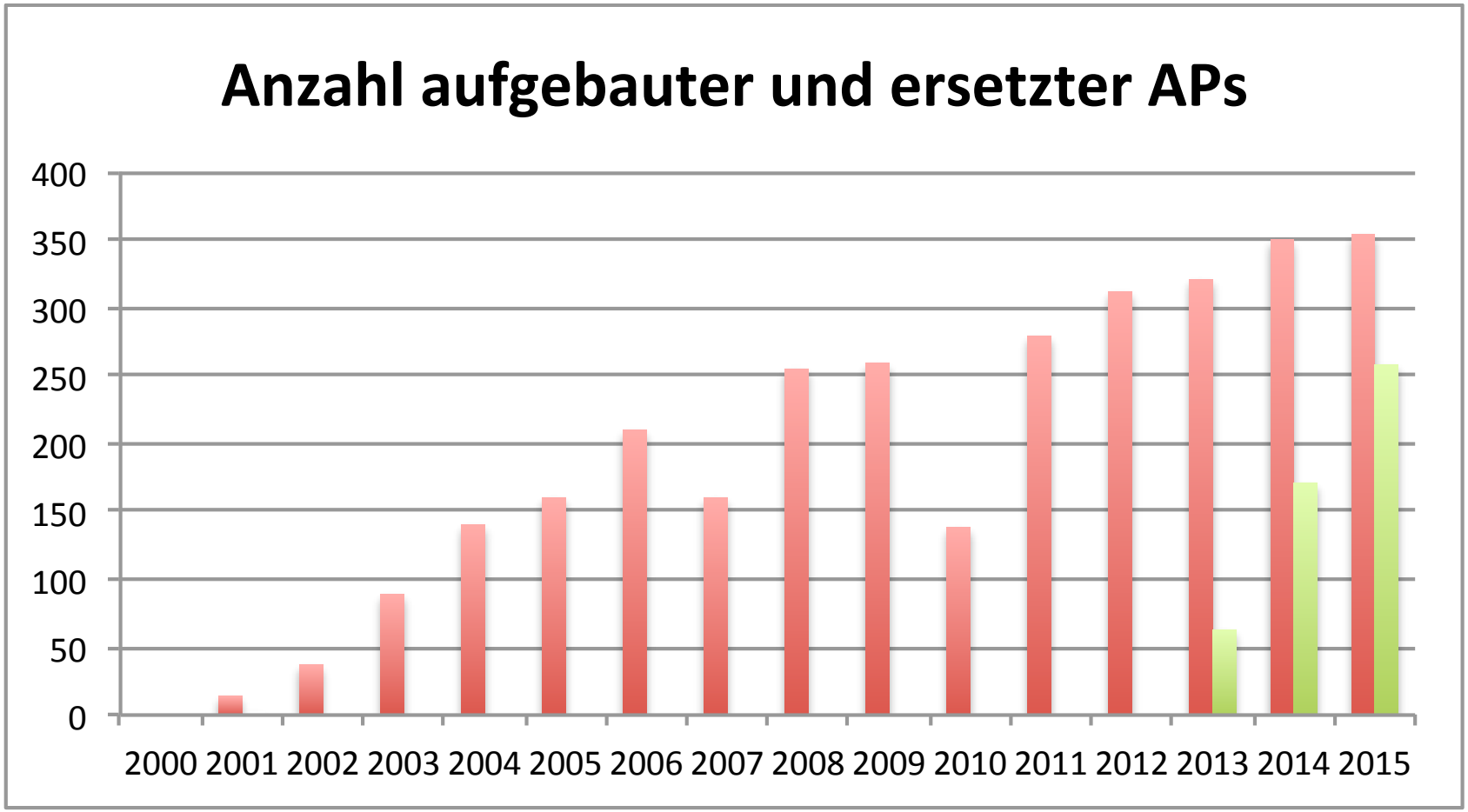


WLAN-Technik

- Controller-basierte APs von Alcatel-Lucent (seit 2013)
  - APs werden über Controller administriert und provisioniert
  - Controller an allen zentralen Netzknoten (B,G,I,Q,R,W)
  - Ausfallsicher: Master-Controller im LRZ kann bei Ausfall eines Controllers übernehmen
- Betrieblich sehr gute Erfahrungen

WLAN Herausforderungen

- Gemischte WLAN-Infrastruktur (HP, Alcatel)
- Knapp 1.500 HP-Accesspoints, davon ~500 veraltet
- Modernisierung wird zur Herausforderung



WLAN: hochbelastete Bereiche

- Nachverdichtung in hoch belasteten Bereichen:
  - Bibliotheken
  - Staatsbibliothek
  - Große Hörsäle
- 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 versorgen
- Wünsche nach APs über Ticket am Service-Desk: https://servicedesk.lrz.de

Veranstaltungs-WLAN: mwn-events

- Kein offenes WLAN mehr für Veranstaltungen
- Gesicherte SSID mwn-events
- Beantragung über Formular, unter:
  http://www.lrz.de/wlan
- Zugangsdaten pro Veranstaltung (Benutzername, Passwort)
- Entsprechendes Profil erhältlich über:
  http://www.lrz.de/services/netz/wlan/mwn-events/
- Erfahrungen 2015:
  - 528 Veranstaltungen beantragt, 503 genehmigt
  - 25.909 Nutzertage

Eduroam off Campus

- Stadtwerke München betreiben M-WLAN
  - Seit April 2014 wird eduroam auf allen (auch neu installierten) APs mit ausgestrahlt
  - derzeit 21 Standorte, s. http://www.muenchen.de/leben/wlan-hotspot/anleitung.html
- Augsburg:
  - Stadtbusse sind mit WLAN und eduroam ausgestattet
  - Straßenbahnen folgen nach bahnrechtlicher Zulassung
- Rosenheim; KomRo betreibt City-Netz und stahlt eduroam aus

@BayernWLAN

- BayKOM 2017 Ausschreibung; Los für offenes WLAN
  - eduroam soll neben @BayernWLAN ausgestrahlt werden
  - Mögliche Kooperation mit den Unis und Hochschulen: strahlen @BayernWLAN aus
  - Zuschlagserteilung noch 2016
- Prototyp für Kooperation im Wissenschaftszentrum Straubing
  - Kommerzieller Provider realisiert @BayernWLAN; IP-Adresse des Client kommt von Provider und nicht vom LRZ
  - Kommerzielle Anbindung über Vodafone, da Verkehr nicht über X-WiN geführt werden darf (100 Mbit/s Down; 12 Mbit/s Up)
  - Aktiv seit 1.12.15
- Straubing wird WLAN-Stadt; Koordinierungsbüro @BayernWLAN
  - @BayernWLAN wurde am 18.12.15 in Betrieb genommen

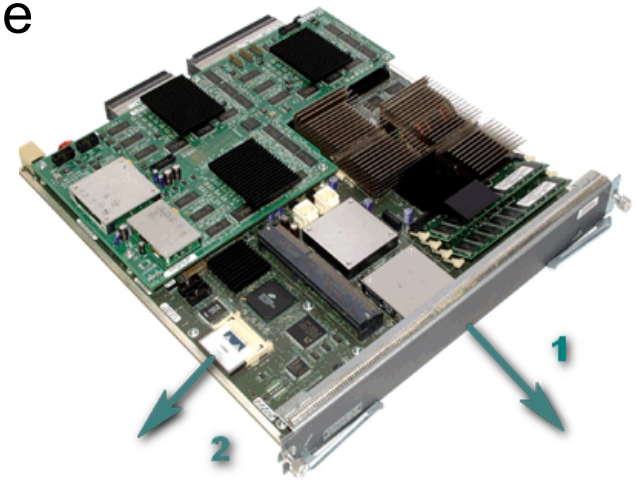
Agenda

- Aufgaben eines NV
- Neues im MWN (Reiser)
- Dienste im MWN (Tröbs)
  - Virtuelle Firewalls
  - Incident und Change Management
  - VPN und Secomat
- Sicherheitsmonitoring (Hommel)

Virtuelle Firewalls im MWN (Stand)

- Auf MWN zugeschnittenes, vorkonfiguriertes System
- Tägliche Sicherung der Konfiguration der Firewalls
- Konfiguration/Regelpflege durch Firewall-Administratoren an Instituten
- „eigene Instanz“ pro Kunde

- Bisher Firewall-Blades als Router-Einschübe (Cisco-FWSM-Module)
- Keine Wartung/Updates/
  Support mehr für diese Systeme.
  Kein Weiterbetrieb dieser Systeme mehr,
  Migration erforderlich



Quelle: https://ruhann.files.wordpress.com

Virtuelle Firewalls im MWN (zukünftig)

- Keine Grundsätzliche Änderung des Dienstes
- Kundenbefragung (Ende 2013); Definition diverser Key-Features: u.a. VPN
  - Anbieteranfragen/Evaluation verschiedener Systeme im Lauf des Jahres 2014, Gewinner: pfSense
  - (*pfSense ist eine open-source Firewall-Distribution auf Basis von FreeBSD und des Paketfilters pf).*
  - *Betrieb von virtuellen Maschinen auf dedizierter Firewall-Infrastruktur*
- Pilotbetrieb einer Firewall seit Februar 2015 (LRZ-Infrastruktur)
- Antragstellung GG (2014/2015), Beschaffung(Mitte 2015) und Inbetriebnahme der neuer Firewall-Systeme, basierend auf pfSense (ab Oktober 2015)

pfSense-Logo; Quelle: Screenshot

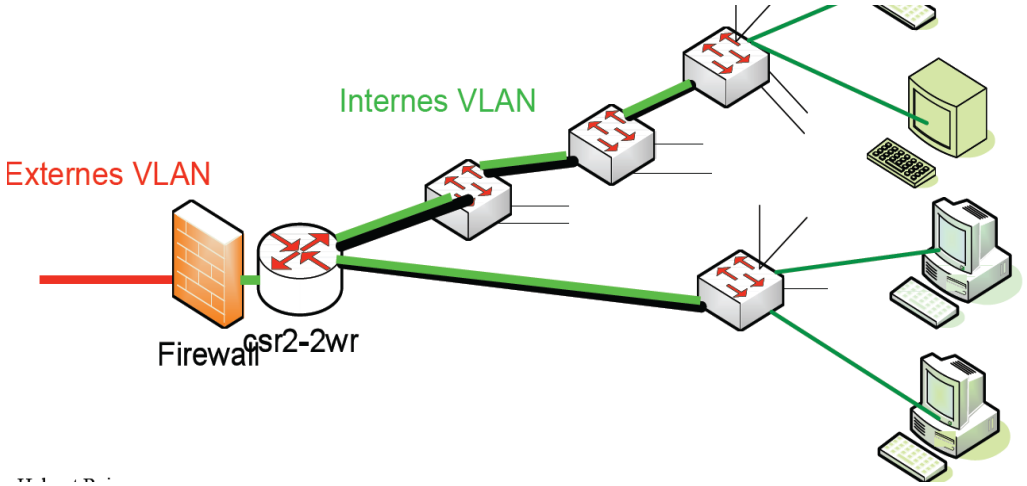
Vorteile der neuen Lösung

- HA: Jeder Kunde erhält Firewall-Paar (Neu: 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)
- Firewall-Authentifizierung mit SIM/AD-Kennungen, die der Masteruser verwalten kann. Keine gesonderten Firewall-Kennungen mehr.
- Java-freie Web-Oberfläche
- Migration von bisherigen Konfigurationen möglich
- Hohe Flexibilität durch Zusatzpakete (LRZ wird nicht alles unterstützen!)
- Kommerzieller Support erhältlich; aktive Entwicklergemeinde

Integration der virtuellen Firewalls im MWN

- Standortkonzept wird beibehalten (B,G,W5,WR, Q)
- Jeweils 2 (WR 4)x HP Server DL380 (56 cores, 128 GB RAM)
- Virtualisierung mittels ESXi 6.0
- 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 möglich
- Firewall wie zuvor logisch vor den Kundennetzen.

Quelle: www.hp.com / LRZ



Migrationszeitplan

- Migration wird standortweise durchgeführt, bisherige Konfiguration auf neue Plattform konvertiert.
- Möglichkeit mit einem neuen System zu starten
- Grober Zeitplan:
  - Umstellung der Standorte (Q bereits abgeschlossen), einige Systeme in B und G
  - Alle Standorte werden nach und nach migriert
  - Plan (G, W5,B,WR) bis zum Ende des Jahres, möglicherweise schneller.
  - Information und Möglichkeit der Einsicht in das neue System vorab.
  - Umschalttermine individuell vereinbar.

Informationsquellen / Kontakt

- Das LRZ bietet einen Grundkurs für die neue Plattform an (Termine: 13.04.16, 31.05.16)
- Anmeldung nur über das Kursbuchungssystem; ggf. folgen weitere Kurse
- Zusätzliche Anleitung demnächst auf unseren Webseiten

  https://www.lrz.de/services/security/virtuelle-fw/
- Weiterführende Links:

Website	https://www.pfsense.org/
Doku	https://doc.pfsense.org/index.php/Main_Page
Forum	https://forum.pfsense.org/index.php

- Anfragen zum Thema Firewall bitte an das Service-Desk.

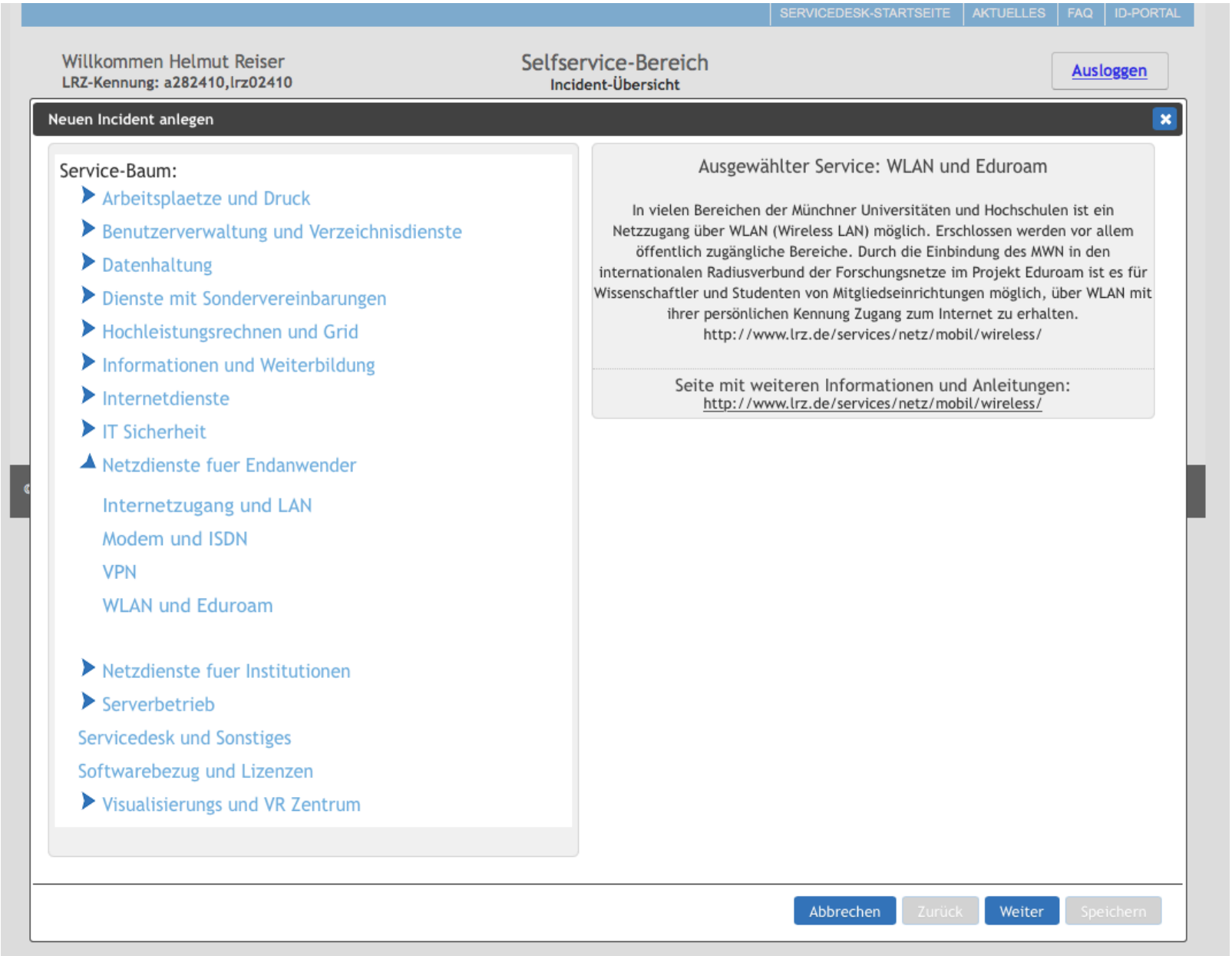
Agenda

- Aufgaben eines NV
- Neues im MWN (Reiser)
- Dienste im MWN (Tröbs)
  - Virtuelle Firewalls
  - Incident und Change Management
  - VPN und Secomat
- Sicherheitsmonitoring (Hommel)

Incident und Change Management

- LRZ ist bestrebt ein Service Management nach ISO 20000 zu betreiben
- Störungen und Service Requests werden über Tickets erfasst
- Ticket über Self-Service Portal oder Hotline erfassen
  - https://selfservice.lrz.de
  - 089 / 35831 – 8800
- Aus Service Request (z.B. Wunsch nach WLAN) wird i.d.R. ein Change
  - Abwicklung und interne Koordinierung von Änderungen an der Infrastruktur

Incident-Selfservice



Agenda

- Aufgaben eines NV
- Neues im MWN (Reiser)
- Dienste im MWN (Tröbs)
  - Virtuelle Firewalls
  - Incident und Change Management
  - VPN und Secomat
- Sicherheitsmonitoring (Hommel)

VPN im MWN

- Zugang zu internen Diensten im MWN
  - Zuordnung meist über IP-Adressen und nicht über Kennungen
- Verschiedene Betriebsysteme und Clients werden unterstützt (siehe Tabelle nächste Folie)
  - Oft erfolgt die Installation des Clients direkt vom VPN-Server
- IP-Adresszuordnung über die Kennung
  - HM, HSWT, LMU, TUM, LRZ
- ab AnyConnect 4.x:
  - Unterstützung von mehr Clients: Windows Phone und Chrome
  - Neues Lizenzmodell:
    - nicht mehr maximale Anzahl von Verbindungen pro Server
    - pro Nutzer ist eine Lizenz nötig (dieser kann aber mehrere Geräte verwenden)

Vergleich von verfügbaren Clients zu Betriebssystem

	Cisco AnyConnect	Cisco IPsec	openConnect (OSS)	vpnc (OSS)
Android	Google Play	————	Google Play	Google Play (vpncilla)
iOS	App Store	Integriert	————	————
Windows Phone	Microsoft Store	————	————	————
Chrome	Chrome Web Store	————	————	————
Linux	Webdeploy	————	Standard-Software	Standard-Software
Mac OS X	Webdeploy	Integriert	MacPorts	Macports
Windows	Webdeploy	Shrew VPN Client	————	————

https://asa-cluster.lrz.de

VPN im MWN (was ist neu)

- Auto-Reconnect nach Ruhezustand seit April 2015
- IPv6 Client-IP bei AnyConnect und openConnect
- IPv6 Verbindung zum Server (DS-Lite DSL Nutzer)
  - direkte IPv6 Verbindung zum Server

- Split-Tunneling deaktivieren: „!“ vor die Kennung setzen

- Bei Problemen: FAQs lesen und Servicedesk kontaktieren.

Secomat

- NAT- und Security-Gateway (siehe http://www.lrz.de/services/netzdienste/secomat/).
- Security: Beobachtung der Paketanzahl von und zu bestimmten Zielen (Scan-, DOS-, DDOS-Angriffe).
- Die meisten regulären Protokolle funktionieren reibungslos.
- Ausnahmen: z.B. skype.
  - Grund: Kommunikationsverhalten lässt sich nicht immer zuverlässig von Angriffen unterscheiden.

Secomat

- Skype-Protokoll ist nicht dokumentiert.
- Bis vor ca. 3 Jahren: Fast jeder Skype-Client konnte Supernode werden (Ausnahmen: z.B. Skype-Clients auf Mobile Devices).
- Seit ca. 3 Jahren: Skype-Protokoll soll zentrale Supernode-Rechner in Microsoft-Rechenzentren nutzen.
- Mögliche Probleme: z.B. ältere Skype-Clients oder Situationen, die möglicherweise einen Rückfall in alte Verhaltensweise auslöst.
- Sicherheitshalber Supernode-Feature verhindern (siehe http://www.lrz.de/fragen/faq/netz/netz10/).

Secomat

- Incidents mit dem Service IT-Sicherheit/Secomat:
  - Jahr Zeitraum Incidents Gleichzeitige Benutzer
  - 2016 Jan 8 -
  - 2015 Jan-Dez 79 ca. 36.000 maximal
  - 2014 Jan-Dez 36 ca. 28.000 maximal
  - 2013 Jan-Dez 38 ca. 24.000 maximal
- Unschärfe:
  - skype-fremde Incidents enthalten.
  - skype-Incidents mit anderem Service nicht enthalten.
  - Dunkelziffer nicht gemeldeter Probleme
- Weist nicht auf eine Verbesserung der Situation durch zentrale Supernodes hin.

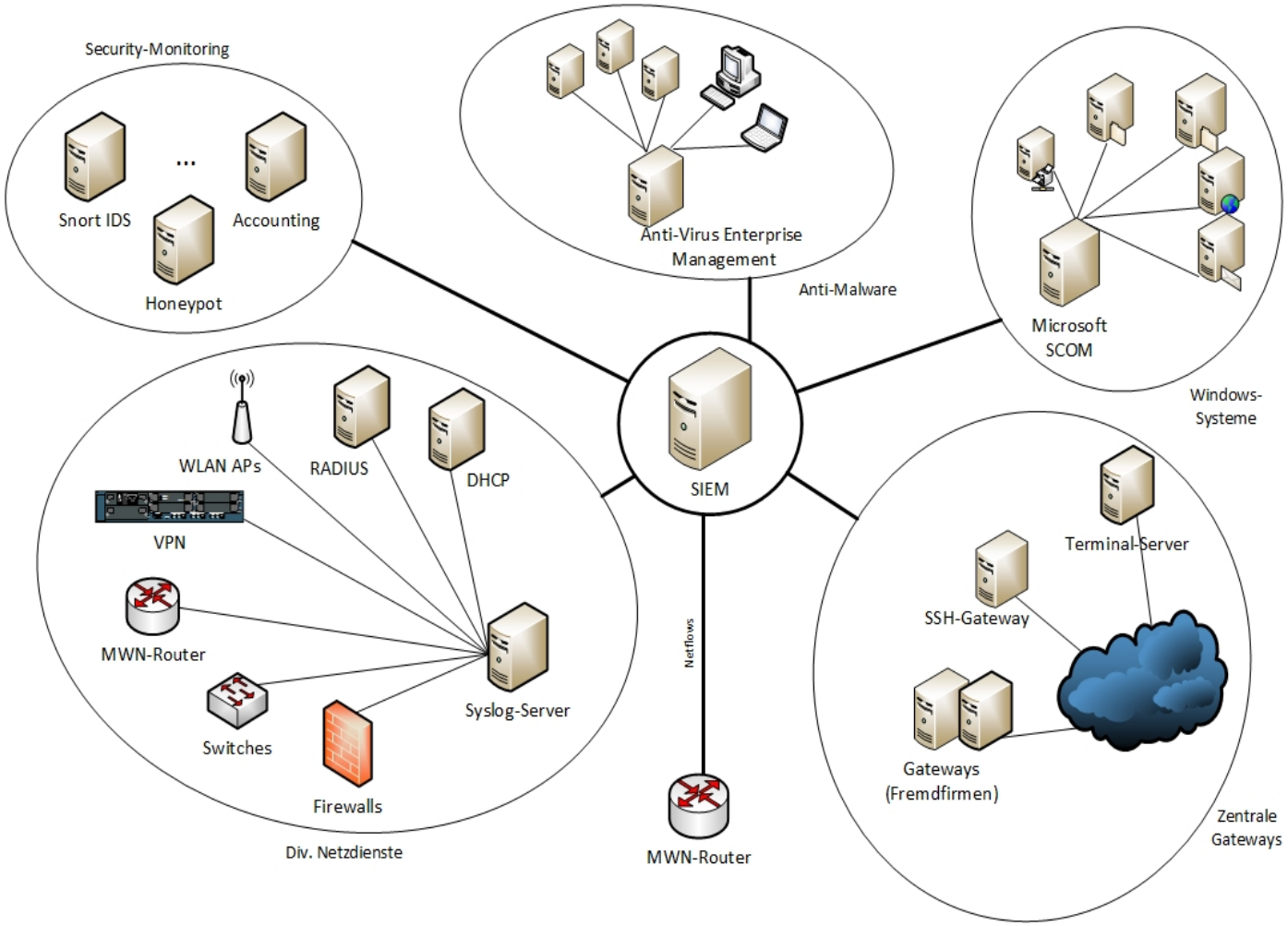
Agenda

- Aufgaben eines NV
- Neues im MWN (Reiser)
- Dienste im MWN (Tröbs)
- Sicherheitsmonitoring
  - Security Information & Event Management (SIEM)
  - Verwaltung gesperrter IP-Adressen
  - Neues im Self-Service-Web-Portal NeSSI
  - Aktuelle DFN-CERT-/CERT-Bund-Meldungen
  - Mail-Sicherheit: DKIM / DMARC

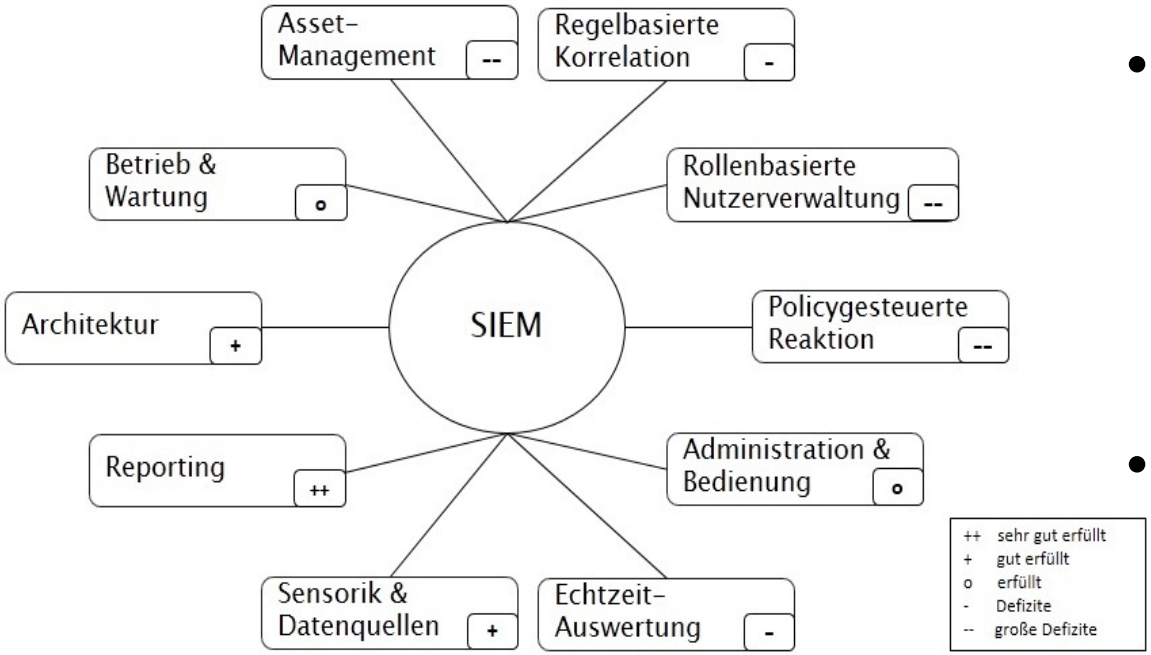
Security Information & Event Management (SIEM) am LRZ

- Motivation für den SIEM-Einsatz:
  - Zahlreiche Quellen für Security-Events, z.B. Suricata IDS, Netzkomponenten- und Server-Logfiles, …
  - Automatisierung und Vereinheitlichung von Aggregation, Korrelation, Auswertung und Reaktion
- Bis 2013 im Einsatz: AlienVault OSSIM
  - Open Source, aber mit Performance-Bremse
  - Kein IPv6-Support trotz Beta-Programm

SIEM-Einsatz im LRZ



SIEM-Evaluation



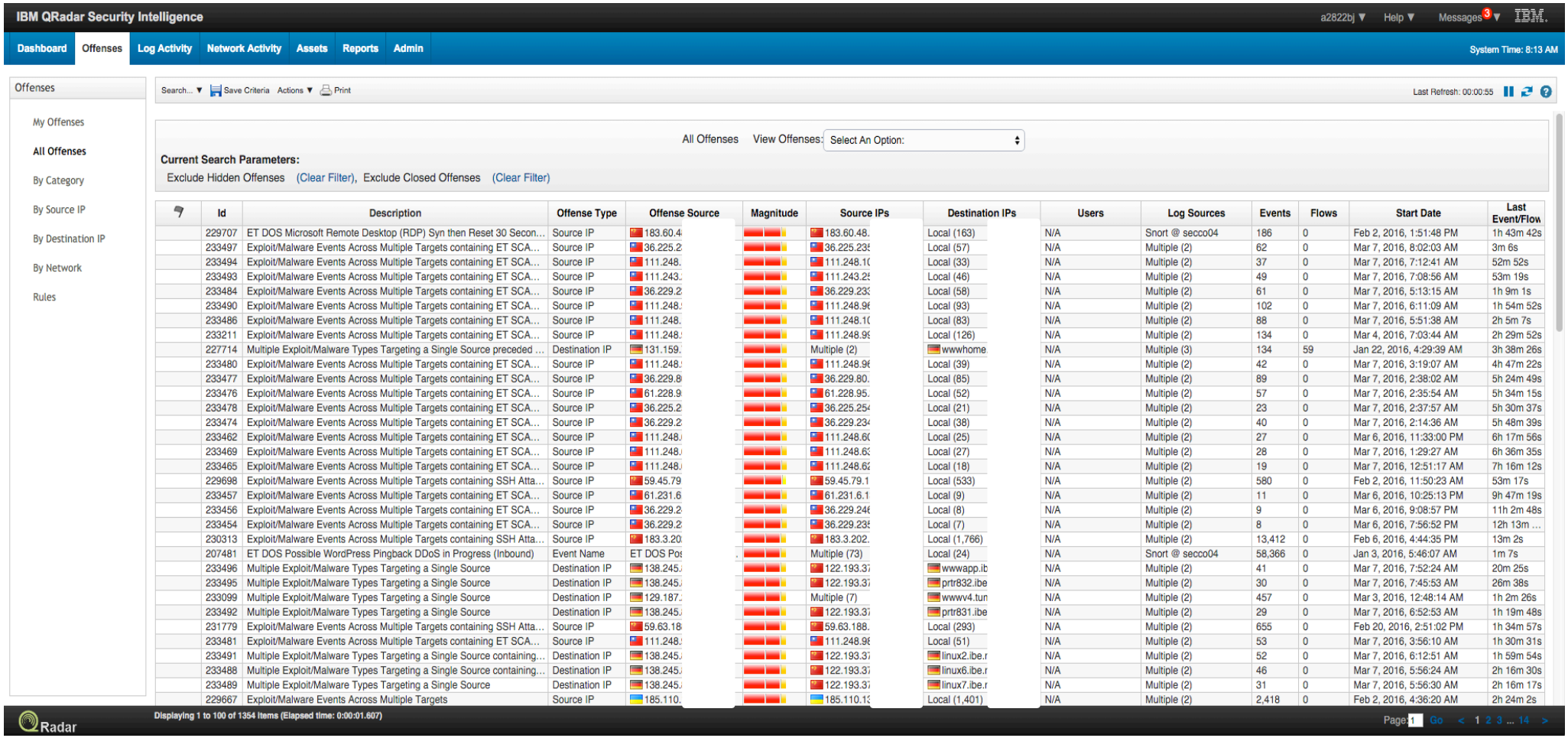
- Evaluation auf Basis von mehr als 100 Anforderungen in 11 Kategorien
- Charakteristische Stärken und Schwächen aller getesteten SIEM-Systeme

- Ausgewähltes Produkt: IBM Q1 Labs QRadar
  - Beste der getesteten Lösungen, aber nur 75% der Anforderungen erfüllt
  - IPv6-Support bis Mitte 2016 nur partiell
  - Beschaffung über IBM-Landeslizenzvertrag

Einführung des neuen SIEM-Systems IBM QRadar

- Zweistufiges Vorgehen:
  1. Ablösung der OSSIM-Funktionalität nahezu 1:1
  2. Customizing neuer Funktionen, u.a. Integration von IP-Traffic-Accounting und Nutzung der Anomalie-Erkennung
- Zwischenbilanz:
  - Integration zusätzlicher Datenquellen unproblematisch
  - Brauchbare vorgefertigte Regelsätze mit Auto-Updates
  - Schwierigkeiten mit asymmetrischem Routing und bei Netflow-Lastspitzen
- In Arbeit:
  - Reduktion von False Positives, u.a. bei “internal SSH attacks”
  - Migration herkömmlicher Monitoring-Tools für die Erkennung von Portscans und Spam-Versand

QRadar-Einsatz am LRZ



Ziele:

Fokus auf aktuelle, relevante Angriffe + Minimierung von False Positives, automatisierte Weiterleitung der Informationen an Netzverantwortliche in Echtzeit

Agenda

- Aufgaben eines NV
- Neues im MWN (Reiser)
- Dienste im MWN (Tröbs)
- Sicherheitsmonitoring
  - Security Information & Event Management (SIEM)
  - Verwaltung gesperrter IP-Adressen
  - Neues im Self-Service-Web-Portal NeSSI
  - Aktuelle DFN-CERT-/CERT-Bund-Meldungen
  - Mail-Sicherheit: DKIM / DMARC

Verwaltung gesperrter IP-Adressen (“SperrAPI”)

1. Self-Service für Anwender zur Secomat-Entsperrung

2. Verwaltung von Ausnahmelisten-Einträgen nach Meldung durch Netzverantwortliche:
   - Eintrag verhindert automatische Sperre bei Auffälligkeit
   - Netzverantwortliche werden dennoch informiert (!)
   - Gültigkeit von Einträgen:
     - Maximal 1 Jahr
     - Erinnerung an Verlängerung zwei Wochen / 48h vor Ablauf

3. LRZ-interne Web-Service-Schnittstellen und Web-Frontend erleichtern Arbeit des Abuse Response Teams

SperrAPI: Beispiele für E-Mails

From: **MWN/LRZ Abuse Response Team** abuse@lrz.de
Subject: [AUSNAHMELISTE] Vermutlich Ponmocup-infiziertes System - 10.152.24
Date: 3 March 2016 at 17:02
To: ar-team@lrz.de
Cc

Sehr geehrte Netzverantwortliche,

beim Security-Monitoring am X-WiN-Zugang ist aufgefallen, dass der in Ihrem
Verantwortungsbereich liegende Rechner

IP-Adresse: 10.152.2
FQDN: 001cc02a

Standort:
W4
TUM, Geb. 5500 (Bauteil , Maschinenwesen

Switchport:
MAC: 00:1C:C0:
Device : SWG1-0W4
Location: Bau 4 Raum 04
Port:
First seen: 2016-02-29 13:08:27.0
Last seen: 2016-03-03 16:50:18.0

Weitere Informationen:

Source-Port: 1157
Destination-IP: 192.42.1
Destination-Port: 80

Timestamp: 03.03.2016 17:01:00

aufgrund charakteristischer Auffälligkeiten im Kommunikationsverhalten mit sehr
hoher Wahrscheinlichkeit mit dem
Ponmocup-Virus infiziert ist.

Ponmocup ist in der Lage nahezu beliebigen Schadcode auf das System nachzuladen.
Außerdem können Dateien auf dem System
gelöscht oder sensible Daten über das Internet verbreitet werden. Desweitern werden
meist Sicherheits-relevante
Dienste beendet, wodurch der vermutete Schutz eines Systems ausgehebelt wird.

Mit freundlichen Grüßen
--
+---+
| MWN/LRZ Abuse Response Team |
| |
E-Mail: abuse@lrz.de	Leibniz-Rechenzentrum
Phone: +49 89 35831 8800	Boltzmannstraße 1
Fax: +49 89 35831 9700	D-85748 Garching, Germany
+---+

*** Diese E-Mail wurde automatisch erzeugt und an Sie verschickt ***

From: abuse@lrz.de
Subject: [SperrDB] Ausnahme endet in weniger als 2 Wochen: 141.84.6
Date: 7 March 2016 at 07:55
To: ar-team@lrz.de,

Sehr geehrte Damen und Herren,

wir führen eine Ausnahmeliste für IP-Adressen, die im Rahmen unseres Sicherheits-
Monitorings auf keinen Fall automatisch gesperrt werden sollen.

In der Regel handelt es sich dabei um Gateways (z.B. NAT oder Firewall), die den
Internet-Zugang für mehrere dahinter liegende Rechner realisieren, oder Server, die
einen besonders wichtigen Dienst erbringen. Die Einträge in der Ausnahmeliste haben
eine Laufzeit von einem Jahr und müssen danach verlängert werden. Bei dieser
Gelegenheit wird die Aktualität der Einträge überprüft:

IP/Netz: 141.84.6
Gültig bis: 2016-03-20 19:50:02
Kontakt:
Kommentar: DNS-Server und Resolver

Um den Ausnahmelisteneintrag für diese IP-Adresse zu verlängern bzw. zu löschen,
beantworten Sie bitte diese E-Mail. Sie können uns bei der Gelegenheit auch
Änderungen der Kontaktdaten oder des Rechnerzwecks mitteilen.

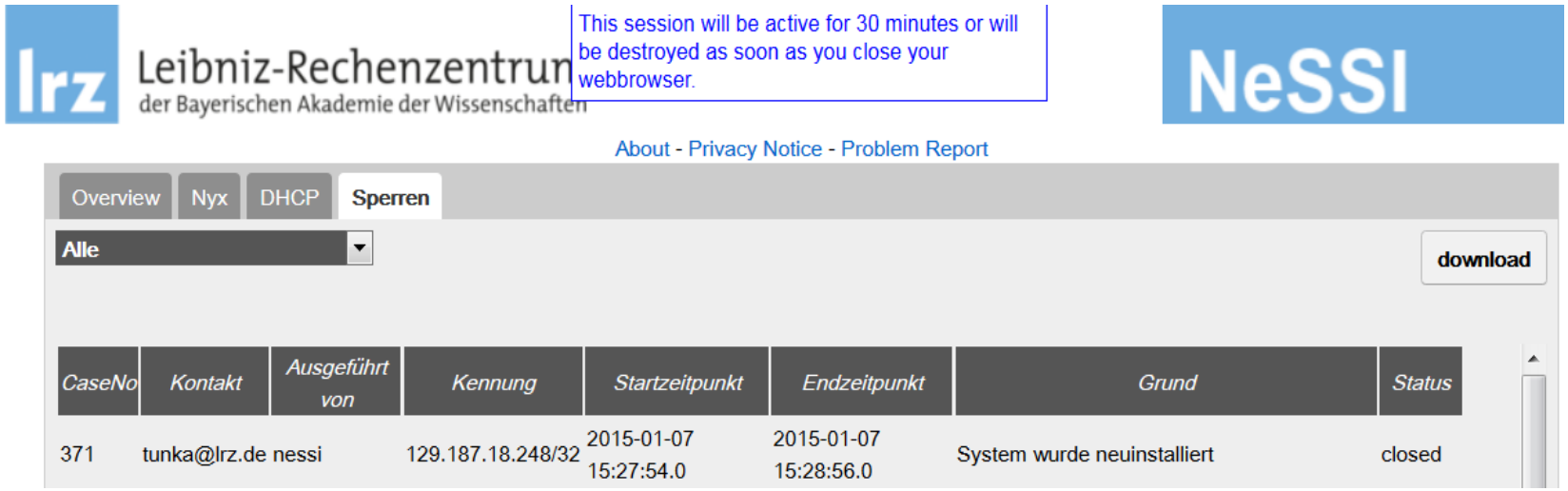
Mit freundlichen Grüßen

- --
+---+
| MWN/LRZ Abuse Response Team |
| |
E-Mail: abuse@lrz.de	Leibniz-Rechenzentrum
Phone: +49 89 35831 8800	Boltzmannstraße 1
Fax: +49 89 35831 9700	D-85748 Garching, Germany
+---+

Subject enthält “[AUSNAHMELISTE]”: Reine Information, keine Sperre erfolgt!

NeSSI – Netzverantwortlichen-Self-Service-Interface

- Web-Frontend u.a. zur Abfrage von
  - MAC-Adress-zu-Switchport-Zuordnung
  - per LRZ-DHCP zugewiesenen IP-Adressen
- 2014 vollständig neu implementiert, modularere Architektur
- Netzverantwortliche können jetzt auch gesperrte Rechner selbst entsperren
- Integration der SperrAPI-Ausnahmeverwaltung in Arbeit



DFN-CERT-/CERT-Bund-Meldungen

- Aktuelle Schwerpunkte durch Integration des Shadowserver-Projekts:
  - Ungeschützte Datenbank-Server (MongoDB, Redis, …), Netzwerkdrucker etc.
  - “Offene”, für Amplification Attacks anfällige Server (DNS, NTP, SNMP, …)
- LRZ Abuse-Response-Team gibt Meldungen zeitnah an Netzverantwortliche weiter
- Bitte Umkonfiguration der betroffenen Systeme oder Maßnahmen wie virtuelle Firewalls in Erwägung ziehen!

Agenda

- Aufgaben eines NV
- Neues im MWN (Reiser)
- Dienste im MWN (Tröbs)
- Sicherheitsmonitoring
  - Security Information & Event Management (SIEM)
  - Verwaltung gesperrter IP-Adressen
  - Neues im Self-Service-Web-Portal NeSSI
  - Aktuelle DFN-CERT-/CERT-Bund-Meldungen
  - Mail-Sicherheit: DKIM / DMARC

Mail: DMARC / DKIM

- Mail-Adressen können leicht gefälscht werden; Gegenmaßnahmen
  - Sendender Mail-Server signiert mit Domain Keys (DKIM) aus DNS
  - Empfangender Mail-Server prüft Signatur
  - Entscheidet anhand DMARC-Policy des **Absenders** was mit Mail bei ungültiger Signatur zu tun ist
    - None = annehmen und Bericht schicken (Monitor Mode)
    - Quarantine = Mail in Quarantäne und als Spam markieren
    - Reject = Mail zurückweisen
- Google (gmail) stellt **ab Juni 2016** DMARC auf **reject**
  - Große Sichtbarkeit, einer der größten Freemail-Provider
  - Grundsätzlich Wünschenswert aber Probleme möglich

Mögliche Probleme bei DMARC

- Web-Formulare (Konferenzanmeldung, Heise-Artikel an Freunde mailen, ...)
  - Adresse des Ausfüllers wird als Absender-Adresse verwendet (keine Signatur oder ungültige Signatur)
- Mailinglisten die Mail verändern (z.B. Listen-Tag), Signatur wird ungültig
  - Absender gmail an Liste; Empfangende Mailserver lehnen ab
  - Passiert das öfter wird Empfänger (**NICHT** Sender) abgemeldet
- Weiterleitungen können Signatur ungültig machen
  - Per Script (Sieve, procmail)
  - Per Mail-Server Exchange oder Novell Groupwise
  - Betrifft > 20 Mailserver im MWN
- Mail mit Absender gmail kommt **nicht** mehr an
- **Dringend** um DMARC konformen Versand kümmern

DKIM / DMARC am LRZ

- DKIM
  - Ziel: Bis Ende des Jahres soll Großteil der Mails signiert werden!
  - Installation eines neuen Mailman (in Arbeit)
  - Warum zerstört Exchange DKIM Signaturen ?
  - Signatur für lrz.de und tum.de
  - Anbindung von Web-Anwendungen für Signatur (mit TUM)
    - TUMOnline, Moodle, TUM-OTRS
- DMARC
  - DMARC-Record mit Policy = none, d.h. „nur“ Monitor-Mode


Fragen ?