Informationsveranstaltung für Netzverantwortliche im Münchner Wissenschaftsnetz (MWN)

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

Wolfgang Beyer, Wolfgang Hommel, Helmut Reiser

Agenda

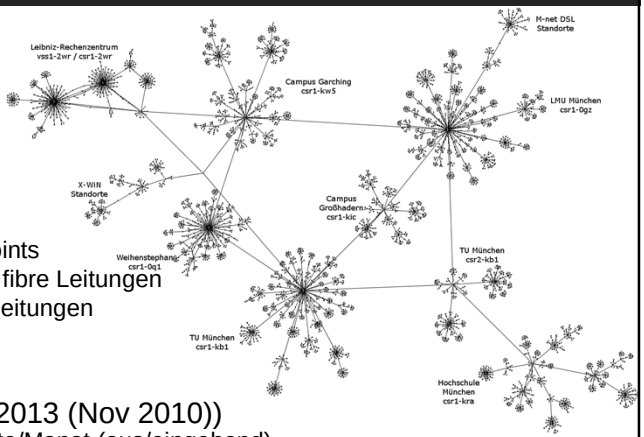
- **Neues im MWN** (Dr. H. Reiser)
- **Dienste im MWN** (W. Beyer)
- **Sicherheit** (Dr. W. Hommel)
- **Diskussion und Abschluss** („open end“)

Agenda

- **Neues im MWN** (Dr. H. Reiser)
  - **Redundanz im MWN**
  - **Aufgaben eines NV; Planung neuer Netze**
  - **Neue Verkabelungsrichtlinie, BayITR**
  - **Netzinvestitionsprogramm (NIP V) an der LMU**
  - **Migration der Routerplattform**
  - **Switch-Auswahl**

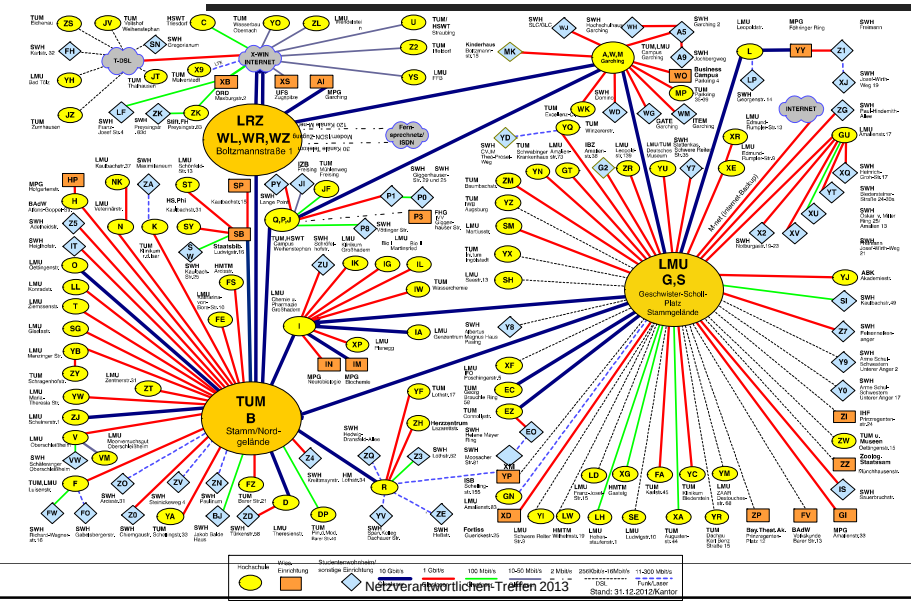
MWN-Überblick

- Nutzer
  - 90.000 Studenten
  - 30.000 Mitarbeiter
- Kennzahlen
  - 12 (2010: 11) Router
  - 1.300 (1000) Switches
  - 2.060 (1400) Accesspoints
  - 63 (51) gemietete dark fibre Leitungen
  - 30+ private dark fibre Leitungen
  - 100.000 Endgeräte

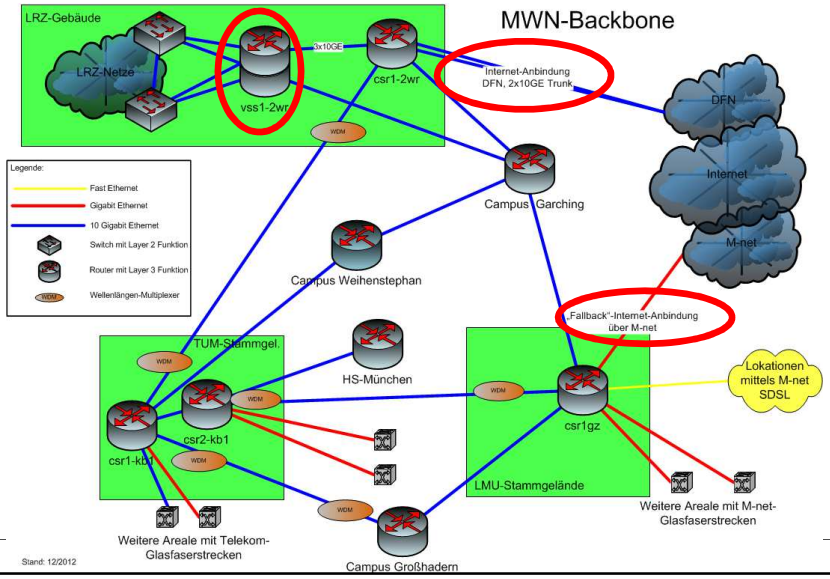


- Übertragene Daten (Jan 2013 (Nov 2010))
  - 500/890 (360/450) Tbyte/Monat (aus/eingehend)
  - 16 (8,3) PByte/Monat über Backbone

MWN Ende 2012



Ausfallsicherheit / Redundanz



Stand: 12/2012

Agenda

- **Neues im MWN** (Dr. H. Reiser)
  - **Redundanz im MWN**
  - **Aufgaben eines NV; Planung neuer Netze**
  - **Neue Verkabelungsrichtlinie, BayITR**
  - **Netzinvestitionsprogramm (NIP V) an der LMU**
  - **Migration der Routerplattform**
  - **Switch-Auswahl**

Aufgaben eines Netzverantwortlichen

- Unser Kontakt und Ansprechpartner
- Aufgaben:
  - zuständig für einen (Netz-) Bereich
  - (alleinige) Schnittstelle zum LRZ (Arealbetreuer) in Netzfragen
  - Schnittstelle für Benutzer in seinem Bereich für Netzfragen
  - **Dokumentation**
  - **Fehlerverfolgung**
  - **Mithilfe bei Netzmissbrauch und kompromittierten Systemen**
  - Planung und Inbetriebnahme von Erweiterungen der Gebäudenetze
- Wer ist mein Arealbetreuer ?
  www.lrz.de/services/netz/arealbetreuer/
- Wer ist mein Netzverantwortlicher ?

  Servicedesk des LRZ

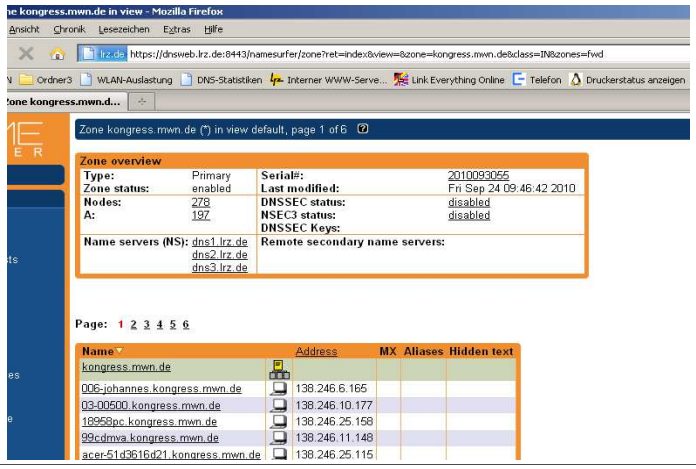
Adressverwaltung

- Neuer Adressbereich erforderlich: ⇨ Arealbetreuer
- Verwaltung der Adressen; 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:D2:28:43	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							

Verwaltung von Namen und Adressen: DNS

- Verwaltung über WebDNS ⇨ eigener Abschnitt



Sonstige Aufgaben und Problemfelder

- Fehlerhafte Dosen/Patchfeldinstallation
- Unzureichende Dokumentation/Beschriftung
- Fehlende Mittel für Netzanschluss bei neuen Rechnern
- Kabelschleifen (Vorsicht bei Miniswitches!)
- Falsche VLAN-Zuordnung
- Defekte Patchkabel
- Client IP-Konfiguration (Empfehlung: DHCP)
- Firewall-Konfiguration
- Nützliche Werkzeuge für den NV: www.lrz.de/services/schulung/unterlagen/nv-basiswissen/nv-basiswissen.pdf

Abuse Bearbeitung

- Ermittlung des Verursachers (Rechner bzw. Kennung)
- Benachrichtigung weiterleiten an
  - Benutzer → Kennung, priv. Rechner
  - Ansprechpartner für Kennung
  - Netzverantwortlicher → MWN-Rechner
- Nutzer säubert Rechner
- Antwort an den Beschwerdeführer
- Bei Bedarf Eskalation

Planung und Realisierung neuer Netzstrukturen

- Beteiligte Institutionen:
  - Bauämter
    - der TUM
    - der LMU
  - Planungsbüros
  - Hochschulverwaltungen
  - Nutzer des Datennetzes (Netzverantwortliche)
  - Eigentümer und/oder Verwalter (i.A. technische Betriebsabteilungen der Hochschulen) der Gebäude
  - Netzbetreiber (LRZ)
  - Hauswerkstätten bei kleineren Vorhaben (ohne Bauamt zu realisieren)
  - installierende Firmen

Neue Netze: Aufgaben der Beteiligten (1/2)

- Bauämter und deren beauftragte Planungsbüros:
  - Erstellen passiven Teils des Netzes
  - Erstellen „Haushaltsunterlage-Bau“ (HU-Bau)
  - Erstellen Leistungsverzeichnisses (Ausschreibung)
  - Durchführung der Ausschreibung
  - Betreuung und Überwachung der Installationsarbeiten, incl. Abnahme
  - Bestellung der aktiven Netzkomponenten
- Hochschulverwaltungen /Hauswerkstätten (bei kleineren Vorhaben)
  - Erstellen des passiven Teils des Netzes
  - Betreuung und Überwachung der Installationsarbeiten, incl. Abnahme
  - Bestellung der aktiven Netzkomponenten

Neue Netze: Aufgaben der Beteiligten (2/2)

- Nutzer des Datennetzes (Netzverantwortlicher)
  - Spezifikation der anzubindenden Räume
  - Netzverantwortlichen benennen (falls noch nicht geschehen)
  - Netznutzungskonzept
  - Nennung besonderer Einschränkungen (z.B. Hochspannung)
- LRZ
  - Auswahl, Installation und Betrieb der aktiven Netzkomponenten
  - Betrieb des fertigen Kommunikationsnetzes
  - Fehlersuche und Ausbauplanung in Rücksprache mit den Netzverantwortlichen
- Eigentümer und/oder Verwalter der Gebäude:
  - Gewährung von Nutzungs- und Zutrittsrechten für Verteilerräume und Einrichtungen, soweit für Installation und Netzbetrieb notwendig

Neue Netze: Vorgehen und Zusammenarbeit (1/2)

- Information über Bauvorhaben
  - **Rechtzeitige Information des LRZ** und der Nutzer (NV) über geplante Bauvorhaben, auch wenn explizit kein Kommunikationsnetz errichtet werden soll. Oft kann dies kostengünstig bei anderen Baumaßnahmen mit realisiert werden.
- HU-Bau
  - Einsichtnahme der HU-Bau für das LRZ und den Nutzern (NV) vor Abgabe
  - Fester Betrag pro aktivem Anschluss für die aktiven Komponenten
- Ausschreibung
  - Mitspracherecht für das LRZ bei der Festlegung der auszuschreibenden Materialien (z.B. Kabel), da rasche Weiterentwicklung
- Planungsunterlagen für die Bauausführung
  - Planungsunterlagen sollte das LRZ sehen und mit Nutzern (NV) abstimmen
  - Mitspracherecht des LRZ bei Netzverteilerstandorten

Neue Netze: Vorgehen und Zusammenarbeit (2/2)

- Abnahme
  - LRZ bei der Abnahme des DV-Netzes beteiligen
  - Fertigstellung: d.h. vollständige Dokumentation des (passiven) Netzes vorhanden
    - Prüf- und Abnahmeprotokolle der LWL- und Kupferleitungen
    - Installationspläne
    - Vollständige und eindeutige Beschriftung der Anschlusseinheiten (z.B. Patchfelder, Anschlussdosen)
- Aktive Netzkomponenten
  - LRZ wählt nach Rücksprache mit den Nutzern (NV) aktive Komponenten aus
  - Bauamt oder die Hochschulverwaltung bestellen Komponenten

Neue Netze: Voraussetzungen für Inbetriebnahme

- Alle Installationsarbeiten abgeschlossen
- Abnahme erfolgt
- Ungehinderter Zugang zu allen Räumen mit Netzeinrichtungen
- Übergabetermin rechtzeitig bekannt (mindestens vier Wochen vorher)

Agenda

- **Neues im MWN** (Dr. H. Reiser)
  - **Redundanz im MWN**
  - **Aufgaben eines NV; Planung neuer Netze**
  - **Neue Verkabelungsrichtlinie, BayITR**
  - **Netzinvestitionsprogramm (NIP V) an der LMU**
  - **Migration der Routerplattform**
  - **Switch-Auswahl**

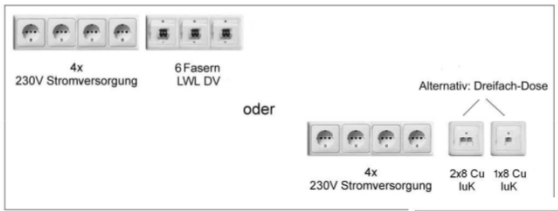
Oberste Baubehörde im
Bayerischen Staatsministerium des Innern

http://www.lrz.de/services/netz/verkabelung/richtlinien.pdf

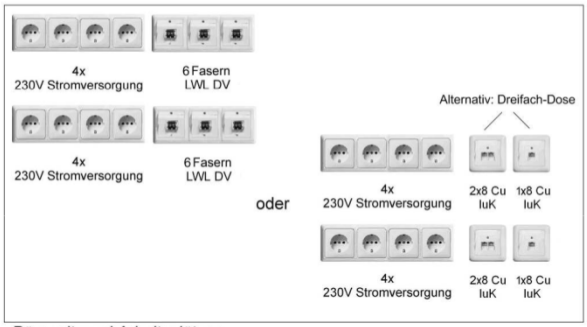
Verkabelungsrichtlinie: BayITR03

- Gilt für alle staatlichen Gebäude und Baumaßnahmen
- Aktualisiert im Jahr 2010, wegen
  - Technischen Neuerungen
  - Prüfung ORH: Energetische Prüfung von Serverräumen
- Neue Regelungen
  - Nur noch ein Kabeltyp Cat 7
  - KEINE separate Telefonverkabelung (Cat 3)
  - KEIN Cable-Sharing
  - Qualitätssicherung:
    - Zertifizierte Produkte
    - Messungen und Messprotokolle bei der Abnahme

BayITR 03: Büroarbeitspätze



Büro mit einem Arbeitsplatz



Büro mit zwei Arbeitsplätzen

Agenda

- **Neues im MWN** (Dr. H. Reiser)
  - **Redundanz im MWN**
  - **Aufgaben eines NV; Planung neuer Netze**
  - **Neue Verkabelungsrichtlinie, BayITR**
  - **Netzinvestitionsprogramm (NIP V) an der LMU**
  - **Migration der Routerplattform**
  - **Switch-Auswahl**

Netzinvestitionsprogramm V (NIP V)

- Netzinvestitionsprogramm V im Jahr 2009 vom Landtag genehmigt
  - Finanzierung 1.Bauabschnitt im Rahmen eines Konjunkturprogramms erfolgt
    - Bereits sanierte Standorte:
      Sternwarte Bogenhausen Scheinerstraße 1
      Oettingenstraße 67
      Leopoldstraße 13 Haus 1 – 3
      Theresienstraße 37- 41
  - Volumen: 4,5 Mio Euro
- Beginn des zweiten Bauabschnitts im Jahr 2013 erwartet
  - Erstellung der HU Bau
  - Beginn der Arbeiten noch in diesem Jahr möglich, spätestens 2014
  - Volumen: 6,6 Mio Euro für 19 Standorte
    mit veralteter Netzwerkverkabelung der Kategorie 5(e) bzw. Cable-Sharing

NIP V – Prioritäten der Standorte

- Vorläufige Prioritäten
  - Butenandtstraße 5-13 Fakultät für Chemie und Pharmazie Großhadern
  - Marchioninistraße 17 Wasserchemie
  - Schellingstraße 3 Vorder- und Rückgebäude
  - Veterinärstraße 13 Gebäude K+Q Tierklinik
  - Schellingstraße 12 Historicum
- Weitere Standorte, offene Reihenfolge der Prioritäten
  - Akademiestraße 1
  - Geschwister-Scholl-Platz 1 – Gedenkstätte Weiße Rose + Telefonzentrale
  - Kaulbachstraße 45
  - Leopoldstraße 3

NIP V – Prioritäten der Standorte

- Weitere Standorte Fortsetzung
  - Leopoldstraße 5
  - Leopoldstraße 15 EG Bereich Psychologie/Pädagogik
  - Ludwigshöhe 8 Fürstenfeldbruck
  - Ludwigstraße 25
  - Ludwigstraße 33
  - Maria-Theresia-Straße 21
  - Schellingstraße 5, 7, 9
  - Schellingstraße 10 (3.- 6.Obergeschoss)

Agenda

- **Neues im MWN** (Dr. H. Reiser)
  - **Redundanz im MWN**
  - **Aufgaben eines NV; Planung neuer Netze**
  - **Neue Verkabelungsrichtlinie, BayITR**
  - **Netzinvestitionsprogramm (NIP V) an der LMU**
  - **Migration der Routerplattform**
  - **Switch-Auswahl**

Migration der Routerplattform

- Bestehende Router im MWN nicht mehr zukunftsfähig
  - Geräte im Jahr 2000 beschafft
  - 2004 Upgrade der Supervisor Engines
  - 2007 Upgrade der Policy Feature Card
  - Kein Migrationspfad zu höheren Geschwindigkeiten: 40 oder 100 Gbit/s
- Auswahl potentieller Nachfolge-Geräte Herbst 2011 bis Frühjahr 2012
  - Anforderungsmatrix
  - Aufforderung an Hersteller für Lösungsvorschläge anhand der Matrix
  - Analyse der technischen Dokumentation
  - Auswahl von Testkandidaten
  - Praxistest (im Labor und im MWN)
  - Bewertung und Entscheidung

Routerauswahl

- Hersteller:
  - Alcatel, Brocade, Cisco, Extreme, Force10, HP, Huawei, Juniper
- Testkandidaten:
  - Alcatel
  - Cisco
  - HP
- Bewertung mit einem (relativen) Punktesystem
  - 0 Punkte: Anforderung erfüllt
  - -1 Punkt: Anforderung nicht erfüllt
  - +1 Punkt: Anforderung besser erfüllt als die Konkurrenz

Routerauswahl: Entscheidung und weiteres Vorgehen

- Ergebnis
  - Cisco: 5 Punkte
  - HP: 0 Punkte
  - Alcatel: -5 Punkte
- Entscheidung für Cisco Nexus 7010
- Antrag für „Ausbau des MWN“ als „Großgerät der Länder“ nach Art. 143c GG im Mai 2012
- Genehmigung im August
- EU-weite Ausschreibung am 24.08.2012
- Erteilung des Zuschlags am 5.11.2012 an T-Systems

Router-Ersetzung: Projektplan

- Erste Lieferung von 6 Geräten Ende Januar erfolgt
  - 1 Ersatzgeräte (Spare)
  - Austausch in den Semesterferien
  - csr1-kic (Großhadern) am 12.02.13
  - csr1-kra (Hochschule München) am 19.02.13
  - csr1-kw5 (Maschinenwesen) am 26.02.13
  - csr2-kb1 (TUM) am 05.03.13
  - csr1-kb1 (TUM) am 12.03.13

Router-Ersetzung: Projektplan

- 2. Lieferung in KW16 ab 15.04.13 mit 3 Geräten
  - csr1-1wr (SuperMUC) am 23.04.13
  - csr2-2wr (SuperMUC) am 30.04.13
  - csr1-krr (Hochschule München) am 07.05.13 (redundante Anbindung der HM)
- 3. Lieferung in KW 29 ab 15.07.13 mit 5 Geräten
  - csr1-0gz (LMU) am 23.07.13 (Semesterferien)
  - vss (2 Chassis, LRZ) am 30.07.13 (Semesterferien und kein Hochschulstart)
  - Aufbau der 100 GE Strecke zwischen den beiden VSS Chassis
  - csr1-2wr (LRZ) am 06.08.13 (X-WiN, kein HSS, Semesterferien)
  - csr1-0q1 (Weihenstephan) am 13.08.13 (Semesterferien)

Agenda

- **Neues im MWN** (Dr. H. Reiser)
  - **Redundanz im MWN**
  - **Aufgaben eines NV; Planung neuer Netze**
  - **Neue Verkabelungsrichtlinie, BayITR**
  - **Netzinvestitionsprogramm (NIP V) an der LMU**
  - **Migration der Routerplattform**
  - **Switch-Auswahl**

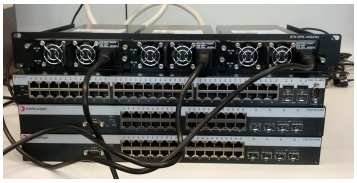
Switches: Auswahl, Rahmenvertrag

- Derzeit HP-Switches:
  - Seit 2000 im MWN verbaut
  - Letzte Marktuntersuchung 2009
  - Rahmenvertrag zur Beschaffung läuft noch bis April 2013
- Neue Marktuntersuchung 2012:
  - Anforderungskatalog aktualisiert
  - 11 Produkte von Alcatel, Cisco, Enterasys, HP und Juniper auf Papierlage untersucht
  - Labor- und Praxistest mit Cisco 3750, Enterasys C5 und HP 3800

Hardware-Anforderungen u.a.:
- Backplane bzw. des Stacking Bus >=25 Gbit/s pro Slot
- Portdichte pro Modul bzw. Switch
  - >=24 Ports 10/100/1000-TX
  - >=24 Ports 1000-SFP
  - >=2 Ports 10G-SFP+
- Redundante Netzteile
- 40G/100G Uplink

Software-Anforderungen u.a.:
- Mindestens 256 VLANs pro Switch-Chassis bzw. –Stack
- Multicast-Filter (IGMP, MLD)
- QoS-Funktionen (Layer 2, Layer 3)
- Rapid Spanning Tree (IEEE 802.1w)
- Port Based Network Access Control (IEEE 802.1X)
- MAC Based Network Access Control
- SNMP-Management (SNMPv2, SNMPv3)
- Sicherheitsfunktionen (SSH, SSL, SCP, SNMPv3)
- RADIUS-Authentifizierung für das CLI-Login
- Syslog (RFC 3164)
- NTP (RFC 1305) oder SNTP (RFC 1361)
- PoE (IEEE 802.3af) und PoE+ (IEEE 802.3at)
- Loop Protection (Loop Guard)
- DHCP Snooping
- Uni-Directional Link Detection (UDLD)
- Uplink Failure Detection
- Virtualisierung

Switches: Auswahl, Rahmenvertrag



- Ergebnisse:
  - Geräte von Cisco und HP sind funktional geeignet
  - HP-Geräte sind bzgl. Investitions- und Betriebskosten aber erheblich günstiger
  - Auch zukünftig Einsatz von modularen HP-Switches
- Ausblick:
  - Ausschreibung für neuen Rahmenvertrag läuft 12/2012-02/2013

Agenda

- **Neues im MWN**
- **Dienste im MWN** (W. Beyer)
  - **IPv6 Rollout**
  - **DHCP und DNS Dienst**
  - **WLAN**
- **Sicherheit**
- **Diskussion und Abschluss** („open end“)

IPv6 Rollout im MWN

- IPv6 ist in der Welt
- MWN: Vollständiges natives IPv6-Rollout im Backbone seit 2005
  - gleiche Hardware, gleiche Verfügbarkeit, gleiche Geschwindigkeit
- IPv6 in verschlüsseltem WLAN (eduroam)
- Alle Netze mit offiziellen Adressen, alle privaten hinter Firewalls (außer bei Widerspruch, insgesamt 837 Netze)
- 2013: Restliche private Netze, Routing über Secomat (keine Verbindungen von außen, erst mit neuen Routern möglich)
- LRZ-Dienste fast alle IPv6-fähig
- Ausführlich in http://www.lrz.de/services/schulung/unterlagen/netzverantwortliche/NV-Treffen_2010.pdf

Adressierung

- Adressen bestehen wie bei IPv4 aus einem Prefix (Subnetz) und einem Hostteil

  129.187.254.123

  2001:4ca0:dead:beef:1234:5678:9abc:def0

- Methoden für die Vergabe des Hostteils
  - Statisch (nicht empfohlen)
  - Stateful DHCPv6 (nicht empfohlen)
  - **Router Advertisement (RA), Stateless Address Autoconfiguration (SLAAC)**
    - **Privacy Extensions** (wechselnder Hostteil, durch Endgerät)
    - **Stateless DHCPv6** (nur dns/ntp-Serveradressen, hinter Firewalls problematisch)

Sicherheit

- Policy wird durch IPv4 bestimmt
  - Öffentliches IPv4 Netz: IPv6 global erreichbar (Umstellung in der Regel durchgeführt)
  - Virtuelle Firewall: Bei Einrichtung Verbindungen von außen geblockt
  - privates IPv4-Netz (ohne Firewall): Über Secomat, nur ausgehende Verbindungen (geplant)

Ipv6 in der Praxis (1)

- Voreinstellung in der Regel ok
- IPv6 native in der Regel problemlos (durch alle gängigen Betriebssysteme, auch in den Firewalls unterstützt)
- IPv6 ist oft unwissentlich schon in IPv4 Netzen aktiv (Tunnelmechanismen: Terredo/ ISATAP über LRZ-Gateways)
- Nachverfolgbarkeit oft schwieriger (z.B. bei privacy extensions)
- Monitoringtools für IPv6 z.T. noch unter Entwicklung
- Sicherheitskonzept überdenken (unter IPv4 gesicherte Systeme werden u.U. durch IPv6 erreichbar)

Ipv6 in der Praxis (2)

- Handlungsbedarf:
  Einige Anwendungen fordern zwingend IPv6 (Microsoft Direct Access / Lync, aggressives Auftreten von Microsoft bezüglich IPv6); manche Kontakte nur noch über IPv6 erreichbar
- IPv6 auf vielen Gebieten mehr als nur längere Adressen
- Umstellung und Kompatibilität von Anwendungen zu IPv6 nicht immer gegeben (z.B. SAP, spezielle VPN-Lösungen)
- Vorsicht mit „Internet Connection Sharing“ unter Windows Vista
- Testhilfe: An-/Abschaltung per Firefox Addon „ToggleV6“

Agenda

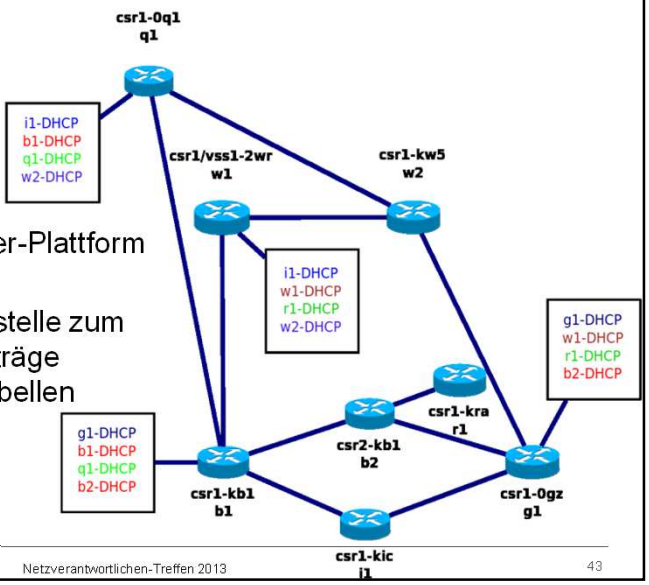
- **Neues im MWN**
- **Dienste im MWN** (W. Beyer)
  - **IPv6 Rollout**
  - **DHCP und DNS Dienst**
  - **WLAN**
- **Sicherheit**
- **Diskussion und Abschluss** („open end“)

DHCP

Zentraler DHCP-Dienst
für das MWN

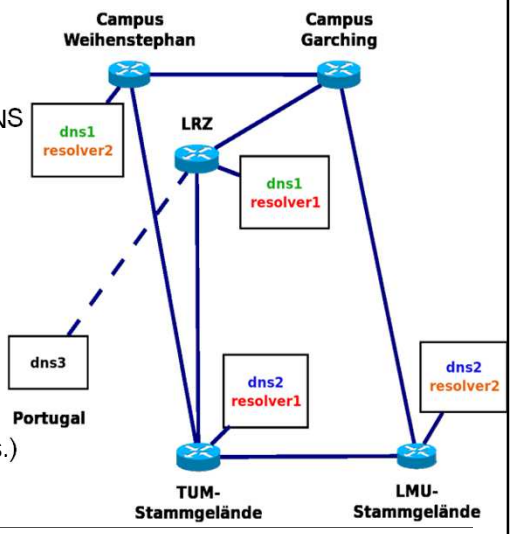
Neu:

- Läuft jetzt auf DNS-Server-Plattform
- Pilotbetrieb einer Schnittstelle zum Definieren statischer Einträge automatisch über csv-Tabellen (bei Interesse Mail an dhcpadmin@lrz.de)



DNS

- Zentraler DNS-Dienst im MWN
- 4+1 phys. Server an 5 Standorten
- Trennung Resolving / Authoritativer DNS
- Doppelte Redundanz (anycast)
- Webschnittstelle für Institute
  (302 Nutzer, Software Nixu Namesurfer)
- Second-Level Domains über Reseller (dopoly)
- 2000 Eigene Zonen
  540 Slave-Zonen
  78.000 A-Records
- Ca. 8.5 Mio Queries / Stunde (rek. Res.)

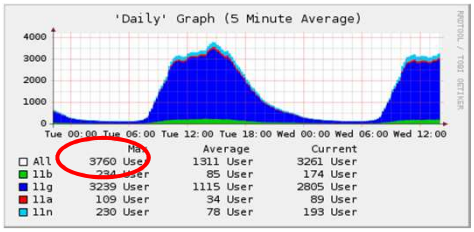


Agenda

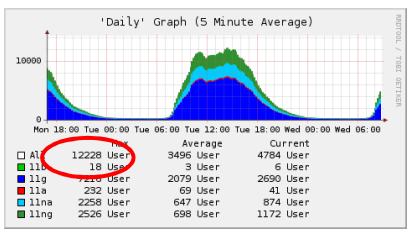
- **Neues im MWN**
- **Dienste im MWN** (W. Beyer)
  - **IPv6 Rollout**
  - **DHCP und DNS Dienst**
  - **WLAN**
- **Sicherheit**
- **Diskussion und Abschluss** („open end“)

WLAN im MWN: Ausbaustatus

- Entwicklung seit letztem NV-Treffen (Oktober 2010)
- Anzahl der APs:
  - 2010: 1.412 APs;
  - 2013: 2.066 APs;
- Anzahl der Nutzer:



07.07.2010



15.1.2013

WLAN Probleme

- Adressen-Knappheit
  - Subnetze hinzugefügt
  - Bessere Verteilung
  - SSID IPv6-only
- APs überlastet, 2.4 GHz Frequenzband voll
  - Zusätzliche APs, Austausch alte HP MSM 310
  - Abschaltung IEEE 802.11b
  - Band Steering (5 GHz Band bevorzugt)
- Sicherheit
  - Abschaltung WPA

WLAN-Auswahl

- Regelmäßige Überprüfung der Produkteignung
- Marktuntersuchung ergab 15 potentiell geeignete Hersteller
- Erstellung einer Anforderungsliste mit 50 Punkten
- Rücklauf von 11 Firmen
- Erfüllung der Kernanforderungen durch Aruba, Cisco und HP
- Testinstallationen von Aruba und Cisco-Geräten
- Testergebnis: 11 / 0 / -2 Punkte für Aruba / Cisco / HP
- Entscheidung für Aruba / Alcatel-Lucent (trotz höherem Preis)
- Controller-basiert statt Stand Alone APs

WLAN – Altes und Neues

- Ca. 300 neue APs pro Jahr
  Wünsche (nur für öffentliche Bereiche – nicht für Büros)
  an Reiser@lrz.de
- Offenes Konferenznetz:
  http://www.lrz.de/services/netz/mobil/kongress/
- Gastkennungen:
  Einrichten durch Masteruser per ID-Portal
  Maximal 7 Tage gültig
  Zur Eduroam-Nutzung

WLAN: Zusammenfassung

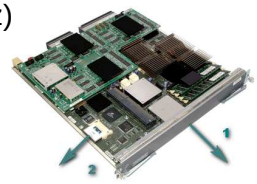
- (Noch) kein Ersatz für Festverkabelung
- Derzeit keine flächendeckende Versorgung finanzierbar
- Versorgt werden **öffentliche** Bereiche
  - Hörsäle, Seminarräume
  - Bibliotheken
  - Labore, studentische Projekträume, Cafeterien
- Weitere Infos unter: **www.lrz.de/wireless**

Agenda

- **Neues im MWN**
- **Dienste im MWN**
- **Sicherheit** (Dr. W. Hommel)
  - **Firewall-Auswahl**
  - **Security Information & Event Management (SIEM)**
  - **Security Monitoring Mails**
  - **DFN-CERT Netzwerkprüfer**
- **Diskussion und Abschluss** („open end“)

Firewall-Auswahl

- Im Einsatz: 99 Virtuelle Firewalls über Cisco FWSM
  2 VFW über Cisco ASA 5580 (RZ-Netz)
- FWSM nicht kompatibel mit neuer Routerplattform
- Produkt-Support für FWSM ist abgekündigt
- Übergangsweise Betrieb in alten Cisco 6509



Firewall-Auswahl: Anforderungen

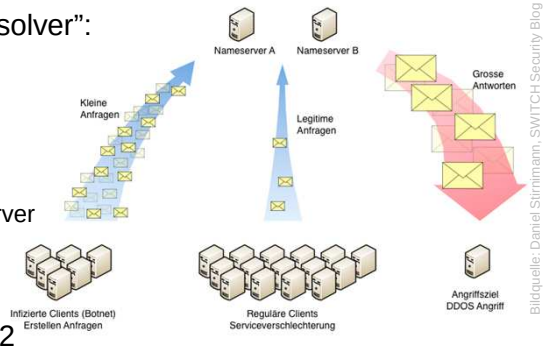
- Charakteristische Herausforderungen im MWN:
  - Unterstützung möglichst hoher Bandbreiten (gesamt und pro Verbindung)
  - Mandantenfähige virtuelle Firewall-Instanzen
- Grundlegende Anforderungen:
  - Migrationspfad von Cisco-Konfiguration
  - Zentrales Management
  - Volle IPv6-Unterstützung
  - Feingranulare Ressourcenprovisionierung
- Verbesserungen gewünscht gegenüber Status quo u.a. bei:
  - Redundanz durch HA
  - VPN-Integration
  - Integrierte IDS-Funktionalität und SIEM-Anbindung
- (Viele andere, Anforderungskatalog mit insg. über 50 Positionen)

Firewall-Auswahl: Mögliche Alternativen

- Evtl. übergangsweise Open-Source-Lösungen
  - Linux-Server mit iptables
  - pfsense
- Kommerzielle Lösungen (in Evaluation)
  - Cisco ASA Appliances
  - FWSM-Module für Cisco Nexus 7000
  - FW-Lösung von Palo Alto
  - FW-Lösung von Stonesoft
  - FW-Lösung von Checkpoint
  - ...

DNS-Sicherheit: Offene Resolver

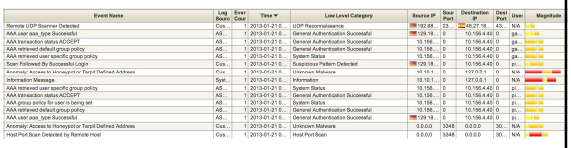
- DNS-Server werden seit 2012 verstärkt für (D)DoS-Angriffe missbraucht (DNS Amplification Attack)
- Betroffen sind primär “offene Resolver”:
  - Beantworten beliebige Anfragen
  - auch für Clients aus dem Internet
- MWN im September 2012:
  - Ca. 58 weltweit erreichbare DNS-Server
  - 26 davon beantworten Anfragen rekursiv
- LRZ-Resolver im November 2012 umkonfiguriert
- DNS-Verwaltung über das LRZ: http://www.lrz.de/services/netzdienste/dns/



Bildquelle: Daniel Stirnimann, SWITCH Security Blog

Security Information & Event Management

- SIEM-Systeme
  - aggregieren Logdaten/NetFlows/…
  - korrelieren dienstübergreifend,
  - erkennen potentielle Sicherheitsvorfälle regelbasiert und
  - stoßen automatisiert Reaktionen an (z.B. E-Mail an Netzverantwortlichen)
- Bisher am LRZ für den X-WiN-Übergang im Einsatz: OSSIM v4
  - Keine IPv6-Unterstützung: mehrfach angekündigt, nie realisiert
- Evaluation IPv6-fähiger SIEM-Systeme 01/2013-03/2013, u.a.
  - IBM Q1 Labs QRadar
  - McAfee Enterprise Security Manager
- Neues System soll auch div. Security-Monitoring-Skripte ablösen



Security-Monitoring-Mails

Quelle	Subject	Quell-IP	Q-FQDN	Ziel-IP	Z-FQDN	Q-Port	Z-Port	Timestamp	Switch-Port	Standort
OSSIM	**Virus detected**	ja	ja	1	nein	1	1	ja	ja	ja
OSSIM	**Internal SSH-Attacker**	ja	ja	nein	nein	nein	ja (22)	ja	nein	ja
Accounting	**DoS-Verdacht**	ja	ja	ja	nein	ja	ja	Dauer	nein	nein
Accounting	**Portscans (outbound)**	ja	ja	ja	nein	ja	ja	Dauer	nein	nein
Accounting	**Traffic Limit (Stunde)**	ja	ja	nein	nein	nein	nein	Interv. 1h	nein	nein
Accounting	**Traffic Limit (halber Tag)**	ja	ja	nein	nein	nein	nein	Interv. 12h	nein	nein
Accounting	**Scans outgoing over Limit**	ja	nein	nein	nein	nein	ja	Interv. 1h	nein	nein
Accounting	**Erhöhter Mailversand**	ja	ja	ja	ja	nein	25 (SMTP)	Interv. 5m	nein	nein
Accounting	**Erhöhter Mailversand**	ja	ja	ja	ja	nein	25 (SMTP)	Interv. 1h	nein	nein
Accounting	**Extremer Mailversand**	ja	ja	ja	ja	nein	25 (SMTP)	Interv. 5m	nein	nein
Accounting	**Extremer Mailversand**	ja	ja	ja	ja	nein	25 (SMTP)	Interv. 1h	nein	nein

Portscans mit DFN-CERT Netzwerkprüfer

- nmap-basiertes Portscan-Werkzeug:
  - Meldet vom DFN-System aus erreichbare offene TCP-Ports
  - Alle 4 Wochen automatisiert wiederholbar
- Anwendung u.a.
  - Prüfen der eigenen Firewall-Regeln
  - Auffinden unerwünschter Serverdienste
- Scanbereich beschränkt auf registrierte Netze der DFN-Mitgliedseinrichtung
- Derzeit noch nicht mandantenfähig -> bei Interesse an LRZ Servicedesk wenden!
- https://www.cert.dfn.de/fileadmin/CERT/DFN78_Netzwerkpruefer.pdf

Agenda

- **Neues im MWN**
- **Dienste im MWN**
- **Sicherheit** (Dr. W. Hommel)
- **Diskussion und Abschluss** („open end“)