Informationsveranstaltung für Netzverantwortliche im Münchner Wissenschaftsnetz (MWN)

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

München, 11. Oktober 2010

W. Beyer, Dr. W. Hommel, Dr. H. Reiser, B. Schmidt

Agenda

- **Neues im MWN** (~15 Min.) (Dr. H. Reiser)
- **Aufgaben von Netzverantwortlichen an praktischen Beispielen** (~15 Min.) (Dr. H. Reiser)
- **Self Service Portal NeSSI** (~10 Min.) (W. Beyer)
- **„Kurznachrichten“: Änderungen an Netzkomponenten und Diensten** (~15 Min.) (Dr. W. Hommel)
- **IPv6 im MWN** (~20 Min.) (B. Schmidt)
- **DNSSEC und Teilnahme am DENIC-Testbed** (~20 Min.) (B. Schmidt)
- **Diskussion und Abschluss** („open end“)

Agenda

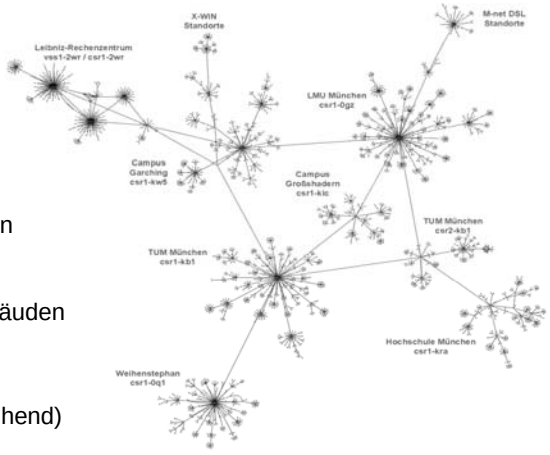
- **Neues im MWN** (Dr. H. Reiser)
- **Aufgaben von Netzverantwortlichen an praktischen Beispielen** (Dr. H. Reiser)
- **Self Service Portal NeSSI** (W. Beyer)
- **„Kurznachrichten“: Änderungen an Netzkomponenten und Diensten** (Dr. W. Hommel)
- **IPv6 im MWN** (B. Schmidt)
- **DNSSEC und Teilnahme am DENIC-Testbed** (B. Schmidt)
- **Diskussion und Abschluss** („open end“)

Agenda: Neues im MWN

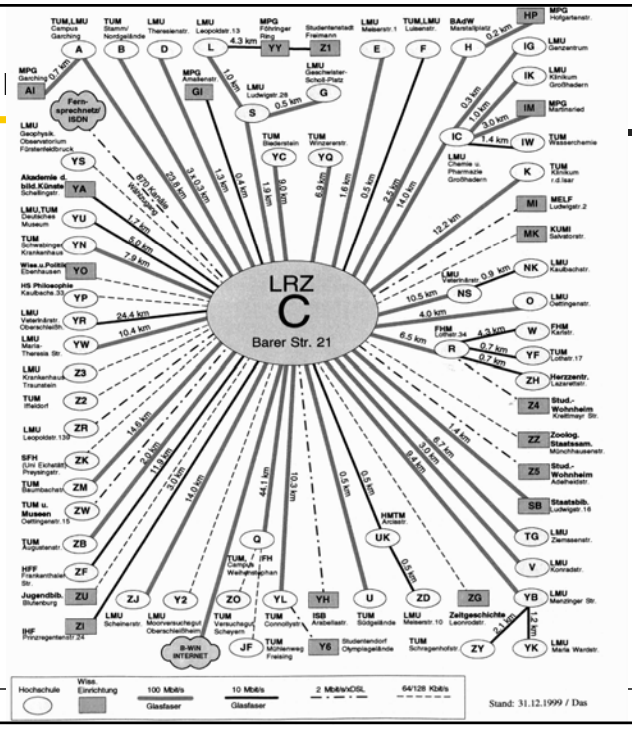
- Überblick über das MWN
- Backbone Struktur
- Erhöhte Redundanz und Ausfallsicherheit
- Versorgung mit WLAN

MWN - Überblick

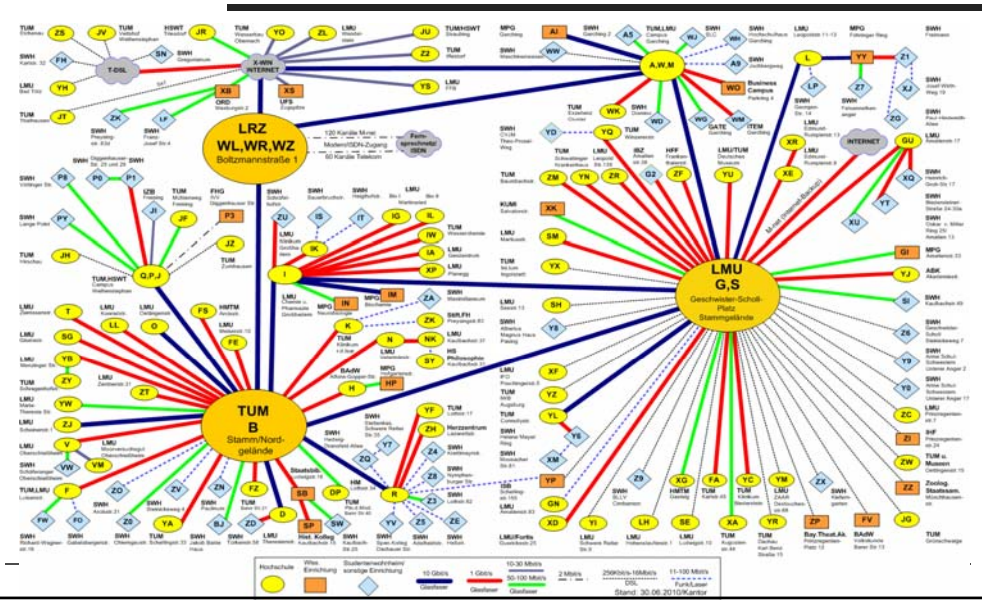
- Nutzer
  - 90.000 Studenten
  - 30.000 Mitarbeiter
- Kennzahlen
  - 11 Router
  - 1000 Switches
  - 1400 Accesspoints
  - 51 gemietete dark fibre Leitungen
  - 30+ private dark fibre Leitungen
  - Fast 80.000 Endgeräte
  - 50 Lokationen mit über 500 Gebäuden
- Übertragene Daten (Juni 2010)
  - 360/450 Tbyte/Monat (aus/eingehend)
  - 8,3 PByte/Monat über Backbone



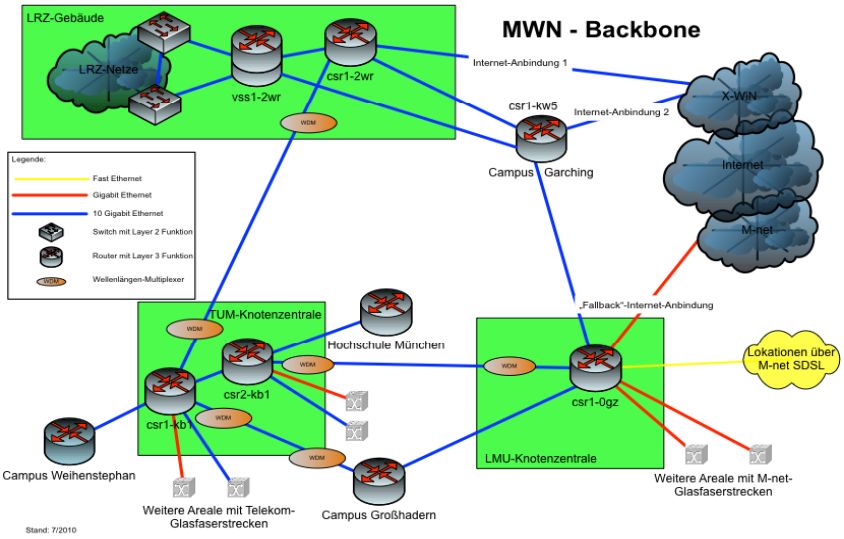
Entwicklu



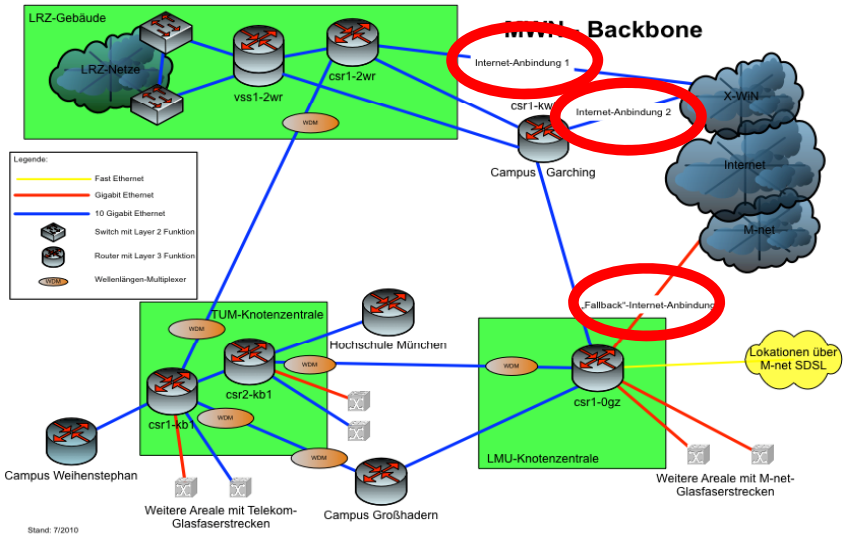
MWN 2010



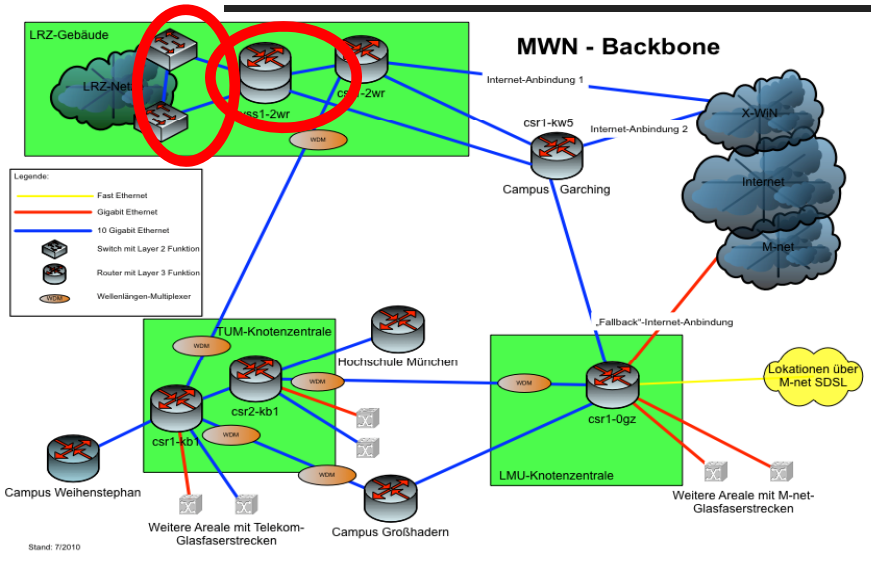
MWN-Backbone



Ausfallsicherheit / Redundanz



Ausfallsicherheit / Redundanz

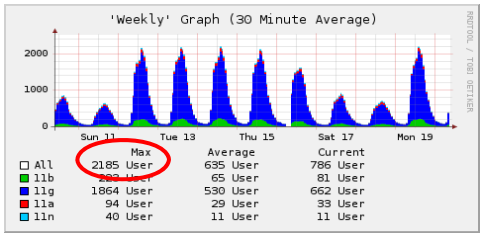


Wireless LAN im MWN

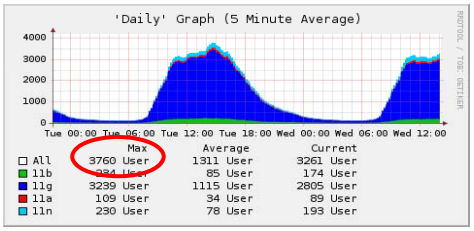
- Standards und Bandbreiten
  - 802.11b 2,4 GHz bis 11 Mb/s
  - 802.11g 2,4 GHz bis 54 Mb/s
  - 802.11a 5 GHz bis 54 Mb/s
  - 802.11n 2,4 und 5 GHz bis 300 Mb/s
- Zugang erfordert Authentisierung
  - Über 802.1x (SSID: 802.1x oder eduroam)
  - VPN-Client (SSID: lrz)
  - SSID für Institut möglich
  - Kongresse und Tagungen (nur temporär) (SSID: con)
- Nutzung durch reisende Wissenschaftler
  - Über eduroam (SSID: eduroam)
  - Jeder europäische Wissenschaftler kann mit **seiner** Kennung WLAN im MWN nutzen

Ausbaustatus WLAN im MWN

- Entwicklung seit letztem NV-Treffen (März 2009)
- Anzahl der APs:
  - 2009: 1.127 APs; (802.11n im Testbetrieb)
  - 2010: 1.412 APs; (802.11n im Regelbetrieb mit gut 300 APs)
- Anzahl der Nutzer:



20.01.2009



07.07.2010

WLAN Ausblick

- (Noch) kein Ersatz für Festverkabelung
- Derzeit keine flächendeckende Versorgung finanzierbar
- Versorgt werden **öffentliche** Bereiche
  - Hörsäle, Seminarräume
  - Labore, studentische Projekträume, Cafeterien
- Wünsche an **reiser@lrz.de**

- Weitere Infos unter:
  www.lrz.de/wireless

Agenda

- **Neues im MWN** (Dr. H. Reiser)
- **Aufgaben von Netzverantwortlichen an praktischen Beispielen** (Dr. H. Reiser)
- **Self Service Portal NeSSI** (W. Beyer)
- **„Kurznachrichten“: Änderungen an Netzkomponenten und Diensten** (Dr. W. Hommel)
- **IPv6 im MWN** (B. Schmidt)
- **DNSSEC und Teilnahme am DENIC-Testbed** (B. Schmidt)
- **Diskussion und Abschluss** („open end“)

Agenda: Aufgaben für Netzverantwortliche

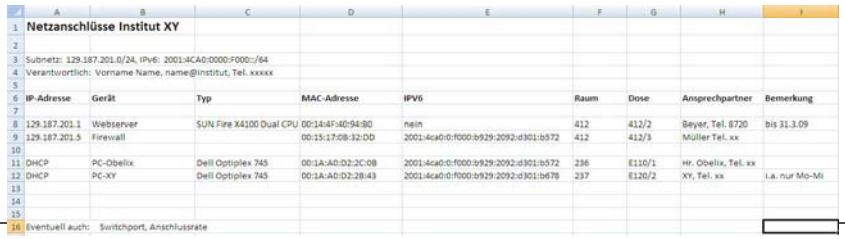
- Rolle des Netzverantwortlichen
- Adressverwaltung
- DNS: Namen eintragen
- Sonstige Aufgaben und Problemfelder
- Mithilfe bei der Abuse-Bearbeitung
- Planung neuer Netzstrukturenm

Netzverantwortlicher

- 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 ?
  www.lrz.de/services/netz/db_netzverantwortliche

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.



Netzanschlüsse Institut XY

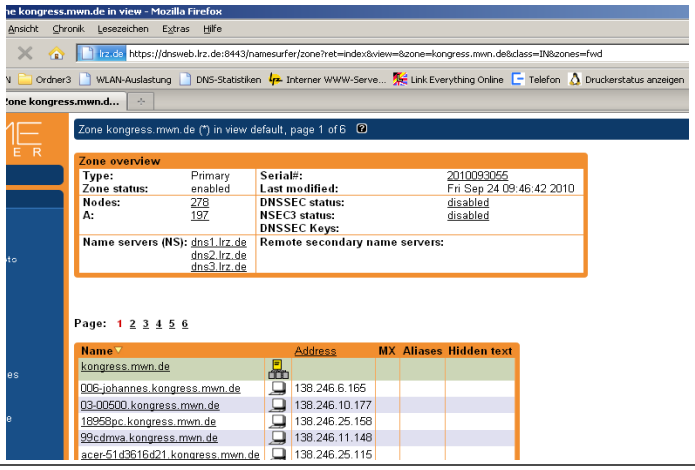
Subnetz: 129.187.201.0/24, IPv6: 2001:4CA0:0000:F000::/64
Verantwortlich: Vorname Name, name@institut, Tel. xxxxx

IP-Adresse	Gerät	Typ	MAC-Adresse	IPV6	Raum	Dose	Ansprechpartner	Bemerkung
129.187.201.1	Webserver	SUN Fire X4100 Dual CPU	00:14:4F:40:94:80	nein	412	412/2	Beyer, Tel. 8720	bis 31.3.09
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	
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	
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

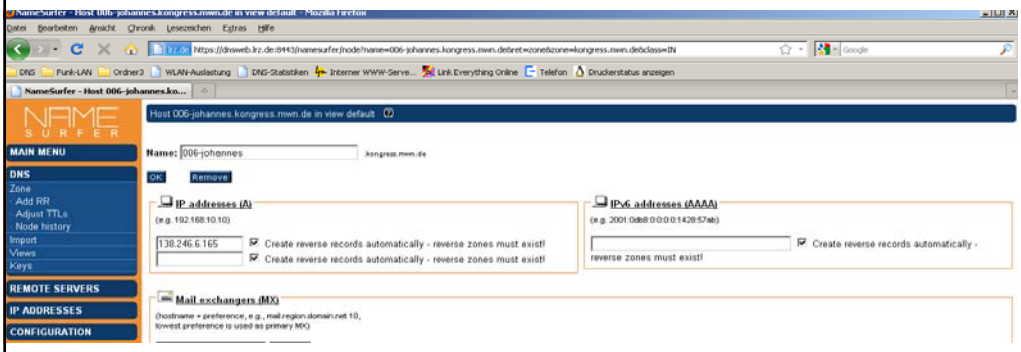
Eventuell auch: Switchport, Anschlussrate

Verwaltung von Namen / Adressen: DNS

- Self-Service über WebDNS



Eintrag von Namen in WebDNS



- Weitere Informationen:

  www.lrz.de/services/netzdienste/dns

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 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 Abnahmeprotokollen 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)
- **Aufgaben von Netzverantwortlichen an praktischen Beispielen** (Dr. H. Reiser)
- **Self Service Portal NeSSI** (W. Beyer)
- **„Kurznachrichten“: Änderungen an Netzkomponenten und Diensten** (Dr. W. Hommel)
- **IPv6 im MWN** (B. Schmidt)
- **DNSSEC und Teilnahme am DENIC-Testbed** (B. Schmidt)
- **Diskussion und Abschluss** („open end“)

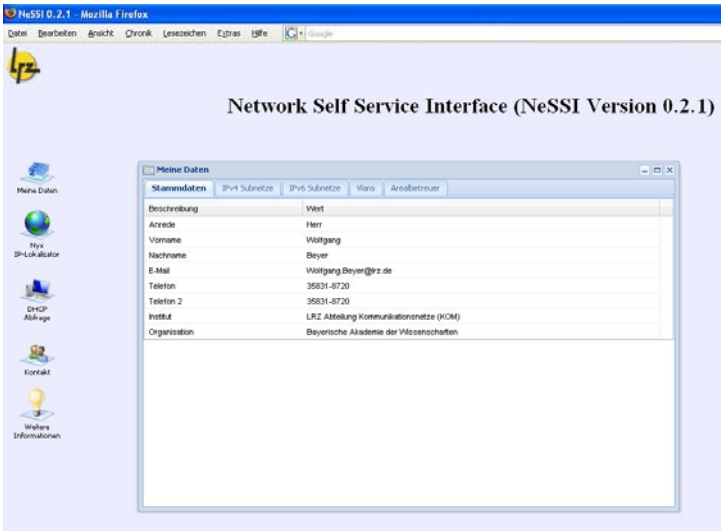
Webseite Netzverantwortliche

Informationen für Netzverantwortliche (bisher)

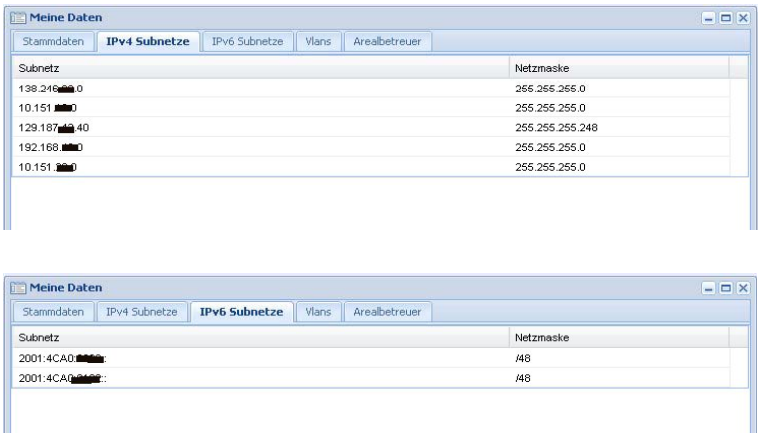
NeSSI - Portal für Netzverantwortliche

- Network Self Service Interface
- Einführung geplant für Mitte November 2010
- Anzeige der Daten des eigenen Zuständigkeitsbereichs
- Voraussetzung: LRZ-Benutzerkennung
- Module:
  - Anzeige der gespeicherten Daten (Subnetze, persönliche Daten)
  - Mitteilungen/Anfragen an LRZ
  - Nyx: Suchen nach Endgeräten
  - DHCP: Anzeige von DHCP-Informationen
  - geplant: Entsperren von gesperrten Rechnern

NeSSI

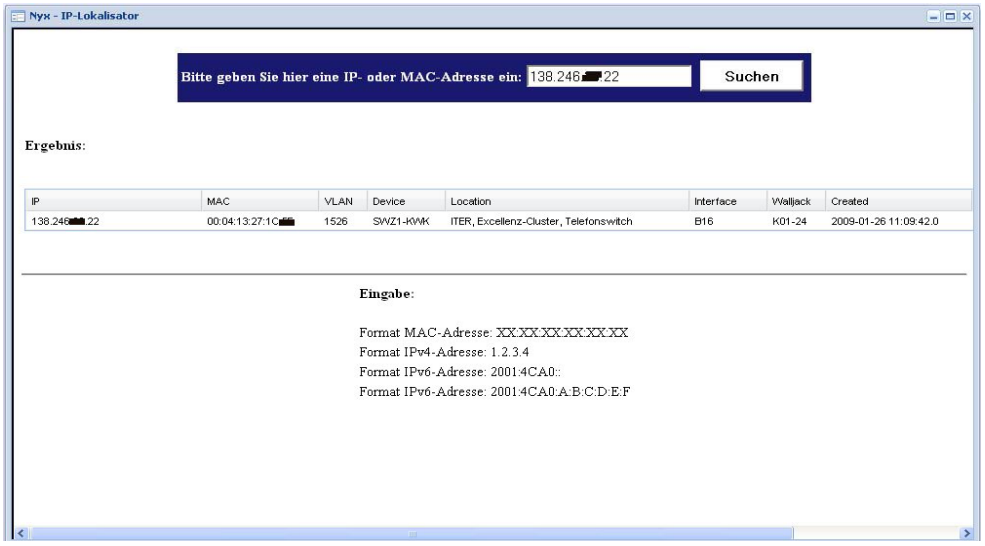


NeSSI -Subnetze



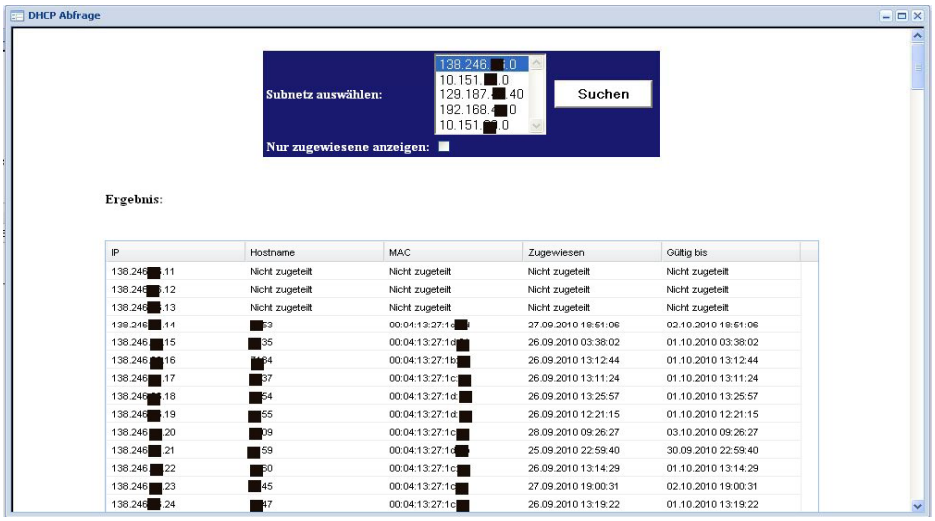
NeSSI - Arealbetreuer

NeSSI - Nyx

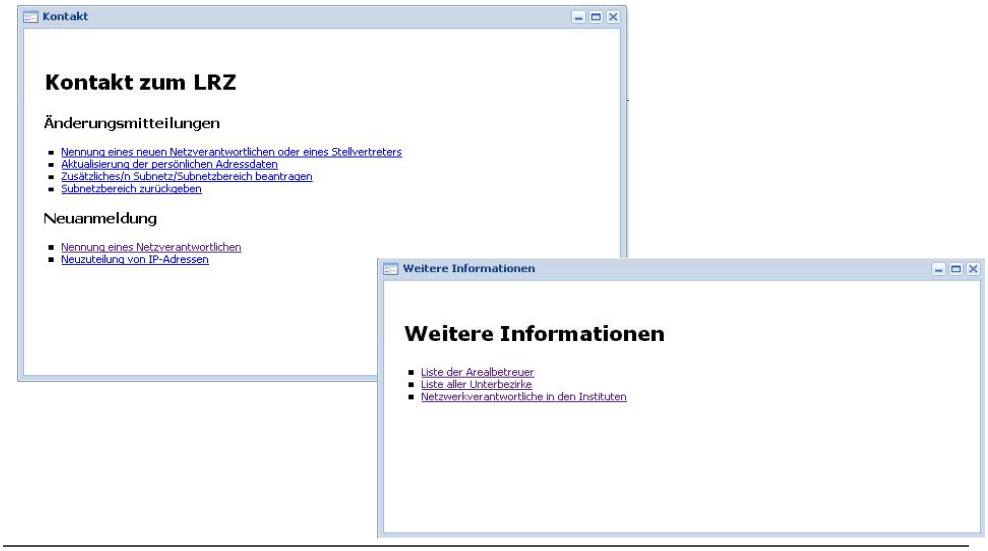


NeSSI - Nyx

NeSSI - DHCP



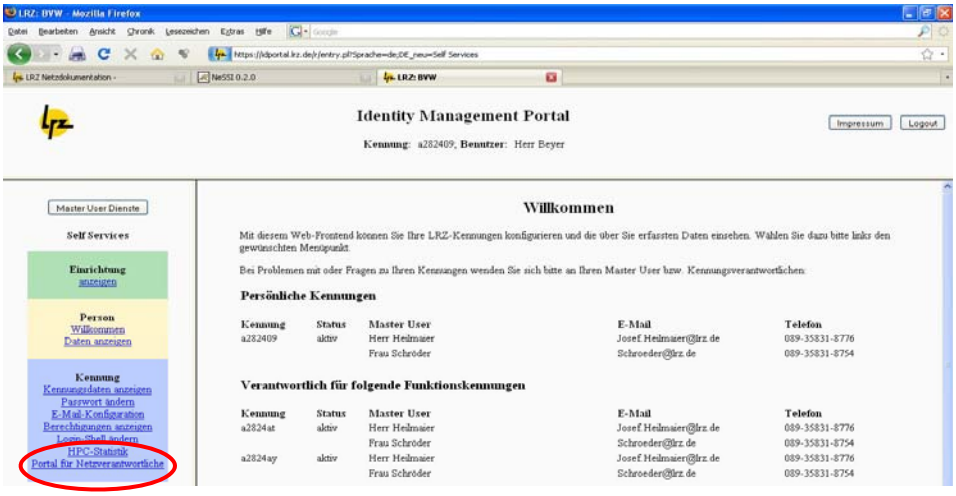
NeSSI - Kontakt, Weitere Informationen



NeSSI - Interna

- alles Open Source unter Linux
- Backend (Server) Entwicklung:
  - Tomcat 6
  - Java 1.6 von Oracle (Sun)
  - Java Server Faces (JSF) 2.0 (My Faces von Apache (http://myfaces.apache.org/)
- Webdesktop
  - geschrieben in Javascript mit Extjs (http://www.sencha.com/products/js/)
  - Entwicklung mit Eclipse 3.4 und Apache Maven 2.2.1 ("make for Java")
- ca. 5.000 Codezeilen

NeSSI - Aufruf über ID-Portal



Vergabe von Kennungen

- Grundlage: LRZ-Projekt (Vertrag mit LRZ, Papierform nötig)
- Kennungsvergabe durch Master User, LRZ-Kontakt: Betreuer
- LRZ-Kennung nicht „sprechend“, z.B. lu23rip
- Verwaltung über ID-Portal https://idportal.lrz.de/r/entry.pl
- Informationen unter http://www.lrz.de/wir/kennung/

Agenda

- **Neues im MWN** (Dr. H. Reiser)
- **Aufgaben von Netzverantwortlichen an praktischen Beispielen** (Dr. H. Reiser)
- **Self Service Portal NeSSI** (W. Beyer)
- **„Kurznachrichten“: Änderungen an Netzkomponenten und Diensten** (Dr. W. Hommel)
- **IPv6 im MWN** (B. Schmidt)
- **DNSSEC und Teilnahme am DENIC-Testbed** (B. Schmidt)
- **Diskussion und Abschluss** („open end“)

eduroam mit PEAP/MS-CHAPv2

- Weltweite Nutzung von Hochschul-WLANs mit eigenen Kennung

eduroam mit PEAP/MS-CHAPv2 (2/2)

- Neue Radius-Zone für Authentifizierung über PEAP/MS-CHAPv2
- Benutzername ist lrzkennung@eduroam.mwn.de
- Nutzbar mit
  - allen über Master User und von CampusLMU vergebenen LRZ-Kennungen
  - von TUMonline vergebenen LRZ-Kennungen erst ab Anfang 2011
- Keine zusätzliche Software unter Windows 7, Linux, Mac OS X und vielen Smartphone OS (Blackberry, Android, Bada) notwendig
- Konfigurationsanleitungen unter: http://www.lrz.de/services/netz/mobil/eduroam/

Cisco AnyConnect VPN Client

- Cisco AnyConnect SSL-VPN-Client
  - Unterstützt 64-Bit-Versionen von Windows, Linux und Mac OS X
  - Auch für Windows Mobile verfügbar
  - Einfache, über Webseite angestoßene Installation unter https://asa-cluster.lrz.de
  - Telekom- und DFN-Zertifikate müssen installiert sein, siehe http://www.lrz.de/services/netz/mobil/vpn/anyconnect/

Switching-Infrastruktur-Modernisierung (1/2)

- Derzeit noch rund 300 ältere Modelle im Einsatz:
  - HP ProCurve 4000M (seit rund 10 Jahren)
    - Hardware: Nur 3,8 GBit/s Backplane, niedrige Portdichte
    - Firmware unterstützt weder Spanning Tree Protocol noch 802.1X
    - Seit 2006 nicht mehr im HP-Portfolio

  - HP ProCurve 4100gl
    - Hardware: Keine Module mit 10 Gbit-Ports verfügbar
    - Firmware wird seit zwei Jahren nicht mehr weiterentwickelt
    - Seit 2008 nicht mehr im HP-Portfolio

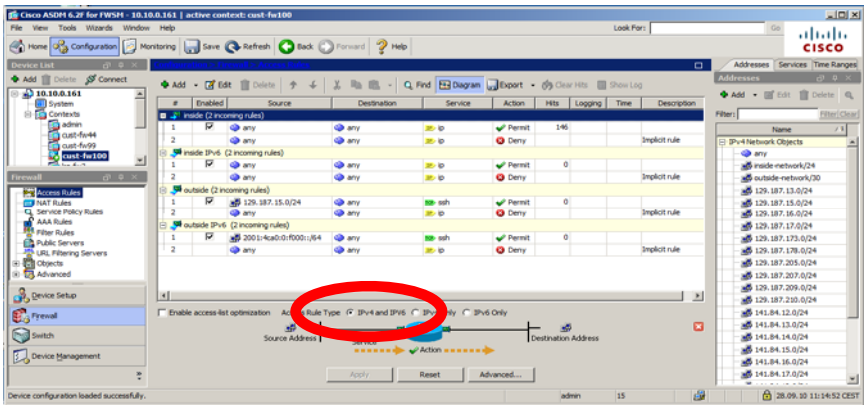
- Ersetzung über mehrere Jahre verteilt:
  - Nachfolgesysteme: HP ProCurve 4200vl und HP ProCurve 5400zl
  - Damit Upgrade der Office-Anbindung von 100 MBit/s auf 1 GBit/s

Switching-Infrastruktur-Modernisierung (2/2)

- Miniswitches in Fiber-to-the-Office-Netzen
  - bislang häufig nur 100-MBit-Ports
  - Ablösung durch GBit-fähige Geräte
    - 4x GBit TP-Ports für Endgeräte, Gigabit SFP Slot Uplink
    - Lüfterlos, vrsl. externes Netzteil
  - Kompletter Austausch in LMU Biologie I (Martinsried)

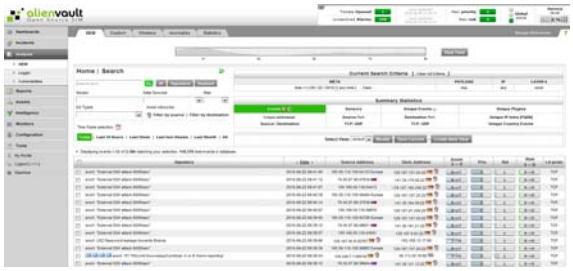
Virtuelle Firewalls: IPv6-fähiges Management-GUI

- Derzeit 53 gehostete vFW im Produktiveinsatz (+ 18 in Vorbereitung)
- 60 neue VFW-Lizenzen beschafft



Zentrales Security-Monitoring mit OSSIM

- Korrelation der vom Intrusion Detection System Snort gemeldeten Events
- Automatisches Alerting (24x7)
- Eskalationsmechanismus (Mail, Erinnerung, Sperrung)
- Erkannte Angriffe:
  - Mariposa-Botnet
  - Botnet-C&C-Kommunikation
  - Viren/Trojaner (Conficker, Bredolab, Torpig, Sality, …)
  - Ausgehende SSH Scans
  - FTP-Server
  - …



Groupware: Microsoft Exchange (1/2)

- Nutzungsmöglichkeit:
  - TUM:
    - Nur für persönliche tum.de und mytum.de Adressen
    - Benutzer wählt individuell über TUMonline zwischen myTUM-Mailserver und Exchange
  - LMU:
    - Pilotbetrieb für Tiermedizin
    - „LRZ-projekt“-weite Umstellung erforderlich
    - bisher nur für persönliche Kennungen
- Planung:
  - Umstellung auf Exchange 2010 ist in Arbeit
  - Danach LMU-weite Nutzung mit einrichtungsspezifischen Maildomains möglich
  - Funktions- und Ressourcenobjekte ab Q2/2011
  - Anschließend auch einrichtungsspezifische Maildomains für TUM

Groupware: Microsoft Exchange (2/2)

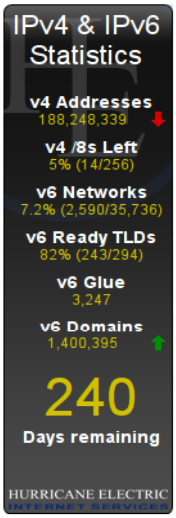
- Kosten:
  - LRZ übernimmt Server-Lizenzkosten
  - Einrichtungen müssen Microsoft Client Access Licenses haben
  - CAL-Kosten pro Exchange-Version (ca. 3-4 Jahre im Einsatz) einmalig rund 10 Euro pro User

Agenda

- **Neues im MWN** (Dr. H. Reiser)
- **Aufgaben von Netzverantwortlichen an praktischen Beispielen** (Dr. H. Reiser)
- **Self Service Portal NeSSI** (W. Beyer)
- **„Kurznachrichten“: Änderungen an Netzkomponenten und Diensten** (Dr. W. Hommel)
- **IPv6 im MWN** (B. Schmidt)
- **DNSSEC und Teilnahme am DENIC-Testbed** (B. Schmidt)
- **Diskussion und Abschluss** („open end“)

Protokoll

- Nachfolger von IPv4
- Entwicklung seit 1994 (IPng)
  - wegen erwarteter Adressknappheit
- Adressen: 128 Bit statt 32 Bit
- andere Schreibweise:
  - IPv4: 129.187.254.78, 127.0.0.1
  - IPv6: 2001:4ca0:0:103::81bb:fe12, ::1
- Konzeptionell weitgehend ähnlich zu IPv4
  - Einige Sonderfälle aufgeräumt
  - Namen ändern sich, sonst sehr ähnlich
    - Address Resolution Protokoll (ARP) → Neighbor Discovery (ND)



MWN-Deployment

- Vollständiges natives IPv6-Rollout im Backbone seit 2005
  - gleiche Hardware, gleiche Verfügbarkeit, gleiche Geschwindigkeit
- IPv6 in verschlüsseltem WLAN (eduroam)
- Aktuell etwa 60 Netze
- Teilnahme am Testbed von Google und Wikipedia
- Viele Dienste sind schon IPv6-fähig
  - unter anderem DNS, NTP, virtuelle Webserver, Teile der Mail-Infrastruktur, VPN
- Weitere Dienste geplant
  - TSM-Backup, Exchange, Filer, Windows-Updates und vieles mehr

L1 prüfen
LRZ; 28.09.2010

Anbindung – bisher

- Netzverantwortlicher füllt Auftrag auf http://www.lrz.de/services/netz/ipv6/ aus
- bekommt einen Netzbereich zugewiesen (/48 = 65536 Subnetze)
- wendet sich an ipadmin@lrz.de für eine Konfiguration
  - Absprache welches Subnetz, welche Adressierungsoption, welche Sicherheitsoption
  - Konfiguration erfolgt

Anbindung – neu (zusätzlich)

- Zuweisung eines Subnetzes nach 2-Jahres Migrationsplan
- Benachrichtigung der Netzverantwortlichen
  - üblicherweise zwei Wochen Frist, zur Urlaubszeit mehr
- Bei ausbleibenden Änderungswünschen:
  - Konfiguration der Netze
    - RA/SLAAC (siehe spätere Folie)
    - Stateless DHCPv6 mit DNS-Informationen (wo möglich)
  - Sicherheitspolicy wird durch IPv4 bestimmt
    - Öffentliches IPv4-Netz: IPv6 global erreichbar
    - Privates IPv4-Netz: kein TCP/SYN aus dem Internet
    - Virtuelle Firewall: Verbindungen von außen geblockt

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

- Für die Vergabe des Hostteils gibt es verschiedene Methoden
  - Statisch
  - Router Advertisement (RA), Stateless Address Autoconfiguration (SLAAC)
    - Privacy Extensions
    - Stateless DHCPv6
  - Stateful DHCPv6

Adressierung – statisch

- Üblicherweise vier Blöcke mit je vier Hexadezimalziffern zur Verfügung
  - 0000:0000:0000:0000 reserviert
  - 0000:0000:0000:000* LRZ-Systeme
  - Sonst freie Auswahl

- Empfehlung: IPv4-Adresse einkodieren
  - 129.187.254.216
    → 2001:4ca0:0:103::129.187.254.216 = 2001:4ca0:0:103::81bb:fed8

Adressierung – Router Advertisement (RA)

- Host erstellt nach dem modified EUI-64-Standard aus seiner MAC-Adresse (eindeutig!) einen 64bit-Interface Identifier
  - 00:21:9b:80:d1:cd wird zu 0221:9bff:fe80:d1cd
  - Ausnahme Vista/7/Win2k8 mit randomized IID
- Router „broadcasted“ regelmäßig und auf Aufforderung ein Router Advertisement ins Subnetz (enthält /64-Prefixe)
- **Alle** IPv6-fähigen Hosts generieren sich aus Prefixen und Interface-Identifier globale Adressen
- Kein automatisches Reverse-DNS
- Rechner ist weltweit identifizierbar
  - Bei NIC-Tausch ändert sich die Adresse
- Keine weitergehenden Konfigurationsinformationen

Adressierung – RA/SLAAC

- Privacy Extensions
  - Host generiert regelmäßig (alle zwölf Stunden) eine **zusätzliche**, zufällige IPv6-Adresse und nutzt diese für ausgehende Verbindungen
  - Standardmäßig aktiviert auf Windows, optional (sysctl) auf MacOS X und Linux
- Stateless DHCPv6
  - Ähnlich bekanntem DHCPv4
  - Verteilt keine Adressen (stateless!) und Routen, sondern ausschließlich Konfigurationsinformationen (DNS, Domain, NTP)
  - (noch) keine Möglichkeit für automatische DNS-Einträge
  - Client mitgeliefert auf Windows Vista/7/2k8
    - 3rd Party Clients (dibbler, wide-dhcpv6, ISC dhclient) für Windows XP, Linux, MacOS X
  - aktuell nicht hinter virtuellen Firewalls

Adressierung – stateful DHCPv6

- Fast wie bekanntes DHCPv4
  - Adresse(n), Konfigurationsinformationen
  - (noch) keine Default-Route, muss aus Router Advertisement kommen
  - Automatisches individuelles Reverse DNS möglich (allerdings noch nicht in der gleichen Vorwärtszone)
  - ebenfalls nicht hinter virtuellen Firewalls

Adressierung – ISATAP

- Automatischer Tunneldienst für Clients
- weist pro IPv4-Adresse exakt eine IPv6-Adresse zu
  - Adressen im MWN 2001:4ca0:0:fe00::5efe:<ipv4adresseinHex>
- Redundante Infrastruktur
- Automatische Konfiguration durch DNS (Host isatap.<domain>)
  - Eingetragen in vielen Client-Zonen (VPN etc)
  - Im eigenen Lehrstuhl isatap.<domain> CNAME isatap-relay.lrz.de eintragen
- Nur auf Windows mitgeliefert
  - extra Client für Linux, schwierig auf MacOS X
- http://www.lrz.de/services/netz/ipv6/isatap1/

Sicherheit

- Ungezielte Scans ganzer Subnetze nicht mehr möglich
  - bei bekannter Adresse eines Zielhosts (DNS, Verkehr nach außen) aber weiterhin angreifbar (Exploits etc)
- keine privaten IP-Adressen, kein NAT mehr
  - alle IPv6-Netze haben globale Adressen
- Sicherheit über
  - Hostfirewalls
  - Netzfirewalls (virtuelle Firewall)
  - nicht-reflexive Routerfilter
    - Kommunikation nur mit dem MWN – VORSICHT
    - Kein TCP-SYN (aus dem Internet)
  - Secomat-Erweiterung in Planung

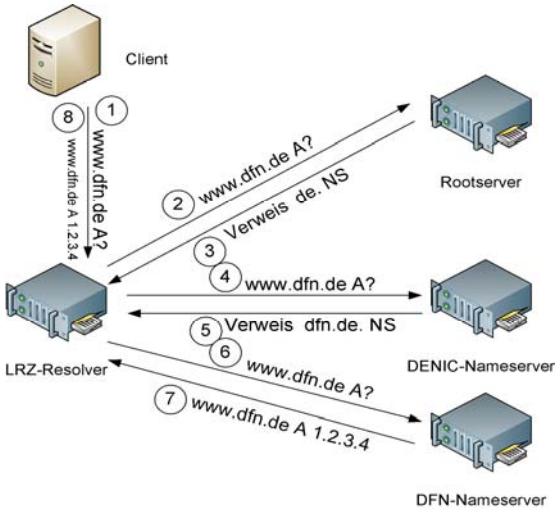
Agenda

- **Neues im MWN** (Dr. H. Reiser)
- **Aufgaben von Netzverantwortlichen an praktischen Beispielen** (Dr. H. Reiser)
- **Self Service Portal NeSSI** (W. Beyer)
- **„Kurznachrichten“: Änderungen an Netzkomponenten und Diensten** (Dr. W. Hommel)
- **IPv6 im MWN** (B. Schmidt)
- **DNSSEC und Teilnahme am DENIC-Testbed** (B. Schmidt)
- **Diskussion und Abschluss** („open end“)

DNSSEC

- Informationsvortrag
- Erfordert **keine** Aktivität der Netzverantwortlichen
  - DNS funktioniert weiter wie gewohnt
- Teilnahme an Tests optional

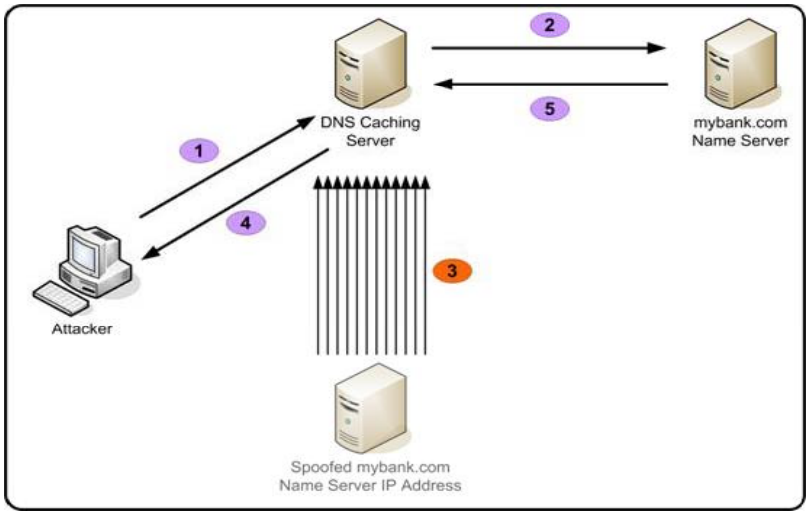
DNSSEC – warum?



DNSSEC – warum?

- DNS-Anfragen erfolgen im Allgemeinen über UDP (verbindungslos)
  - Einfach(er) spoofbare Absenderadressen
- Anfragen/Antworten enthalten nur eine begrenzte Menge an zufälligen Informationen
  - Resolveradresse (bekannt)
  - Adresse des autoritativen Nameservers (üblicherweise zwischen 2 und 5)
  - Quellport (zufällig 1-65535, etwa 15 Bit Zufallswert)
  - Zielport (fest, 53/UDP)
  - QNAME (angefragter Name)
  - DNS Transaktions-ID (1-65536, 16 Bit Zufallswert)
- Angreifer kann Resolver mit gespooften Antworten bombardieren und damit einen falschen Eintrag im Cache hinterlegen.

DNSSEC – warum?

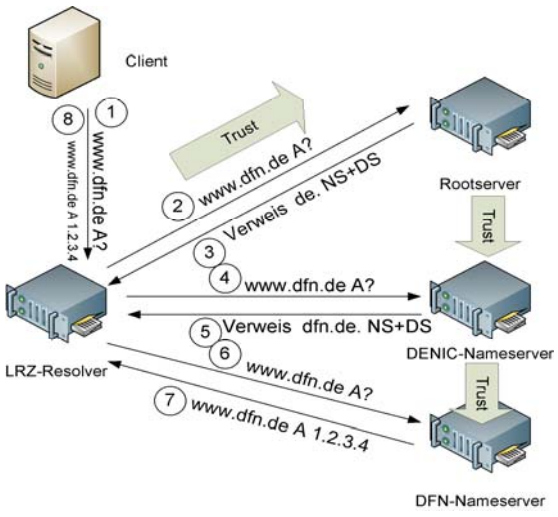


DNSSEC – warum?

- DNSSEC bietet kryptographische Validierung von
  - (Nicht)Existenz von Namen im DNS
  - (Nicht)Existenz von RR-Typen (A/AAAA/NS/MX/…) zu existierenden Namen
  - Inhalt von DNS-Einträgen
- Schutz gegen Replay-Attacken
- Schutz auch bei Man-in-the-Middle Attacken

- Sicherheits- und Komfortgewinn
  - SSHFP Fingerprints
  - IPsec-Schlüssel für Opportunistic Encryption

DNSSEC – wie?



DNSSEC – wie?

- Signierte Zonen haben (mindestens) einen Zone Signing Key (ZSK), bestehend aus einem Public-Key und einem Private-Key
  - Public-Key wird in der Zone hinterlegt, Private-Key bleibt auf dem signierenden System
    - mhn.de. 86400 IN DNSKEY 256 3 10 Av85rnA+N…. ; key id = 56759
- Alle Resource-Records werden mit diesem Key signiert
    - mhn.de. 86400 IN SOA dns1.lrz.de. hostmaster.lrz.de. 2010092913 …
      mhn.de. 86400 IN RRSIG SOA 10 2 86400 20101030000000 20100929070558 56759
      mhn.de. …
- Alle Namen haben zusätzlich einen signierten NSEC-Record (Next SECure)
  - Aneinanderreihung der NSEC-Records ermöglicht Zone-Walking (Abhilfe: NSEC3)
    - mhn.de. 86400 IN NSEC aa.mhn.de. NS SOA RRSIG NSEC DNSKEY

DNSSEC – wie?

- Parent-Zone (zum Beispiel .de) enthält neben der Delegation (NS-Record) einen oder mehrere DS-Records, die den Hash der gültigen Zonenschlüssel enthalten

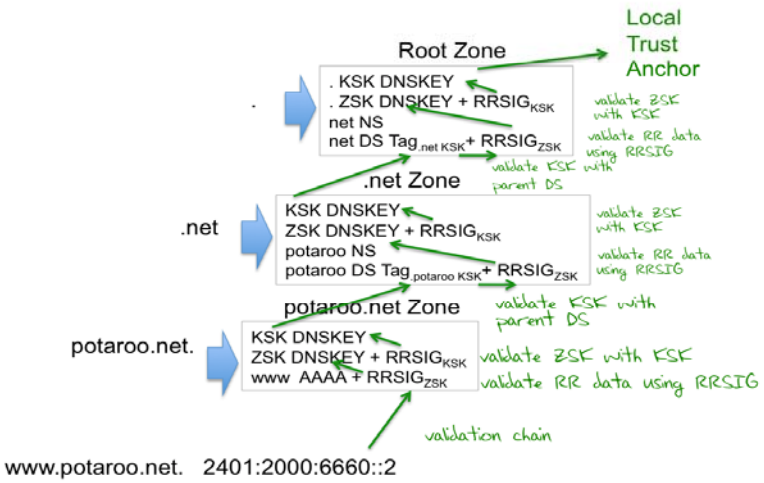
- mhn.de.	86400	IN	NS	dns1.lrz.de.
mhn.de.	86400	IN	NS	dns2.lrz.de.
mhn.de.	86400	IN	NS	dns3.lrz.de.
mhn.de.	86400	IN	NS	ws-han1.win-ip.dfn.de.
mhn.de	86400	IN	DS	56759 10 1 718d...
mhn.de	86400	IN	DS	56759 10 2 2bad…

- Resolver vertrauen manuell konfiguriertem Key der Root-Zone, alle Zonen in der Hierarchie müssen signiert und sicher delegiert sein
  - Alternative: DLV-Dienst (Dynamic Lookaside Validation) des ISC

DNSSEC – wie?

- Private Schlüssel können durch Brute Force oder Unachtsamkeit kompromittiert werden
  - Regelmäßiger Wechsel des Schlüssels muss möglich sein
  - Schlüsselwechsel bedingt Änderung des DS-Records in der delegierenden Zone
- Split zwischen KSK (Key Signing Key) und ZSK (Zone Signing Key)
  - ZSK signiert alle Änderungen der Zone
  - KSK signiert nur die ZSK bei Schlüsseländerung (kann offline erfolgen)
  - Sichere Delegation (DS-Records) mit dem KSK
  - ZSK-Wechsel ohne Interaktion mit der delegierenden Zone

DNSSEC – wie?



DNSSEC am LRZ

- Vollständig DNSSEC-fähige Infrastruktur seit 2008
  - DNSSEC-fähig bedeutet: kann mit den neuen Datentypen umgehen
- Authoritative (= LRZ signiert) DNSSEC-Fähigkeit im WebDNS Dienst seit wenigen Wochen
  - Signiert Zonen mhn.de und 0.a.c.4.1.0.0.2.ip6.arpa
  - lrz.de geplant ab Mitte Oktober
  - Testkunden mit Erfahrung erwünscht
  - Sichere Delegationen (DS) möglich, aber ohne volle Kette nicht sinnvoll

DNSSEC am LRZ

- Rekursive (= LRZ validiert) DNSSEC-Fähigkeit auf resolver1.lrz.de seit Oktober 2009
  - benutzen den ISC DLV-Dienst und vertrauen der signierten Rootzone
  - Nehmen am DNSSEC-Testbed der DENIC Teil
    - http://www.denic.de/de/domains/dnssec.html
  - resolver2.lrz.de explizit nicht validierend

DNSSEC am LRZ

- % dig -t ns bund.de +dnssec
  […]
  ;; flags: qr rd ra ad; QUERY: 1, ANSWER: 5, AUTHORITY: 0, ADDITIONAL: 9
  ANSWER SECTION:

```
bund.de.          16880        IN     NS     argon.bund.de.
bund.de.          16880        IN     NS     nuernberg.bund.de.
bund.de.          16880        IN     NS     bamberg.bund.de.
bund.de.          16880        IN     NS     xenon.bund.de.
bund.de.          16880        IN     RRSIG  NS 7 2 21600
20101007141801 20100927141801 31322 bund.de. AzpeUjaZ
```

- Achtung:
  - Eigene Zonen (am LRZ gehostet) werden auch bei voller DNSSEC-Delegation nicht als sicher ausgegeben

Agenda

- **Neues im MWN** (Dr. H. Reiser)
- **Aufgaben von Netzverantwortlichen an praktischen Beispielen** (Dr. H. Reiser)
- **Self Service Portal NeSSI** (W. Beyer)
- **„Kurznachrichten“: Änderungen an Netzkomponenten und Diensten** (Dr. W. Hommel)
- **IPv6 im MWN** (B. Schmidt)
- **DNSSEC und Teilnahme am DENIC-Testbed** (B. Schmidt)
- **Diskussion und Abschluss** („open end“)