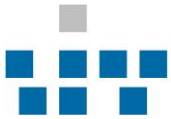
Westfälische
Wilhelms-Universität
Münster

# Das neue Netzkonzept der WWU

## Implementierung eines umfassend überarbeiteten optimierten Designs

Norbert Gietz
gietz@uni-muenster.de

wissen.leben
WWU Münster



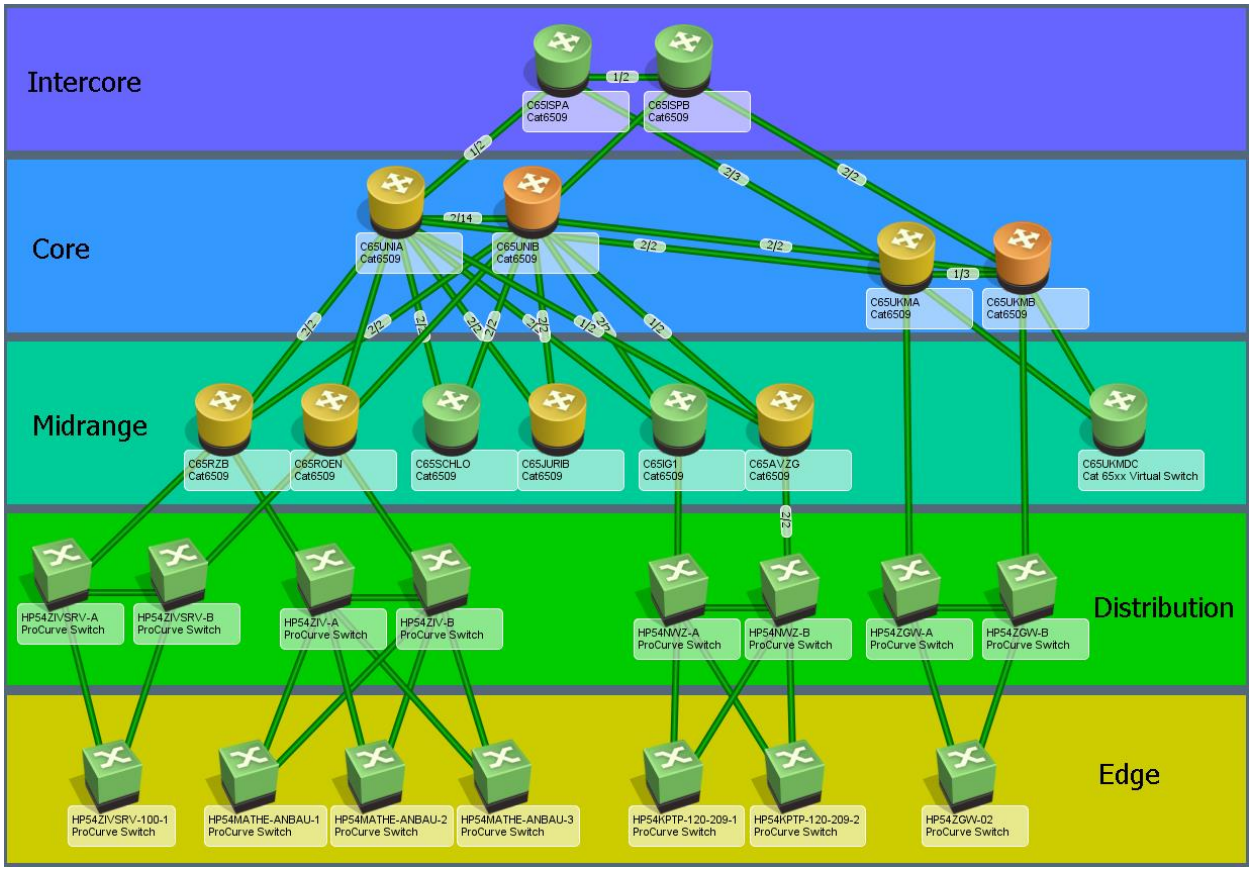
ZENTRUM FÜR
INFORMATIONS
VERARBEITUNG

# Agenda

- Ausgangslage, Motivation und Leitlinien
- Region
- Design
- VPNs und Routing
- Infrastruktur
- Migration
- Ausblick

# Das alte Netzdesign

- Core
  - Cisco Catalyst 6509
- Servicemodule
  - Firewall SM2
  - VPN-SPA
  - WLAN WISM(2)
- Strukturierung
  - L3 VRF-lite / OSPF
  - L2 VLANS / PVST
  - campusübergreifend
- Distribution
  - HP5412
- Access
  - HP ProCurve
  - 3Com (auslaufend)
  - Avaya (auslaufend)



# Motivation

- bisheriges Netzdesign anfällig für Störausbreitungen
- hohe Betriebsaufwände
- hohes Alter des Gerätebestandes
- Lücken in den Redundanzen
- Einführung von VoIP
- IPv6
- SDN-ready
- Bandbreiten 40/100 Gbps
- Zukunftsicherheit
- Modernisierung der Strukturen aus vergangenen Medienbrüchen (FDDI, ATM)

# Leitlinien

- Erhöhen der Verfügbarkeit
- Begrenzen der Störungsausbreitung
- Steigern der Performance
- Gewährleisten der Skalierbarkeit
- Schaffung durchgängiger Redundanzen
- Verringern der Betriebsaufwände
- VoIP-fähigkeit herstellen
- Trennen von Datentransport und Servicesfunktionen
- Vermeiden einer starken Herstellerbindung
- Vermeiden von herstellerspezifischen Protokollen

# Kernpunkte

- Gliedern des Netzes in Bereiche und Regionen
  - Bereiche WWU, UKM, WNM, Fremdnetze (FH Münster, MPI, Studentenwerk, … )
- Bereich WWU
  - geografische Regionen (zurzeit 8)
  - funktionale Regionen (zurzeit 4)
- Zentrales Routing für eine Region
- Zentrales Routing und Funktionen einer Region hochverfügbar
  - HW-Redundanz (Router-Cluster)
  - Standortredundanz (Cluster auf 2 Standorte verteilt, nur LWL-Koppelung)
  - LWL-Trassenredundanz (Anbindung Core und Standortkoppelung)
- Regionsübergreifende VPNs zur Sicherheitszonenbildung
  - Koppeln der VPNs nur über Sicherheitsgateways
- Nur offene Standards verwenden (z.B. keine WCCP, PVST, OTV, … )

# Clustern der Router

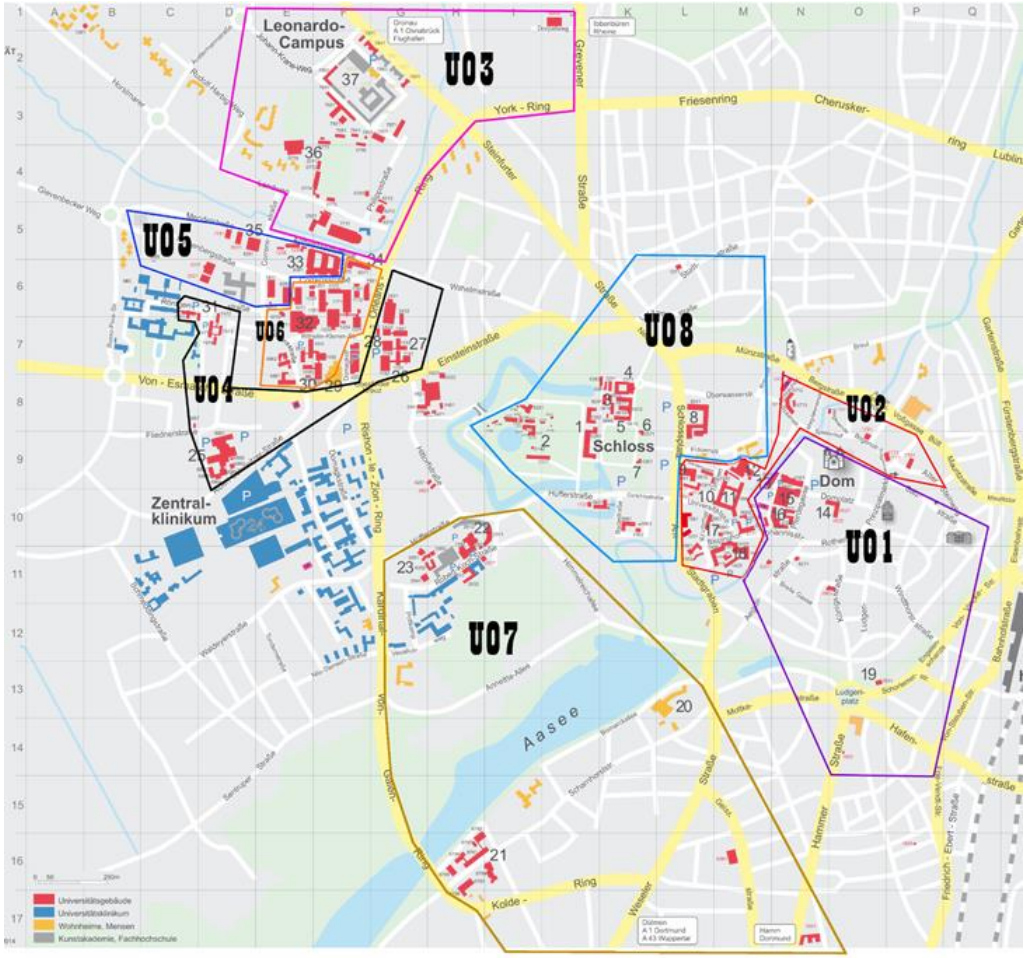
- Vermeiden von Maschen im Netz
- Vereinfachung im Spanning Tree
  - LAG statt STP
- Kein Gateway-Redundance-Protokoll (VRRP)
- Optimale Wegewahl im Routing
- Reduzierung der Komplexität
- Reduzierung des Konfigurationsaufwandes
- Vereinfachung in der Softwareupdates (ISSU)
- Cluster wird zur Black Box
- sehr gute Erfahrung im DataCenter (HPE) und RZ im UKM (Cisco)
- Verteilen der Geräte auf 2 Standorte

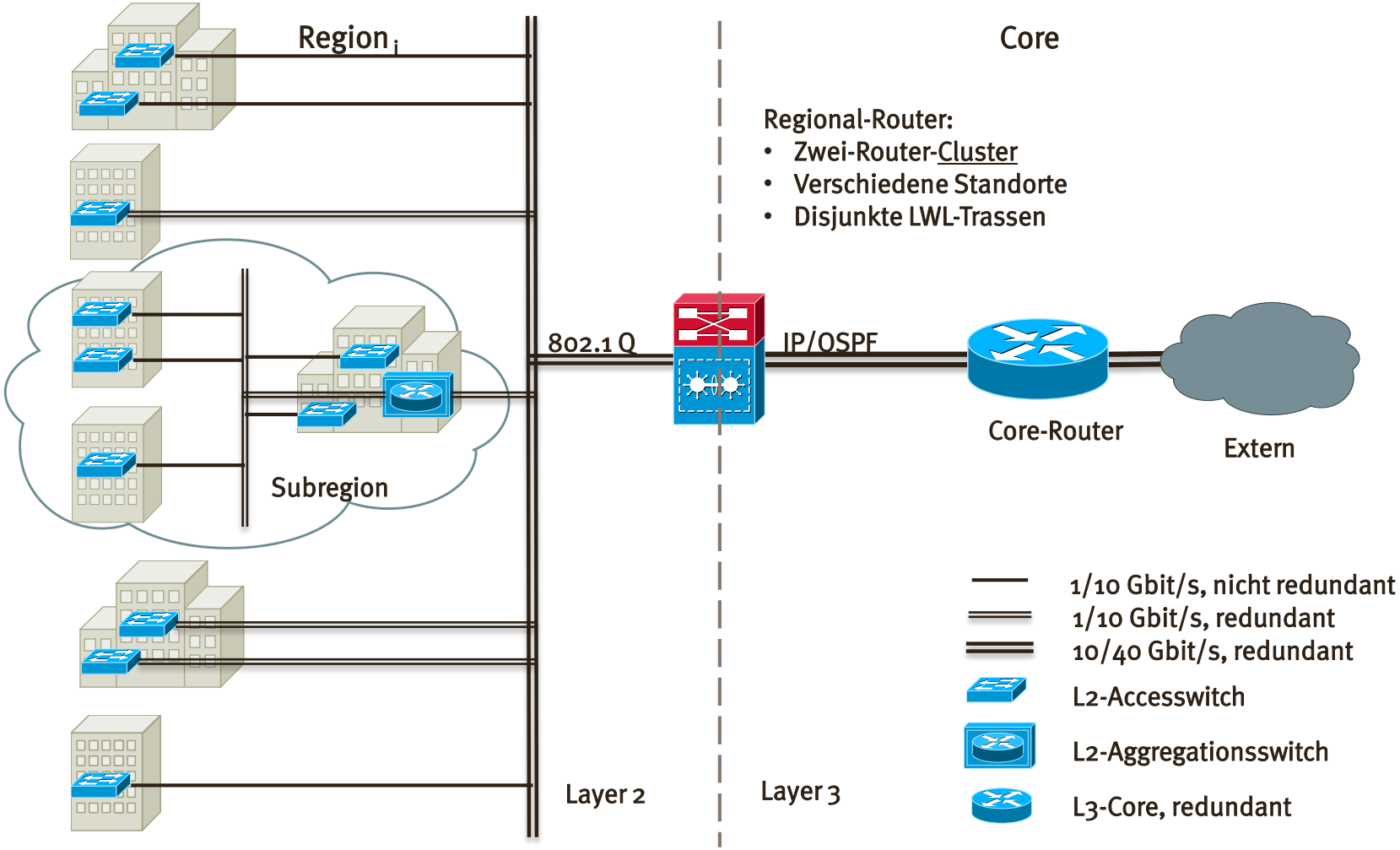
# Regionsansatz

Regionskopplung per Router
- Vlans nur innerhalb einer Region
- keine L2 zwischen Regionen

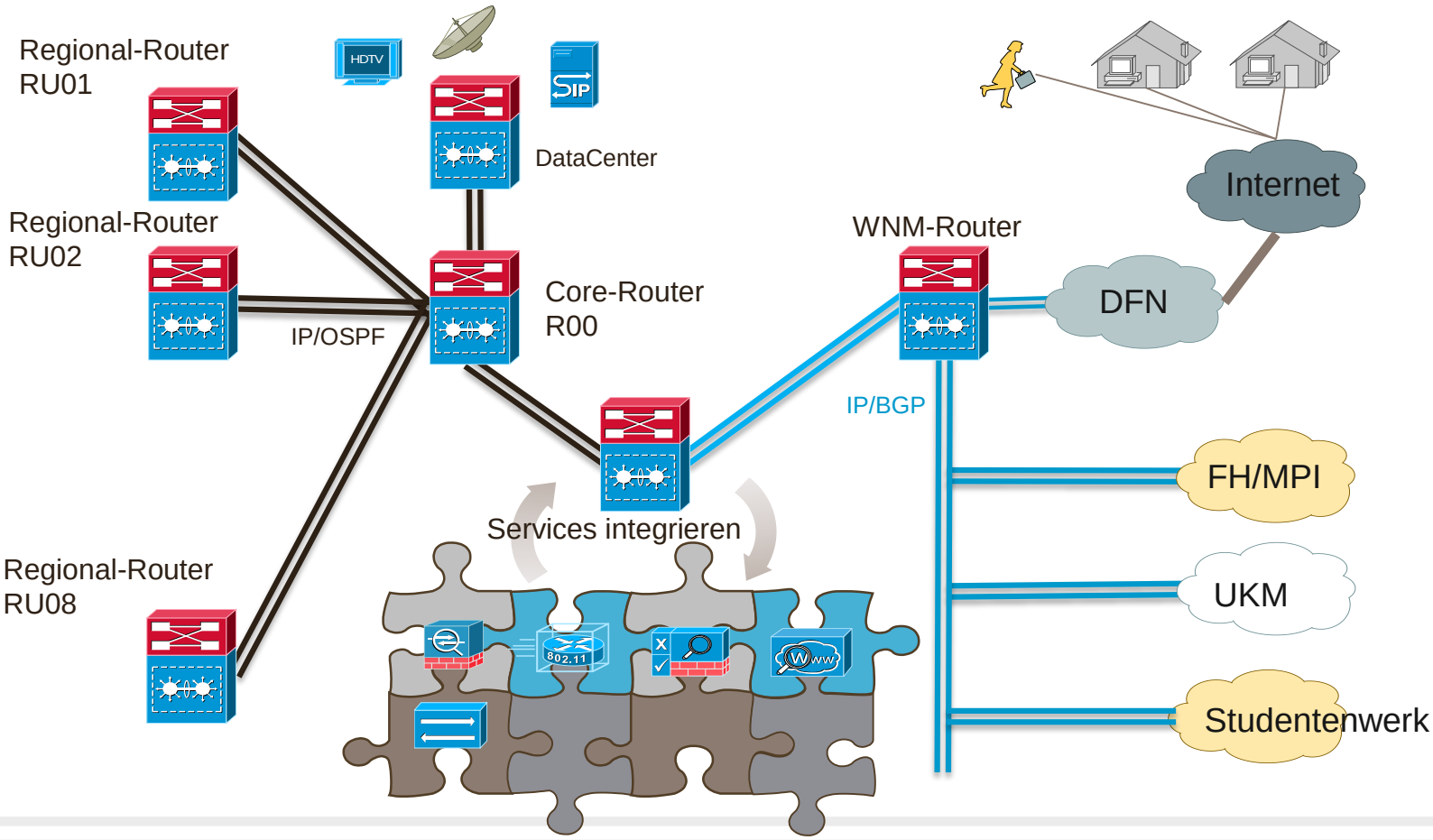
geografisch (U01 bis U08)
- Endgeräte aller Art
- Server (lokal)
- Steuergeräte (z.B. KNX)
- Telefone

funktional
- Datacenter
- Service (Security, VPN, CNS, WLAN-Controller, NAT, ... )
- Core
- Management Outband

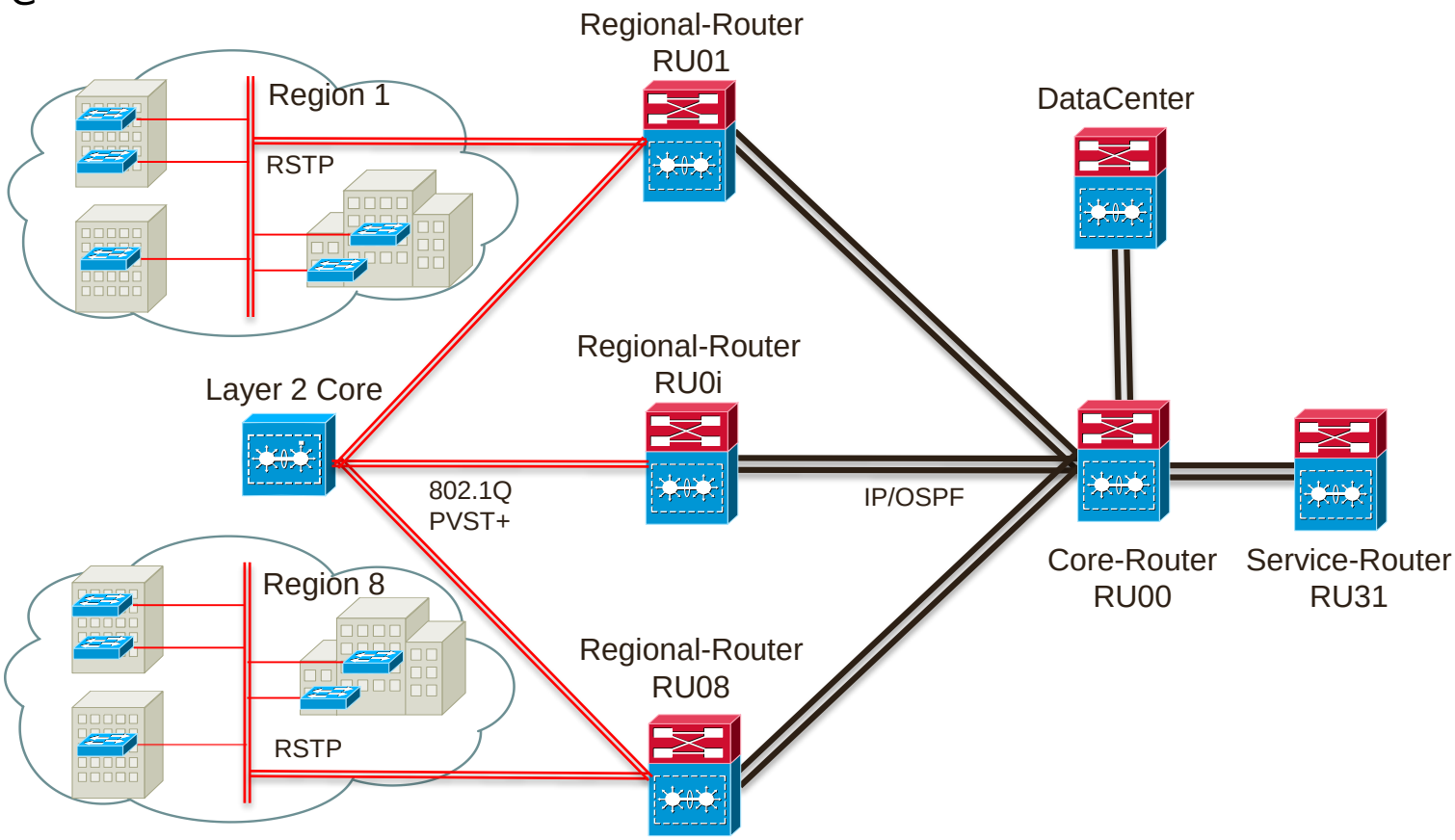



Region i
Core
Regional-Router:
• Zwei-Router-Cluster
• Verschiedene Standorte
• Disjunkte LWL-Trassen
802.1 Q
IP/OSPF
Core-Router
Extern
Subregion
1/10 Gbit/s, nicht redundant
1/10 Gbit/s, redundant
10/40 Gbit/s, redundant
L2-Accesswitch
L2-Aggregationsswitch
L3-Core, redundant
Layer 2
Layer 3

# Ziel


Regional-Router
RU01
Regional-Router
RU02
Regional-Router
RU08
HDTV
SIP
DataCenter
Core-Router
R00
IP/OSPF
WNM-Router
Internet
DFN
IP/BGP
FH/MPI
UKM
Studentenwerk
Services integrieren

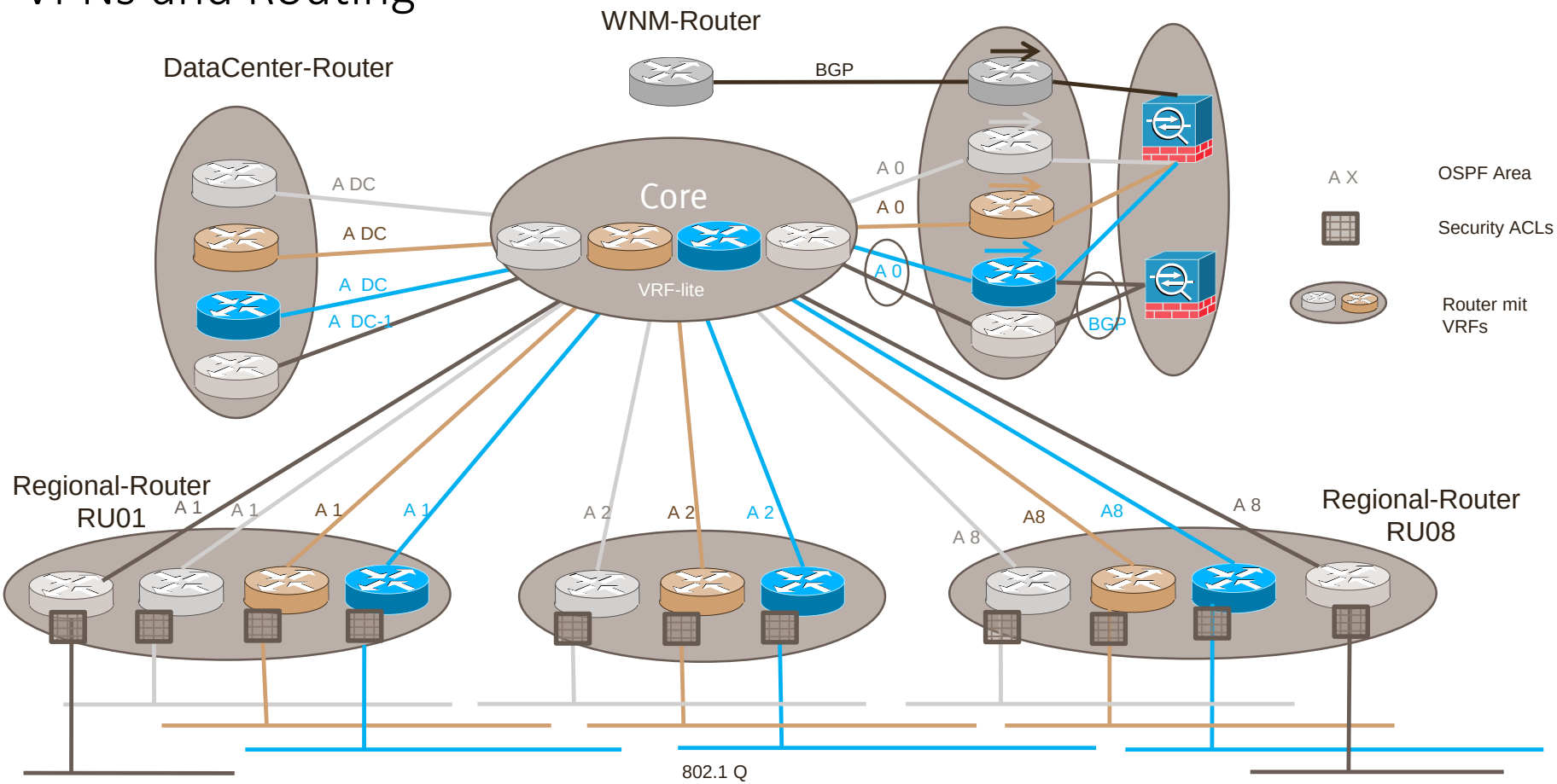
# L2-Core


Regional-Router
RU01
Region 1
RSTP
DataCenter
Regional-Router
RU0i
Layer 2 Core
802.1Q
PVST+
IP/OSPF
Core-Router
RU00
Service-Router
RU31
Region 8
RSTP
Regional-Router
RU08

# VPNs und Routing

- Campusweit wurden Farben (VPNs) definiert
  - kleiner zweistelliger Bereich (z.B. TK, Management, LGA, Campus, Gäste)
  - eine Farbe fasst Netze mit ähnlichen Anforderungen zusammen
- auf den Routern werden bedarfsweise VPN-Instanzen (VRF-lite) definiert
- VPN-Instanzen werden Farben zugeordnet
- Vlans in den Regionen werden einzelnen VPN-Instanzen zugeordnet
- VPN-Instanzen werden innerhalb einer Farbe durch Transfernetze verbunden
- jede Farbe ein eigener OSPF
- Koppelung der Farben nur in der Serviceregion über Securityeinrichtungen
- MPLS zunächst keine Vereinfachung, später aber möglich

# VPNs und Routing



# Infrastruktur

- Routerstandorte
  - aufrüsten bzw. neu schaffen von 15 Standorte
  - 5 neue USV
  - Kühlung, davon 8 Freiluftkühlung
  - 28 Vernetzungsschränke
  - 25 km LWL-Kabel im Primärnetz
  - 160 LWL-Patchfelder
- 12 Routercluster
  - 22 Stück HPE 12504
  - 2 Stück HPE 12508
  - 70 40Gbps-Interfaces

# Migration

- Aufbau der neuen Router, verschalten, schaffen der VPNs
- Schaffen eines Outband-Managementnetz
- Hoher Komplexitätsgrad bei der Firewall/IPS
- Aufbau des L2-Core und Anschluss an den neuen Core
- Entwicklung von Verwaltungstools, Monitoring
- Schulung der Mitarbeiter durch HP in 3 Kursen
- Anschluss des L2-Cores an die alten Router
- Regionsweise umschalten der Accessswitches
- Verlagern des Routings für die Accessnetze in den Core
- Rückbau der Altgeräte

# Offene Aufgaben/Ausblick

- Restarbeiten im Bereich WNM abschliessen
- Nachfolge Projekt „Campus2016“
  - Bestand-Vlans auf Regionen zurückbauen
  - Abbau des L2-Cores
  - IPv6

# Vielen Dank!