TU Graz

TUGRAZngn

Philipp Rammer | ZID

5. November 2014

Themenübersicht

- **Struktur des TUGnet**
- Netzwerkausfälle 09/2014
- Design/Konzept *TUGRAZngn*
- Auswirkungen

TUGnet

TUGnet = *Datennetzwerk* der TU Graz

- **Layer 1**: LWL & Kupfer in strukturierter Verkabelung
- **Layer 2**: Ethernet 802.3, Wireless LAN 802.11
- **Layer 3**: IP (Internet Protocol) [v4]

  129.27.0.0/16

zentrale (Netzwerk-)**Dienste**
(basierend auf TUGnet)

Access
- kabelgebunden
- drahtlos
- VPN

Security
- Firewalling
- Intrusion Prevention

→ „*Institutsnetz*“

= bereitgestelltes privates LAN (VLAN) mit Übergabepunkt in den Layer 3 des TUGnet

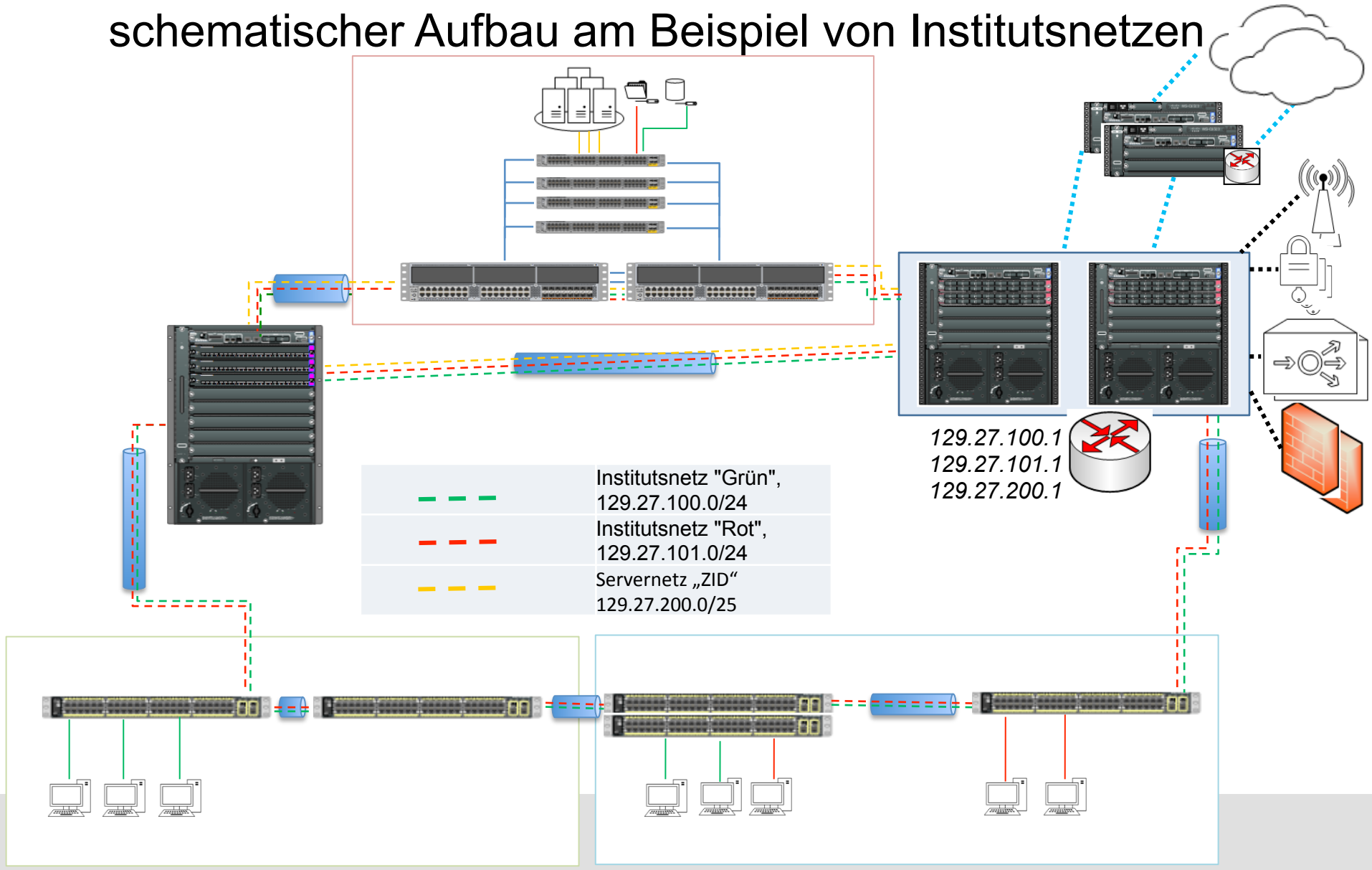
Communication
- (IP-)Telefonie

Serverhousing, -hosting
- *Serverräume*
- *virtuelle Maschinen / IaaS*

Basisdienste
- DNS, DHCP, NTP, ...

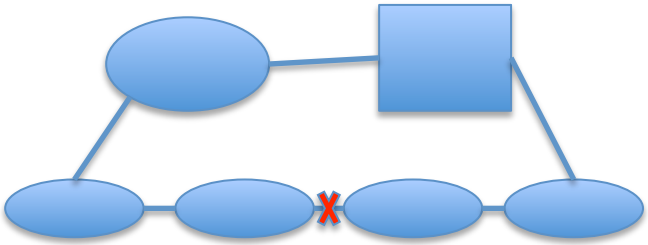
TUGnet

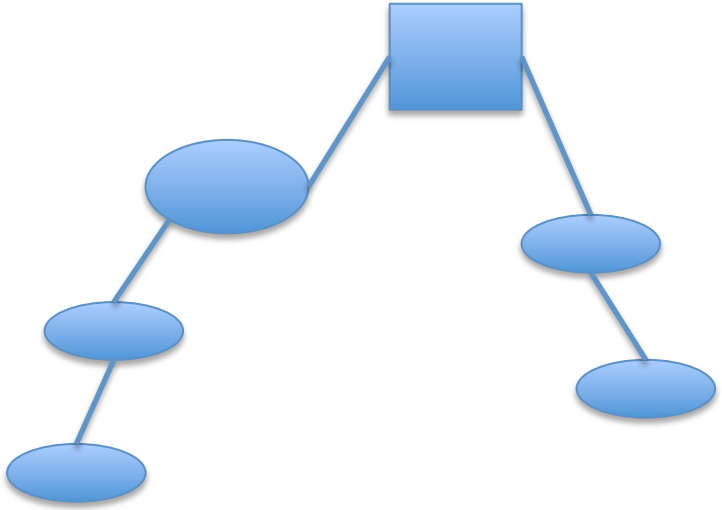
schematischer Aufbau am Beispiel von Institutsnetzen



Strukturelle Eigenheiten der Topologie

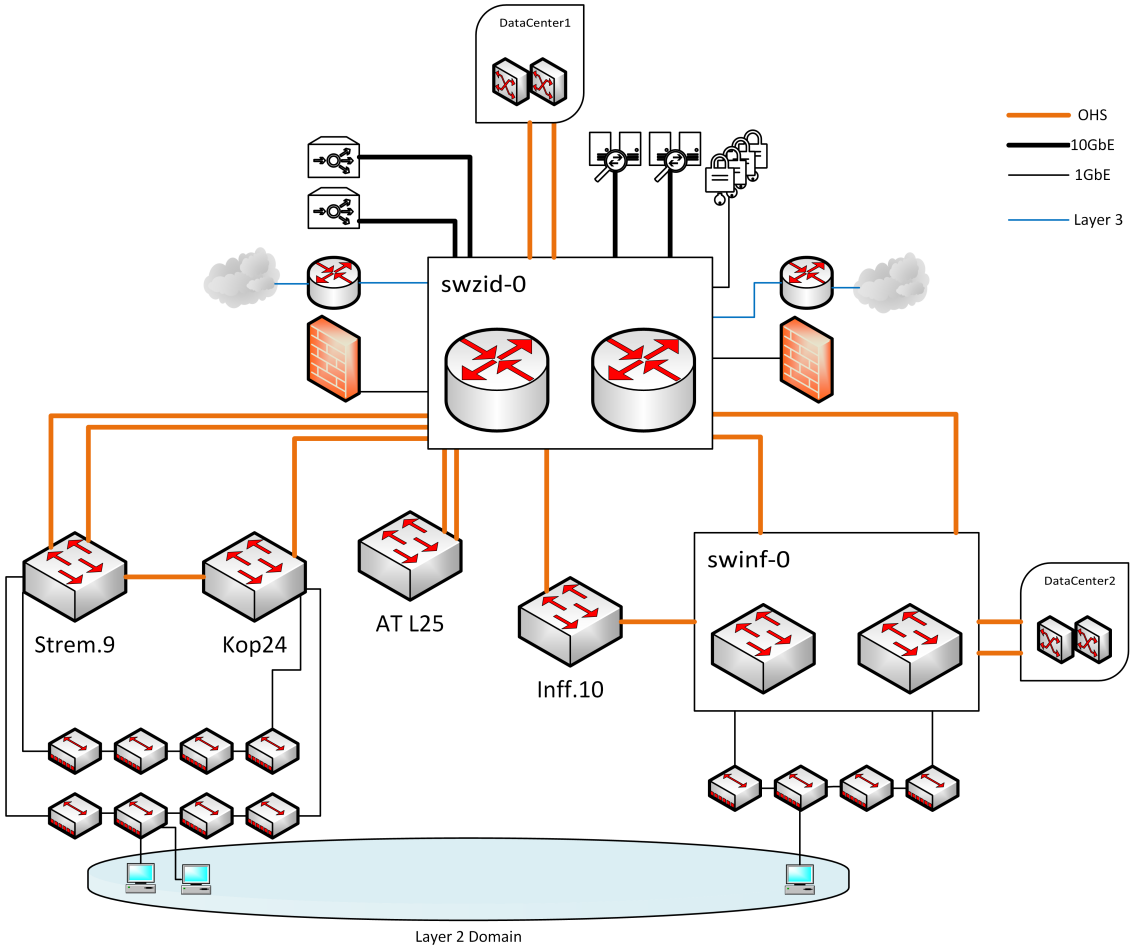
\+ flache Struktur: einfach, flexibel und leistungsfähig
\+ günstige Redundanzen (Preis pro Core-Port)



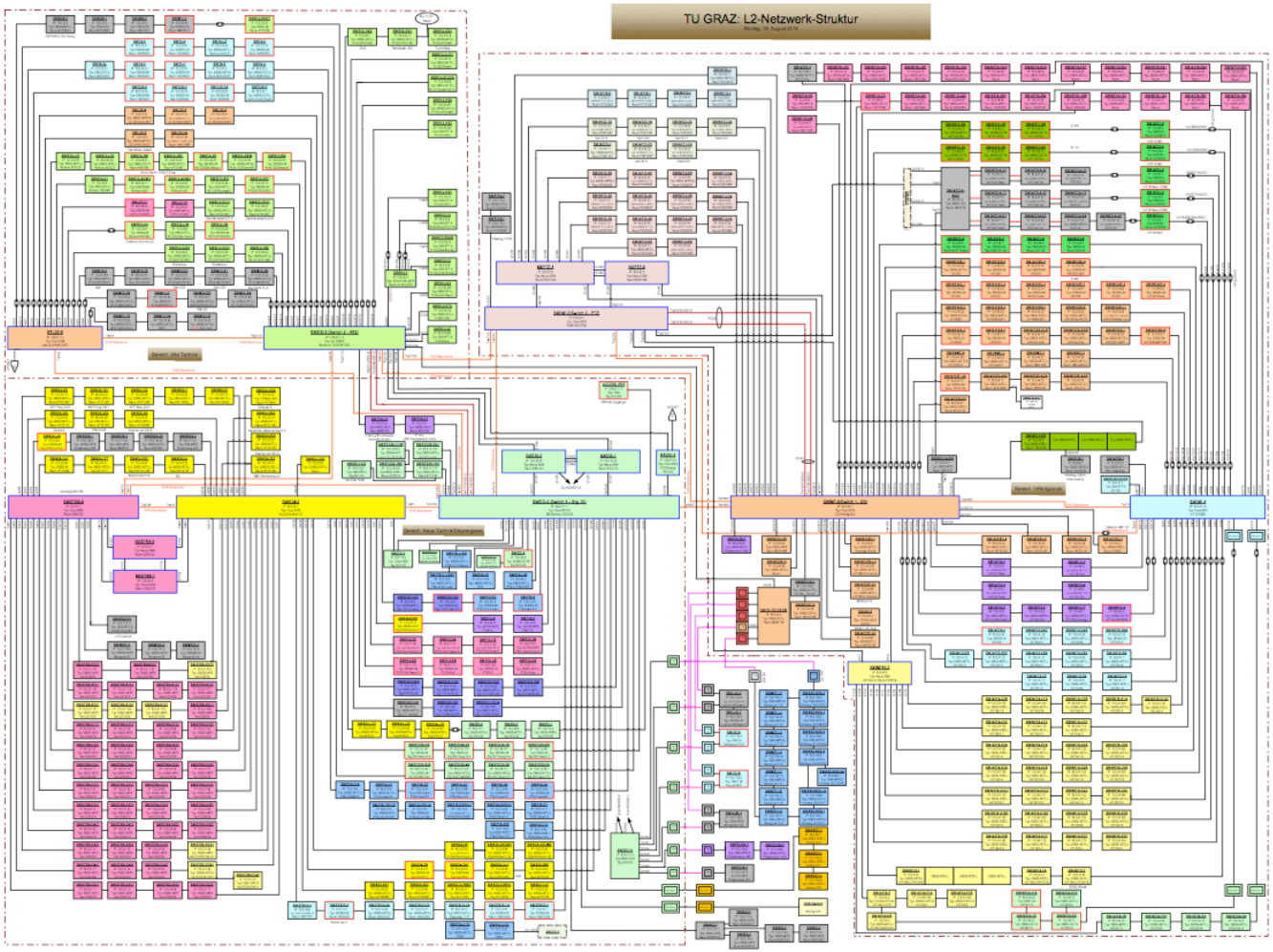


− aufwändiges Steuerungsprotokoll notwendig
− Überbuchung der Uplinks
− Skalierbarkeit (max. Diameter)
− Administrationsaufwand

TUGnet
Strukturschema



TUGnet
physikalischer IST-Zustand



Anmerkungen zum Design

1) Layer 1 ist strukturierte Verkabelung (Baum), darüber werden Schleifen gelegt

2) Design ist „wachstumsbedingt“

3) Design skaliert nicht mehr mit dztg. Wachstum

4) zu zentralistisch?
   - zentralistisches Design (+)
   - immer mehr Services am Hauptknoten (-)

Themenübersicht

- Struktur des TUGnet
- **Netzwerkausfälle 09/2014**
- Design/Konzept *TUGRAZngn*
- Auswirkungen

Probleme im TUGnet

- Netzwerk für Topologie in dieser Größe recht stabil
  - dennoch lokale Instabilitäten

- wenig Teilausfälle, sondern
  problematische Gesamtausfälle
  verursacht durch nicht vorhandene logische Trennung

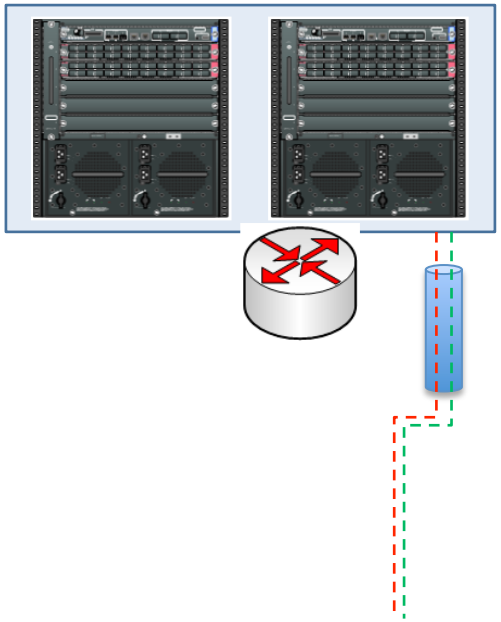
- Kapazitätsengpässe durch Überbuchung
  - im Access-Bereich durch Schleifen
  - [nicht im Backbone]

- Firewallperformance → Flaschenhals

Probleme im TUGnet

Gesamtausfälle, Folgeprobleme

problematischer Knoten:
Core-Router
Firewall
WLAN-Controller
Internet-Uplink
Access für Bereich NT
...



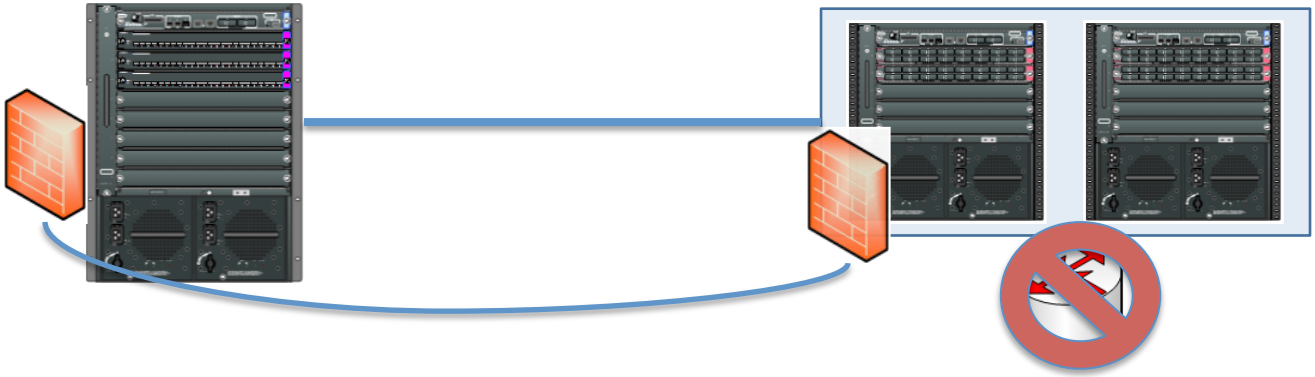
bei Überlastung:

- kein Routing TU-weit
- permanenter Spannbaum-Umbau
  und damit kein Switching TU-weit

→ kein (stabiles) Netzwerk
Fehlersuche diffizil..

Netzwerkprobleme 09/2014 I

Ausfall 1: Layer 3 – Probleme (Überlastung/Loop) zwischen Firewall-Standorten



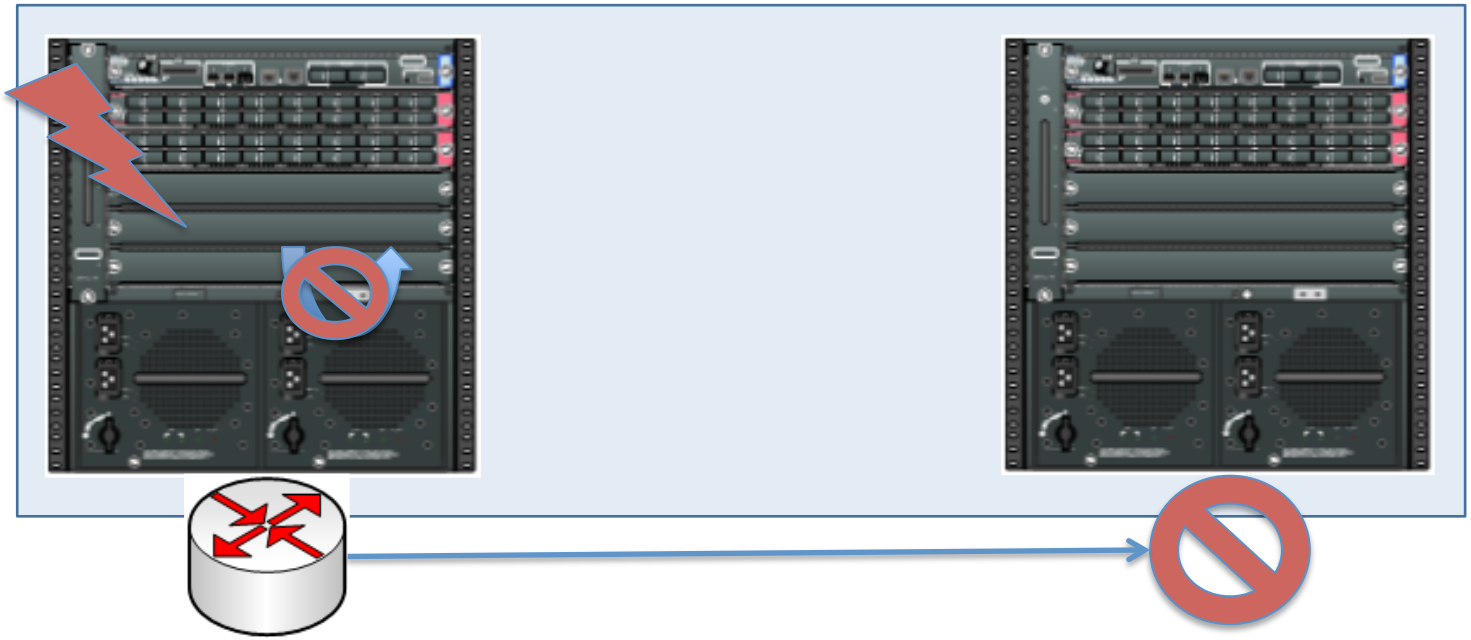
Ursache: defekte 10GBit-Linecard in Inffeldgasse
Lösung: Hardwaretausch

Netzwerkprobleme 09/2014 II

Ausfall 2: Core-Router-Ausfall

1) Crash durch Multicast-Software-Bug -> Umschaltung auf 2. Gerät

2) Software-Bug verhindert Wiederhochfahren des 1. Switches



3) Routing-Prozessor im 2. Switch funktioniert nicht ordnungsgemäß

Lösung: Komplett-Neustart beider Systeme...
Mittlerweile: Software-Update und Austausch der Supervisor-Engine

Themenübersicht

- Struktur des TUGnet
- Netzwerkausfälle 09/2014
- **Design/Konzept *TUGRAZngn***
- Auswirkungen

TUGRAZngn Beweggründe

1. **Stabilität**
   - Backbone stabilisieren und abgrenzen
   - Access-Bereiche (geographisch) abgrenzen

2. **Skalierbarkeit**
   - für zusätzliche Gebäude und Campusbereiche
   - flexibles, erweiterbares, übersichtliches Schema
   - sauberes hierarchisches Design

TUGRAZngn Beweggründe II

3. Zukunftssicherheit

- ausreichend Bandbreite oder Ausbaumöglichkeit (*40/100G-ready*)
- Features (IPv6, QoS, Multicast-Routing, ...)

4. Data Center

- Schaffung eines abgegrenzten *Data Center*
- High Performance (inkl. eigener Firewall)

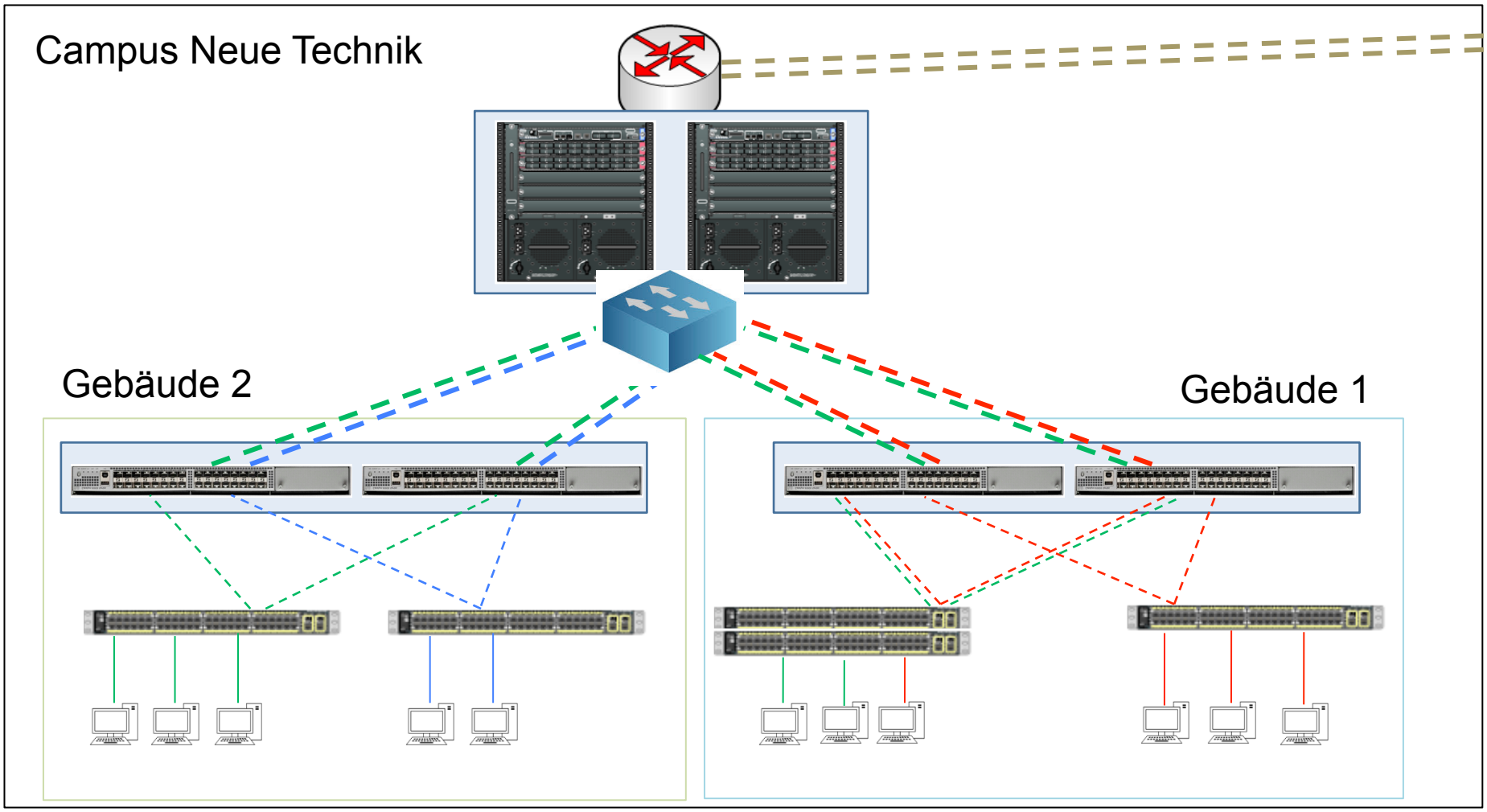
TUGRAZngn Umstrukturierung Access

- Erster Schritt in *TUGRAZngn*:
  Bereinigung und topologische Optimierung

  - Verringerung der logischen Komplexität
  - Anpassung an physikalische LWL-Infrastruktur
  - Erhöhung bzw. effizientere Nutzung der verfügbaren Bandbreite

TUGRAZngn

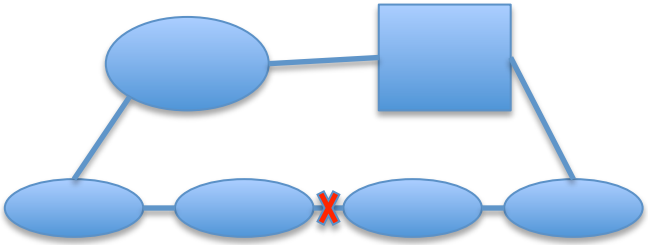
schematischer Aufbau am Beispiel von Institutsnetzen

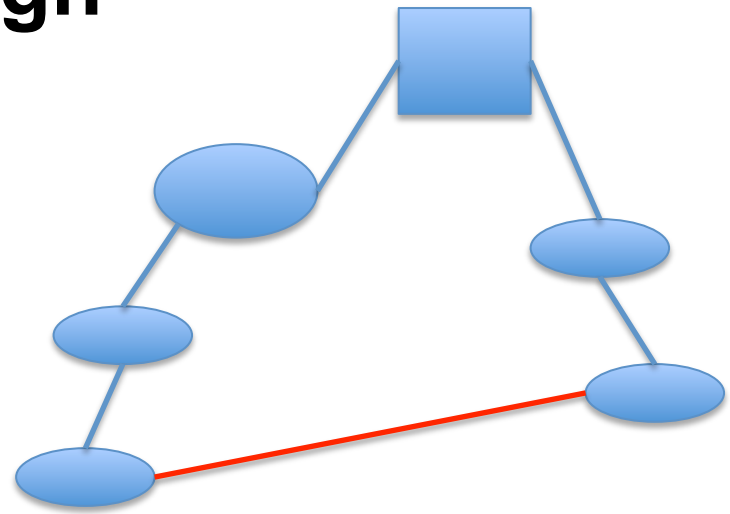


Topologie TUGRAZngn

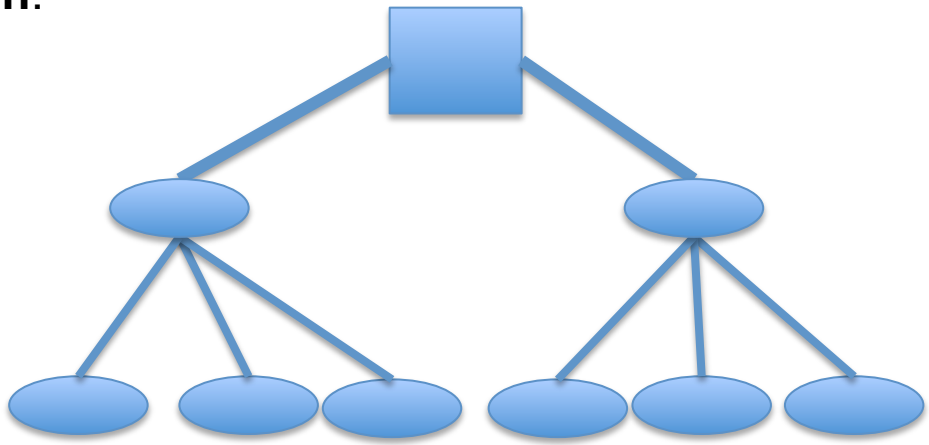
Access/Distribution

bisher:





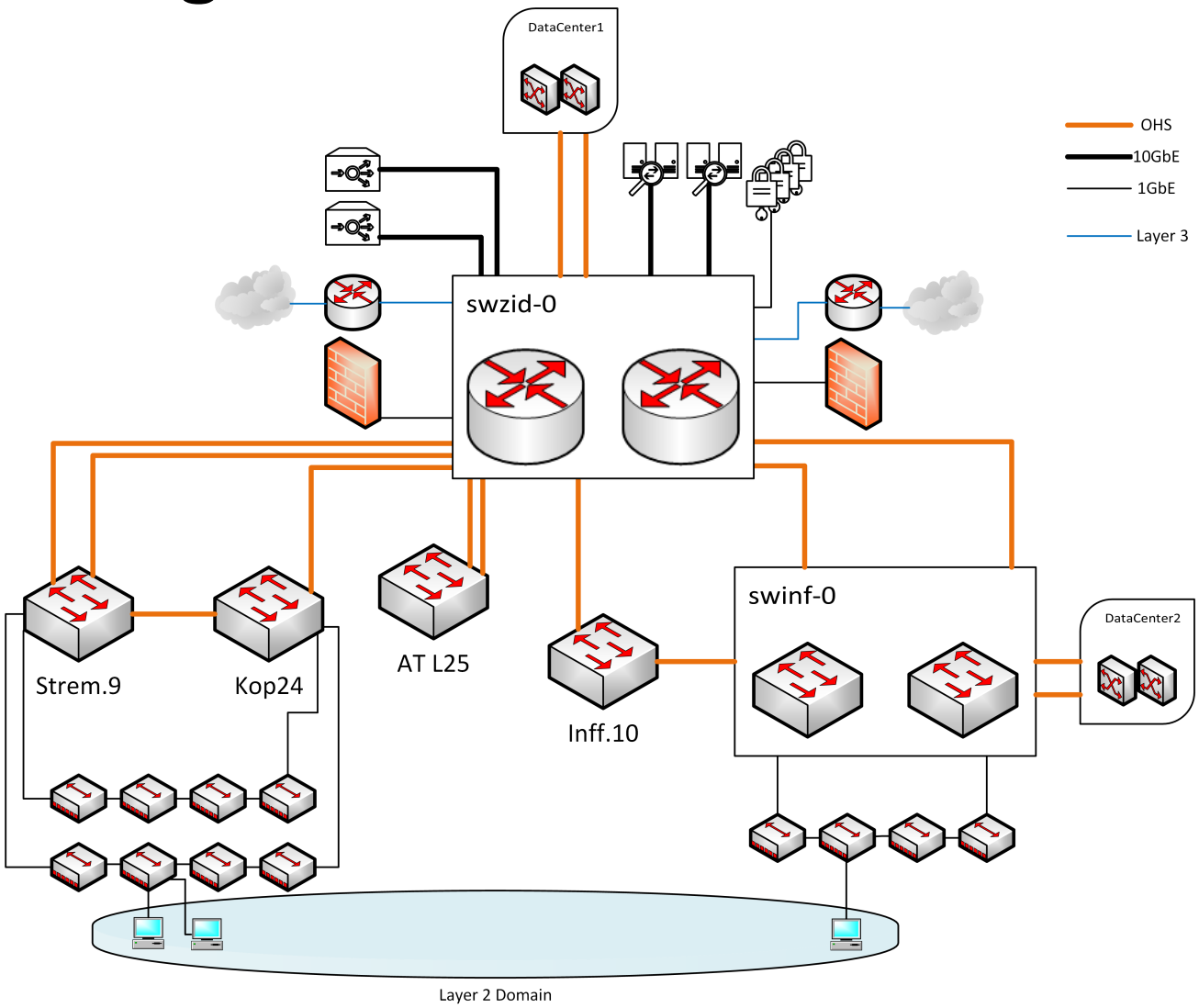
TUGRAZngn:



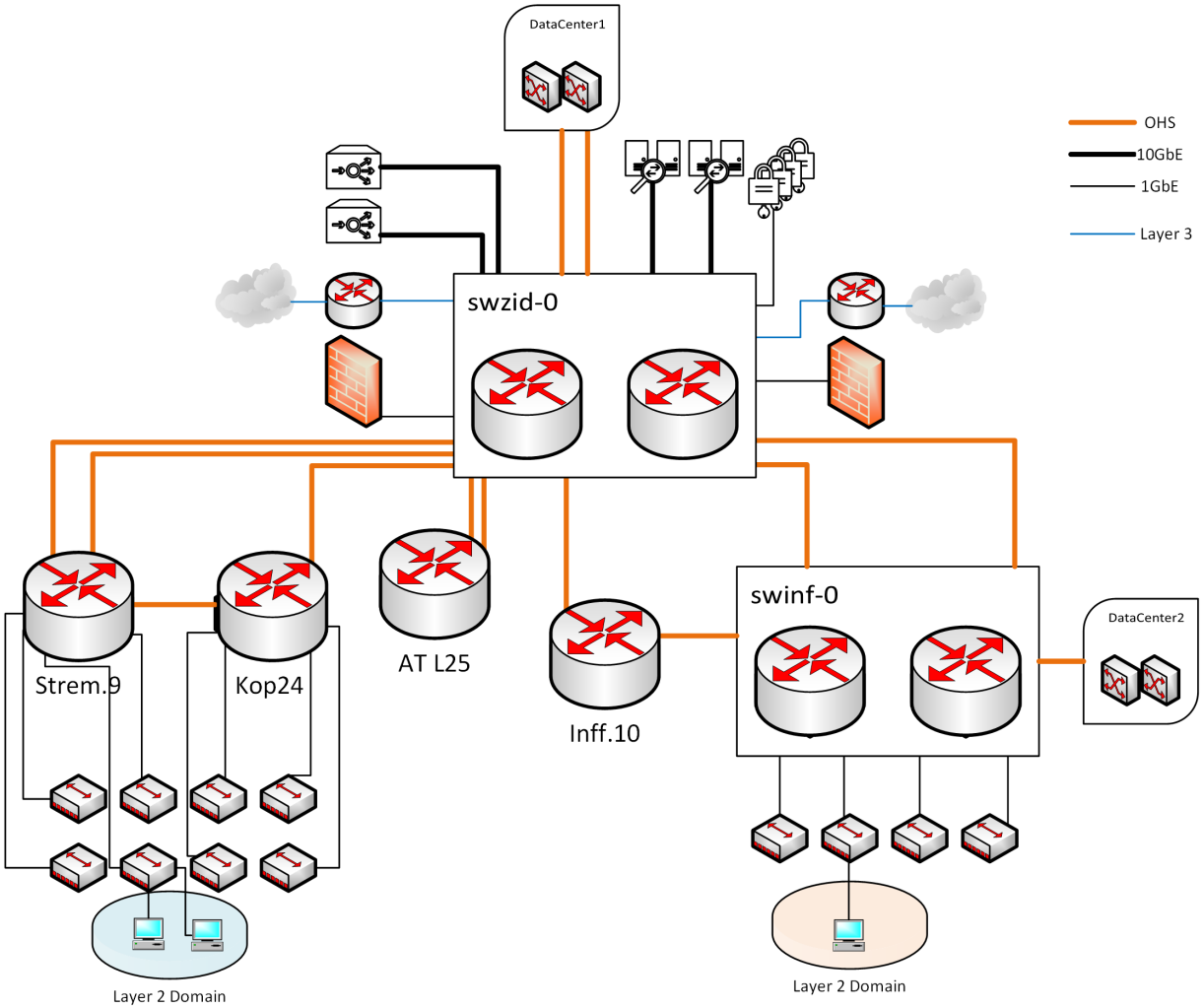
TUGRAZngn Backbone

- Entkoppeln des Backbone vom Access-Netz
- Dezentralisierung des Routings
- *„Single purpose“* anstatt Vermischung von Funktionalität in einem Gerät
- ... unter Beibehaltung der derzeitigen Flexibilität

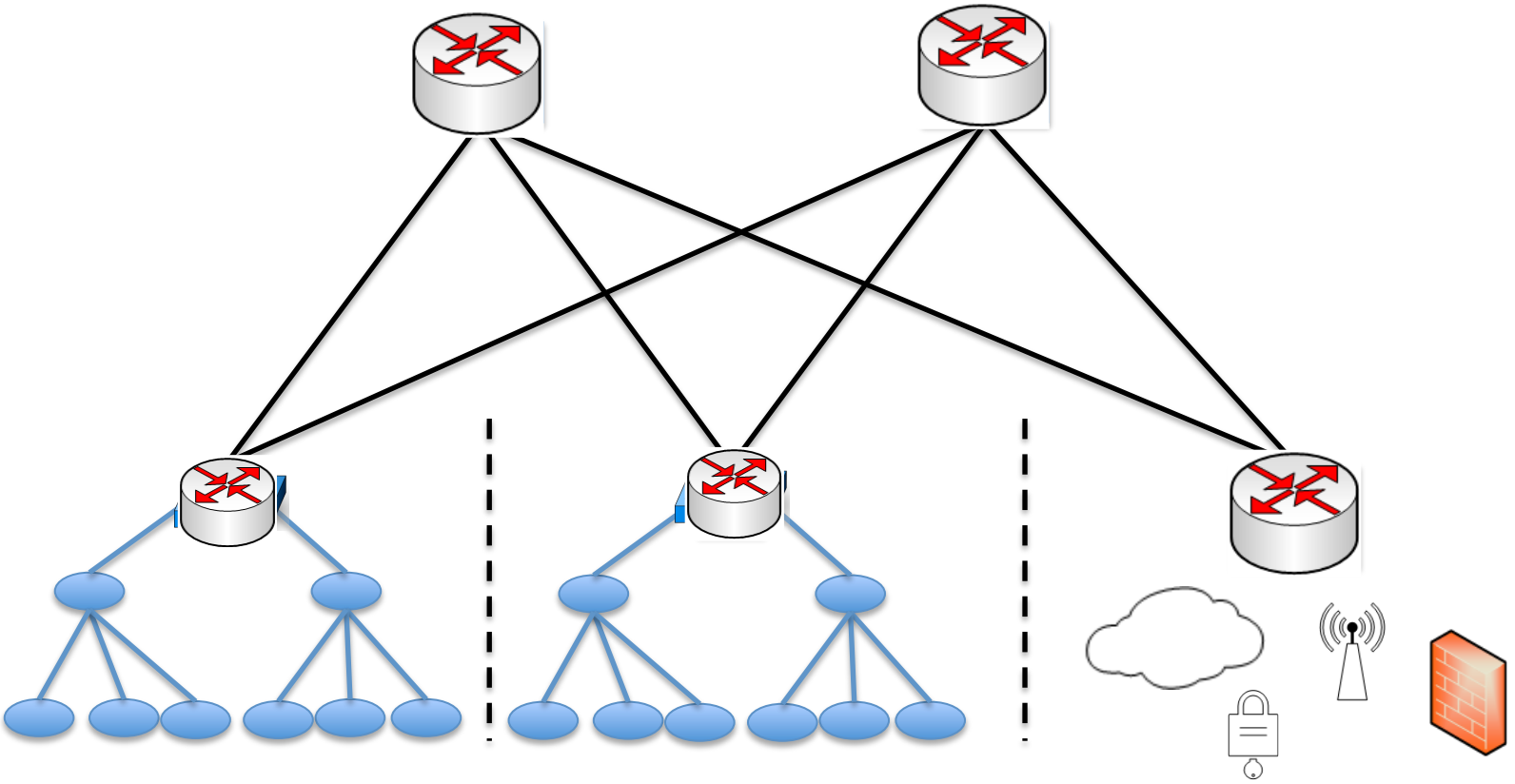
TUGRAZngn Backbone



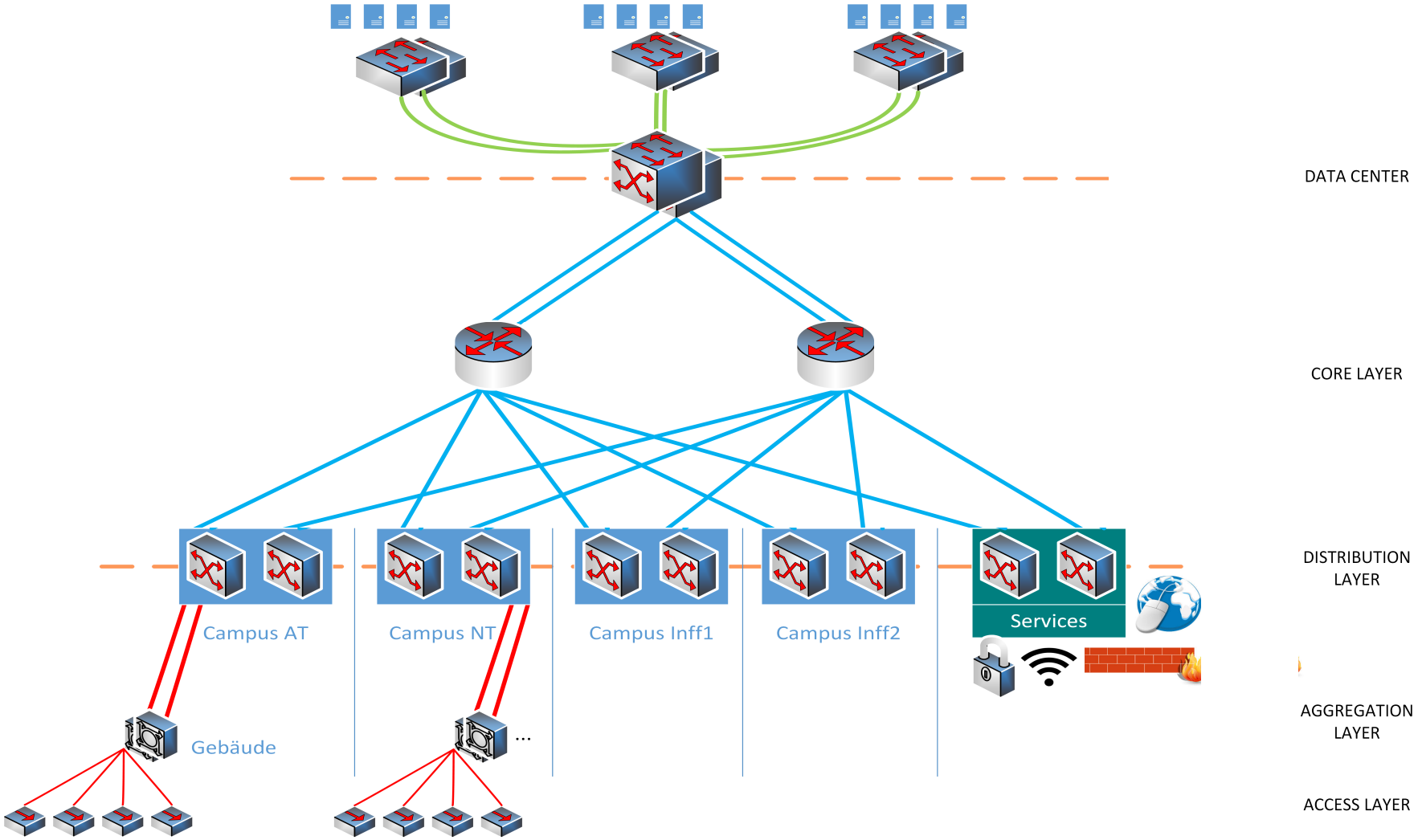
TUGRAZngn Backbone



Topologie TUGRAZngn
Distribution und Core Layer



Struktur TUGRAZngn



TUGRAZngn: Layer 3 Backbone

- Layer 2 -> **Layer 3 im Backbone**
  → Entkoppelung

- ...aber: normaler L3-Backbone zu unflexibel für Anforderungen an der TU Graz

- daher: MPLS-Backbone, darauf Dienste
  - Layer 3 VPN
  - Punkt-zu-Punk-Layer 2-Verbindungen (*AToM*, *EoM*)
  - Layer 2 VPN (*VPLS*)

TUGRAZngn: Distributionsbereiche

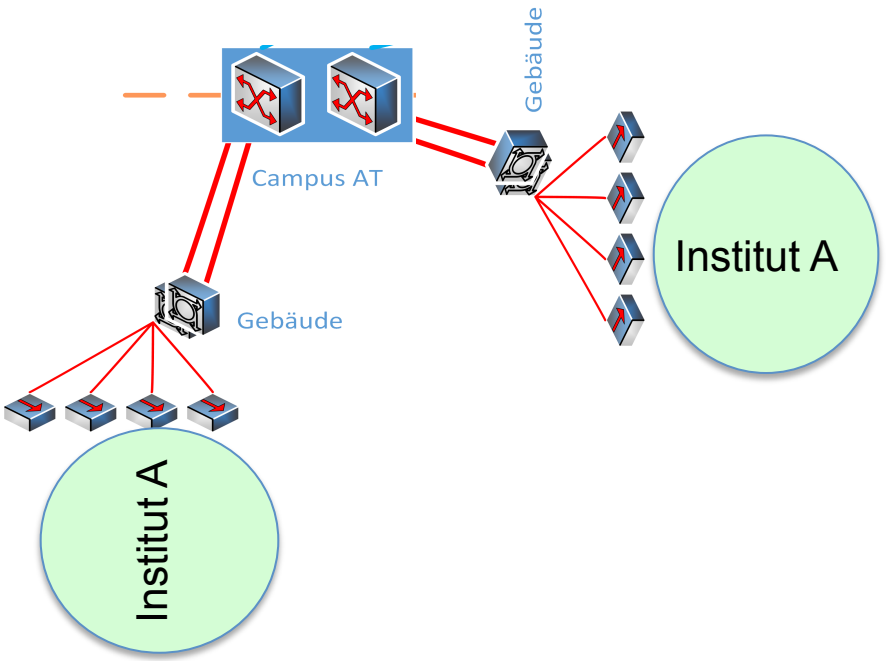
- Aufteilung in vier geographische Bereiche
- basierend auf
  - vorhandener Glasfaserinfrastruktur und damit verbundenen physikalischen Limitierungen

- Bereiche:
  - Neue Technik (inkl. Kronesgasse, Münzgrabenstraße)
  - Alte Technik (inkl. Mandellstraße)
  - Inffeldgasse I (links)
  - Inffeldgasse II (rechts)

Themenübersicht

- Struktur des TUGnet
- Netzwerkausfälle 09/2014
- Design/Konzept *TUGRAZngn*
- **Auswirkungen**

Mögliche Auswirkungen
Variante 1: *Best Case*

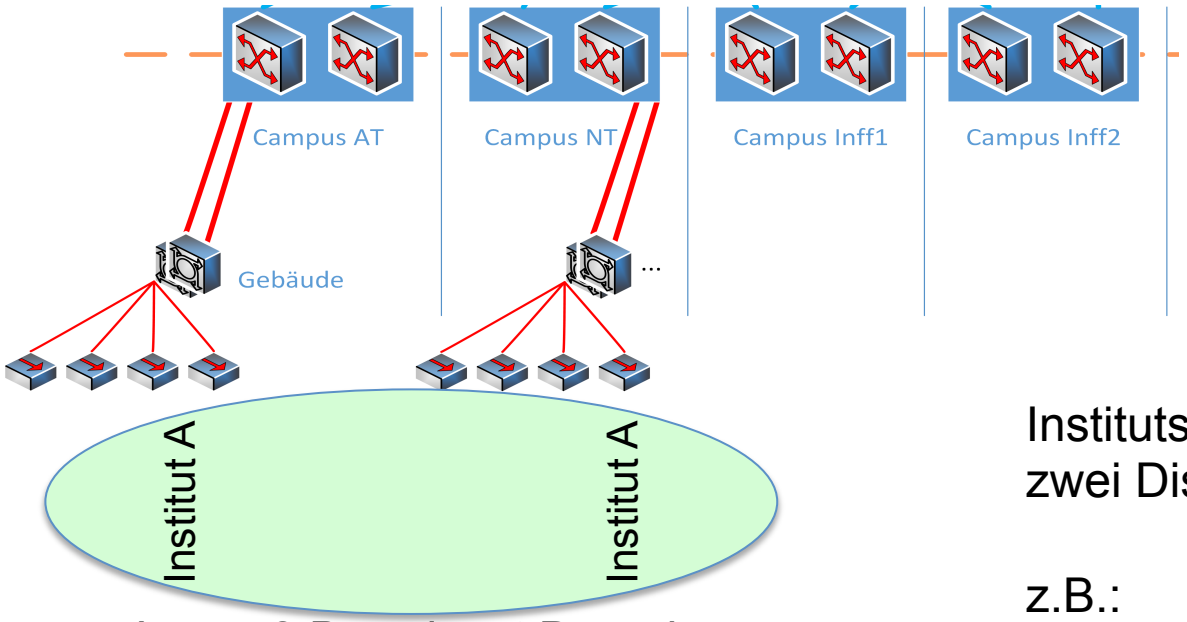


Räumlichkeiten des Instituts sind auf einen der Campus-Distributionsbereich beschränkt

- *Alte Technik* oder
- *Neue Technik* oder
- *Inffeldgasse I* oder
- *Inffeldgasse II*

notwendige Änderungen: **keine**

Mögliche Auswirkungen
Variante 2: *Average Case*

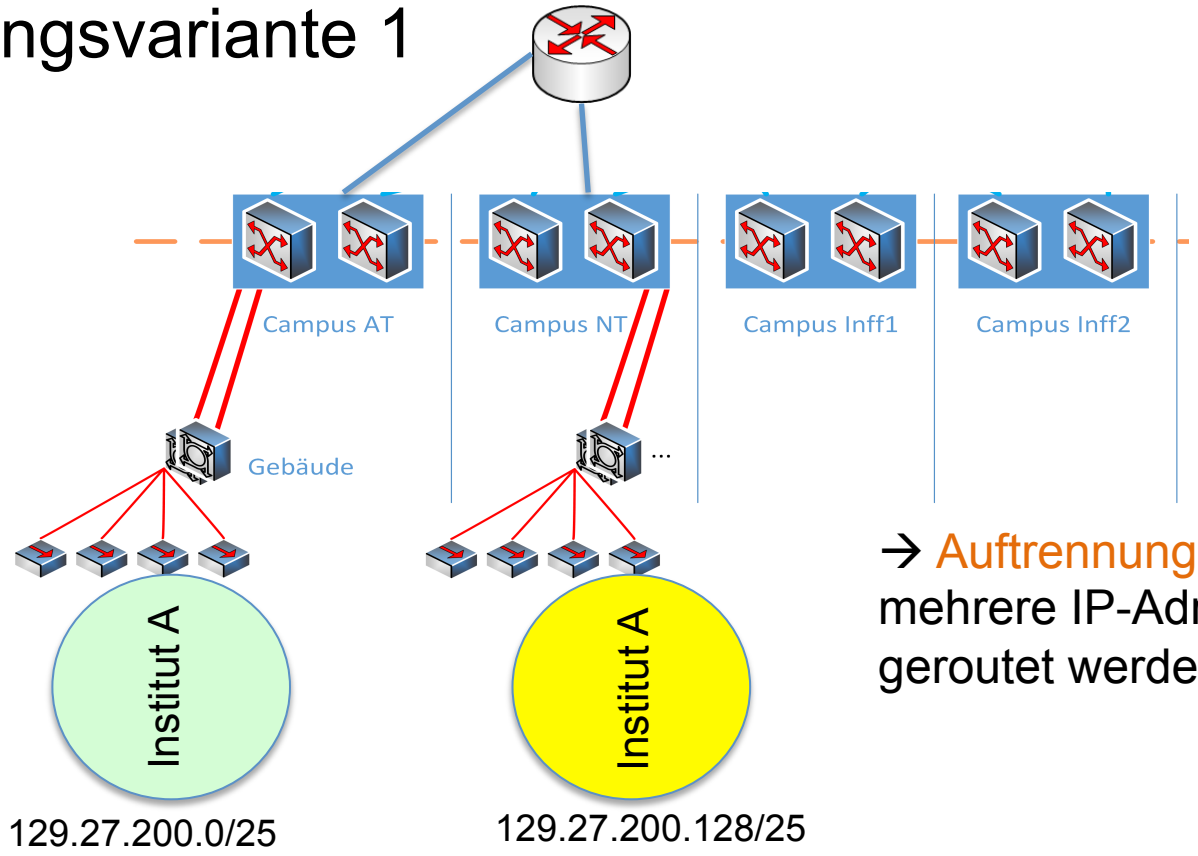


Institutsnetz erstreckt sich über zwei Distributionsbereiche

z.B.:
- Inffeldgasse I (Büros)
- Inffeldgasse II (Serverraum)

Mögliche Auswirkungen
Variante 2: *Average Case*

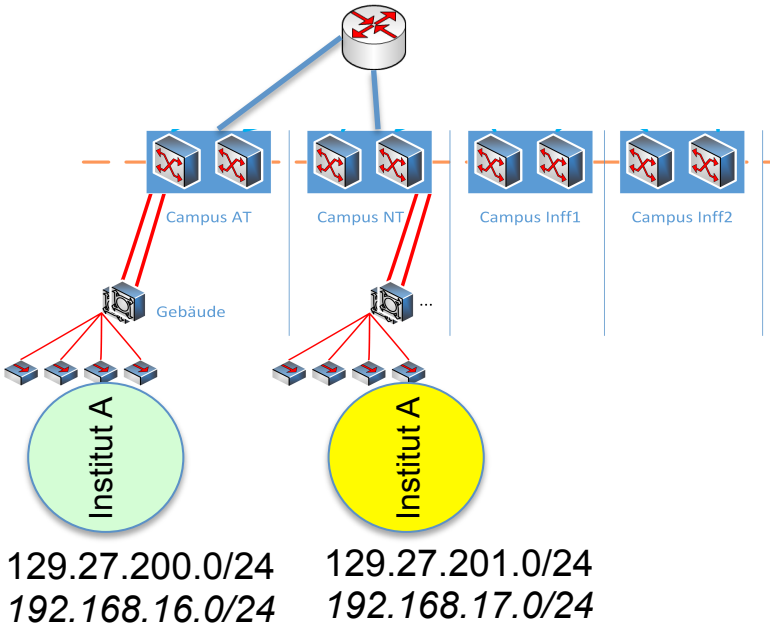
Lösungsvariante 1



→ Auftrennung des Netzes in mehrere IP-Adressbereiche, die geroutet werden können

Mögliche Auswirkungen
Variante 2: *Average Case*

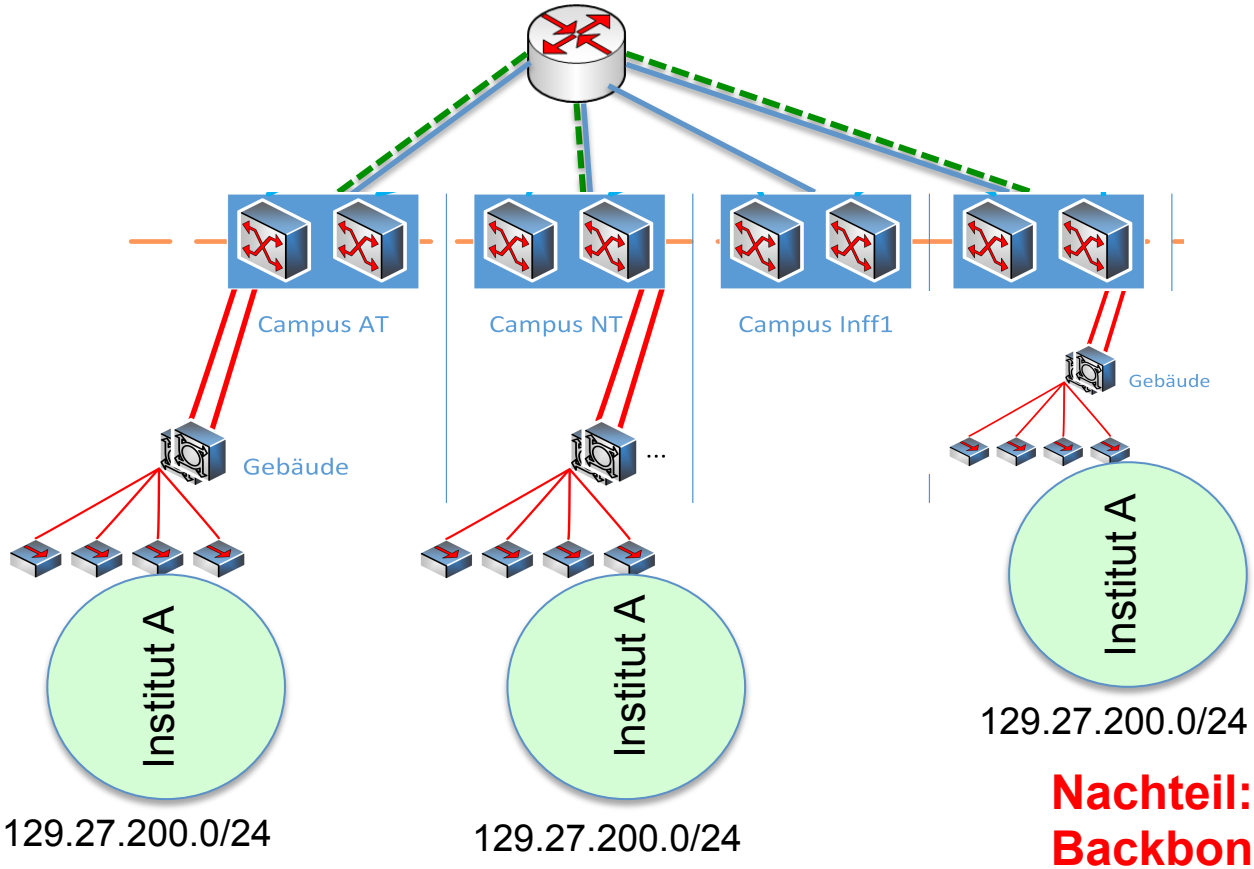
Anmerkungen zu Lösungsvariante 1



- immer noch separates Institutsnetz!
- auch andere Adressbereiche können geroutet werden (zB *private Netze*)
- Vorteil: saubere Trennung, Stabilität!
- „Ready for DataCenter“

Mögliche Auswirkungen
Variante 2: *Average Case*

Lösungsvariante 2: entspricht Lösung für *worst case*



→ Aufspannen eines Layer2 VPN über den MPLS-Backbone

„VPLS“

Nachteil: Störungen werden vom Backbone 1:1 transportiert!!

Exkurs: TUGRAZngn DataCenter

Schaffung eines „echten“ Data Center

Data Center != Serverhousing != Serverhosting

- **Data Center TUGRAZngn**
  - **spezielle Netzwerkinfrastruktur!**
  - Entflechtung aus dem TUGnet
  - vom Access physikalisch & logisch getrennt
  - spezielle Hardware & Steuerungsprotokolle
  - hochredundant

Keine „Instituts-“ oder andere Clientnetze!

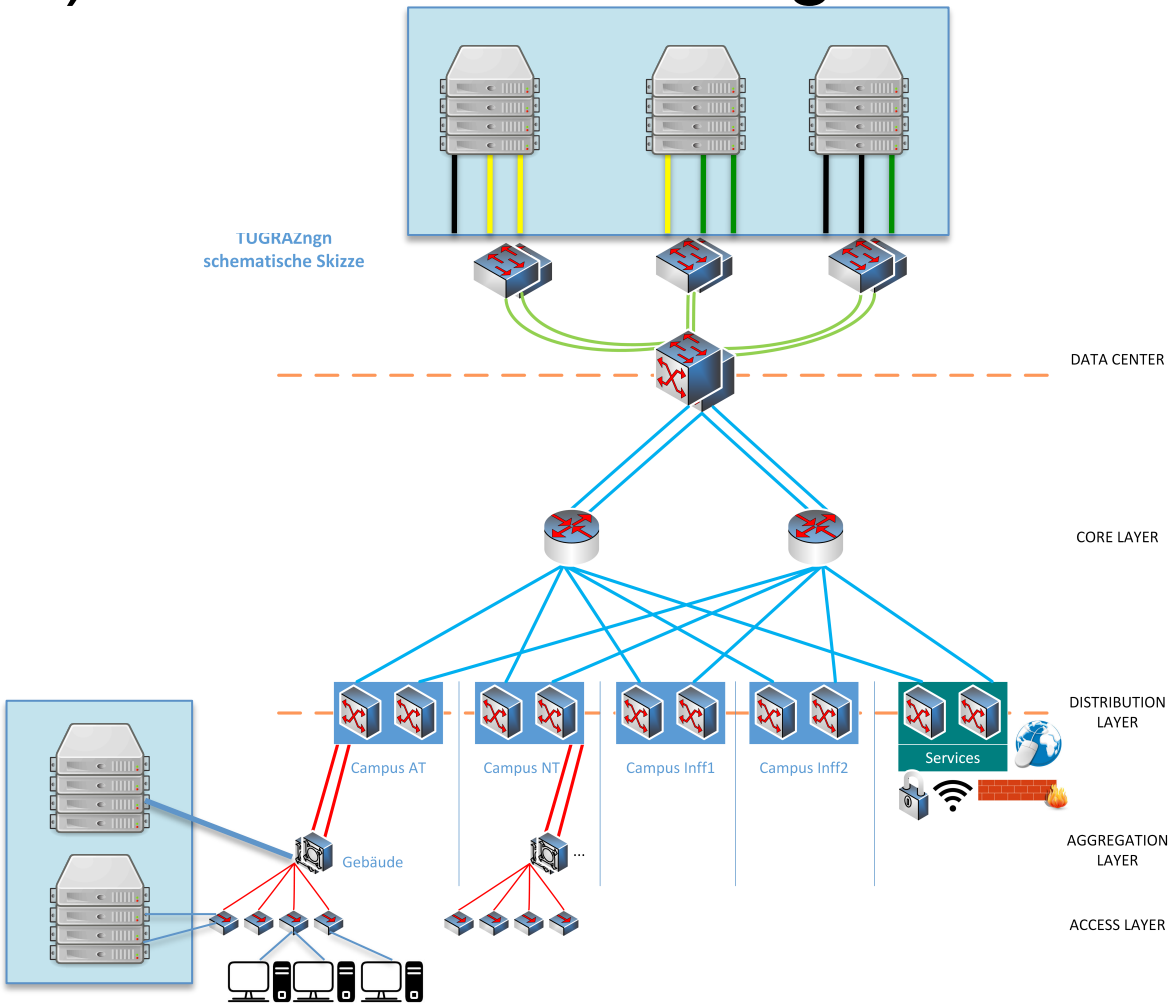
Exkurs: TUGRAZngn DataCenter (cont.)

- logischer Anschluss an das Data Center
  - Institutsserver können dort natürlich platziert werden
  - → bei Herauslösung der Server aus den Institutsnetzen
  - möglich, wenn IP-mäßige Trennung zwischen Servern und Clients vorhanden
  - DC-Subnetz kann Teil des virtuellen Institutsnetzes sein (nicht öffentlich zugänglich)
  - ansonsten: Anschluss an die Access-Infrastruktur (auch 10GBit)

- Layer 2 im Data Center per Design über mehrere Standorte gespannt → Standortunabhängig!

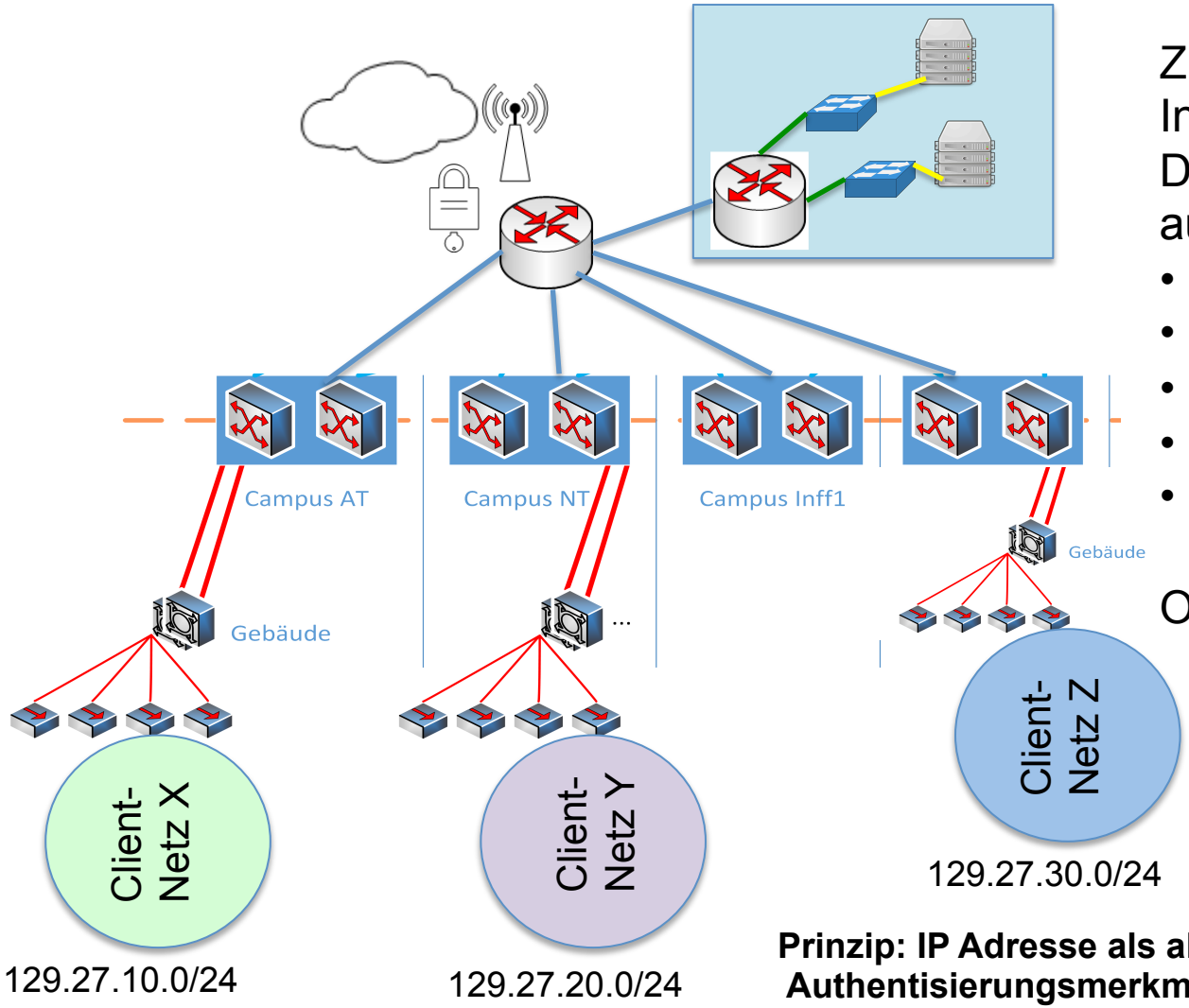
Exkurs: TUGRAZngn DataCenter

(cont.) Veranschaulichung



Ideal Design

(Instituts-)Server im DataCenter



Zugriff auf zentrale (ZID) und Institutsdienste, die im DataCenter gehostet werden aus dem

- WLAN
- Internet
- TUGnet (ggf. VPN)
- Institutsnetzen
- **„Clientnetzen“**

Optional: DC Firewall

Prinzip: IP Adresse als alleiniges Authentisierungsmerkmal war nie „state of the art“

Abschließende Bemerkungen

Zeitplan und Vorgehensweise

- Erster Schritt: Bereinigung Access, Umbau einiger Gebäude (Kop 24 [NT], Inff.16, CEG, PTZ, ...)
  → bis Ende 2014

- Parallel: Beginn der **Planungsphase**
  - Bedarfserhebung
  - Planung Core
  - Migrationsplanung Core
  - Migrationskonzepte/-Varianten Benutzernetze
  - Einzelgespräche

Abschließende Bemerkungen

Zeitplan und Vorgehensweise (cont.)

- Umsetzung
  - parallel neuen MPLS-Core aufbauen
  - „sanfte Migration“ einzelner Dienste
  - Migration Data Center
  - Migration der Institutsnetze/OE-Netze

Zeithorizont: November 2014 - Juni 2015

Weitere Planungen

- „*Gigabit am Arbeitsplatz*“ flächendeckend bis 2016
- Ausbau der PoE-Infrastruktur
- Ausbau VoIP
- Ausbau des Monitoring
- Institutsfirewall neu: 2016

Angefragte Themen

- Zugriff auf Monitoring-Daten
- Kommunikationsplan
- Port- und Downloadsperren
- ..?

ENDE