Nutzen und Vorteile der Netzwerkvirtualisierung

Dominik Krummenacher
Systems Engineer, Econis AG

What's the Meaning of Virtual?

- If you can see it and it is there

  It's **real**

- If you can't see it but it is there

  It's **transparent**

- If you can see it and it is not there

  It's **virtual**

- If you can not see it and it is not there

  It's **gone**

Econis – Ihr starker IT-Partner

- Topanbieter von IT-Dienstleistungen in der Schweiz
- Einzigartiges Lösungs- und Serviceportfolio
- Höchster Partnerstatus mit Zertifizierungen für Cisco Systems, IBM und Microsoft
- Seit 1997 erfolgreich im Markt
- Seit September 2009 in Luzern
- Hauptsitz in Dietikon ZH
- Weitere Niederlassung in Lyss BE

Agenda

- Gründe für Netzwerkvirtualisierung
- Was ist Netzwerkvirtualisierung?
- Grundlagen Netzwerkvirtualisierung
- Business Case Finanzinstitut
  - Anforderungen
  - Zonendesign
  - LAN Design
  - WAN Design
  - Projektablauf
  - Vorteile / Nachteile
- Ausblick

Agenda

- **Gründe für Netzwerkvirtualisierung**
- Was ist Netzwerkvirtualisierung?
- Grundlagen Netzwerkvirtualisierung
- Business Case Finanzinstitut
  - Anforderungen
  - Zonendesign
  - LAN Design
  - WAN Design
  - Projektablauf
  - Vorteile / Nachteile
- Ausblick

Gründe für Netzwerkvirtualisierung

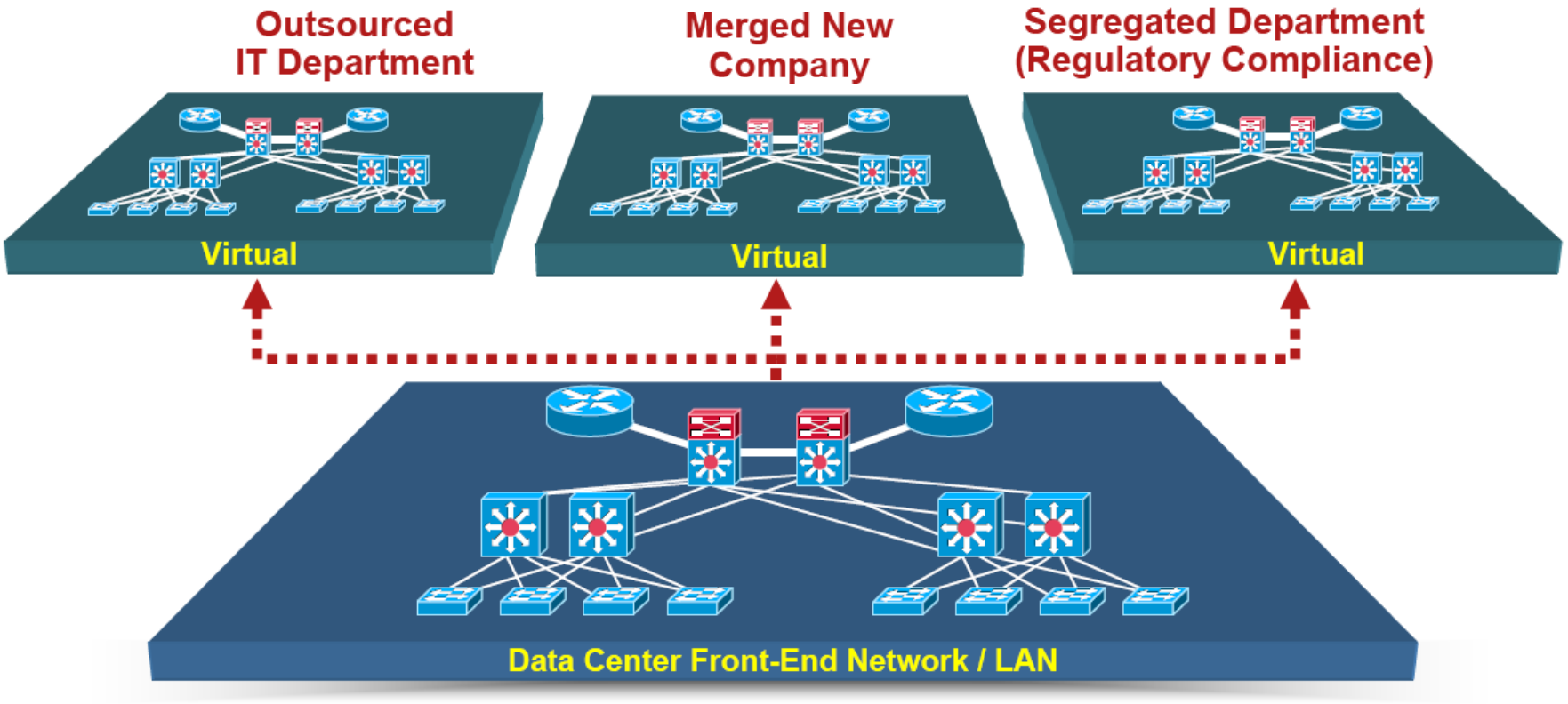
- Erhöhung der Netzwerksicherheit
- Schutz der eigenen Infrastruktur / Ressourcen
- Segmentierung des Netzwerks
  - Netzwerkzugang für Partner
  - Netzwerkzugang für Gäste
  - Trennung von Abteilungen

Agenda

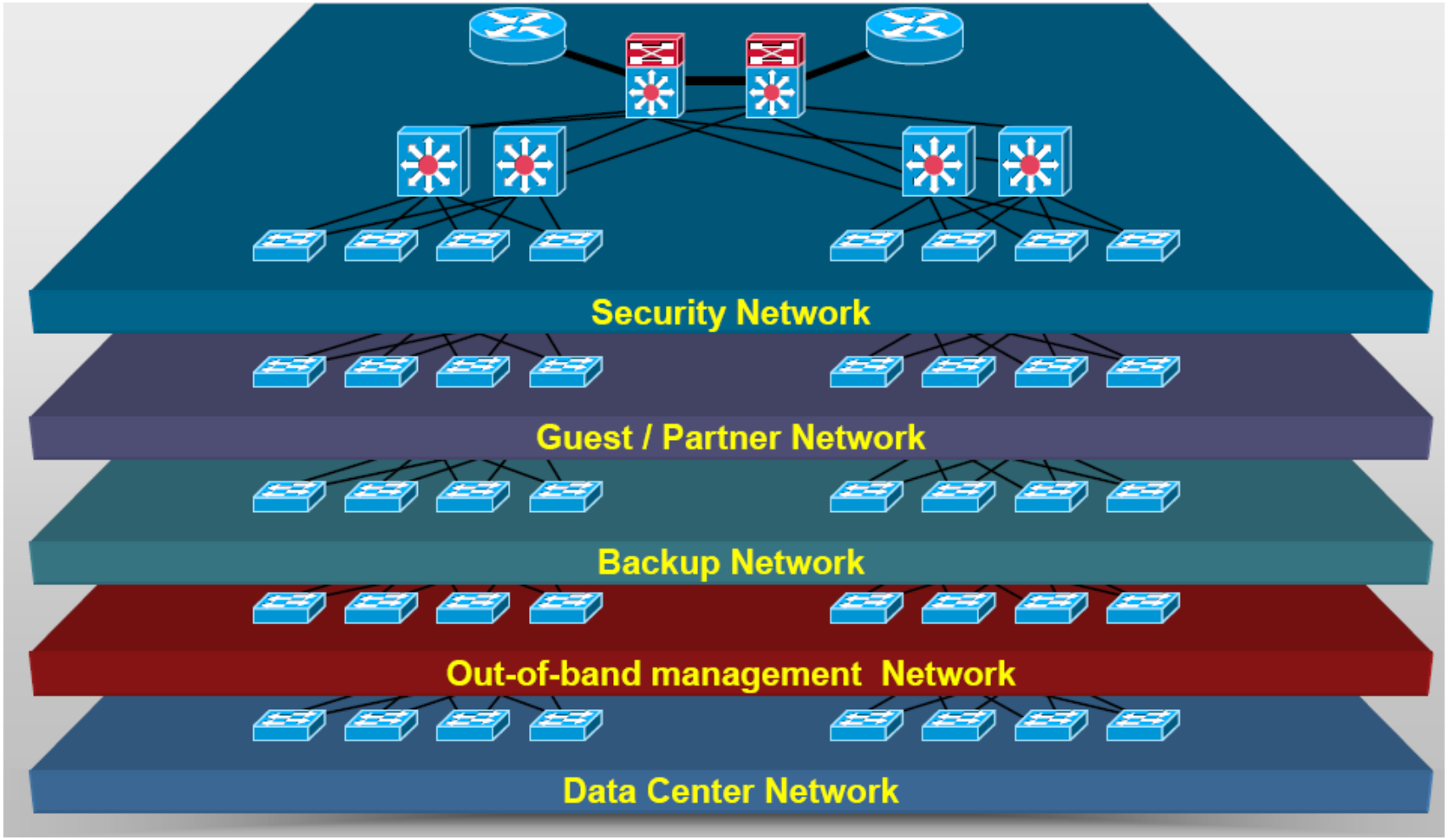
- Gründe für Netzwerkvirtualisierung
- **Was ist Netzwerkvirtualisierung?**
- Grundlagen Netzwerkvirtualisierung
- Business Case Finanzinstitut
  - Anforderungen
  - Zonendesign
  - LAN Design
  - WAN Design
  - Projektablauf
  - Vorteile / Nachteile
- Ausblick

Was ist Netzwerkvirtualisierung?

- Virtualisierung: 1 to Many
- Ein physikalisches Netzwerk unterstützt viele virtuelle Netzwerke



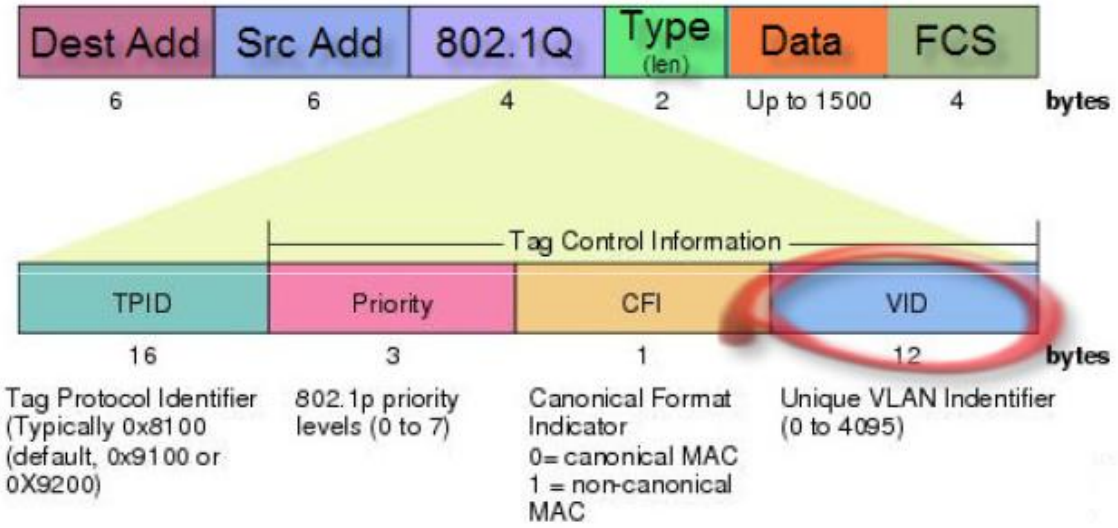
Was ist Netzwerkvirtualisierung?



Agenda

- Gründe für Netzwerkvirtualisierung
- Was ist Netzwerkvirtualisierung?
- **Grundlagen Netzwerkvirtualisierung**
- Business Case Finanzinstitut
  - Anforderungen
  - Zonendesign
  - LAN Design
  - WAN Design
  - Projektablauf
  - Vorteile / Nachteile
- Ausblick

- Virtual LANs (VLANs)
  - IEEE 802.1Q Virtual LANs



  - 12 bits ➔ bis zu 4096 VLANs auf einem physikalischen Kabel

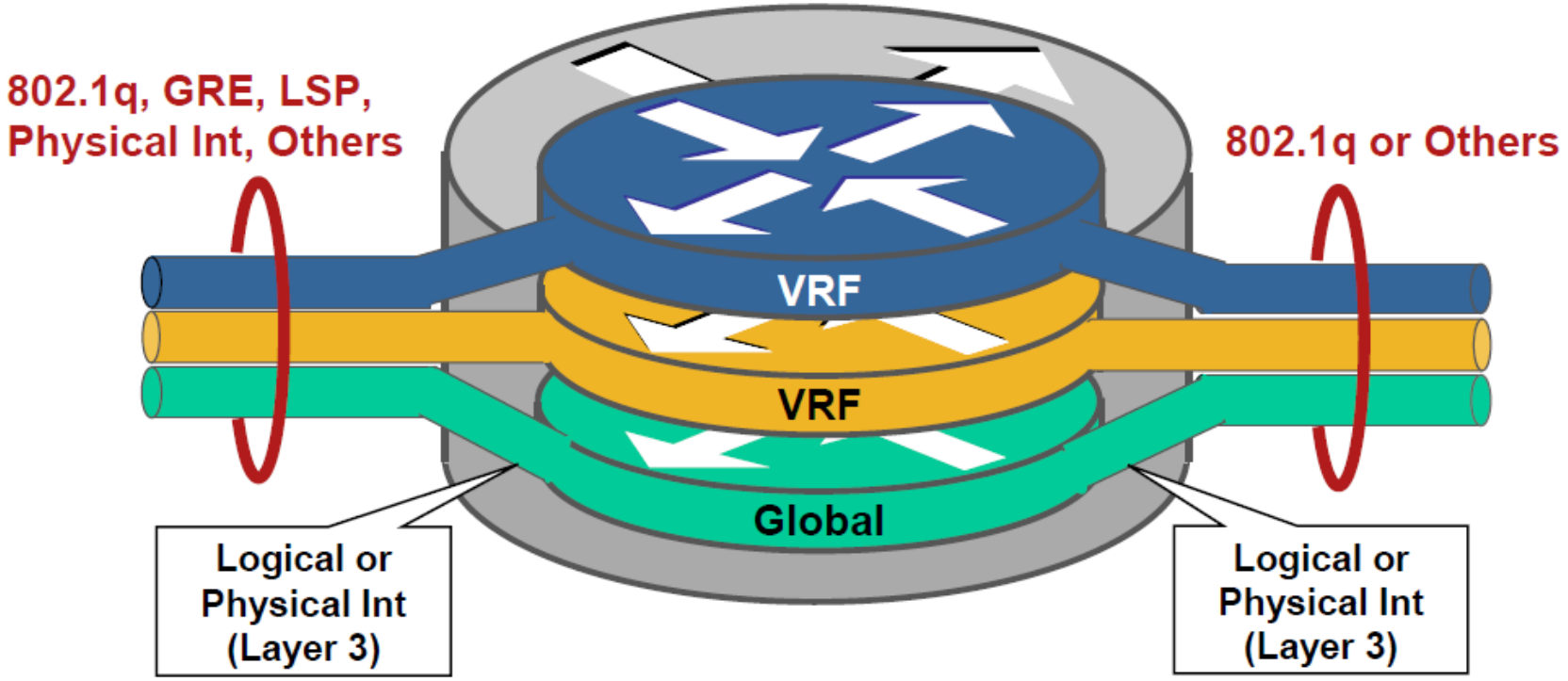
Grundlagen Netzwerkvirtualisierung

- Virtual LANs (VLANs)

```
vlan 10
 name SERVER
vlan 20
 name MGMT

int gi0/1
 switchport access vlan 10
```

- Virtual Routing and Forwarding Instance (VRF)
  - VRFs unterteilt die Routing Tabelle in viele virtuelle Routing Tabellen

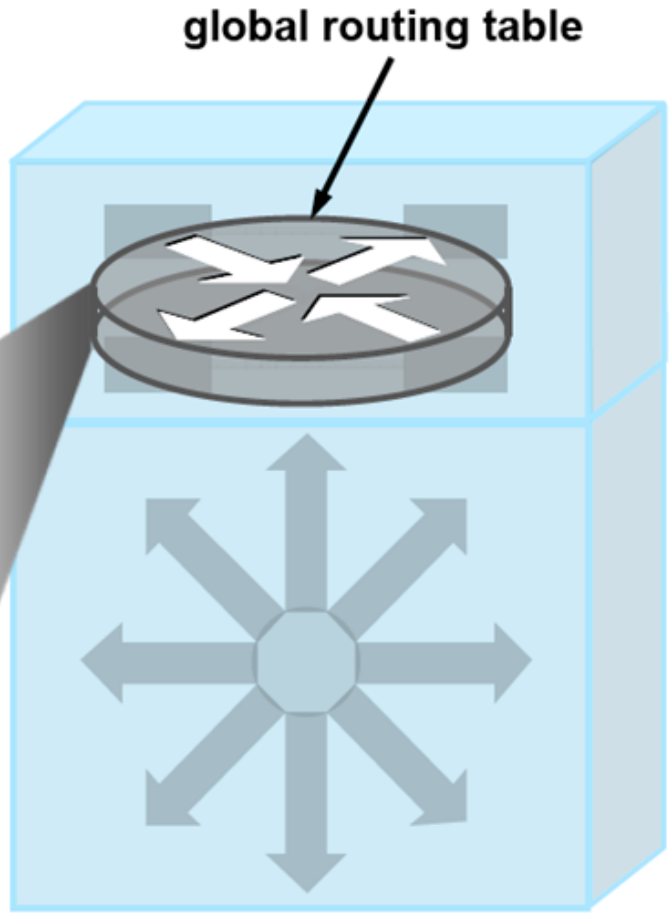


Grundlagen Netzwerkvirtualisierung

- Virtual Routing and Forwarding Instance (VRF)
  - Eignung Routing-Prokolle
    - Grundsätzlich alle geeignet
    - RIPv2, EIGRP und BGP (und statisch) nur ein Prozess
    - OSPF, IS-IS pro VRF ein Prozess

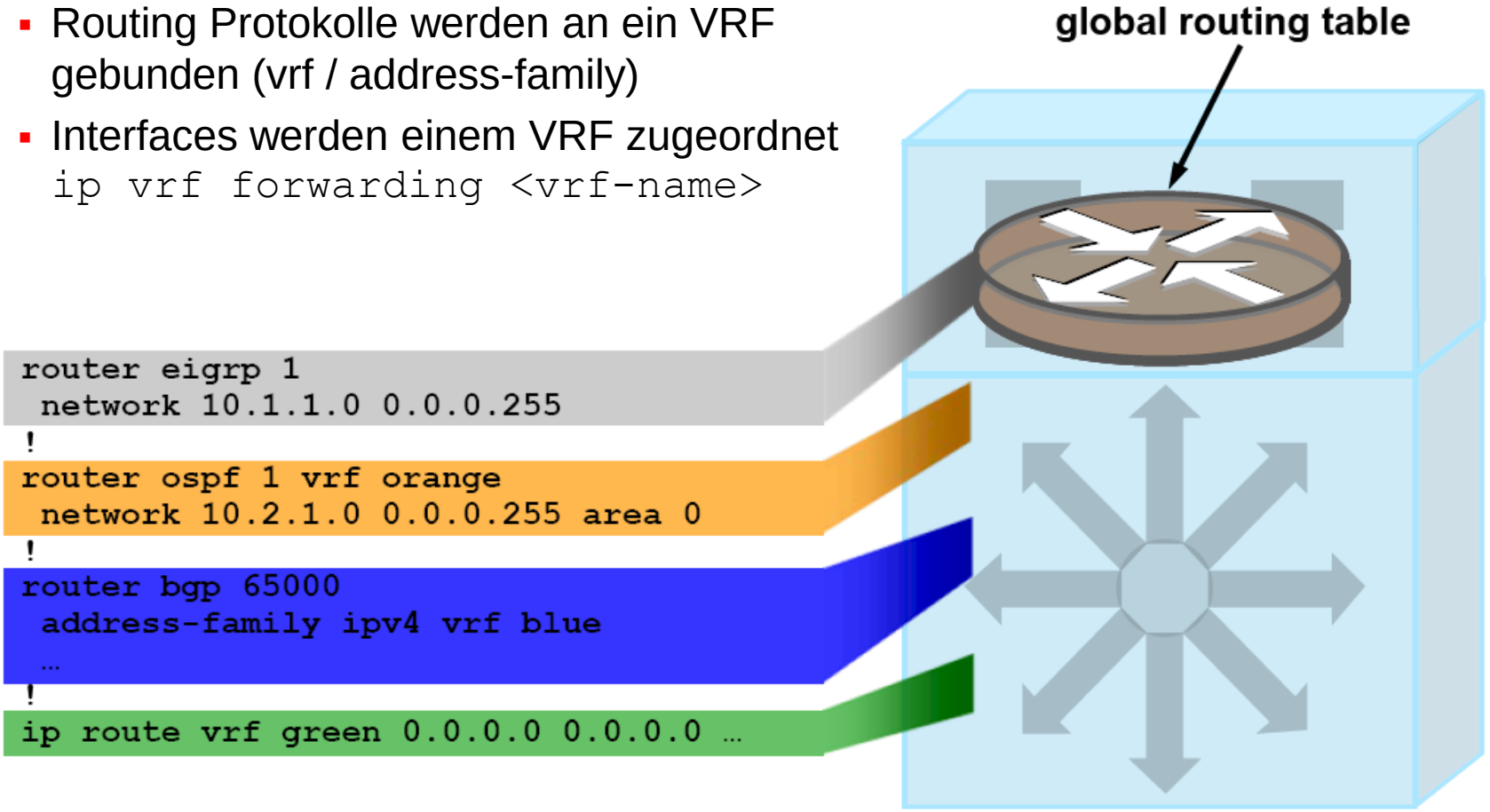
- Virtual Routing and Forwarding Instance (VRF)
  - **Beispiel:** Ein Routing Protokoll pro VRF
    VRF1 läuft mit OSPF, VRF2 mit EIGRP
  - **Ziel:** Isolation von Routing und Forwarding Tabellen
    Erlaubt Überschneidung von IP Adressen
    Mehrere VLANs pro Zone (mit VLANs nicht möglich)

- Virtual Routing and Forwarding Instance (VRF)
  - Typischerweise werden alle Routing Protokolle und statische Routen in einer Routingtabelle zusammengeführt
  - Alle Interfaces sind Teile der globalen Routing Tabelle




```
router eigrp 1
 network 10.1.1.0 0.0.0.255
!
router ospf 1
 network 10.2.1.0 0.0.0.255 area 0
!
router bgp 65000
 neighbor 192.168.1.1 remote-as 65000
!
ip route 0.0.0.0 0.0.0.0 140.75.138.114
```

- Virtual Routing and Forwarding Instance (VRF)
  - VRFs erlauben die Unterteilung in diverse Routing Tabellen
  - Routing Protokolle werden an ein VRF gebunden (vrf / address-family)
  - Interfaces werden einem VRF zugeordnet
    `ip vrf forwarding <vrf-name>`



- Virtual Routing and Forwarding Instance (VRF)

```
Interface Vlan X
 description *** VLAN FOR VL-MGMT-EXTERN ***
 ip vrf forwarding MGMT-EXTERN
 ip address 10.x.x.x 255.255.255.0

router eigrp 200
 [...]
 address-family ipv4 vrf MGMT-EXTERN
 autonomous-system 200
 network 10.x.x.x 0.0.0.0
 no auto-summary
 [...]
 exit-address-family
```

Grundlagen Netzwerkvirtualisierung

- Virtual Routing and Forwarding Instance (VRF)

  `Show ip int brief`

  ➔Zeigt alle IP Interface

  `Show ip route`

  ➔Zeigt globale Routing-Tabelle (nur wenige Interfaces als connected angezeigt.

  `Show ip route` **`vrf MGMT-EXTERN`**

  ➔Zeigt Routing Tabelle des VRF MGMT-EXTERN mit gelernten Routen und directly connected L3 Interfaces

Grundlagen Netzwerkvirtualisierung

- Virtual Private Network (VPN)
  - Tunneling von Netzwerken / Datenverkehr
    - Verschlüsselt → IPSec
    - Unverschlüsselt → GRE Tunnel

- Multiprotokoll Label Switching (MPLS)
  - Vereinfacht gesagt: „VLANs auf Layer 3“
  - Anstelle VLAN-ID → MPLS Label

(b) IEEE 802 MAC Frame

Grundlagen Netzwerkvirtualisierung

- Zusammenfassung der Technologien:
  - VLANs (Layer 2)
  - VRFs (Layer 3)
  - VPNs (Layer 2/3)
  - MPLS (Layer 3)
  - …

  - VRF-Lite: Unterstützung von VRFs, keine Unterstützung von MPLS
  - Auf meisten L3 Switche von Cisco unterstützt (Lizenz)

  - MPLS nur auf Cisco Cat6500 und Cat3750 Metro unterstützt

Agenda

- Gründe für Netzwerkvirtualisierung
- Was ist Netzwerkvirtualisierung?
- Grundlagen Netzwerkvirtualisierung
- Business Case Finanzinstitut
  - **Anforderungen**
  - Zonendesign
  - LAN Design
  - WAN Design
  - Projektablauf
  - Vorteile / Nachteile
- Ausblick

Anforderungen

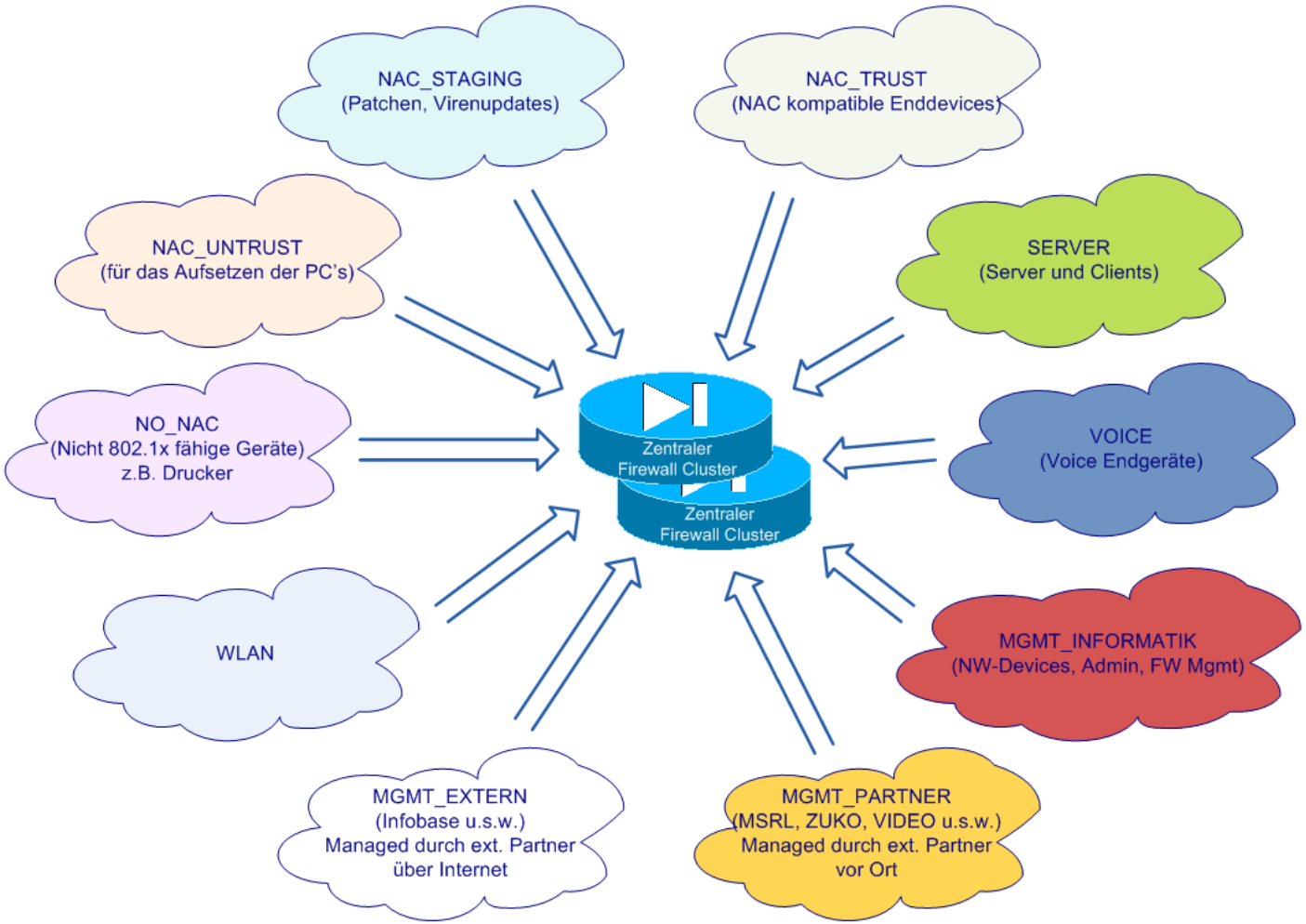
- Projektumsetzung: 2009

- Die Ablösung und Erneuerung der LAN-Infrastruktur am Hauptsitz und in den Filialen
- Erhöhung der Verfügbarkeit
- Verwendung eines Zonenmodells
- Schutz der Zonen durch eine zentrale Firewall

Agenda

- Gründe für Netzwerkvirtualisierung
- Was ist Netzwerkvirtualisierung?
- Grundlagen Netzwerkvirtualisierung
- Business Case Finanzinstitut
  - Anforderungen
  - **Zonendesign**
  - LAN Design
  - WAN Design
  - Projektablauf
  - Vorteile / Nachteile
- Ausblick

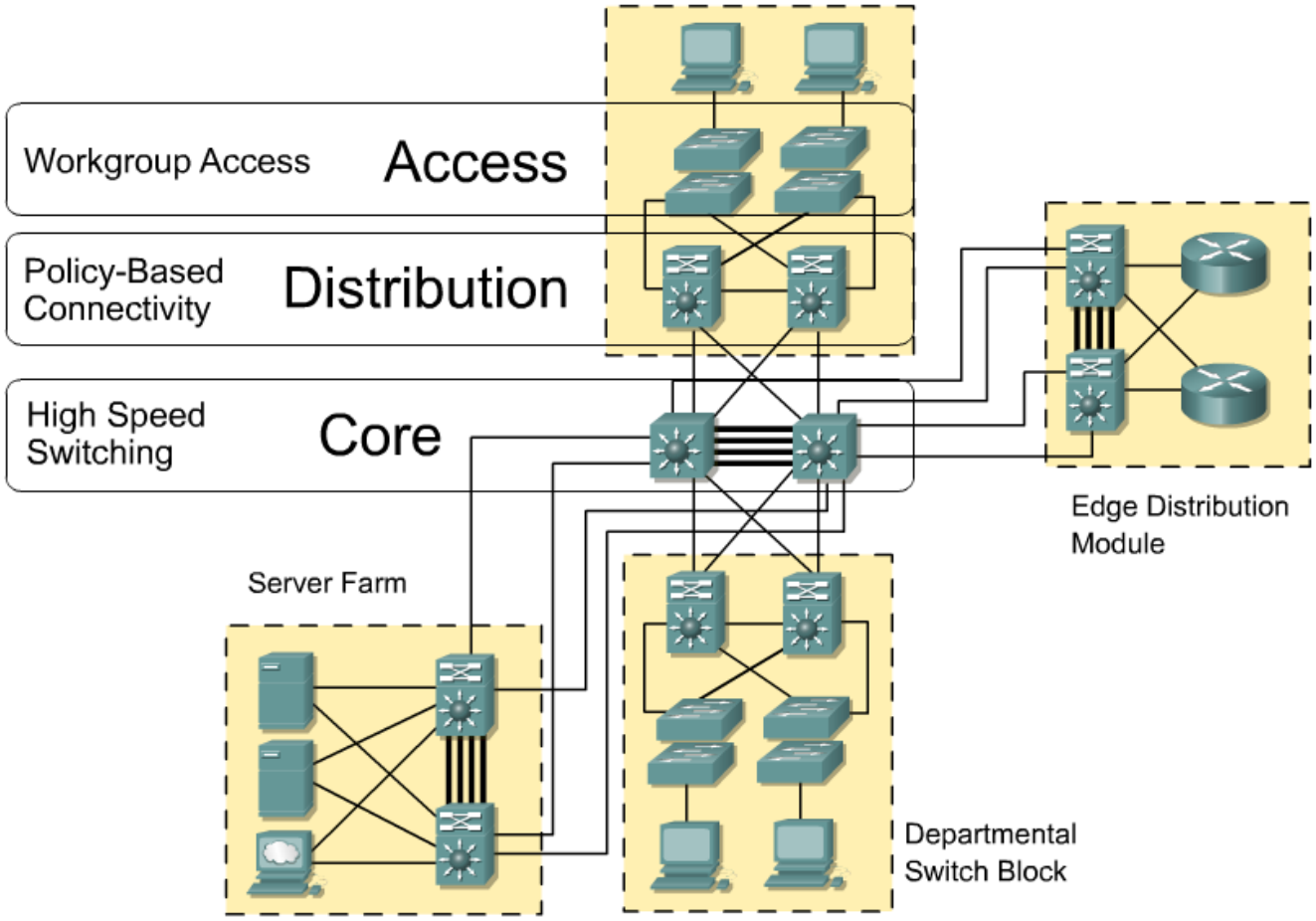
Zonendesign



Agenda

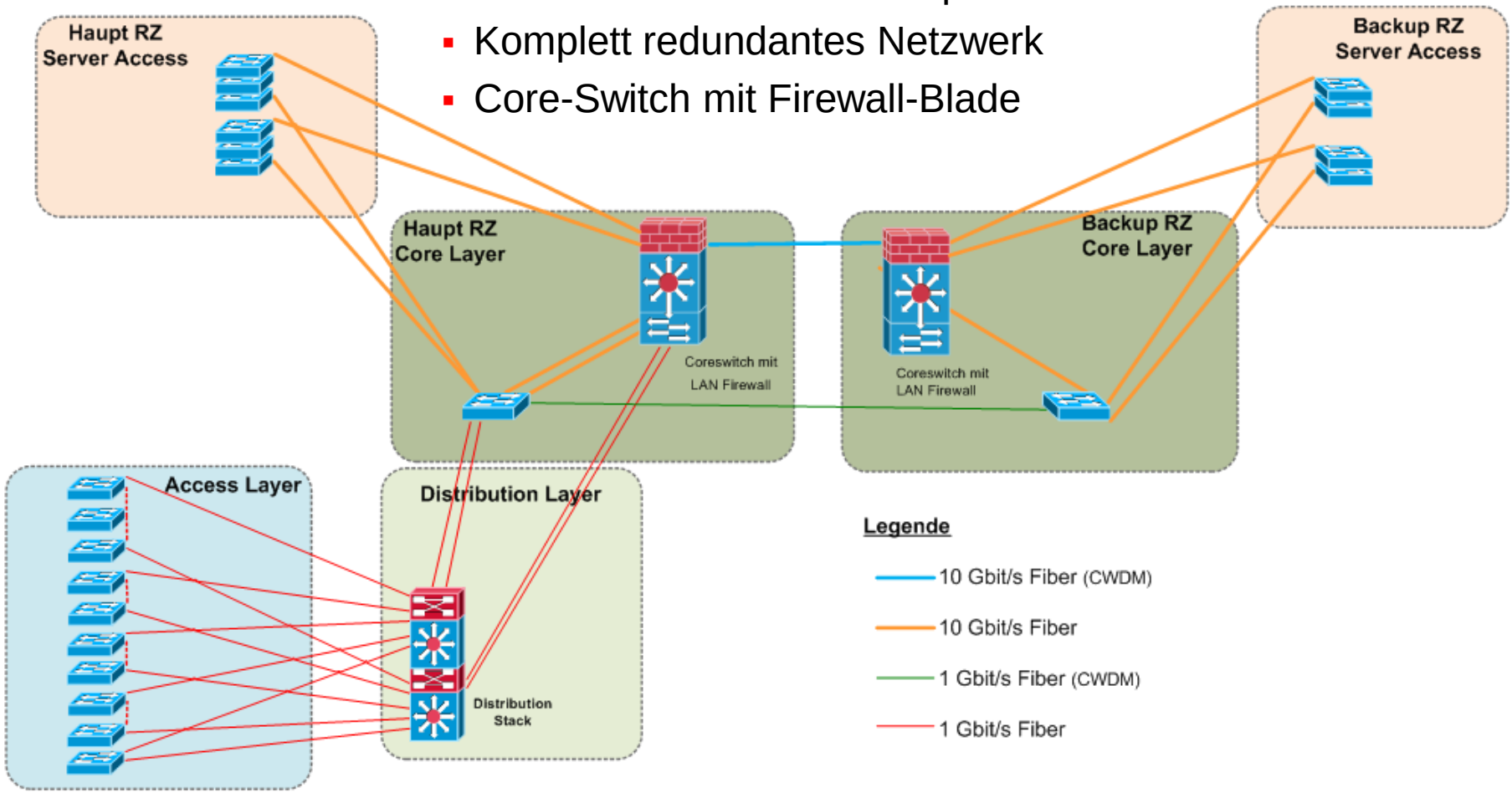
- Gründe für Netzwerkvirtualisierung
- Was ist Netzwerkvirtualisierung?
- Grundlagen Netzwerkvirtualisierung
- Business Case Finanzinstitut
  - Anforderungen
  - Zonendesign
  - **LAN Design**
  - WAN Design
  - Projektablauf
  - Vorteile / Nachteile
- Ausblick

- Grundlagen von Cisco Campus Design



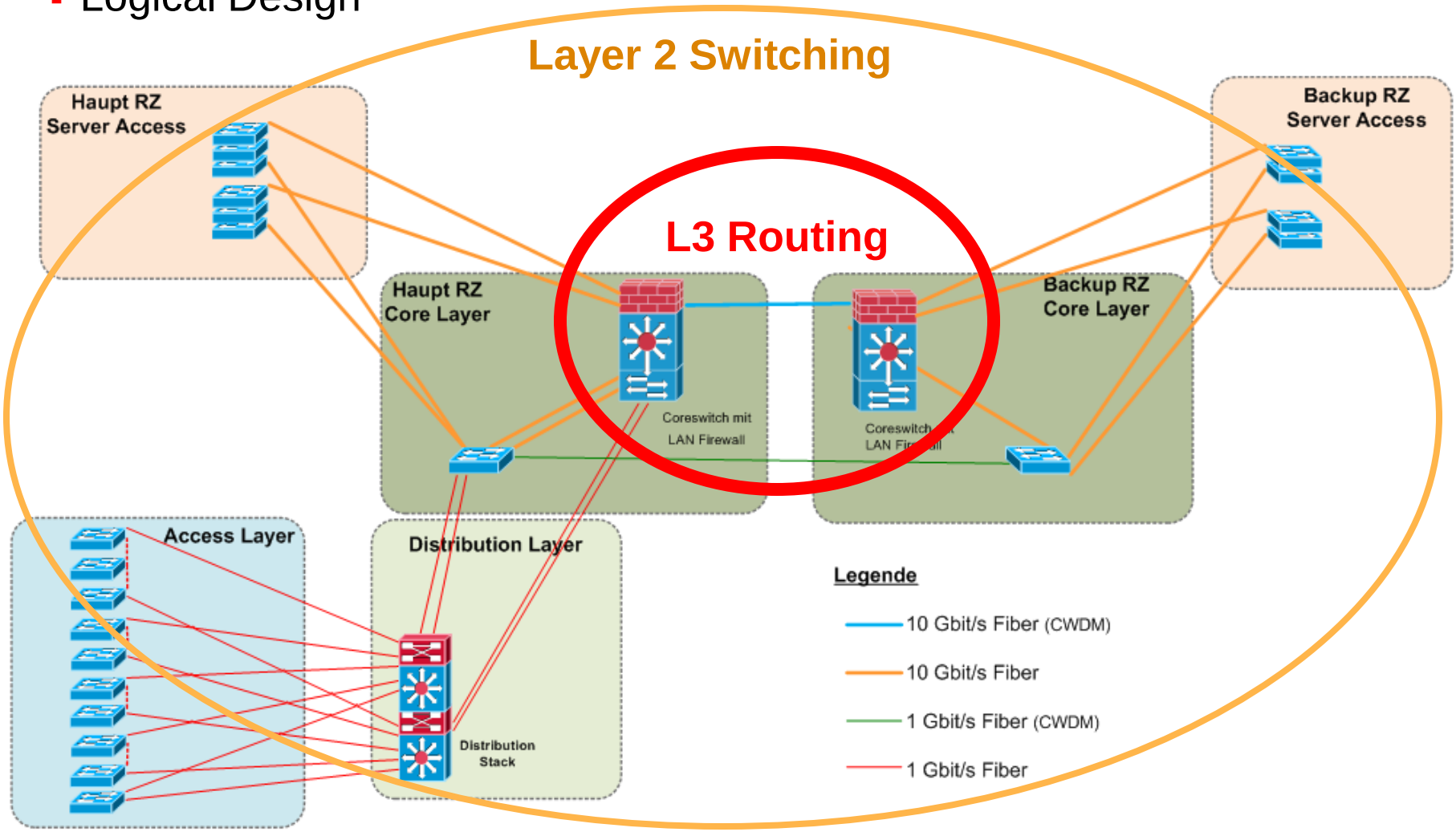
LAN Design

- Physical Design
  - Core und Server mit 10Gbps
  - Komplett redundantes Netzwerk
  - Core-Switch mit Firewall-Blade



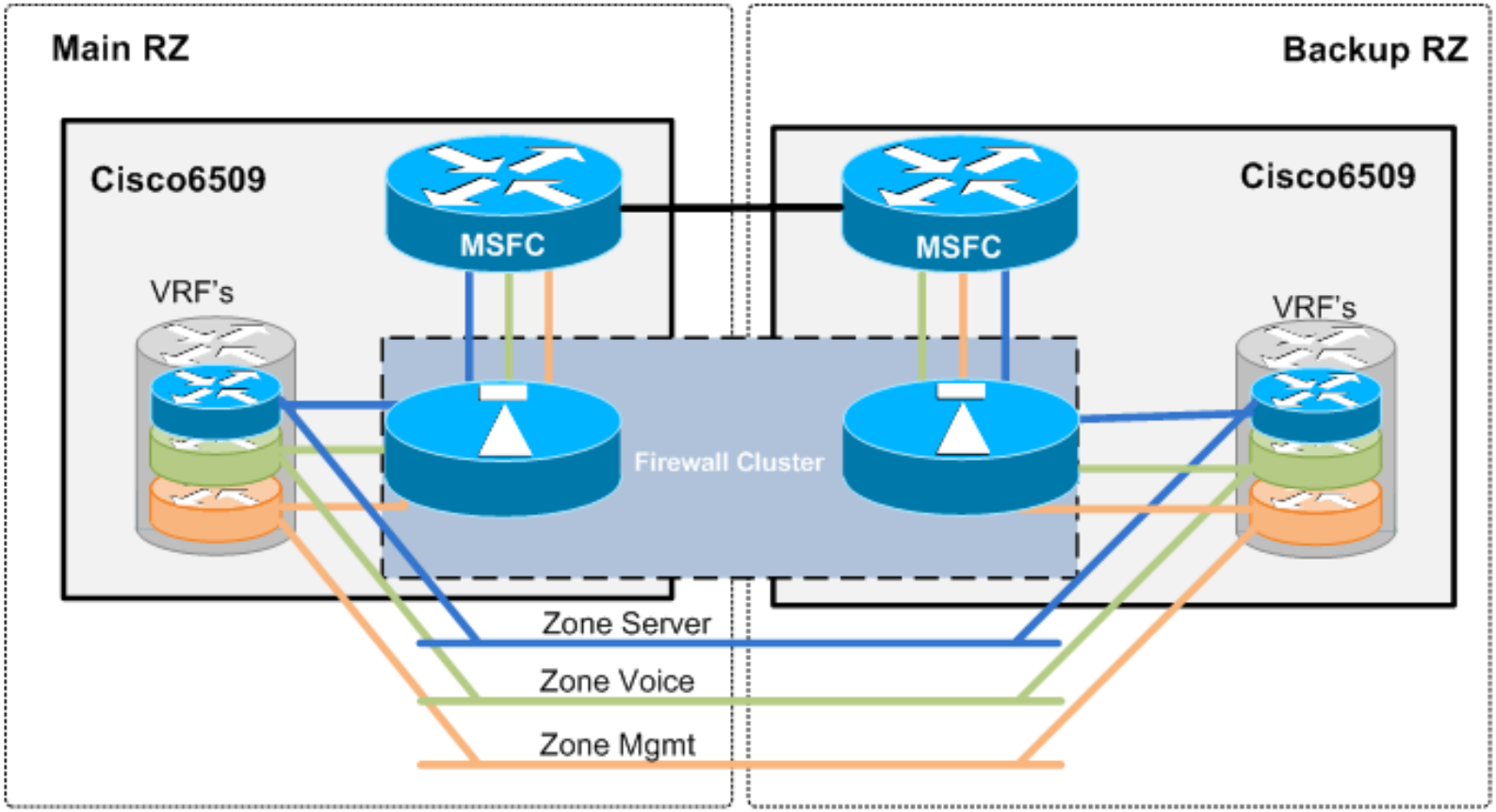
LAN Design

- Logical Design



LAN Design

- Logical Design

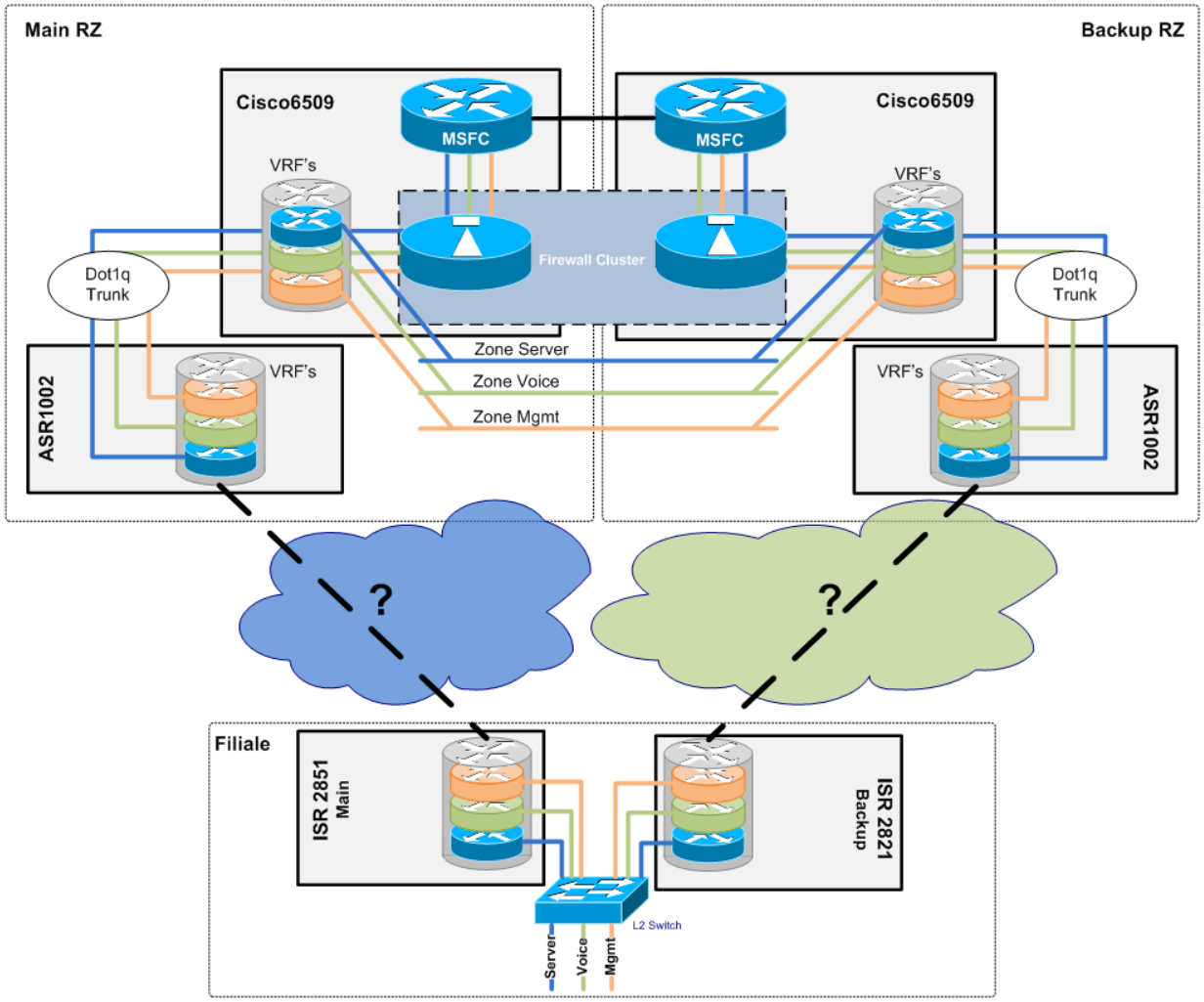


Agenda

- Gründe für Netzwerkvirtualisierung
- Was ist Netzwerkvirtualisierung?
- Grundlagen Netzwerkvirtualisierung
- Business Case Finanzinstitut
  - Anforderungen
  - Zonendesign
  - LAN Design
  - **WAN Design**
  - Projektablauf
  - Vorteile / Nachteile
- Ausblick

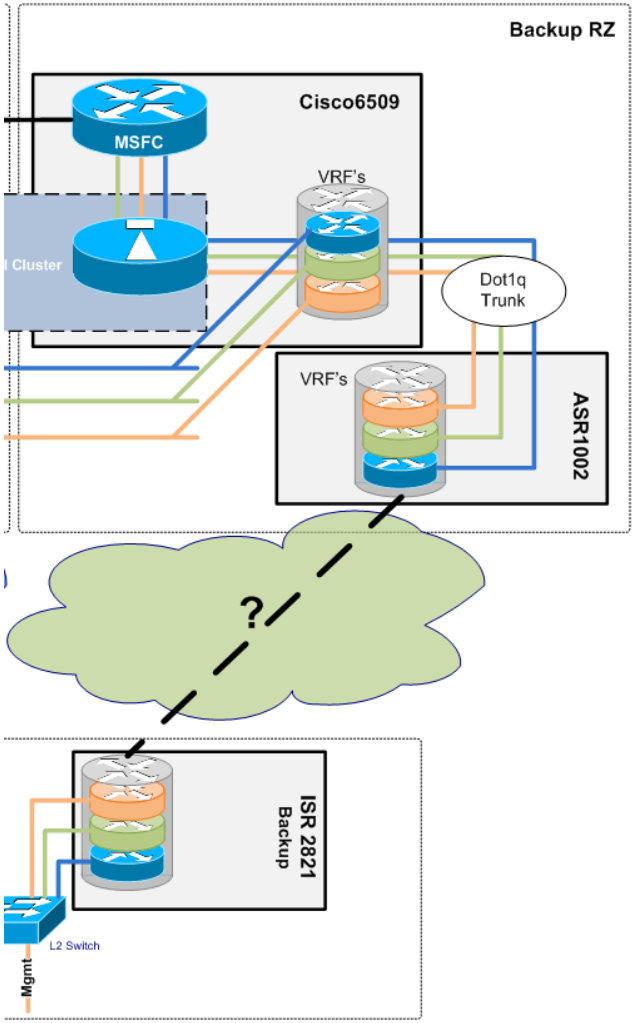
WAN Design

- Zonen in den Filialen – wie?

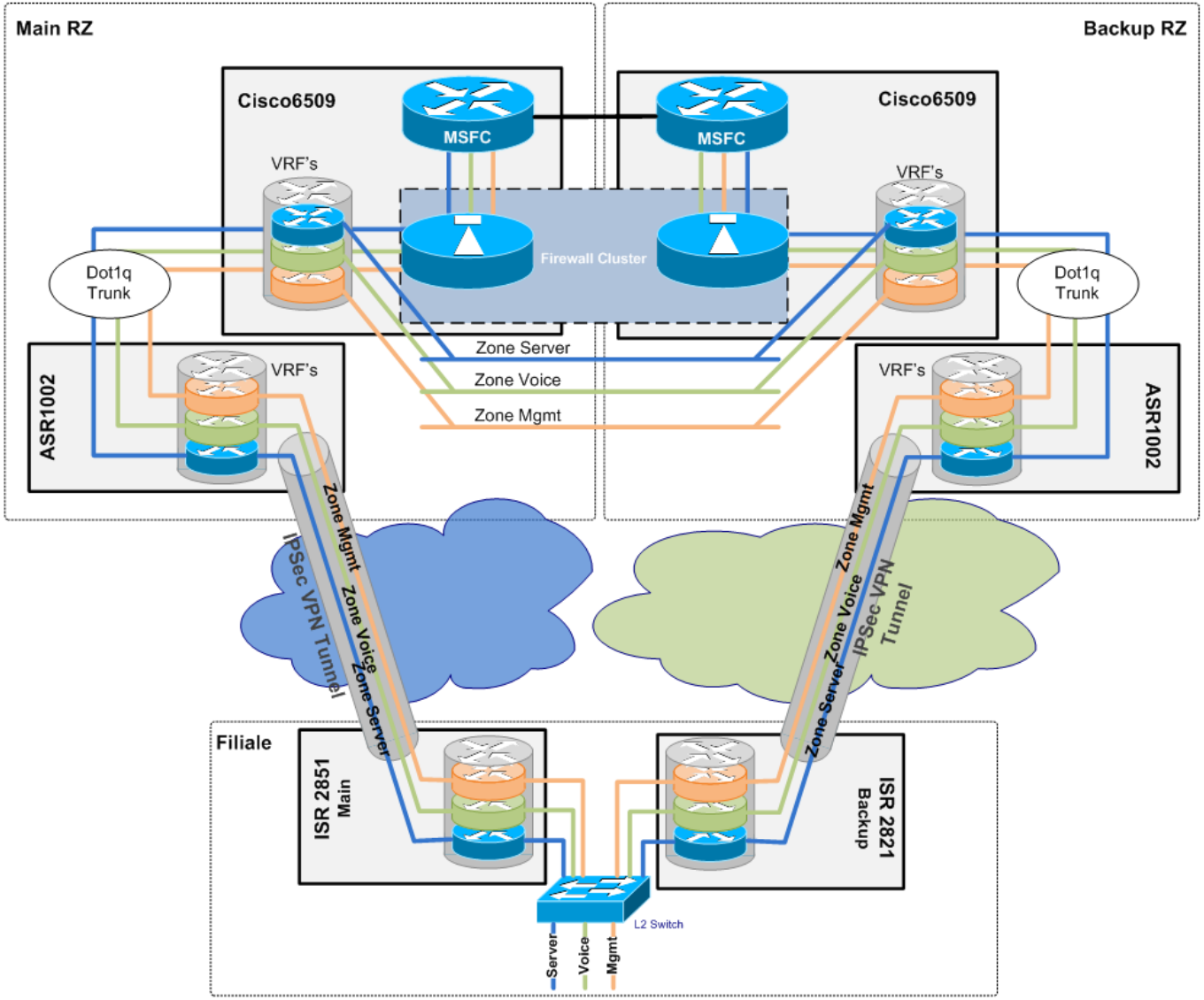


WAN Design

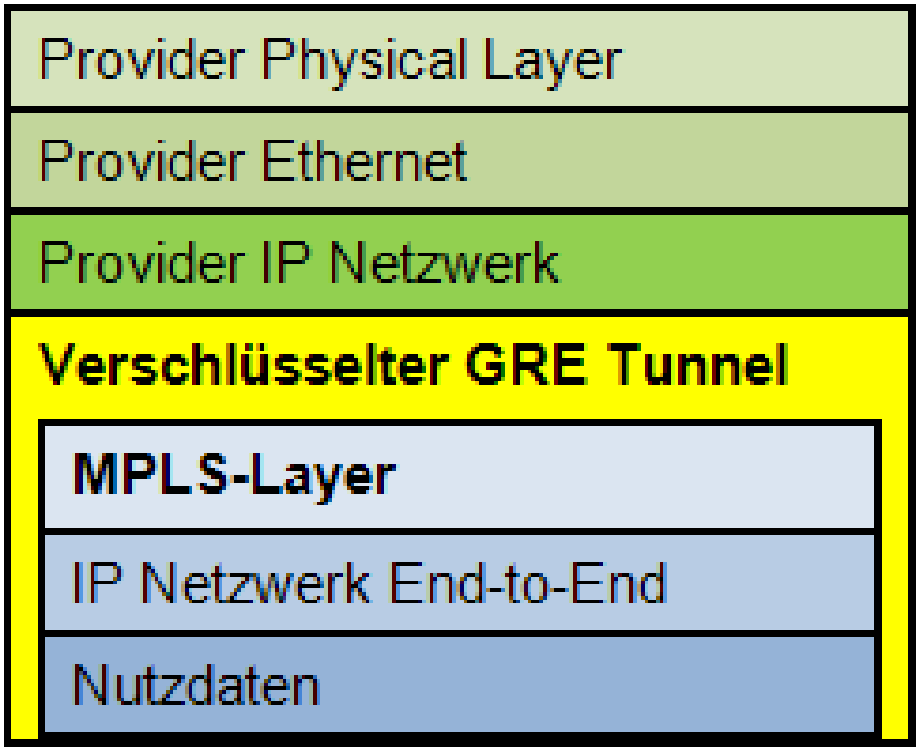
- Zonen in den Filialen – wie?
  - VLANs bei Darkfiber → zu teuer
  - Provider MPLS pro Zone
    → zu grosse Abhängigkeit,
    keine Verschlüsselung
  - Ein VPN Tunnel pro Zone → Möglichkeit
  - MPLS innerhalb eines VPN Tunnels
    → Dies wurde umgesetzt



WAN Design

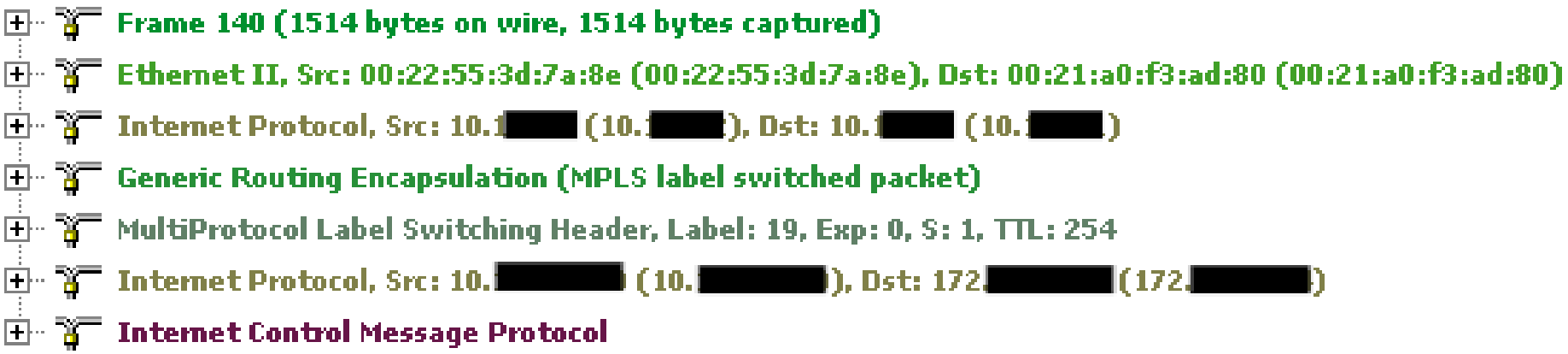


- Paketaufbau im WAN

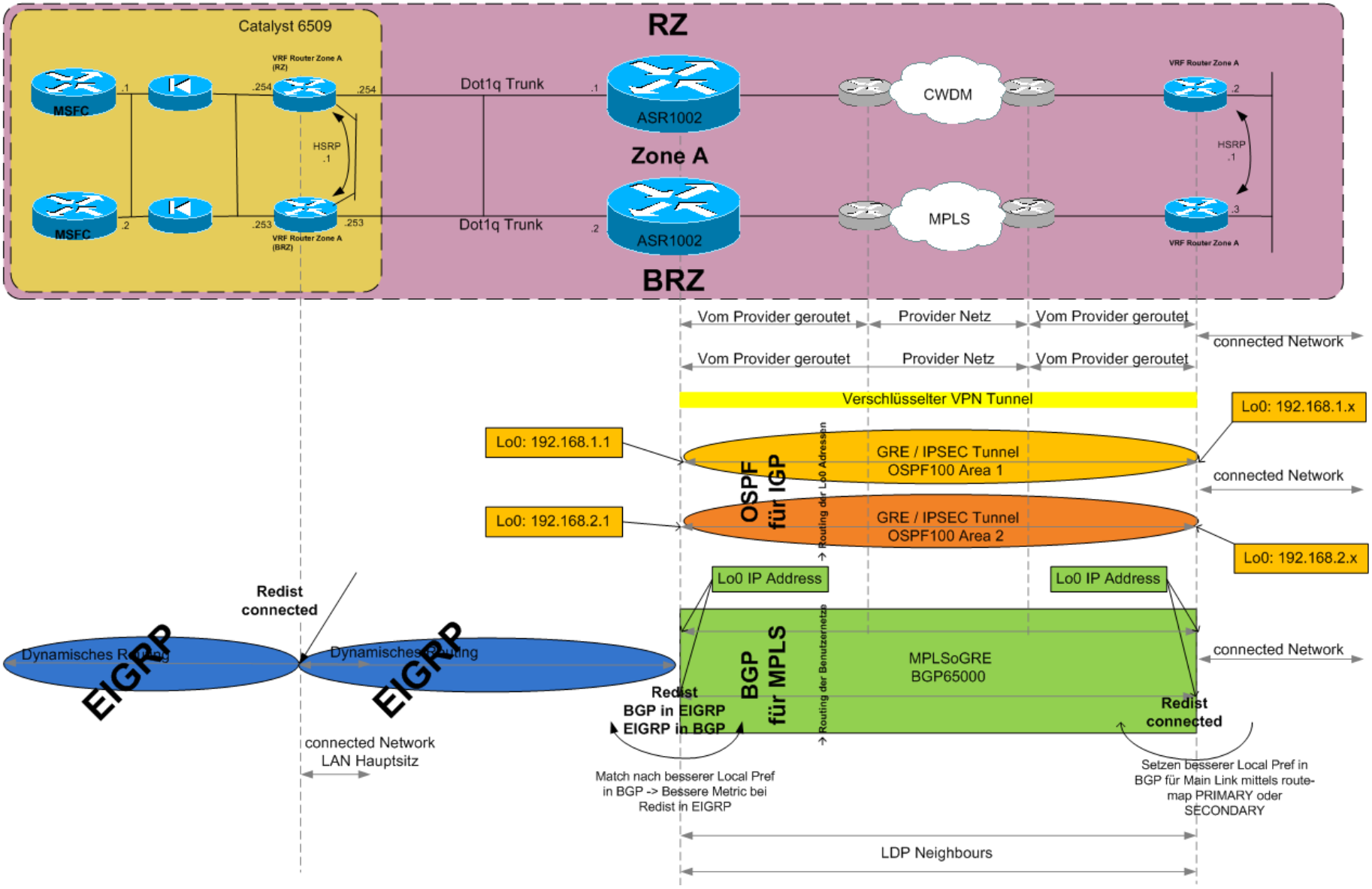


WAN Design

- Paketaufbau im WAN



Routing Design



Agenda

- Gründe für Netzwerkvirtualisierung
- Was ist Netzwerkvirtualisierung?
- Grundlagen Netzwerkvirtualisierung
- Business Case Finanzinstitut
  - Anforderungen
  - Zonendesign
  - LAN Design
  - WAN Design
  - **Projektablauf**
  - Vorteile / Nachteile
- Ausblick

Projektablauf

- Fliessende Migration
- 1. LAN Hauptsitz
  - a) Einbau neuer Core
  - b) Routing auf neuen Core verschieben (bereits virtualisiert als eine Zone)
  - c) LAN Hauptsitz migrieren (Rack für Rack)
  - d) Rückbau alter Komponenten
- 2. WAN Hauptsitz
  - a) Einbau neuer Hardware (Parallelbetrieb)
- 3. WAN/LAN Filialen
  - a) Komplettumbau Filiale mit neuen VPN-Routern und Switchen
- 4. WAN Hauptsitz
  - a) Ausbau alter WAN Komponenten

Agenda

- Gründe für Netzwerkvirtualisierung
- Was ist Netzwerkvirtualisierung?
- Grundlagen Netzwerkvirtualisierung
- Business Case Finanzinstitut
  - Anforderungen
  - Zonendesign
  - LAN Design
  - WAN Design
  - Projektablauf
  - **Vorteile / Nachteile**
- Ausblick

Vorteile und Nutzen

- Kostengünstige Lösung
- Fast beliebig ausbaufähig
- Erhöhung der Sicherheit durch
  - Einführung von Sicherheitszonen
  - Zugriffsregelungen
  - Logging und Überwachung
- Eleganter Zugang für Partner und Gäste

Nachteile

- Neue Technologien – neue Befehle – neues Wissen
- Schwierigeres Troubleshooting

Agenda

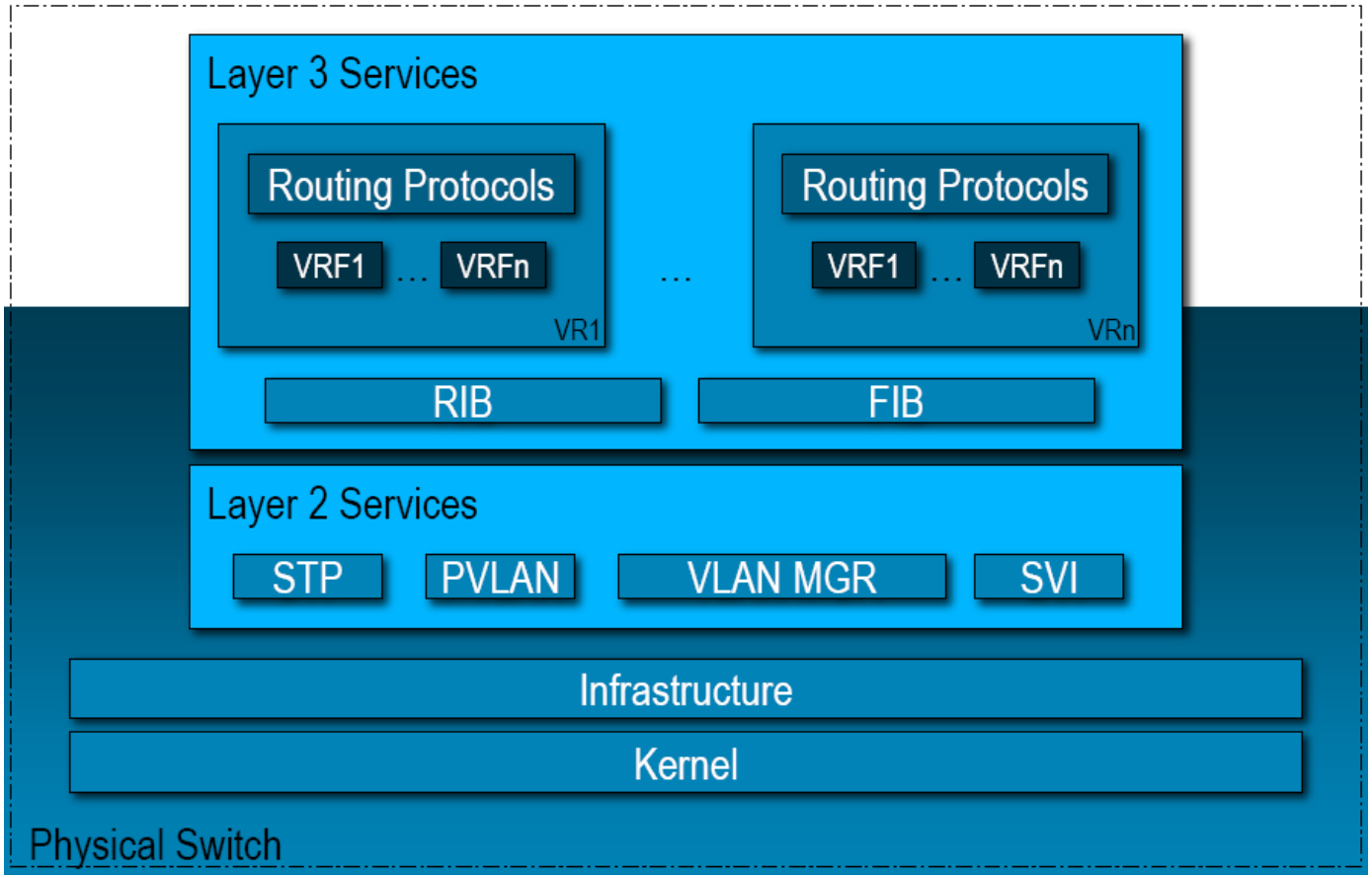
- Was ist Netzwerkvirtualisierung?
- Grundlagen Netzwerkvirtualisierung
- Business Case Finanzinstitut
  - Anforderungen
  - Zonendesign
  - LAN Design
  - WAN Design
  - Projektablauf
  - Vorteile / Nachteile
- **Ausblick**

Ausblick

- 802.1x
- NAC
- Guest Access

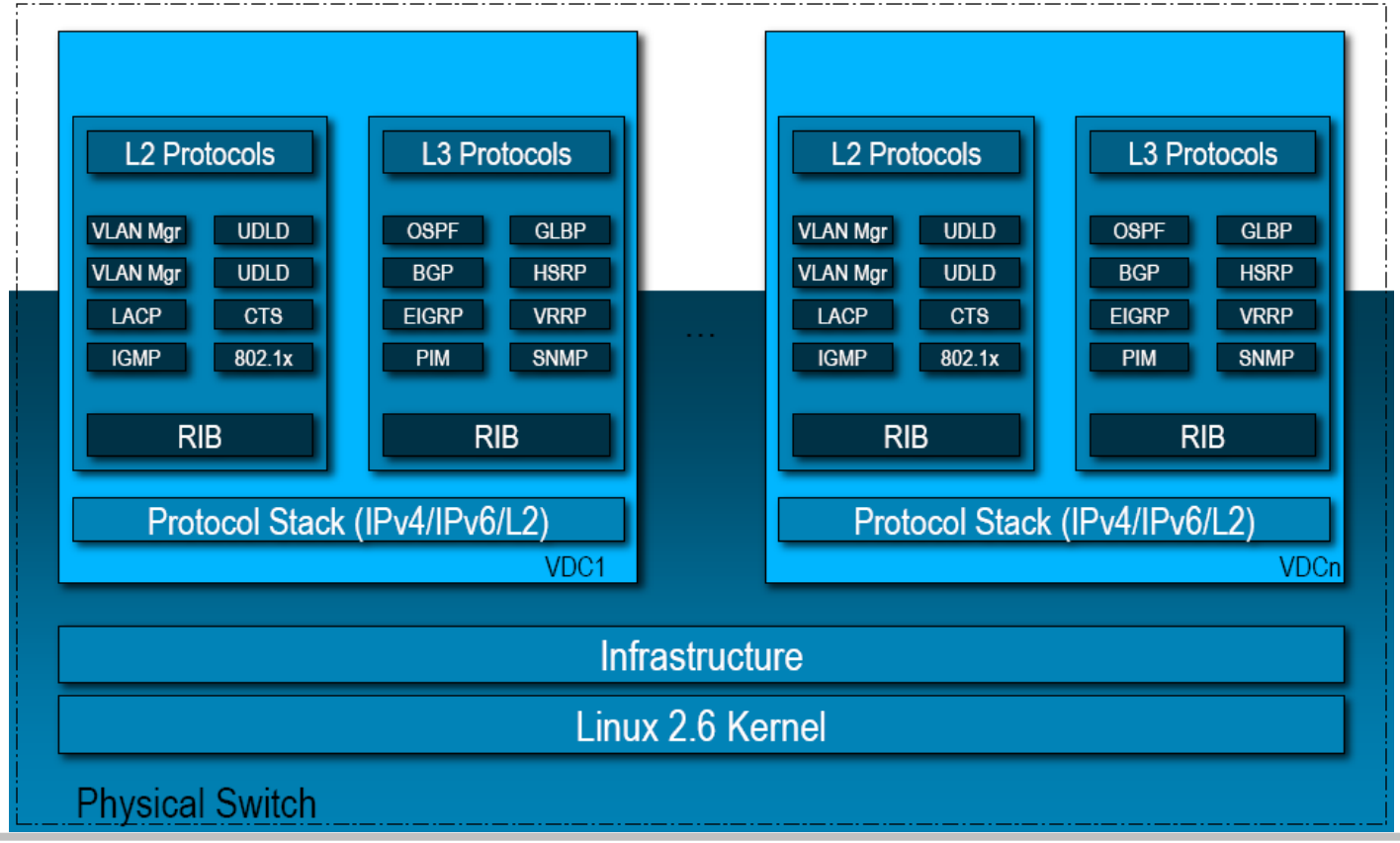
Ausblick (Rückblick)

- Bis Mitte 2009 nur Teilvirtualisierung von Prozessen wie Routing-Protokolle möglich.



Ausblick: Virtualisierung im Netzwerkbereich

- Seit Mitte 2009 Vollvirtualiserung möglich (Nexus 7000)
- z.B. Neustart eines virtuellen Switches (ohne Auswirkung auf andere virtuelle Systeme)



Ausblick

- Virtualisierung im Bereich Firewall ist herstellerabhängig
- Teil- oder Vollvirtualisierung im Markt erhältlich

Quellen / Weiterführende Informationen

- **Enterprise Network Virtualization Design Guides**

  Network Virtualization--Access Control Design Guide

  http://www.cisco.com/en/US/docs/solutions/Enterprise/Network_Virtualization/AccContr.html

  Network Virtualization--Guest and Partner Access Deployment Guide

  http://www.cisco.com/en/US/docs/solutions/Enterprise/Network_Virtualization/GuestAcc.html

  Network Virtualization--Path Isolation Design Guide

  http://www.cisco.com/en/US/docs/solutions/Enterprise/Network_Virtualization/PathIsol.html

  Network Virtualization--Services Edge Design Guide

  http://www.cisco.com/en/US/docs/solutions/Enterprise/Network_Virtualization/ServEdge.html