

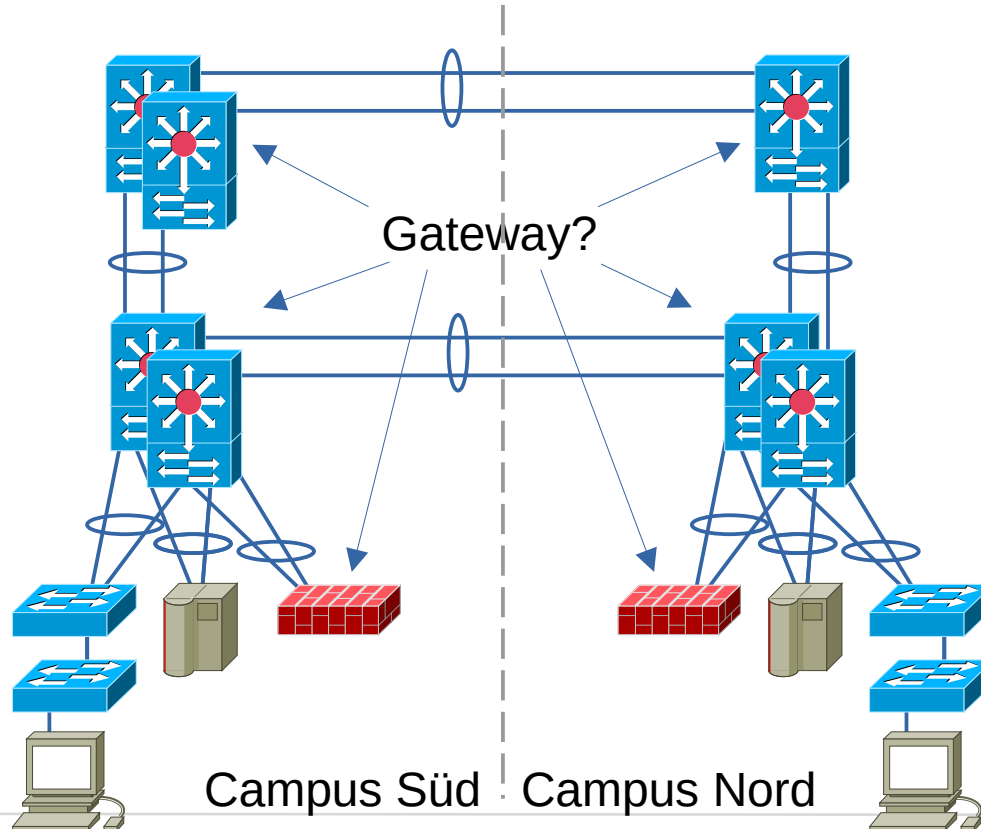
EVPN am KIT



Inhalt

- Bisschen was zu EVPN und warum das KIT sich dafür entschieden hat
- KIT Netzdesign
- Cases & Lessons learned

Motivation: historischer Netzaufbau



- Historisch gewachsene Struktur
- Layer 2 überall, manuelles Legen von VLANs
- Fehleranfälligkeit / große Fehler-Domäne
- Lange Ausfallzeiten
- Gateway unklar
- Shared Control-Plane auf zentralen Komponenten

Neue Lösung gesucht / Anforderung

- Offener Standard
- Unabhängige Control-Plane auf zentralen Komponenten
- Redundanz auf Layer 2 und Layer 3
- Kleinere Fehlerdomänen ermöglichen
- Möglichkeit zur sanften Migration von Layer 2 zentriertem Aufbau zur gerouteten Architektur
- Klare Position des Gateways
- Unterstützung für mehr als 4094 Broadcast-Domains
- Automatische Wegsuche für Broadcast-Domain

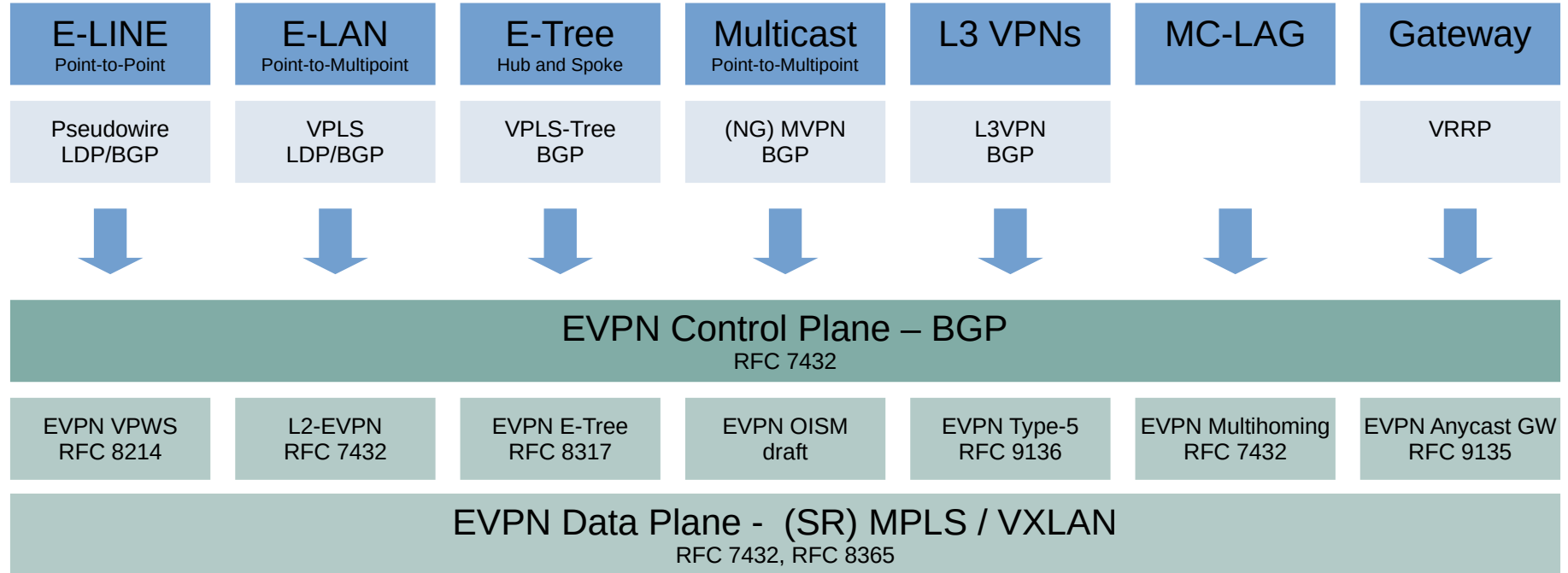
Lösungsansätze

- ~~Proprietäre Lösung~~: kein offener Standard
- OpenFlow: zentrale Controller
- ~~VPLS, TRILL, Shortest Path Bridging~~: Nur Layer 2
- ~~L3VPN~~: nur L3
- EVPN: offener Standard, „kann alles“

EVPN!

- IETF Standard – offen und herstellerübergreifend
- Robustheit: verteilte Control Plane, eingebaute Redundanz-Mechanismen für L2 und L3
- Flexibel einsetzbar: ISP-, Campus- / Enterprise- und DC-Netzwerk
- Reiches Featureset: L2VPN, Loop-Protection, MC-LAG, Anycast-Gateway, ARP-/NDP-Suppression, L3VPN, ...

EVPN – One Protocol To Rule Them All



Hardware KITcore

Spine



Cisco Nexus 9336C-FX2

36 x 40/100G QSFP28

Leaf



Cisco Nexus 93240YC-FX2

48 x 1/10/25G SFP18
12 x 40/100G QSFP28

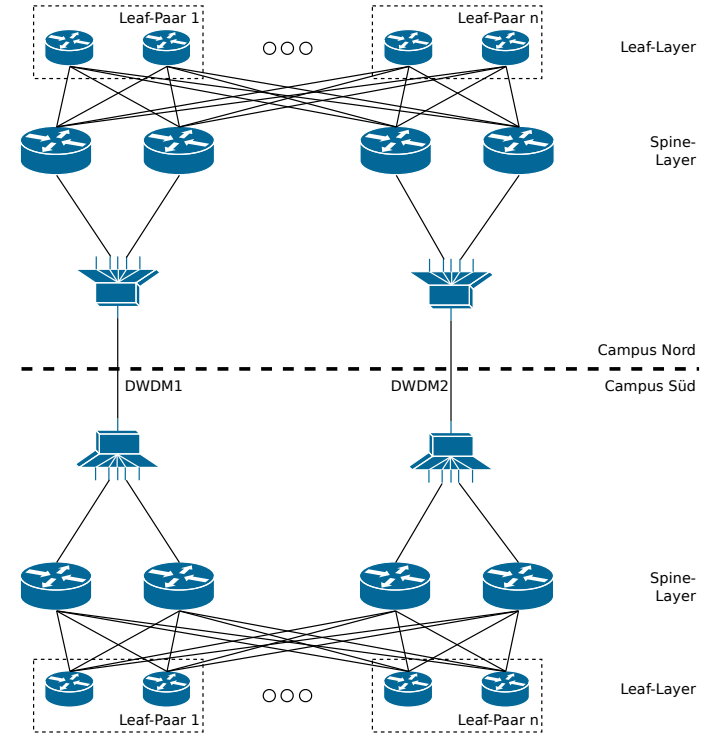
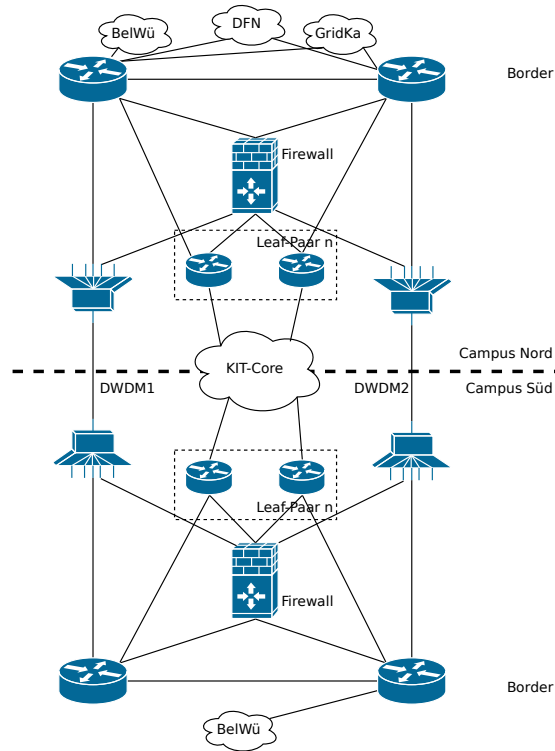
Service Leaf



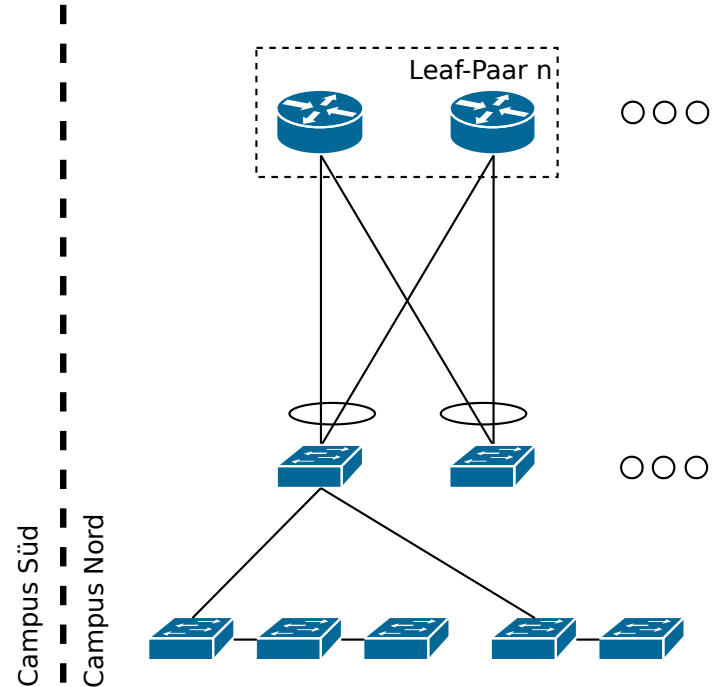
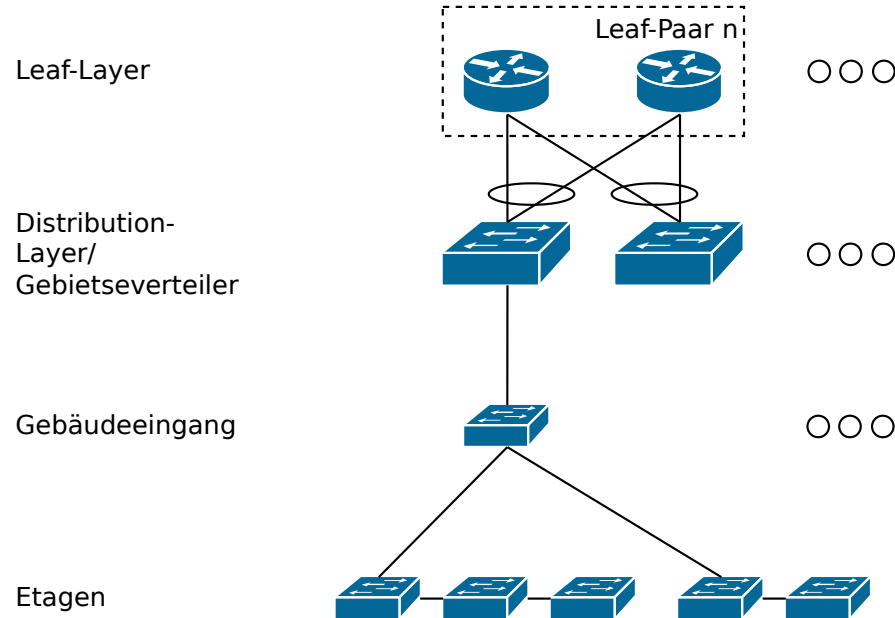
Cisco Nexus 93180YC-FX3

48 x 1/10/25G SFP18
6 x 40/100G QSFP28

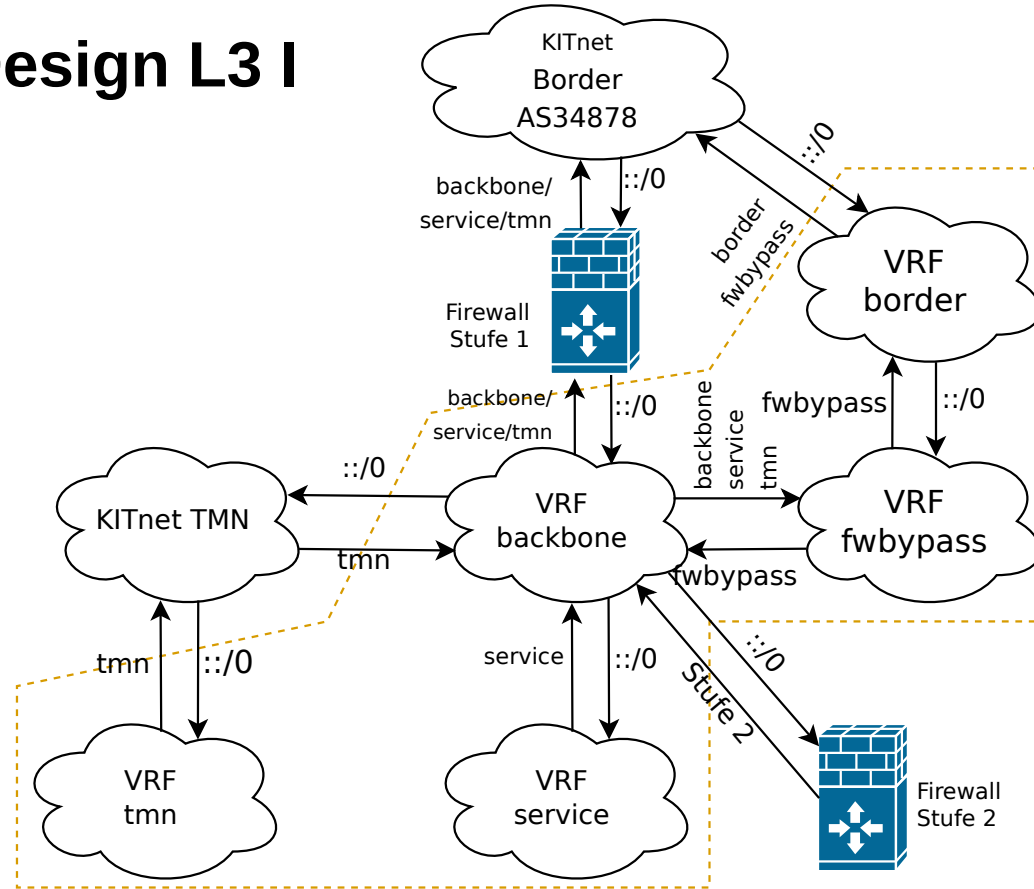
Netzwerk-Design L1 I



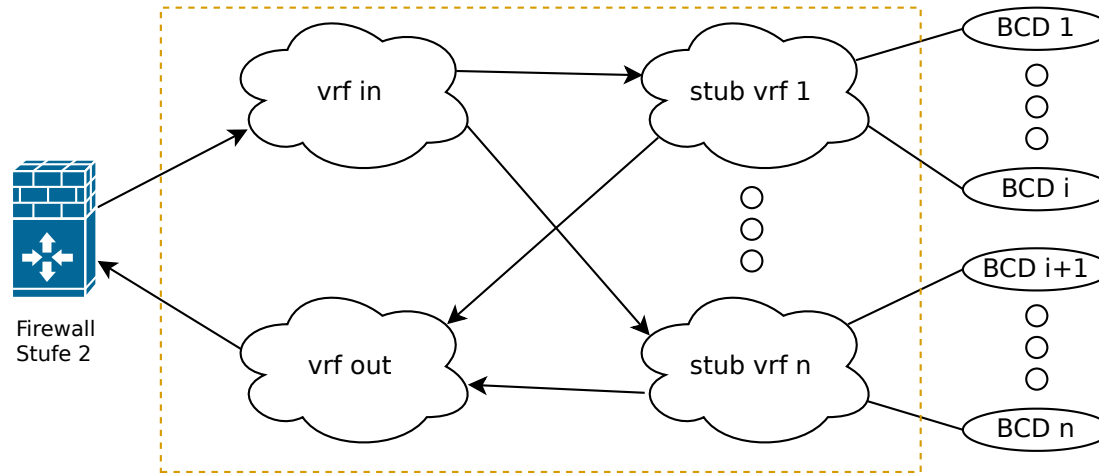
Netzwerk Design L1 II



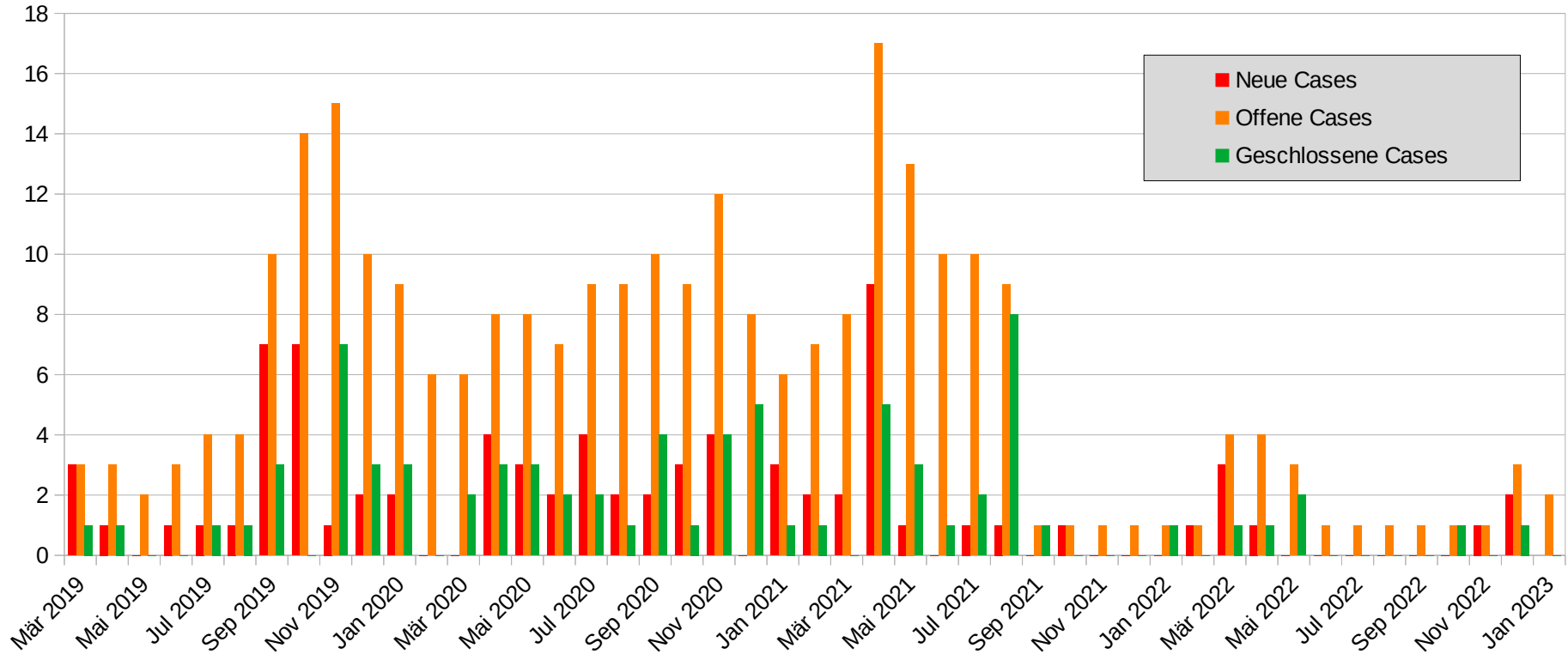
Netzwerk Design L3 I



Netzwerk Design L3 II



Cases I



Cases II

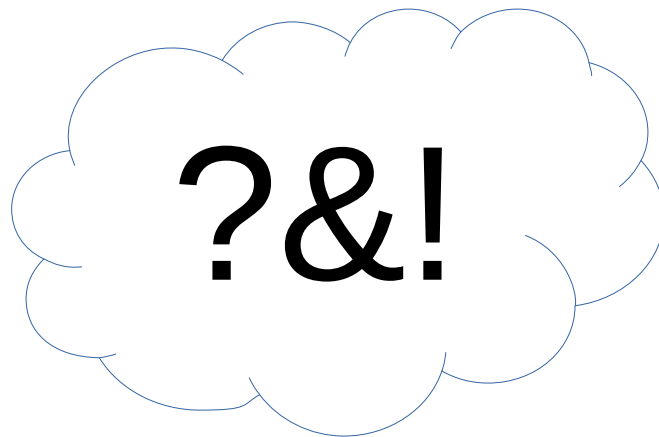
- 78 Cases in den letzten 4 Jahren
 - 3 PEBKAC
 - 5 RMA: 2 defekte ASICs, 3 defekte Lüfter
 - 12 Cases zur Doku (Unklarheit, Korrekturen)
 - 13 Cases zu EVPN
 - 33 Cases mit Netzwerkstörungen
 - 17 Bugs in CLI / ASCII-Config
 - 64 Bug IDs, 7 Hotfixes

EVPN war die richtige
Entscheidung, aber
Qualitätsproblem bei Cisco!

Best of Cases

- CSCvr80704: Configure replace fails when 'switchport trunk allowed vlan' list is too large
- CSCvs15705: UDP fragmented packets punted to CPU as incorrectly parsed as BFDC v4 PACKET IETF
- CSCvt75268: IPv6 routes use wrong VLAN as next hop
- CSCvv04821: Nexus 9000 Series Switches in standalone NX-OS mode Egress RACL Bypass Vulnerability
- CSCvv26464: N9k - IGMP report destined to 224.0.0.x sent back on same port it is received on
- CSCvv64248: N9k- DHCP Relay DHCP OFFER broadcast loop/bounce in EVPN Fabric

Fragen & Antworten



Benedikt Neuffer

mail: benedikt.neuffer@kit.edu

matrix: [@iv4011:kit.edu](https://matrix.to/#/@iv4011:kit.edu)