

82. DFN-Betriebstagung – Forum „Wissenschaftsnetz“

Erneuerung des Clusteranschluss der Uni Würzburg

Markus Krieger
Rechenzentrum Uni Würzburg
markus.krieger@uni-wuerzburg.de

Der Clusteranschluss der Uni Würzburg (vor dem Umbau)

- 5 Clusterteilnehmer, in Summe vertraglich > 10Gbit/s
- Doppelte Teilnehmeranbindung (TNA), je 2x10GE Port-Channel nach Frankfurt und Erlangen
- „Wingate-alt“: 2 x Cisco Cat6500 als VSS-Pärchen
 - Cluster als VRF „XWIN“ abgebildet
 - Uplinks zum DFN als „routed ports“
 - IPv4, IPv6 jeweils eine gemeinsame BGP-Session für alle Teilnehmer
 - Statisches Routing zu den TN-Firewalls
 - TN-Firewalls sind per Port-Channel am „wingate-alt“ angebunden
 - Traffic zwischen den TN wird innerhalb des Clusters abgehandelt (kein Umweg über DFN)
- Urspr. angedachte Ablösung durch Cat6800 durch 100GE-Anforderung hinfällig → neue Hardware will ausgesucht werden...

Anforderungen an neues „wingate“

- VSS / Stackwise virtual
 - keine Änderung an den Anbindungen der TN-FWs bzgl Port-Channels, Routing
- Netflow „unsampled“ / „1:1 Sampling“ für realistische Bandbreite
- „hinreichende Anzahl von Interfaces (10 / 100GE)
- Pro Cluster-TN eigenes VRF + 2 Uplink-VLANs zum DFN
- Route Leaking zwischen VRFs für lokalen Short-Cut zwischen den TN
- Über Rahmenvertrag bestellbar

Kandidaten

- Cisco 9400
- Cisco NCS 57C3 (+ nachgelagerte Switches für Portanzahl)

Projektablauf (Beeinträchtigt durch Tagesgeschäft, Urlaubszeit, ...)

- **07.2023+:** DFN fragt verstärkt freundlich bzgl. 100GE & TN-VLANs nach
 - Initial Ablösung mit Cico 9400 angedacht
 - Aber: **Kein** Route leaking von **statischen, lokal konfigurierten** Routen zwischen VRFs („it's a feature“, „by design“)
- **11.2023:** Vorab Umstellung der TNAs von Routed Ports auf SVIs
 - Pro Cluster-TN das künftige VRF + 2 VLANs zum DFN ausgewürfelt
 - Für VRF XWIN festgelegte VLANs auf TNAs konfiguriert
- **Q1+Q2.2024:** Lösungssuche und POC mit Cisco
 - Cisco NCS 57C3 würde tun, aber ... Lizenzkosten nicht finanzierbar
 - Cisco 9400 kann via BGP dann doch statische Routen leaken → wingate-neu
- **05.2024:** Einschleifen von wingate-neu als „100GE-Medienkonverter“
- **06-09.2024:** Vorbereiten & Testen der VRF-Konfiguration auf wingate-neu
- **10.2024:** Umzug der TN in eigene VRFs / Uplink-VLANs. Parallel Umhängen der physischen Anbindungen wingate-alt → wingate-neu
- **14.10.2024:** rituelle Abschaltung wingate-alt nach über 15 Jahren Betrieb

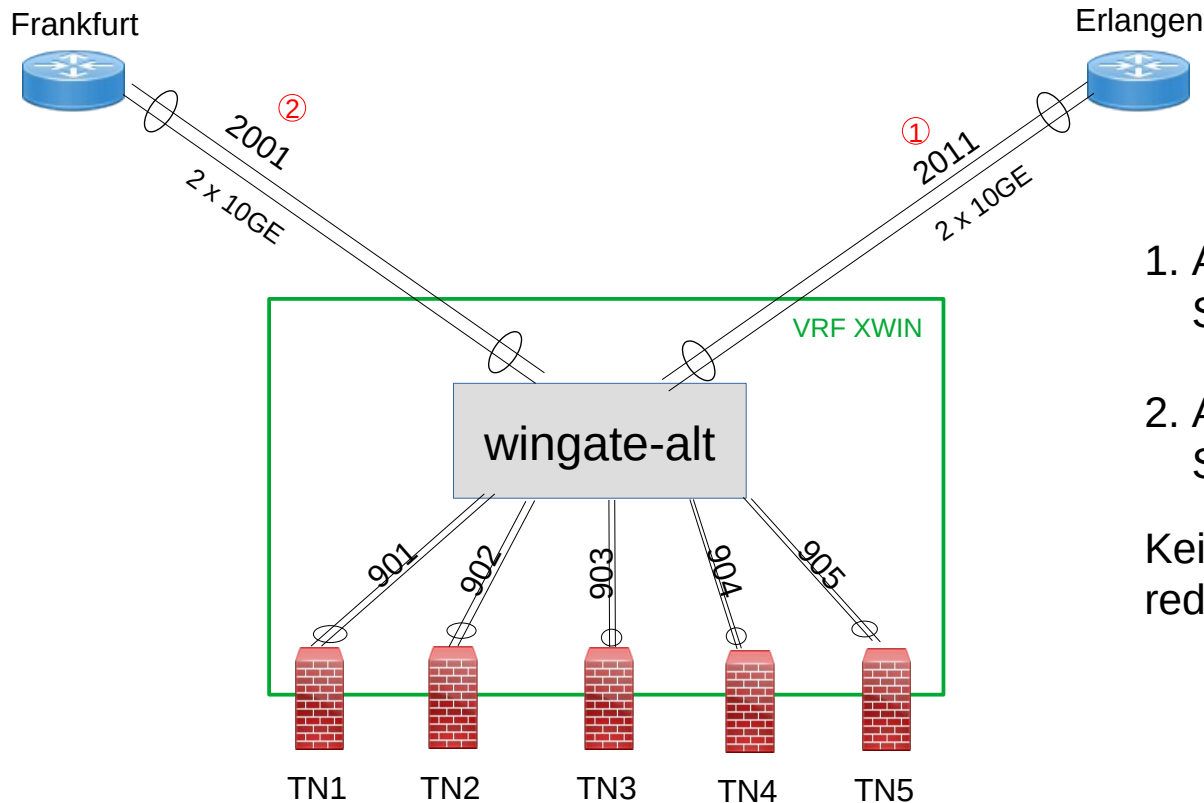
Zusammenfassend

- Vielen Dank an DFN und Cisco für die super Unterstützung!
- Schrittweise Umstellung erleichtert Vorbereitung und Fehlersuche
 - Man kann verschiedene Schritte parallel angehen. Das macht im Fehlerfall das Debugging nicht einfacher.
- Mit doppelter Teilnehmeranbindung und BGP konnten alle Arbeiten zwischen Cluster und DFN ohne Unterbrechungen für die Nutzer durchgeführt werden.
- Nur kurze „Ruckler“ (unter einer Minute)
 - Umhängen der physischen Firewallanbindungen von wingate-alt auf wingate-neu
 - Umhängen der Teilnehmeranbindung in eigenes Teilnehmer-VRF

Implizites Vorgehen auf den folgenden Folien

- TNAs werden per Metrik als Active / Standby genutzt.
- **Arbeiten, welche die TNAs oder die BGP-Sessions betreffen, nur in Abstimmung mit dem DFN**
- Initial geht sämtlicher Nutzertraffic über die Anbindung Frankfurt
 - Arbeiten an der Anbindung nach Erlangen sind ohne Auswirkung auf Nutzer / Cluster-TN
- Schwenk per Metrik auf die Anbindung Erlangen
 - Arbeiten an der Anbindung nach Frankfurt sind ohne Auswirkung auf Nutzer / Cluster-TN
- Abschliessend wieder Schwenk per Metrik auf Anbindung Frankfurt

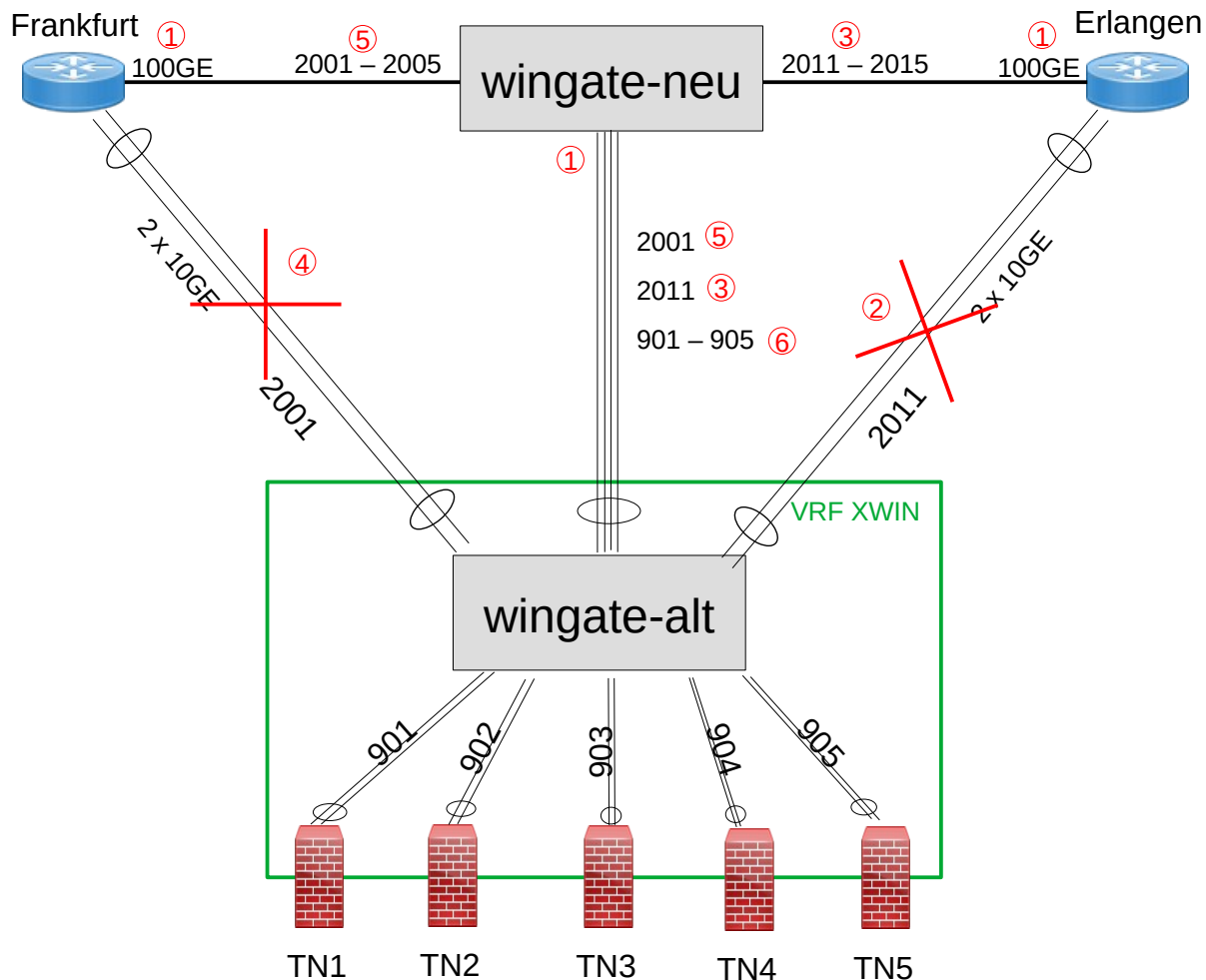
Ausgangspunkt & Umstellung der routed ports



1. Anbindung nach Erlangen auf SVI / VLAN 2011 umstellen.
2. Anbindung nach Frankfurt auf SVI / VLAN 2001 umstellen

Keine Nebenwirkungen, da redundante TNAs & BGP

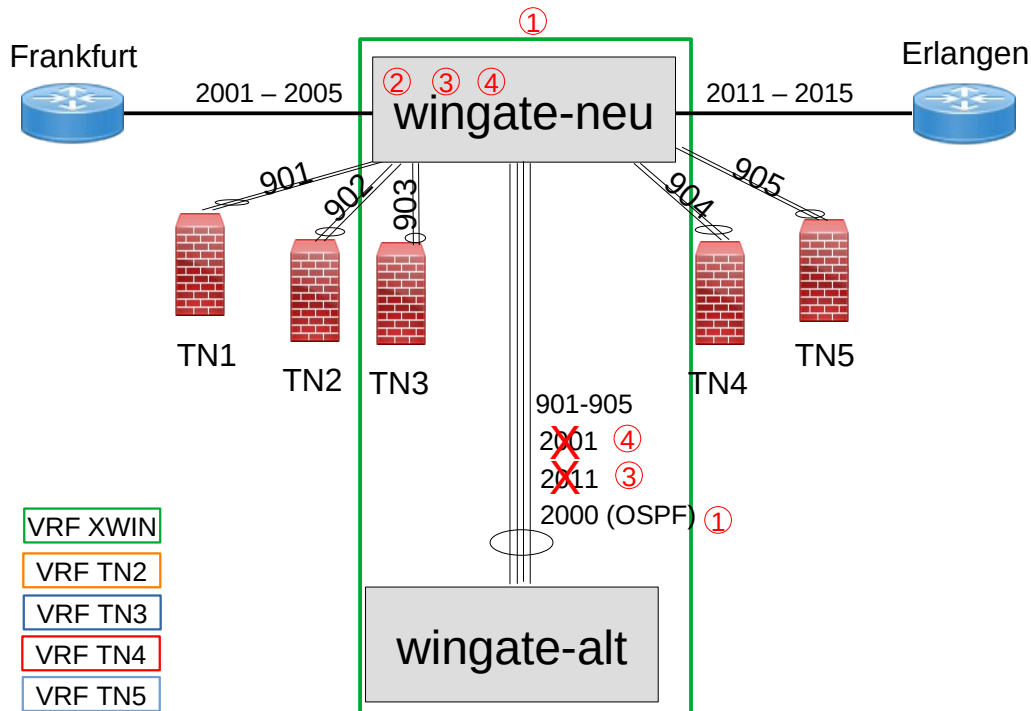
100GE-Umstellung & Umzug der TN-FW-Anbindungen vorbereiten



1. Strecken schalten & testen
2. Alte Anbindung Erlangen deaktivieren
3. VLAN 2011 auf neue Erlangen-Anbindung legen
4. Alte Anbindung Frankfurt deaktivieren
5. VLAN 2001 auf neue Frankfurt-Anbindung legen
6. FW-VLANs auf Querverbindung (FWs physisch an wingate-neu anbinden)

**wingate-neu rein Layer2.
BGP und internes Routing
zu TN-FWs noch durch
wingate-alt.**

BGP „VRF XWIN“ auf wingate-neu umziehen

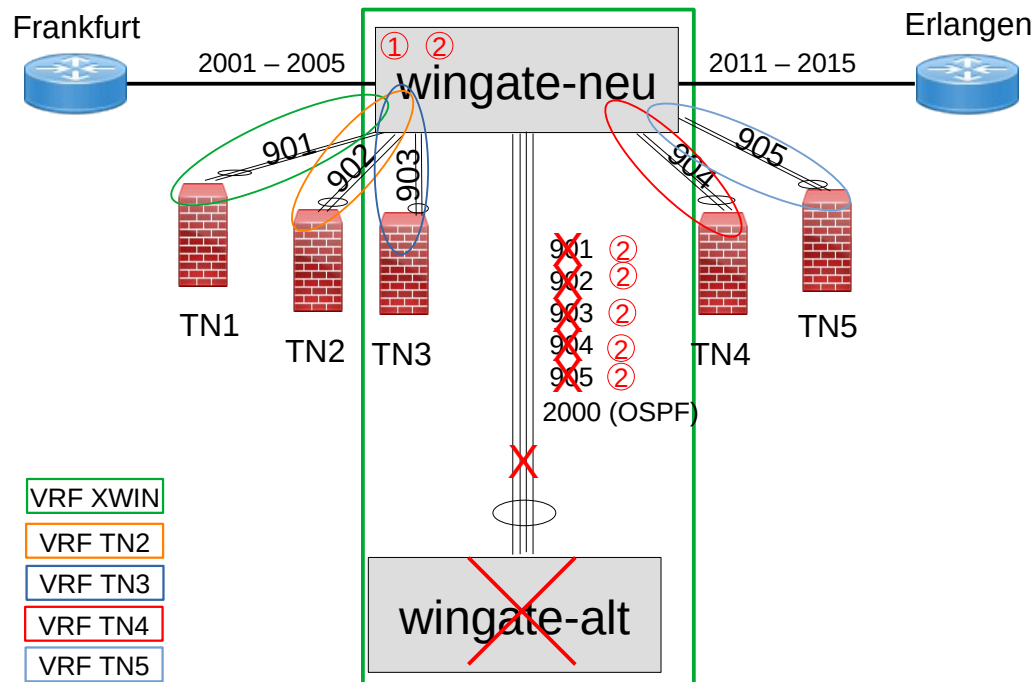


1. wingate-neu in VRF XWIN.
OSPF wingate-alt ↔ wingate-neu
via VLAN 2000
2. Auf wingate-neu BGP-Session und
„int vl2001“ + „int vl2011“ in
shutdown vorbereiten
3. Auf wingate-alt „int vl2011 shut“.
Auf wingate-neu „int vl2011 no shut“
BGP VRF XWIN nach Erlangen neu
4. Auf wingate-alt „int vl2001 shut“.
Auf wingate-neu „int vl2001 no shut“
BGP VRF XWIN nach Frankfurt neu

BGP für VRF XWIN nur noch auf
wingate-neu.

**Routing für alle weiterhin über VRF
XWIN**

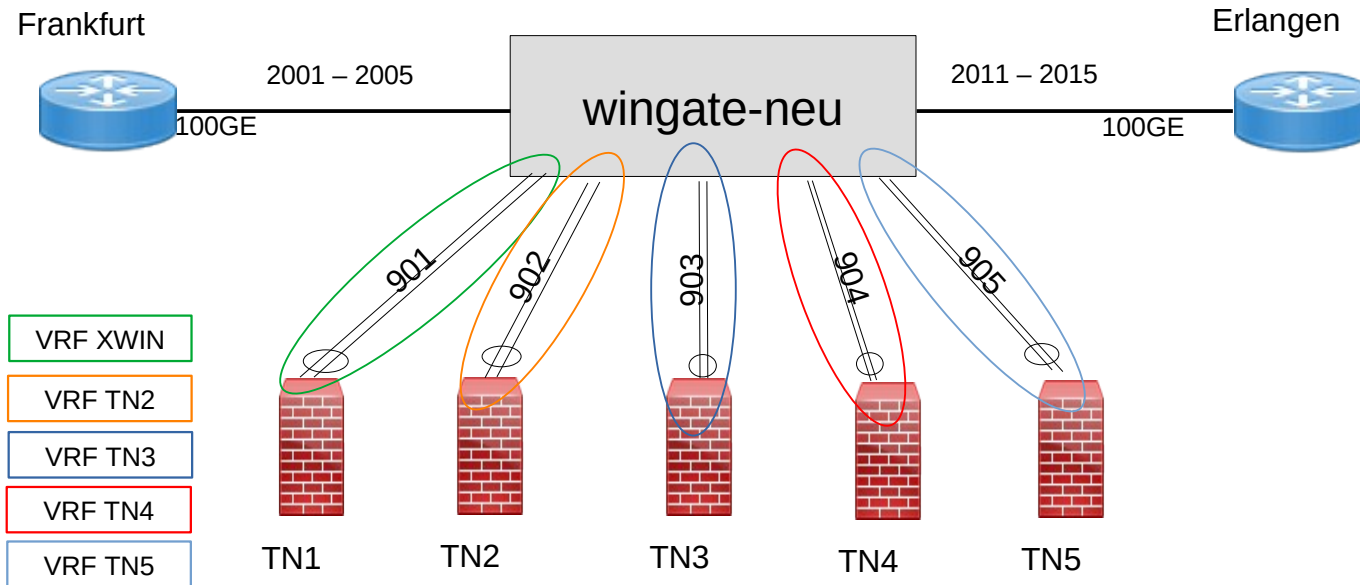
Teilnehmer-Firewalls in dedizierte VRFs stecken



1. TNx: VRF XWIN-TNx & BGP via VLANs 200x / 201x vorbereiten und BGP testen. Statische Routen etc. auf wingate-neu vorbereiten
2. In Absprache mit TNx:
„no int vlan90x“ um TNx aus VRF XWIN zu nehmen und „int vlan90x“ auf wingate-neu im passenden VRF XWIN-TNx neu anlegen
3. Testen!
4. Repeat: Für alle TN

Abschliessend wingate-alt abschalten und Konfiguration auf wingate-neu bereinigen

Grande Finale



- 100GE TNAs
- Pro TN separate BGP-Session & Uplink-VLANs
- Bei passender Config: Cluster-interner Short-Cut