Cisco DNA Center – Admin Spielzeug oder das neue Normal?

Telekom Solution X
27.04.2023 – Frankfurt am Main

Agenda

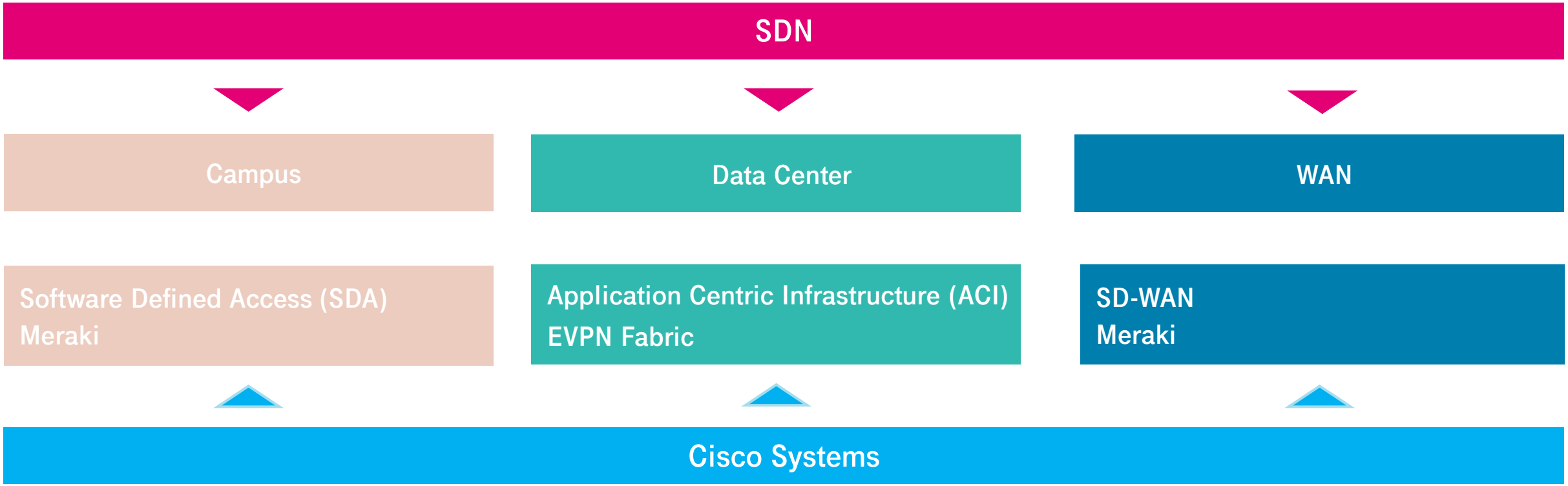
01 Cisco SDA im Kurzüberblick

02 Umsetzung, was nun?

03 Was nehmen wir mit?

01
Cisco SDA im Kurzüberblick

SDN - Auf Cisco Lösungen übertragen



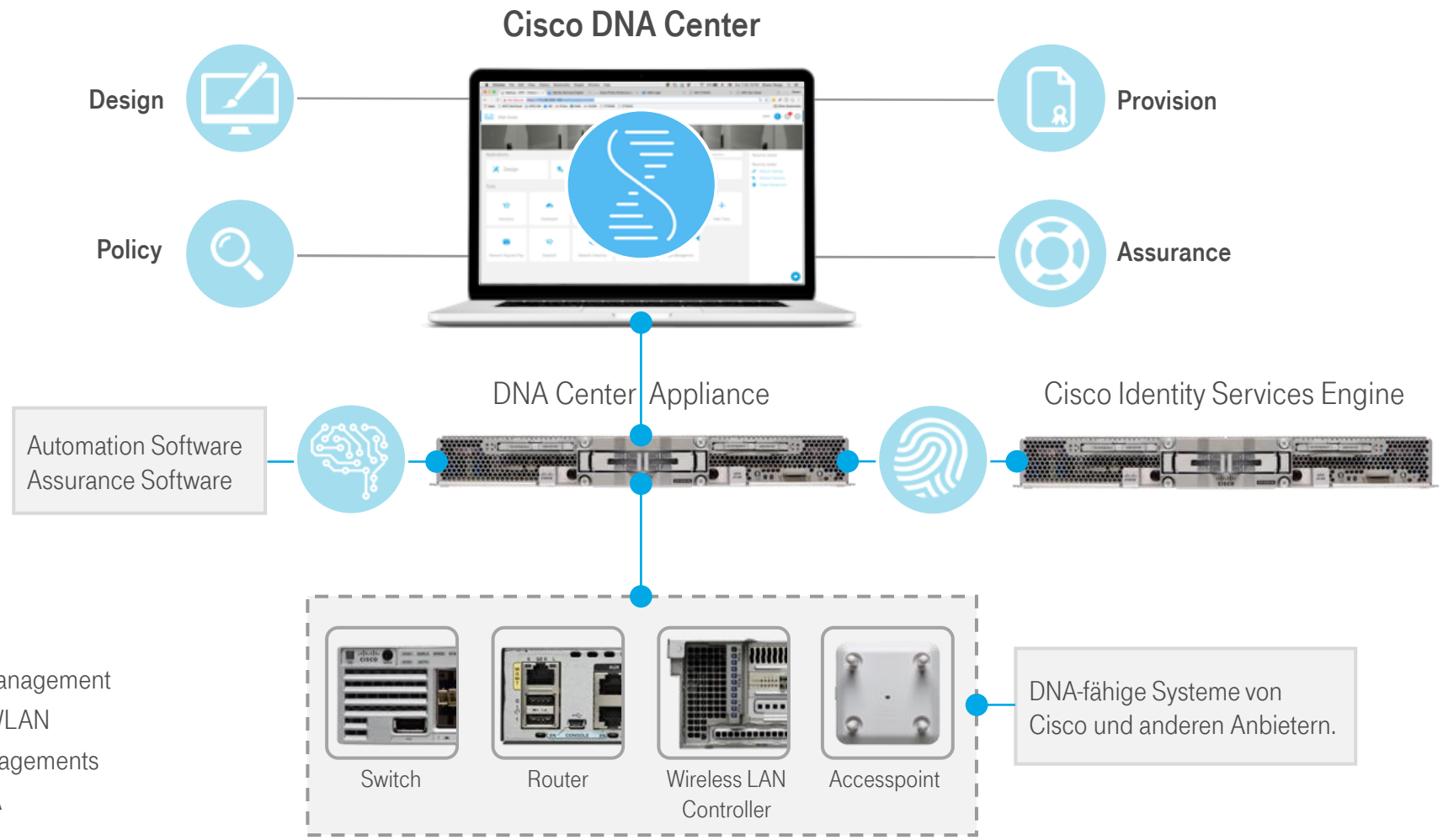
Cisco Software Defined Access - SDA

- **Ist eine Interpretation/Umsetzung von Cisco für Software Defined Networking.**
- **Es ist eine von mehreren SDN-Umsetzungen aus dem Cisco Portfolio.**
- **Es ist eine Hersteller proprietäre Lösung, die auf Standards aufbaut.**
- **Es ist eine Lösung für den Campus.**
- **Es ist eine Lösung für den “Wired“- und “Wireless“-Access.**

Cisco SDA – ein Überblick

VORTEILE

- Automatisierung: Schnellere Reaktionen auf Netzwerkanforderungen
- Schnellere und sichere Einbindung neuer Segmente
- Geringere Kosten für Implementierung und Migration
- Weniger Fehler durch menschliches Versagen
- Massive Reduzierung der Rolloutzeiten
- Mehr Schutz durch zentrale Definition von Richtlinien
- Risiko Reduzierung durch Echtzeit-Analysen auf Netzwerk, Endgeräte und Applikationen
- Automatisierter Hinweis auf Fehlerursachen und Vorschläge zur Fehlerbehebung
- Brownfield Support



GLOSSAR

Software Defined Networking (SDN): Netzwerkzentrisches Management

Software Defined Access (SDA): Softwaregesteuertes LAN/WLAN

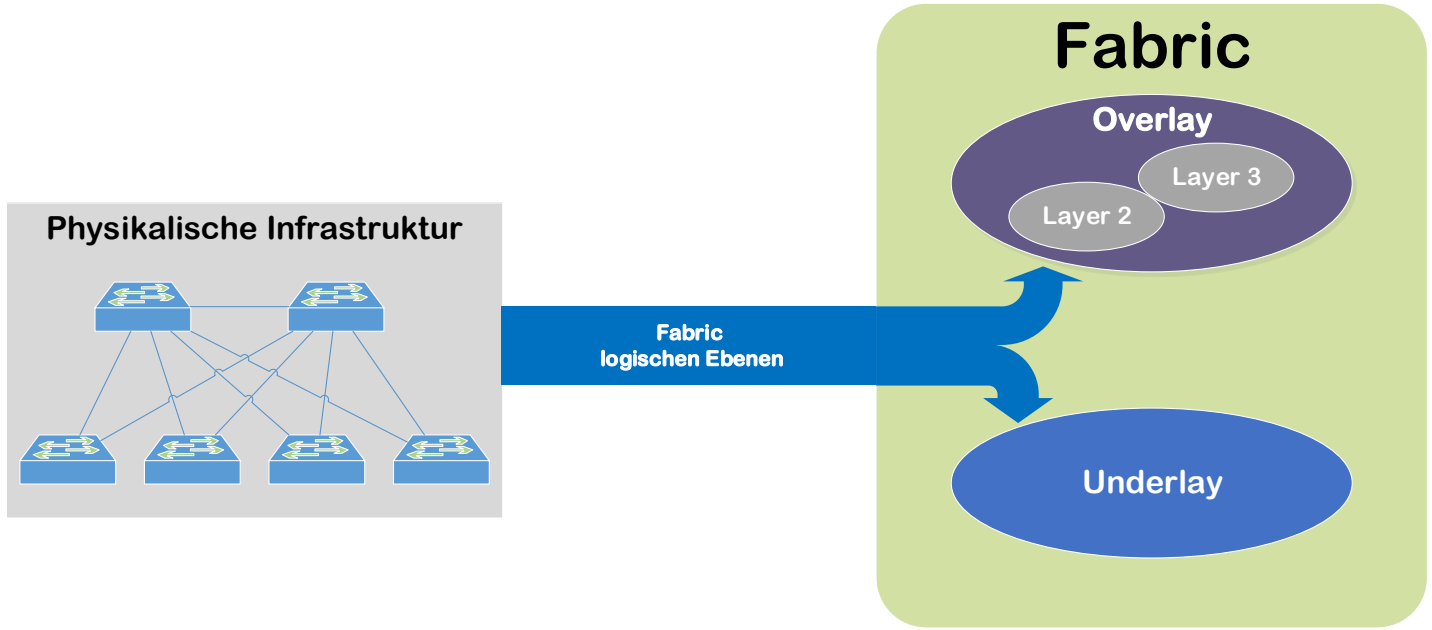
Network Intuitiv: Cisco Begriff eines intuitiven Netzwerkmanagements

Cisco DNA/Center: Cisco eigenes Produkt für SDN und SDA

Cisco SDA Aufbau

Bestandteile des Cisco SDA

- **Fabric, Infrastrukturhardware aufgeteilt in das**
  - **Underlay**
    physikalischen Infrastruktur mit Layer 3
    für den Transport des Overlays
  - **Overlay**
    Logische/virtuelle Netze auf Layer 2 und Layer 3
    für die Kommunikation der angeschlossen Clients



- **DNA Center**
  zentraler Controller für Fabric

- **ISE**
  Authorisierungsinstanz für den Access

DNA Center – Design, Provisioning, Policy, Assurance

DESIGN

DNA Center bietet umfangreiche Funktionen und Hilfen zum Design von Netzwerk-Segmenten.

PROVISIONING

Die Provisionierung von Netzwerk-Geräten oder vollständiger Netzwerk-Abschnitte wird stark vereinfacht durch eine automatisierte Verteilung von Software und Konfiguration.

POLICY

Macht das Ausbringen von Regeln sehr einfach. Segmentierung auf Basis von Benutzergruppen ist ebenso möglich, wie die Nutzung von Identitäts-Informationen der Identity Services Engine (ISE).

ASSURANCE

Um die korrekte Funktionsweise der Netzwerk-Infrastruktur zu gewährleisten, werden umfangreiche Messdaten aus dem Netzwerk konsolidiert, sichtbar gemacht und daraus der „Gesundheitsstatus“ berechnet.

DNA Center – Cisco ISE, DNA Assurance

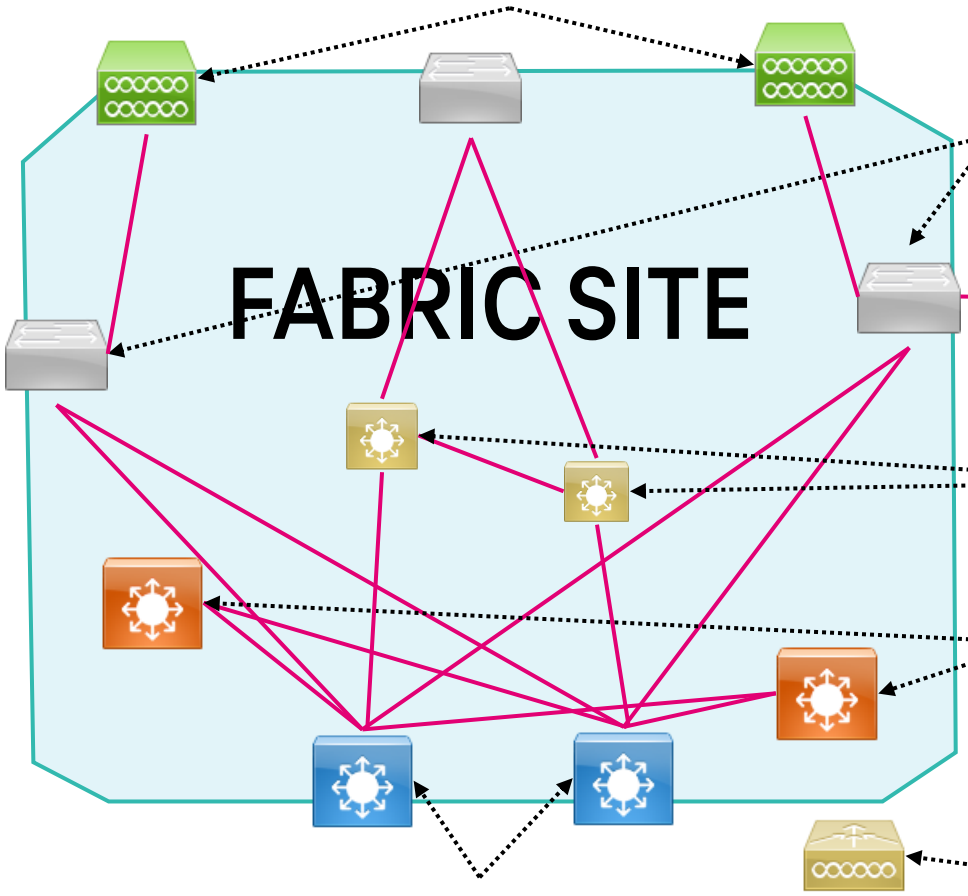
CISCO IDENTITY SERVICES ENGINE (ISE)

Für Identifizierung/Authentifizierung: Regelt den Zugriff von Benutzern und ihren Endgeräten auf das Netzwerk. DNA Center nutzt die ISE-Informationen, z. B. für Regeln zur Segmentierung von Datenverkehr.

DNA ASSURANCE

Sammelt Daten zur Analyse des Netzwerks und bereitet diese auf: Auslastung, Benutzeraufkommen, korrekte Funktionsweise der Systeme. Damit sind sichere Entscheidungen möglich, z. B. Maßnahmen zur Optimierung.

SDA Fabric: Aufbau



Fabric Access Point
Aufnahme und Anbindung von Clients

Fabric Edge Node
Aufnahme und Anbindung von Clients

Extended Node
L2 Erweiterung des Edge Nodes

Intermediate Node
Distribution im Underlay

Control Plane Nodes
Steuerung der Fabric

Fabric Wireless Controller
Steuerung der WLAN AP

Fabric Border Node
Ein- und Ausgang der Fabric

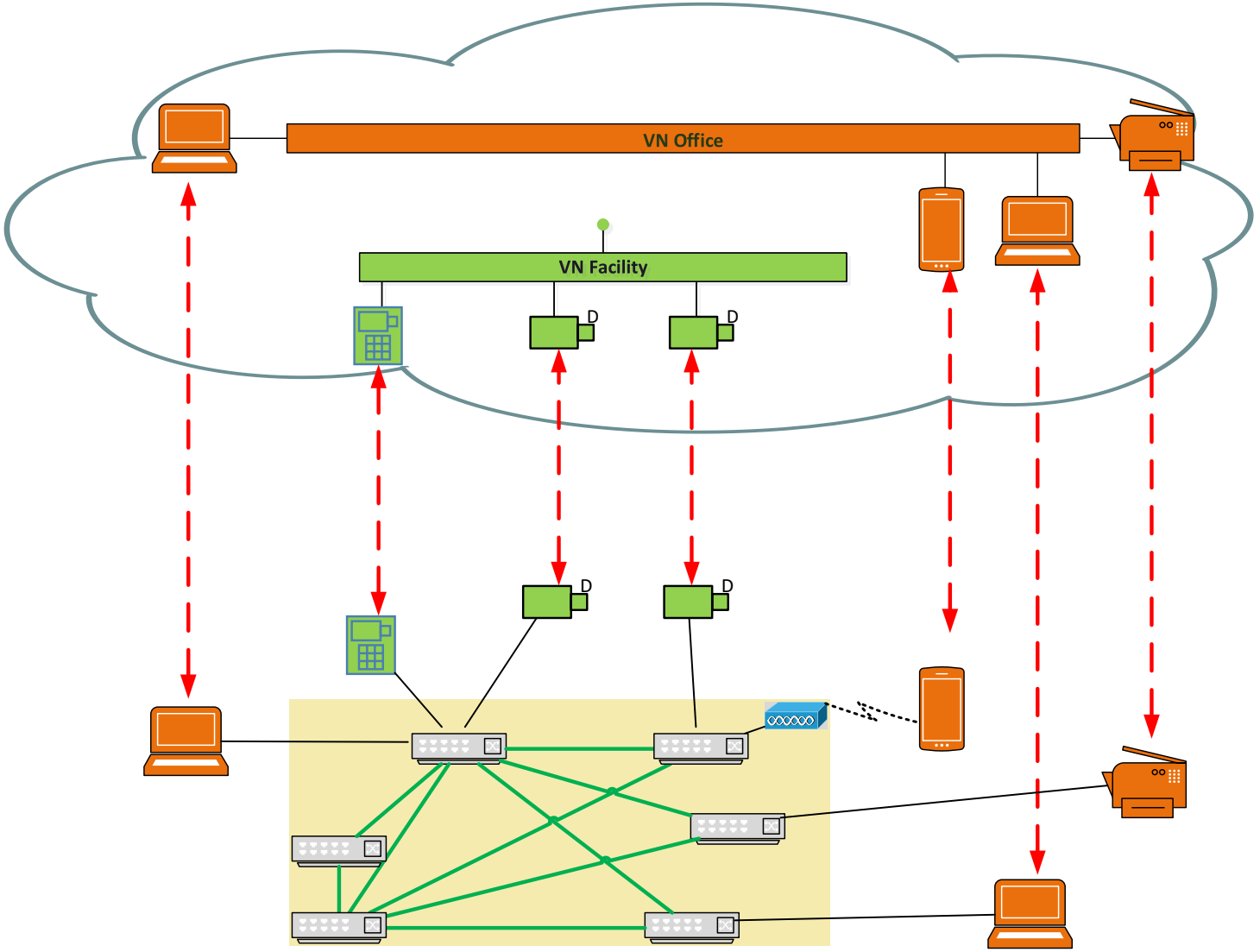
SDA Fabric: Overlay - Underlay

Overlay

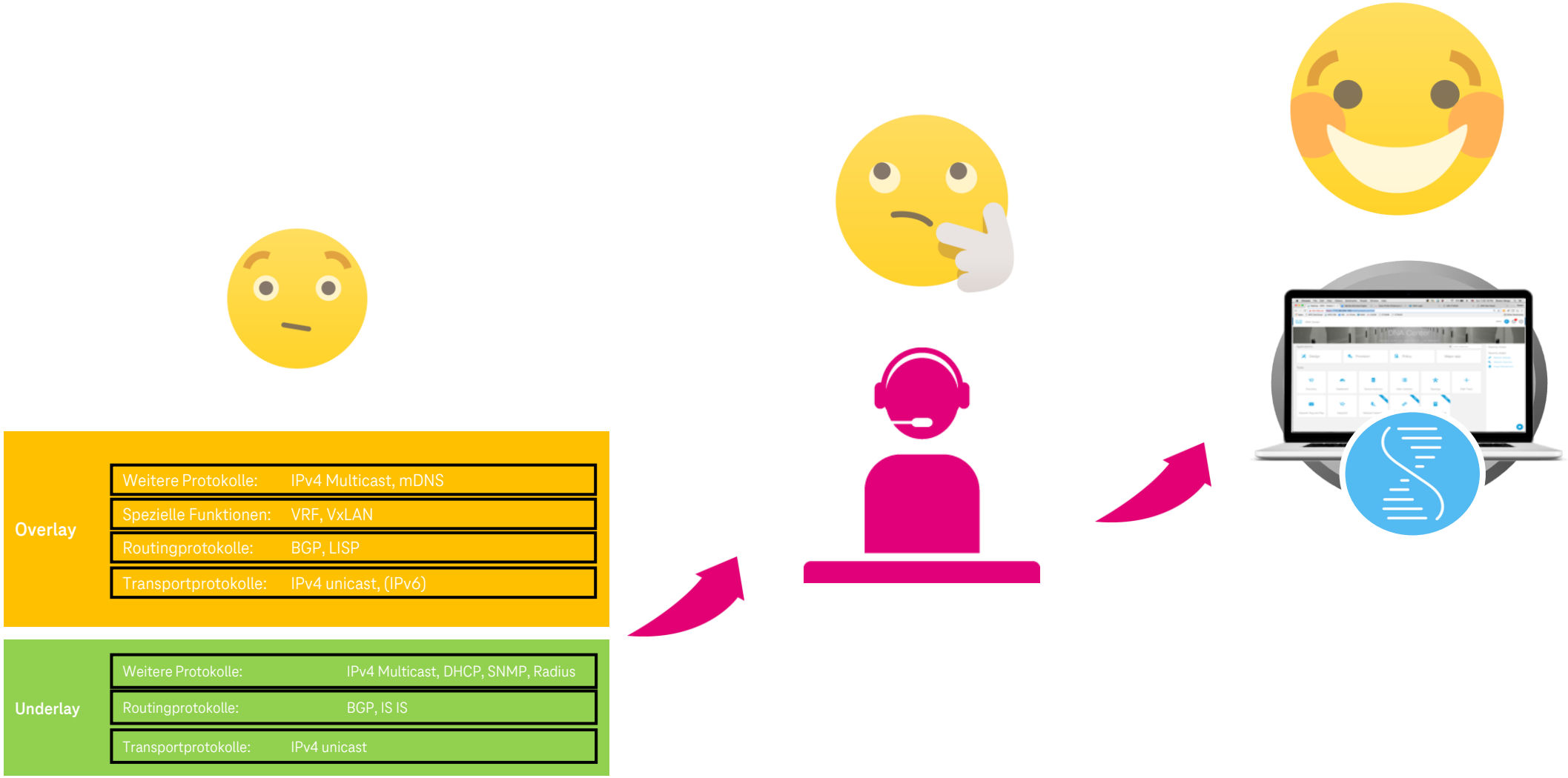
mit mehreren Virtual Network (VN)

Underlay

Transport des Overlay



SDA Fabric: Protokolle, wir helfen



Segmentierung – Was ist das?

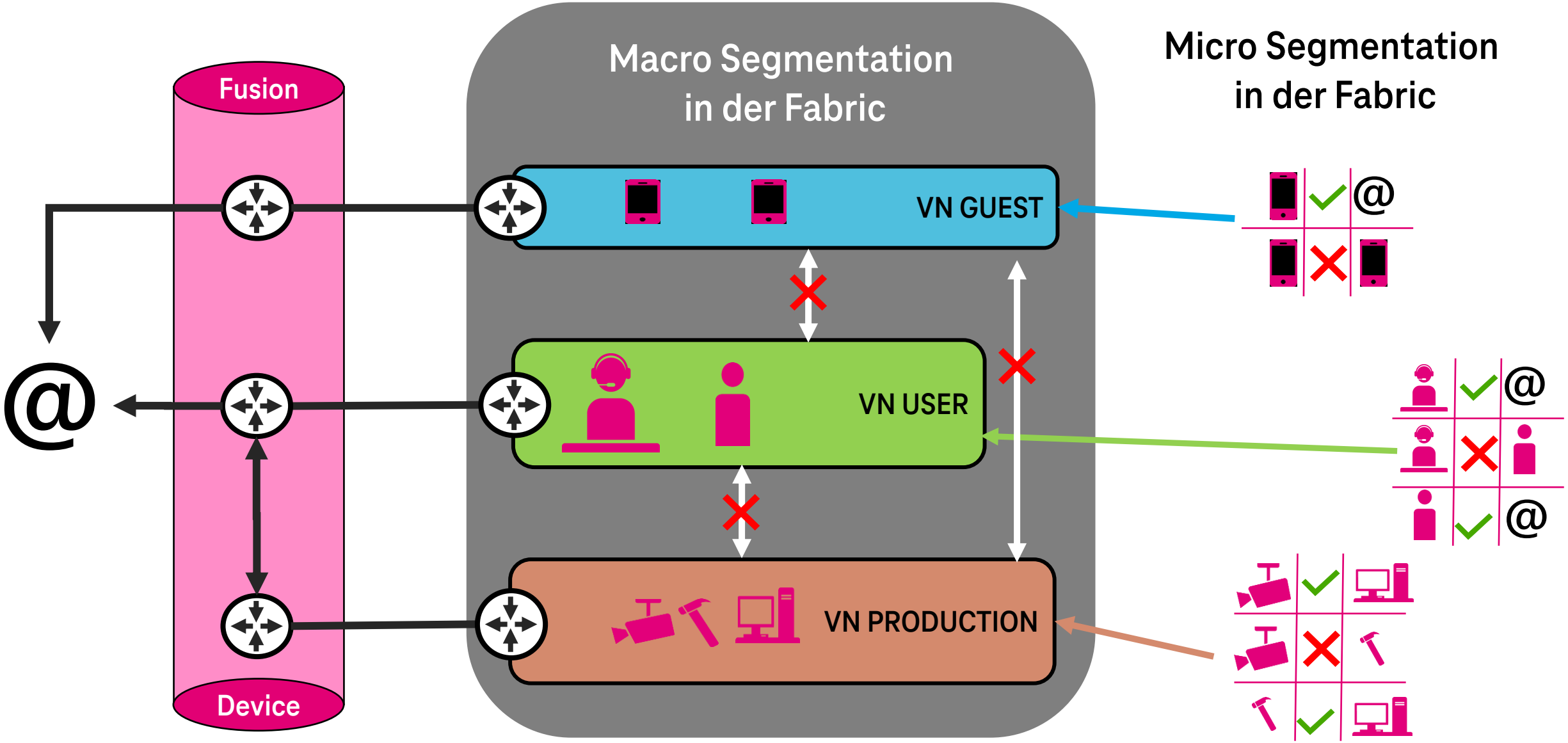
Virtual Network (VN) (Macro Segmentation):

- Separation im Layer 3 und Layer 2 innerhalb einer “fabric site“.
- Bildung eines eigenständigen Routing- und Switching-table je Instanz
- Die in einem VN zugeordneten IP-Netze können miteinander kommunizieren und werden verbreitet.
- VN können innerhalb einer “fabric site“ nicht miteinander kommunizieren.
- Realisiert wird es mittels VRF (Virtual Routing and Forwarding)

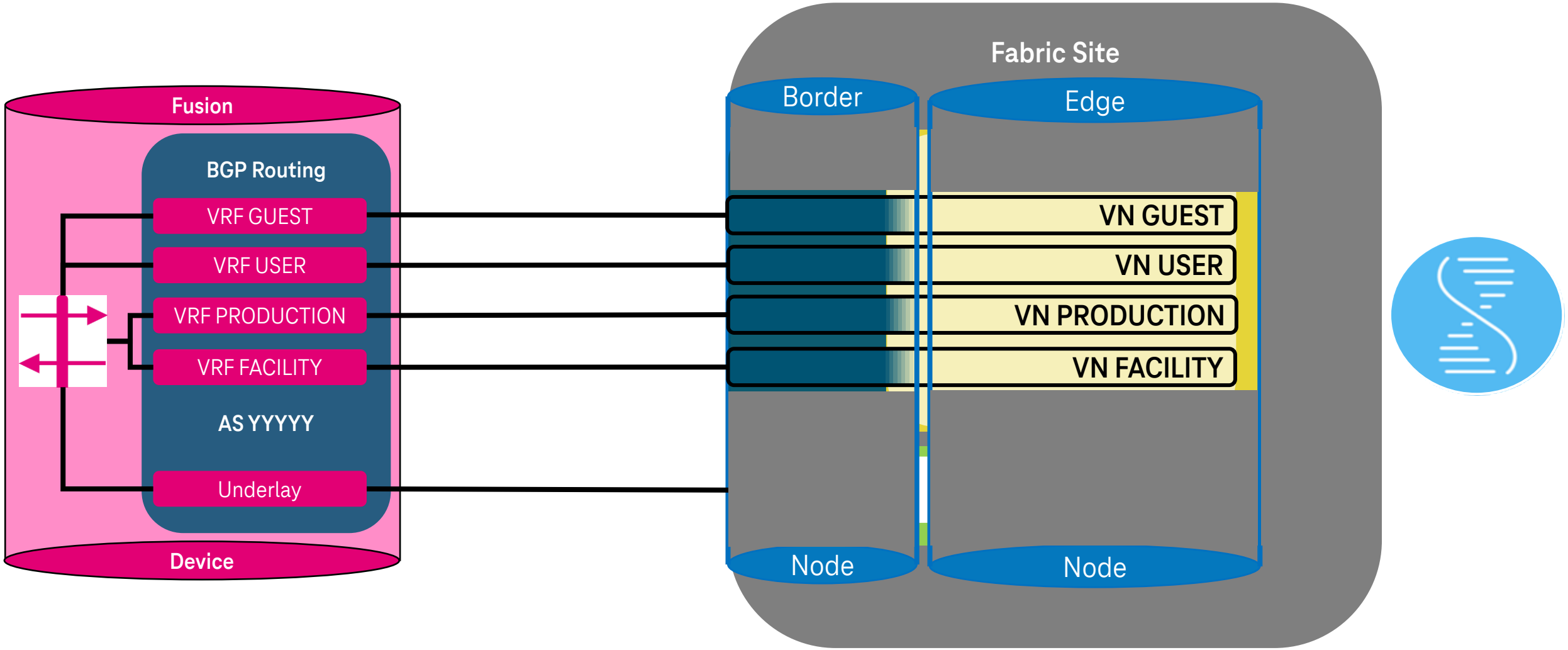
Security Groups (Micro Segmentation):

- Mittel zur Bildung von Gruppenrichtlinien für Endgeräte und Nutzer
- Security Groups werden mittel Secure Group Tags (SGT) dem Endpoint zugewiesen
- Edge- und Border-Nodes verwenden anhand der SGT lokale Filterlisten (SGACL) für den Endpoint Access.
- Es wird die Client Kommunikation eingeschränkt

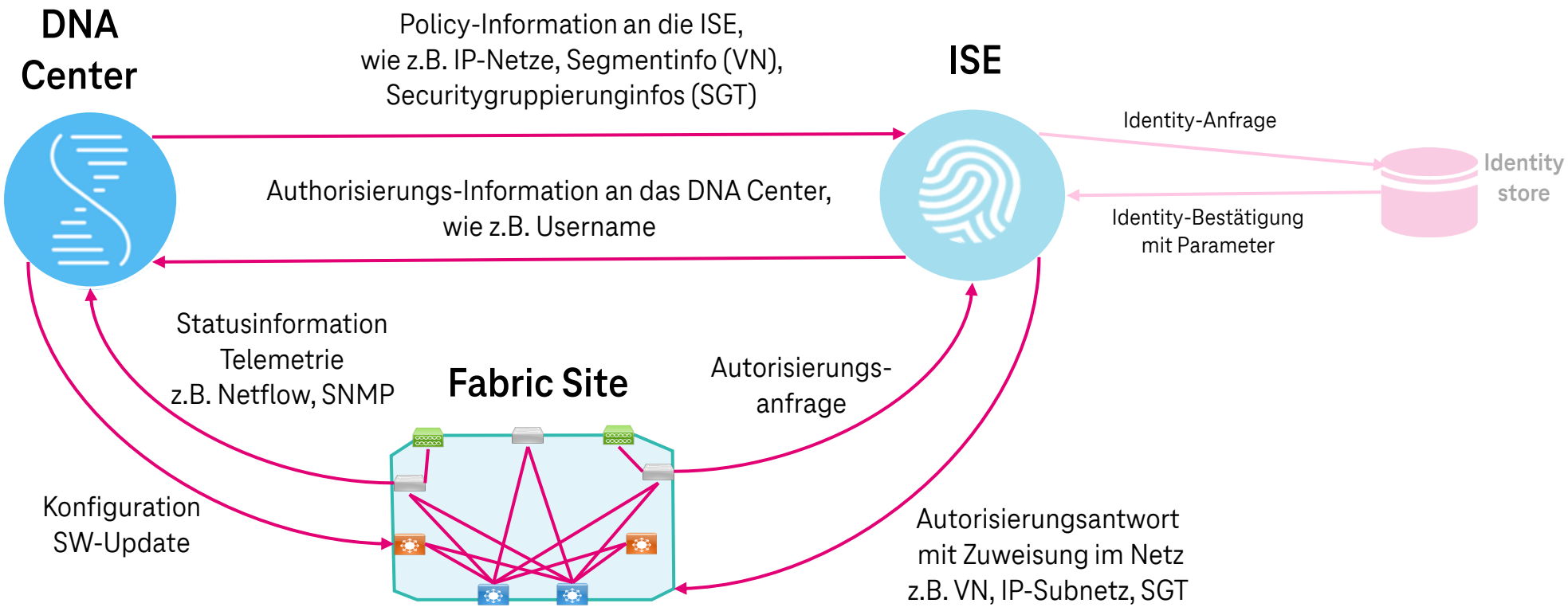
SDA Fabric: Segmentation und die Außenwelt



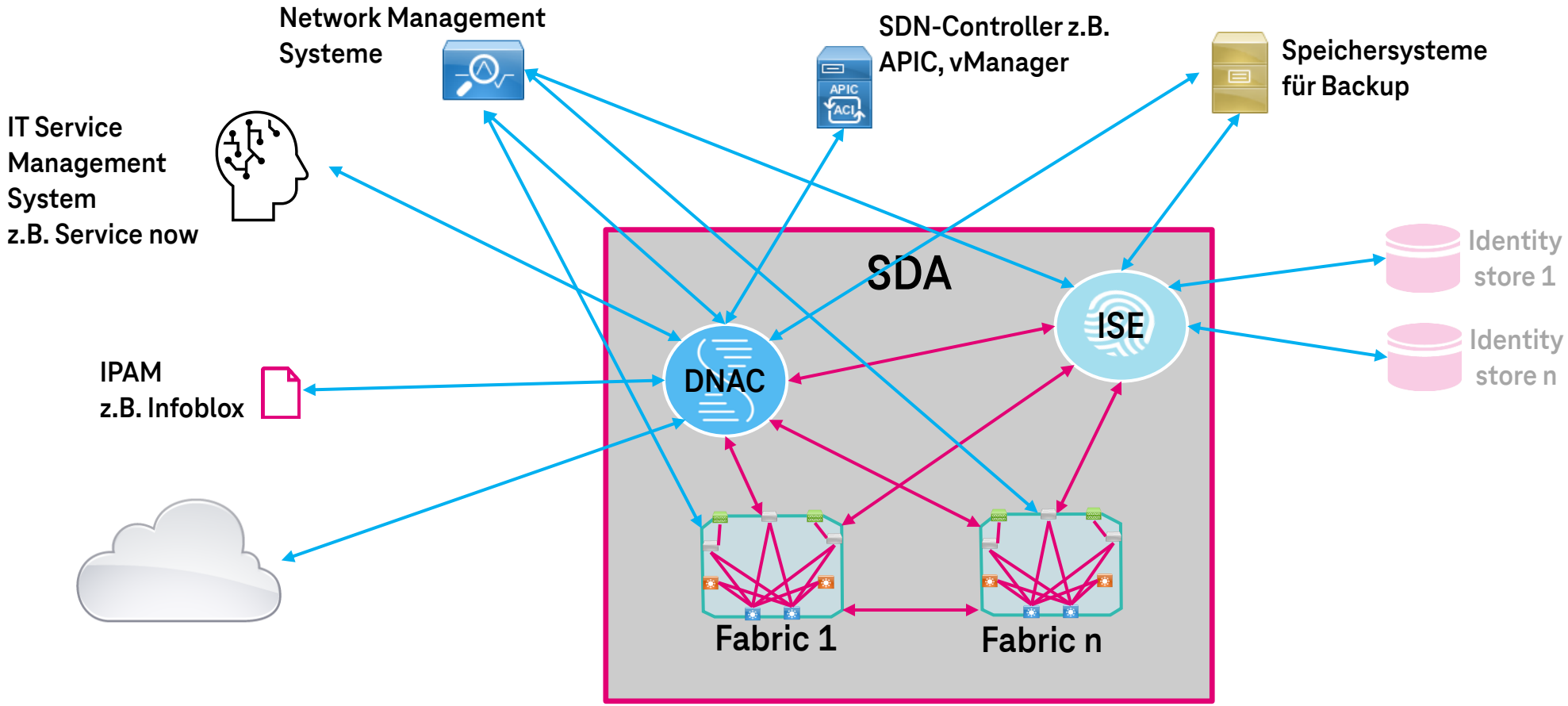
DNAC – Fabric – Fusion Device



DNA Center + ISE + Fabric = SDA



SDA und die Umwelt



Addon:

- Verfügbarkeit, Erreichbarkeit (Cisco Thousand Eyes)
- Security Analyse (Cisco Secure Network Analytics)
- DNS-Sicherheit (Cisco Umbrella)
- Zugangskontrolle (Cisco Duo)

02
Umsetzung, was nun?

DNA Center – Was vereint es?

Configuration Management

Licensing

Fault Management

Accounting Management

Inventory

Profiling

Performance Management

Security Management

Software Advertising

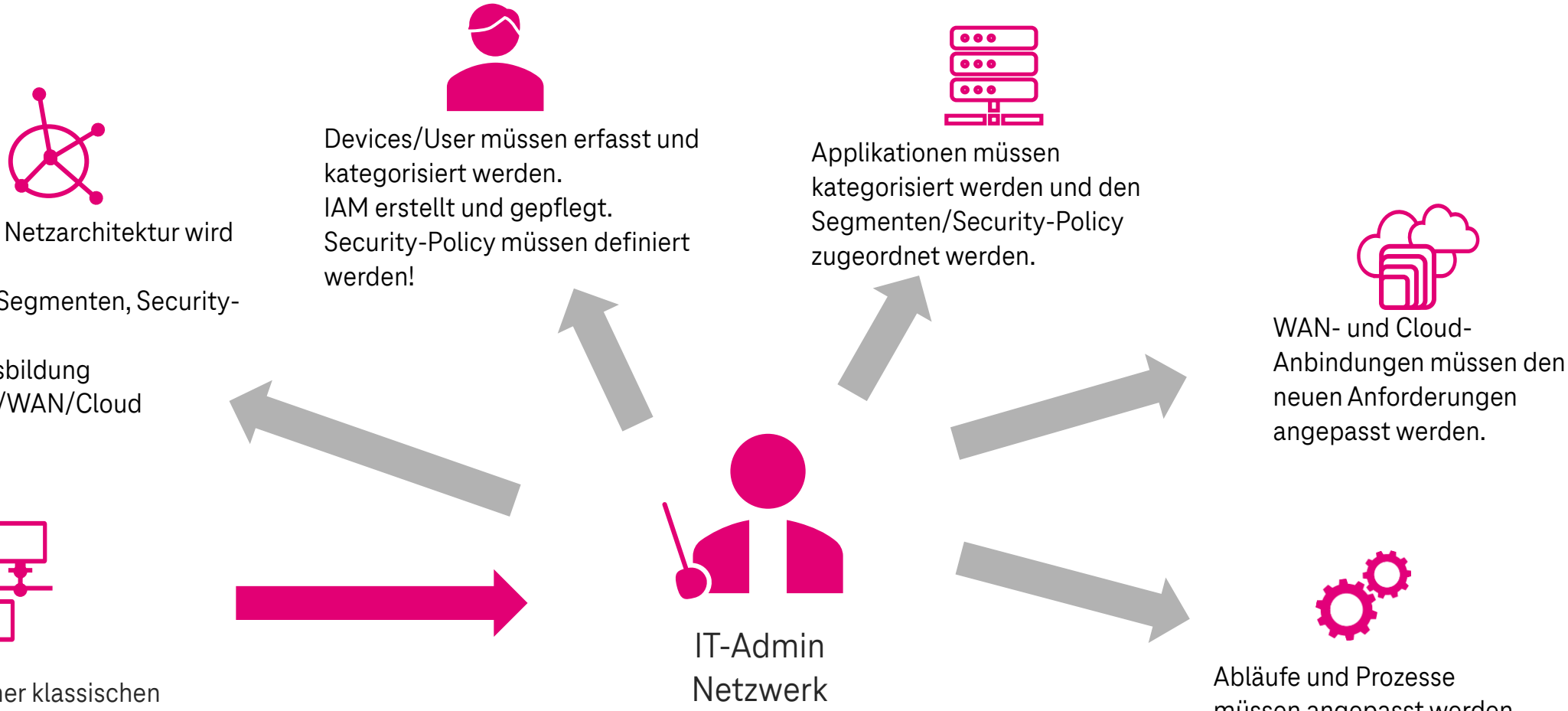
DNA Center – Was sollte man wissen?

Classic Network

Software Defined Access

■ ■ □	Design	■ ■ ■
■ □ □	Provision	■ ■ ■
■ □ □	Policy	■ ■ ■
■ ■ □	Assurance	■ ■ ■

Cisco SDA Einführung – Netzadmin von 0 auf 100



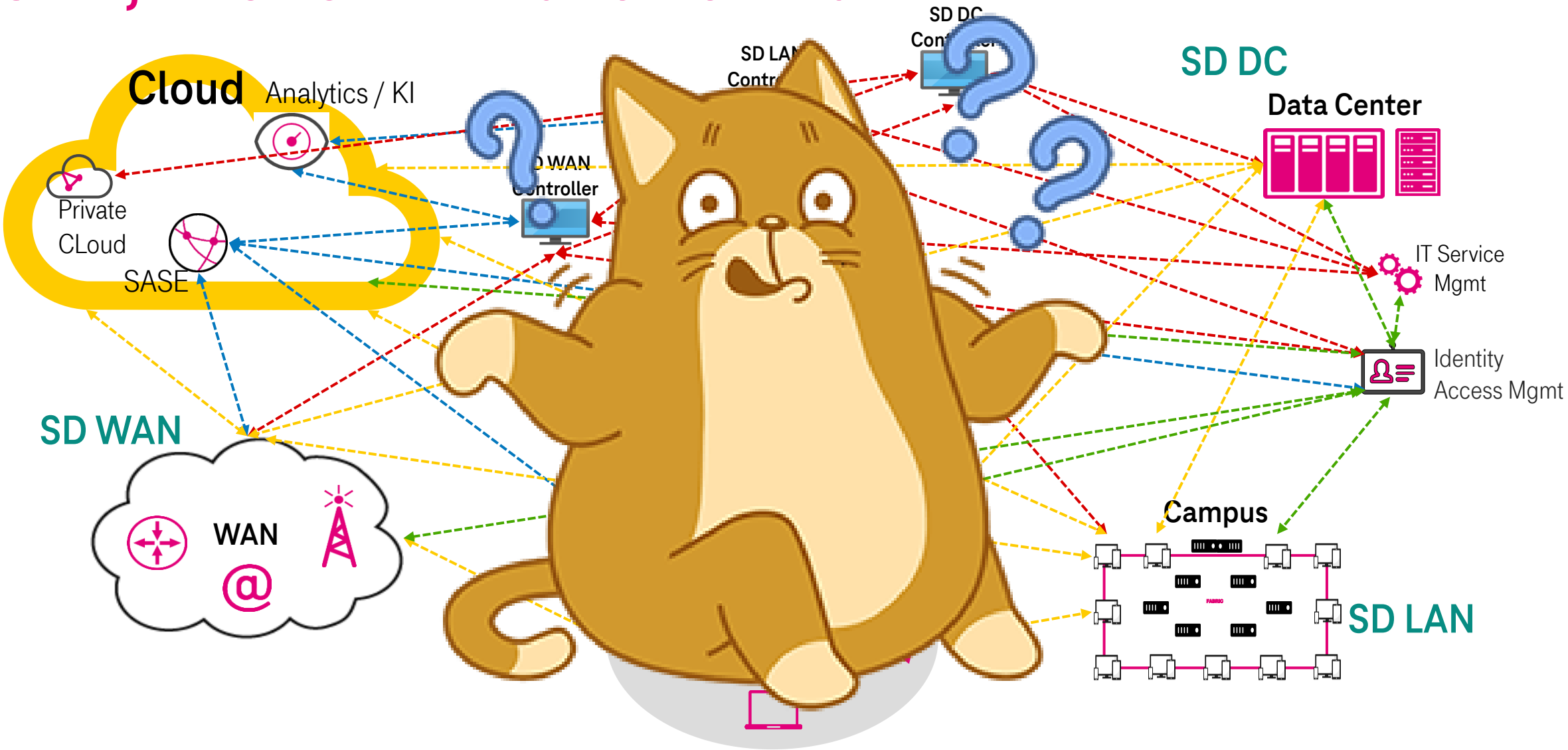
Was ändert sich für den Netzwerk Admin?

IT-Admin
Netzwerk

- Komplexität des LAN ist höher - Fabric-Design
- Knowhow in neuen Netzwerktechniken ist notwendig
- Denken in der SDA-Netzstruktur weicht von klassischen Netzwerk ab
- Mehr Interaktion mit anderen Systemen

- Das Netzwerk ist intensiver in den Betriebsabläufen integriert
- Transparenz im Netzwerk ist vorhanden
- Schnellere Bereitstellung, bei Erweiterung und Austausch
- Detailliertes Monitoring, wer und was ist wo und wie
- Ein Netz (LAN und WLAN eins) mit einem Zugang
- Mehr Informationen aus dem Netzwerk, um es zu optimieren.
- Eliminiert Handarbeit

SDN, was kommt auf einem zu?



03
Was nehmen wir mit?

Was nehmen wir mit?

DNA Center:

- Ist kein reines Management-Tool – es ist mehr!
- Ist ein zentraler Zugang zum Netzwerk für Informationen und Aktionen
- Schnittstelle für die individuelle Automatisierung im Netzwerk
- Gibt eine neue Sichtweise auf das Netzwerk
- Vereinfacht den Umgang mit dem Netzwerk
- Im SDA ist eine von Cisco vorgedachte, erprobte und gepflegte Gesamtlösung
- Ist das Tool für das Campusnetzwerk
- Kann mit anderen SDN-Controllern von Cisco gekoppelt werden
- Kann mit anderen externen System gekoppelt werden

- Macht Spaß!

Vielen Dank!

GEMEINSAM GESTALTEN WIR DIE **DIGITALE ZUKUNFT!**

ERLEBEN, WAS VERBINDET.

PETER WOSNIAKOWSKI

DEUTSCHE TELEKOM INDIVIDUAL SOLUTIONS & PRODUCTS GMBH
Überseering 2, 22297 Hamburg
Telefon +49 40 30600 3158
Mobil +49 170 45 12 430
E-Mail peter.wosniakowski@telekom.de