SDA – Software-Defined Access (SD-Access)

SDA ist innerhalb des IBN (intend-based networking) die SDN (software-defined network) Lösung für das Campus LAN.

SDA bietet ein absichts-orientierte (intend-based) Network Management Lösung für das Campus Fabric Access Network (wired und wireless).

Über eine zentrale Steuerung mit dem Cisco DNA Center, kann das interne Netzwerk richtlinien-basiert und automatisiert verwaltet und analysiert werden.

Zudem werden Sicherheitsanforderungen umgesetzt.

Eingliederung
→ **IBN**
→ Cisco **SDN** Lösungen
→ Ciscos **DNA** – Digital Network Architecture
- Ciscos **ACI** – Application Centric Infrastructure für **Data Center Networks** (Cloud Computing)
- Ciscos **SDA** – Software-defined Access für **Campus LAN** mit **DNA Center** – Digital Network Architecture Center
- Ciscos **SD-WAN** -Software-defined WAN für **WAN Verbindungen**

SDA Releases
- SDA 1.0 → controlled availability
- SDA 1.1, SDA 1.2 → gereral availability

SDA Architektur - Übersicht

.. besteht aus 5 Elementaren Schichten (Layer)

Layer	Erläuterung
Physical layer	Beinhaltet die notwendigen Hardwarekomponenten, wie • Router, Switches und Wireless Geräte • Schnittstellen und Verbindungen, • Clusters, virtual switches, server appliances
Network layer	Beinhaltet die Elemente für das Campus fabric overlay und underlay network: • control plane • data plane • policy plane
Controller layer	Beinhaltet die software-basierten Systeme und Subsysteme zur Steuerung des network layers für • automation, • identiy und • analytics
Management layer	Beinhaltet die Elemente zur Steuerung des Controller layer durch den Administrator, wie • GUI • APIs • CLI
Partner ecosystems	Beinhaltet alle zusätzlichen Systeme von Cisco oder anderen Herstellern, die eingesetzt werden können und die Funktionen innerhalb von SDA zu erweitern oder zu verbessern.

Die wesentlichen Bestandteile der Layer

Management	**Cisco DNA Center**				
	Automation	Design	Policy	Provision	Assurance

Controller	**NCP**	**NDP**	**ISE**
	Network Control Platform	Network Data Platform	Identiy Services Engine

Network	**Fabric overlay** (LISP, VXLAN, CTS) → VN(s) zur Datenkommunikation zwischen den nodes
	Fabric underlay (Settings, Protocols) → zu Grunde liegendes physikalisches Netzwerk

Physical	**Switches**	**Routers**	**Wireless**	**DNAC Appliance**	**ISE Appliance**

.. und **partner ecosystems:** Cloud, DNS, DHCP, IPAM, Firewall, NaaS/ETA, VNF

Physical Layer

Die unterste Schicht der SDA Architecture ist der physical layer.

Diese Schicht beinhaltet
- die Hardwarekomponenten und deren Betriebssysteme,
- sowie die Schnittstellen und Verbindungen zwischen den Hardwarekomponenten.

Die Geräte müssen bestimmte Funktionen bereitstellen, um die Anforderungen von SDA zu erfüllen, wie z.B. Unterstützung bestimmter Frame Formate bzw. Protokolle oder Bereitstellung von APIs.

Daher unterstützen nur neueste Geräte – meist mit IOS XE – diese Anforderungen.
Weiterhin ist der Einsatz der einzelen Geräte innerhalb der SDA Topologie auf bestimmte Funktionen, wie z.B. als fabric border, edge, control oder extension beschränkt.

Damit SDA eingesetzt werden kann empfiehlt sich die "Greenfield" Lösung: Update des bestehenden Equipments auf die enstprechenden Hardwarekomponenten. Nachfolgend eine Auswahl unterstützter Cisco Hardware/Software mit elementarer SDA Funktion:

Switches	**OS**	**Funktion**
Catalyst 9000	IOS XE 16.6.1	fabric edge
Catalyst 9500	IOS XE 16.6.1	fabric border/control
Catalyst 3650	IOS XE 16.6.1	fabric edge
Catalyst 3850	IOS XE 16.6.1	fabric border/control
Catalyst 4500-E	IOS XE 3.10.OE	fabric edge
Catalyst 6800-X oder -XL	IOS 15.4(1)SY2	fabric border/control
Catalyst 6500-E	IOS 15.4(1)SY2	fabric border/control
Nexus 7700	NxOS 8.2(1)	fabric border
Catalyst 3560-CX	IOS 15.2(6)E	extension
Catalyst Digital Building	IOS 15.2(6)E	extension
Industrial Ethernet 4000/5000	IOS 15.2(6)E	extension
Router	**OS**	**Funktion**
ASR 1000-X und -HX	IOS XE 16.6.1	fabric border/control
ISR 4300/4400 Series	IOS XE 16.6.1	fabric border/control
Integrated Services Virtual Router (ISRv)	IOS XE 16.6.1	fabric border/control
Cloud Services Virtual Router (CSRv)	IOS XE 16.6.1	fabric control
Wireless	**OS**	**Funktion**
3504/5520/8510/8540 Wireless Controller	AireOS 8.5.103.0	wireless control
Aironet 1700/2700/3700, 1800/2800/3800	AireOS 8.5.103.0	wireless access
Cisco Appliances		**Funktion**
DNA Center		Controller
Secure Network Server 3500 Series		Cisco ISE Controller

Network Layer

Auf dem physical Layer setzt der Network Layer auf, der innerhalb von SDA als **fabric** bezeichnet und in 2 unterschiedliche Unterkategorien unterteilt wird.

- **fabric underlay**
  mit globalen Einstellungen und Transport Protokollen (MST, IS-IS, OSPF, ..)
  → zugrundeliegendes, physikalisches Netzwerk

  - beinhaltet die Einstellungen, Protokolle und Tabellen der Netzgeräte (inklusive Stacking oder virtuelle Netzgeräte) um Datenverkehr zwischen den Netzgeräte weiterzuleiten.

  - ist das **L2/L3 Netzwerk, das auf der physikalischen Infrastruktur aufsetzt** und Grundlage für das overlay network ist.

  HINWEIS: redundante L2 Topologien mit STP bzw. MST können zwar verwendet werden, es ist jedoch empfohlen, L3 Topologien zu verwenden und ein IGP zu verwenden .. Datenverkehr wird zwischen den Geräten ausnahmlos geroutet. Ciscos DNA Center automated underlay verwendet eine L3 Routing Umgebung.

- **fabric overlay**
  mit LISP, VXLAN und CTS
  → multiple virtuelle Netzwerke (VXLAN, VRF), die Datenverkehr für multiple Nodes unterschiedlicher Bereiche separiert übertragen .. hier findet die eigentliche Datenübertragung für die "Endgeräte" statt.

  - beinhaltet die Einstellungen, die Protokolle zur Weiterleitung und zur Umsetzung der Richtlinien für die logische Topologie des Netzwerks, sowie die dazu notwendigen Tabellen (LISP, VXLAN, VRF, ..).

  - ist das **logische (getunnelte) Netzwerk** bzw. das VN (virtual network) über das alle Netzgeräte und alle Endpunkte miteinander verbunden sind und kommunizieren (die **fabric**) → sie abstrahiert die Komplexität des underlay

Beide Layer formen den "access" und den "fabric" Bereich von SDA und arbeiten zusammen. Alle Informationen beider layer stehen dem controller layer zur Verfügung.

fabric underlay

Das network underlay sollte auf maximale Einfachheit und Flexibilität ausgelegt sein.

Dies beinhalt alle gängigen best-practise Anwendungen auf das Netzwerk:

- **physical layer**
  - hardware redundancy
  - multiple data paths

- **network layer**
  HINWEIS: redundante L2 Topologien mit STP bzw. MST können zwar verwendet werden, es ist jedoch empfohlen, L3 Topologien zu verwenden und ein IGP zu verwenden .. Datenverkehr wird dann zwischen den Geräten ausnahmlos geroutet.
  - protocol redundancy,
  - timers,
  - control-plane protection

Cisco unterstützt zwei Arten des network underlay

- **custom underlay**
  ein existentes Netzwerk oder ein Netzwerk, das manuell (mit CLI oder API) eingerichtet wurde bzw. nicht mit dem DNA Center eingerichtet wurde.
  Dabei muss der Administrator volle IP Erreichbarkeit zwischen allen Netzgeräten, sowie dem DNA Center und dem ISE sicherstellen.
  - Vorteil: basiert auf individuellen physikalischen Topologien
  - Nachteil: Probleme bei der IP Erreichbarkeit erfordern alte manuelle Vorgehensweisen.

- **automated underlay**
  ein neues, voll- automatisiertes Netzwerk, wobei alle Aspekte des Netzwerk über das DNA Center konfiguriert und verwaltet werden.
  Dabei muss der Administrator ledigilich den IP Adressraum bestimmen, allen weiteren Funktionen werden voll-automatisiert (nach manueller Einrichtung eines "Seed"-Geräts) vom DNA Center eingerichtet.
  - Vorteil: die Komplexität der Konfiguration wird verringert und Fehler bei der Konfiguration vermieden.
  - Nachteil: erfordert eine "besonderes" phsikalisches Netzdesign mit ensprechenden Hardwarekomponenten.

fabric overlay – LISP, VXLAN, VXLAN-GPO/VXLAN mit CTS

Das fabric overlay ist/sind ein oder mehrere VN – virtual networks, die mit VXLAN und VRF Technologien erzeugt werden.

Dabei verbinden die VNs die "Endpunkte" der Kommunikation direkt miteinander (Verbindungsnetze und Redundanzen sind Bestandteil des network underlay).
Die VNs des fabric overlay bilden somit die Netzinfrastruktur für die Kommunikation der (End)-Geräte im Netzwerk.

Das fabric overlay wird – nach Einstellungen im DNA Center, wie z.B. die Anzahl der VNs – automatisch konfiguriert.

Aufgaben des fabric overlay

- **Control plane**
  → Bereitstellung von Informationen für die Weiterleitung über VNs
  beinhaltet die Einstellungen, Protokolle und Tabellen für fabric nodes. Stellt logische Informationen für die Weiterleitung bereit.
  Eingesetzte Technologien:
  - LISP
  - VRF

- **Data plane**
  → Tunneling/Framing: Weiterleitung
  Weiterleitung der Daten mittels Mechanismen, die Informationen über die VN Zugehörigkeit beinhalten.
  Eingesetzte Technologien:
  - VXLAN

- **Policy plane**
  → Richtlinienumsetzung
  Zusätzliche Eingliederung des Datenverkehrs in endpoint "identity" groups mit separaten Richtlinien.
  Weiterleitung der Daten mittels Mechanismen, die Informationen über die VN Zugehörigkeit und zugeordneten Richtlinienen beinhalten.
  Eingesetzte Technologien:
  - VXLAN-GPO – Group Policy Option
  - VXLAN mit CTS – Cisco TrustSec

LISP for the fabric overlay control plane

LISP – Locator/ID Separation Protocol (RFC 6830).

LISP verwendet ein Mapping System zwischen EIDs und RLOCs:
- **EID – Endpoint IDs**
  → "identity": Adresse des kommunizierenden Endpunkts
  → EID namespace: end-site Adressierung für Host und Router
- **RLOC – Routing Locators**
  → "location": Angeschlossener Router
  → RLOC namespace: infrastructure Adressierung für LISP Router

Remote DST Informationen (Erreichbarkeit der EIDs) werden zentralisiert auf einem **LISP Map Server/Resolver** innerhalb einer Datenbank aufbewahrt (SDA → fabric control node) - ein Router verwaltet innerhalb seiner lokalen Routing Tabellen nur noch sein "connected" Routen.

Muss Datenverkehr für eine bestimmte "**identiy**" weitergeleitet werden, befragt der Router die LISP Datenbank, um die notwendigen Informationen für die Weiterleitung zu erhalten.

Vorteile:
- geringerer Bedarf an CPU/RAM
- kleinere Routing Tabellen
- "Host Mobility" (endpoint mobility) für wired/wireless einfach möglich
- address-agnostic mapping
- built-in VRF

Ciscos SDA Lösung erweitert den LISP Standard um besonderen Features, wie z.B. distributed anycast GW (multiple Default-Gateways, die über eine einzelne IP angesprochen werden), VN Extranet (VRF für externe Netze) oder fabric wirlesess (SDA WLAN Anbindung)

Übersicht LISP Devices
- **MS – Map Server**: Ein LISP Infrastructure Device, das die EID ↔ RLOC Mappings verwaltet
- **MR – Map Resolver**: Ein LISP Infrastructure Device, das LISP Map Requests beantwortet
- **ITR – Ingress Tunnel Router**: Ein LISP Edge Device, das Datenverkehr von internen Hosts an entfernte LISP Sites oder nicht-LISP Sites weiterleitet
- **ETR – Egress Tunnel Router**: Ein LISP Site Edge Device, das Datenverkehr aus externen Netzen (wie z.B. das Internet) empfängt, und via LISP an lokale EIDs weiterleitet
- **XTR – Extended Trunnel Router**: gleichzeitige ITR/ETR Funktion
- **PXTR – Proxy XTR**: Proxy Funktion für LISP

Geräte Rollen innerhalb des fabric overlay
- **Control plane node** → agiert als LISP Map Server/Resolver
  unterstützt weitere Funktionen wie fabric wireless, SGT mapping (VXLAN-GPO, VXLAN/CTS)
- **Fabric border node** → basiert auf LISP XTR
- **Default border node** → basiert auf LISP ETR
- **Fabric edge node** → basiert auf LISP XTR
  "access" und "connectivity" für Endgeräte bzw. LISP EIDs
- **Intermediate node** → NUR Funktionen innerhalb des fabric underlay
- **Fabric WLC** → basiert auf Proxy XTR
  "access" und "connectivity" für wireless über LISP EIDs

VXLAN for the fabric data plane

VXLAN – Virtual Extensible LAN (RFC 7348, etc.).

VXLAN encasuliert (tunnelt) Datenverkehr IP/UDP-based, d.h. es kann von jedem zu Grunde liegenden IP-based network (underlay network) weitergeleitet werden.

VXLAN Encapsulation wird anstelle der LISP Encapsulation verwendet, da
- VXLAN das gesamte originale OSI 2 Ethernet Frame tunnel (LISP nicht)
- VXLAN spezielle Headerfelder bereistellt um VN Information zu übertragen (LISP nicht).

Encapsulated Frame

VXLAN Encapsulation (RLOC)				**Original Frame (EID)**		
Ethernet/ dot1q	IP	UDP (Port 4789)	**VXLAN**	Ethernet/ dot1q	IP	Payload

So unterstützt VXLAN beliebiege virtuelle L2 (VLAN) und L3 (VRF) Topologien.

Mit VXLAN Tunnel werden direkte Verbindungen zwischen fabric border nodes und fabric edge node geschaffen, die den Datenverkehr innerhalb der fabric und zu Zielen ausserhalb der fabric via LISP Routing weiterzuleiten.

VXLAN-GPO oder VXLAN mit CTI for the fabric policy plane

VXLAN-Group Policy Option ist ein IETF Draft.
Cisco TrustSec ist quasi der "Vorläufer" VXLAN-GPO.

Beide VXLAN Erweiterungen implementieren eine ID – einen SGT - scalable group tag – mit denen "EID"-groups unhabhäging ihres address plans (IP) separiert werden können.

Ein SGT ist ein einzigartiges 16-Bit Tag, das mit unterschiedlichen VNs kombiniert werden kann. Der Tag repräsentiert, die Richtlinien, die für den Datenverkehr innerhalb des VNs umgesetzt werden müssen, wie z.B.
- Security Policys
- QoS
- PBR
- ..

So können zusätzlich differenzierte, unterschiedliche Einstellungen/Richtlinien (Policys) für Datenverkehr vorgenommen werden.
- Separierung des Datenverkehrs in VNs
- Separierung des Datenverkehrs innerhalb eines VNs mit SGTs

VXLAN (GPO) Header

VXLAN Flags (16)	**Group ID (16)**	**VN ID (24)**	Reserviert (8)
Flag Feld	Kennzeichnet SGTs (scalable group tag) → siehe policy plane	Kennzeichnet VRFs	Reserviert

fabric Konzepte - Überblick: VN, SGT, EID Address Pool

Die SDA fabric basiert auf multiplen (standard) Technologien, wie z.B.

- fabric underlay
  - EtherChannel
  - VLAN
  - IGP Routing (IS-IS, OSPF, EIGRP)
  - ...
- fabric overlay
  - LISP
  - VRF-light
  - VXLAN
  - VXLAN mit CTI/VXLAN-GPO

Dabei werden 3 generelle Konstrukte innerhalb der fabric verwendet:

- **virtual network – VN, VRF**
  separate Routing und Switching Umgebungen zur Netzsegmentierung

  VRF VNID → EID Mapping: Zuordnung von EID address pools zu VRFs
  - der LISP Map Server (control node) verwaltet unterschiedliche LISP Datenbanken für die VRFs
  - die VN-ID wird innerhalb des VXLAN Headers transportiert und von fabric edge und border nodes interpretiert

- **scalable (security) group - SGT**
  Umsetzung von Richtlinien für bestimmten Datenverkehr

  SGT → EID Mapping: Zuordung von EID address pools zur SGTs (Richtlinien)
  - SGTs werden via DNAC und/oder ISE definiert und einem address pool zugeordnet
  - das SGT wird innerhalb des VXLAN-GPO bzw. Ciscos TrustSec VXLAN Header transportiert und von fabric edge und border nodes interpretiert. So ist z.B. der Einsatz von SGACL – SGT-based ACLs für bestimmte Datenströme möglich.

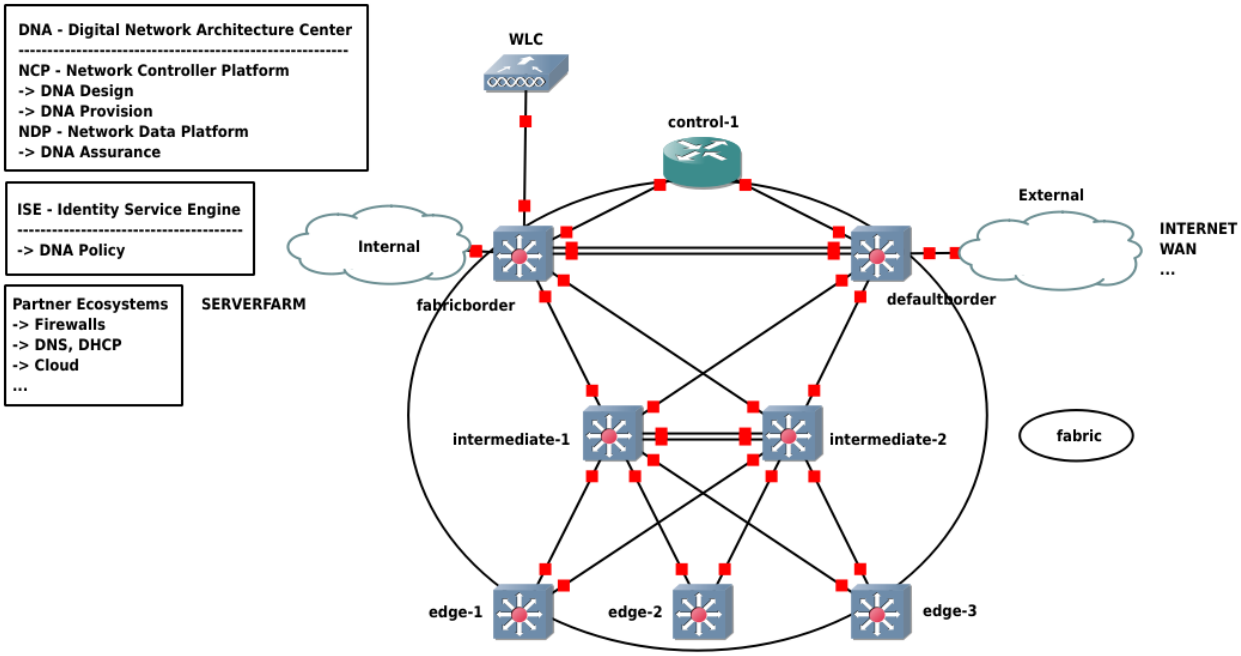
- **host (address) pool – EID namespace**
  Logische Adressierung für EIDs

  IP → EID Mapping: Zuordnung IP Adressierung für EIDs
  - statische oder dynamische Vergabe von IP Adressen für Hosts
  - statische oder 802.1x basierte Hostanbindung (ISE)
  - identische anycast IP (SVI) auf allen fabric edge nodes, ermöglicht ein ausfallsicheres, redundantes first-hop routing
  - erweiterte DHCP Relay Funktion für VN Anforderung

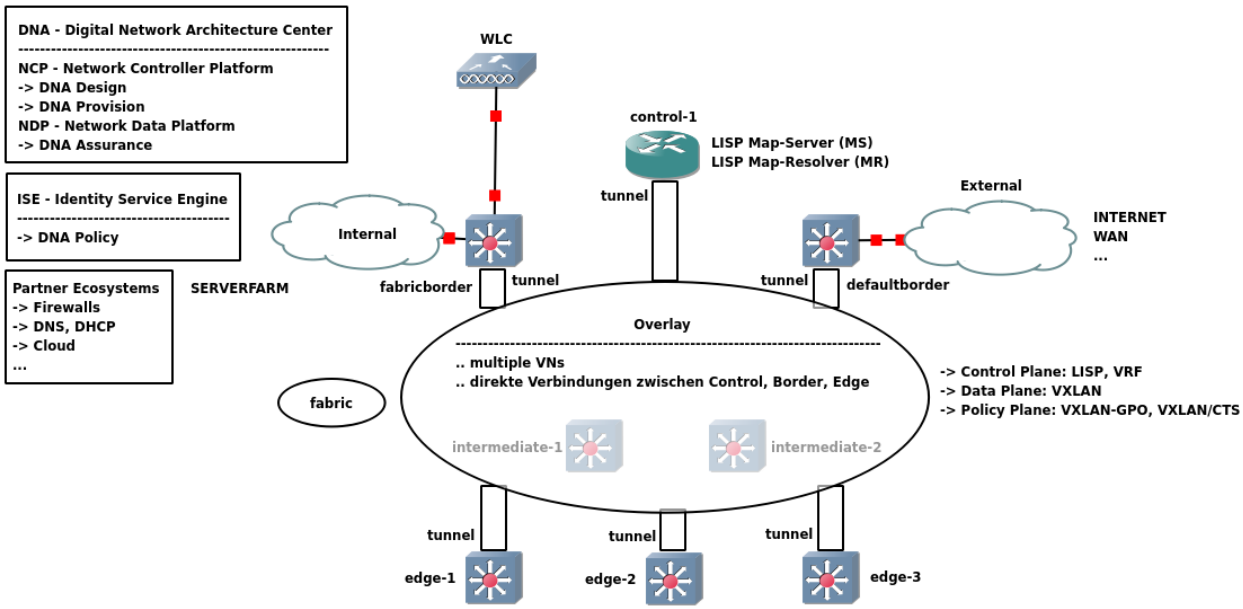
fabric – underlay & overlay Topologien

Darstellung inklusive DNA Center, ISE und Partner Ecosystems (Control & Management)

fabric underlay – physikalische Topologie
→ redundant, ausfallsicher, skalierbar, elementare Routing und Switching Technologien



fabric overlay – VNs
→ virtuelle Netzinfrastrukturen zwischen fabric edge und fabric border nodes
→ mit VRF Segmentierung, LISP Routing und VXLAN Framing und Tagging (VNID – Virtual Network ID, SGT – Scalable Group Tag)



Controller Layer

Der Controller Layer wird durch die Server Produkte **DNAC – Digital Network Architecture Center** (mit NCP und NDP) und **ISE** – **Identity Services Engine** z.B. als Hardware Appliances bereitgestellt.

DNAC und ISE sind die eigentlichen **SDN Controller** (Software-defined network) mit
- northbound interface (Zugriff auf APIs → Managemt Layer und Partner Ecosystems)
- southbound interface (Zugriff auf die fabric)

Sie ermögliche eine automatisierte, absichts-orientierte (intend-based) Konfiguration, Steuerung und Analyse des Netzwerks auf Basis von Applikationen (software-based), die Richtlinien (policies) automatisiert umsetzen.

Controller Layer Komponenten im Detail
HINWEIS: NCP und NDP sind Komponenten des DNA Center, ISE ist eine eigene Komponente. Alle Komponenten kommunizieren und interagieren miteinander (z.B. via REST und PxGrid).

- **DNAC NCP – Network Controller Platform**
  → Automation
- eigentlicher SDN Controller
- bietet Zugriff auf APIs und die fabric (via NETCONF, SNMP, SSH)
- ermöglicht automatisierte Konfiguration und Steuerung der fabric: underlay und overlay
- NCP Apps im DNAC
  - **DNA Design**: base-level workflows wie site profiles, maps and floorplans, network setting, IP address management, wireless, ..
  - **DNA Provision**: SDA workflows wie device provisioning, fabric domains, device roles, host onboarding, ..
- NCP Services im DNAC
  - Device Discovery
  - Device Inventory
  - Plug-and-Play
  - Path Trace
  - Easy QoS
  - EN Service Automation

- **DNAC NDP – Network Data Platform**
- → Assurance
- bietet Zugriff auf APIs und die fabric (via HTTPS, SYSLOG, Netflow, SNMP, SPAN, ..)
- ermöglicht das Monitoring und die Analyse von underlay und overlay traffic
- ermittelt umfangreiche Informationen über den physical und network Layer und stellt diese für NCP Funktionen, ISE Funktionen oder Third Party Subsysteme bereit.
- NDP App im DNAC
  - **DNA Assurance**: workflows and tools für die Anzeige und Auswertung von Netzwerkinformationen in Echtzeit

- **ISE – Identity Services Engine**
- → Identity and Policy
- bietet Zugriff auf APIs und die fabric (southbound via AAA, Radius, EAPOL, ..)
- stellt Identifikationsdienste und Sicherheitsrichtlinien für physical und network Layer bereit.
- ISE App im DNAC
  - **DNA Policy**: workflows und tools für die Verwaltung von VNs und Security Groups, Erstellung von Richtlinien

Management Layer

Administratoren interagieren mit dem Management Layer des Cisco DNAC.

Er stellt Zugriff über das User Interface/User Experience (UI/UE) Modul zur Verfügung, über das alle Informationen über das Netzwerk für den Administrator verfügbar sind.

Um über den DNAC ein SDA aufzubauen, sind keinerlei Kenntnisse über die Arbeitsweisen und Funktionen des network oder controller layer notwendig. Ebensowenig sind Kenntnisse über die Konfiguration eines einzelnen Netzgeräts erforderlich.

Der Management Layer abstrahiert die komplexen Funktionen der anderen Schichten, und stellt dem Administrator eine GUI mit einfachen Tools und Workflows zur Verfügung, um das gesamte SDA Netzwerk zu verwalten.

Das DNA Center stellt zwei Basis App Types zur Verfügung:
DNAC Settings mit ..

- Controller Einstellungen
- APIs
- Einstellungen zur Kommunikation zwischen Subsystemen (ISE, Third Party)
- Einstellung für role-based access (permissions), redundancy, backups, upgrades

DNAC Applications mit ..

- **design**
  - network hierarchy → geo location, floorplan details, site ID
  - network settings → Server (z.B. DNS, DHCP, AAA), device credentials, IP management, wireless settings
  - image management → software management
  - network profiles → LAN, WAN, WLAN connection profiles (z.B. SSID)
- **policy**
  - dashboard → monitor all VNs, Security Groups, Policies, recent changes
  - virtual network → Einstellungen für VNs (or user Default_VN) und Security Groups
  - policy admin → Definition von Zugriffs- und Verkehrsrichtlinien zwischen Security Groups
  - contracts → Festlegung von Applikationen, die für bestimmte Security Groups verwendet werden soll
  - registriy → Anlegen neuer Security Groups, Import von Security Groups (z.B. vom ISE)
- **provision**
  - devices → Zuordung von Site IDs für Geräte, software updates, network underlay configuration
  - fabrics → Definition von fabric domain (or use default LAN fabric)
  - fabric devices → Zuordung von Geräten in eine fabric domain, Festlegung von Geräterollen (control, border, edge, WLC)
  - host onboarding → host authentication type (static/dynamic), Zuordung von host pools zu VNs
- **assurance**
  - dashboard → monitor global health aller Geräte im Netzwerk, incl scoring
  - client 360 → monitor client-specific status (Hosts)
  - device 360 → monitor device-specific status (Netzgeräte)
  - issues and trends → aktuelle Sachverhalte (reaktiv) oder Entwicklungen (proaktiv) aller Geräte im Netzwerk

Partner Ecosystems

Der DNAC ermöglicht (über APIs) einen direkten Zugriff auf Produkte/Applikationen etablierter Cisco Partner.

Dabei können Partner neue Produkte bereitstellen oder bestehenden Produkte aktualisieren bzw. erweitern.

Anbei eine (unvollständige) Liste von Funktionen

- Firewalls
- DNS, DHCP, IPAM
- Cloud
- Naas and ETA
- VNFs

TIPP: Cisco DevNet
https://developer.cisco.com/site/dna/
https://learninglabs.cisco.com/tracks/programming-dna
Eine Platform, um all das zu lernen, was notwendig ist, um mit Ciscos DNA Lösungen umgehen zu können → insbesondere Programmierung und APIs.
Eine Auswahl von SDA Themen:

- DNAC
- device-level APIs
- YANG data models (NETCONF, RESTCONF)
- ..