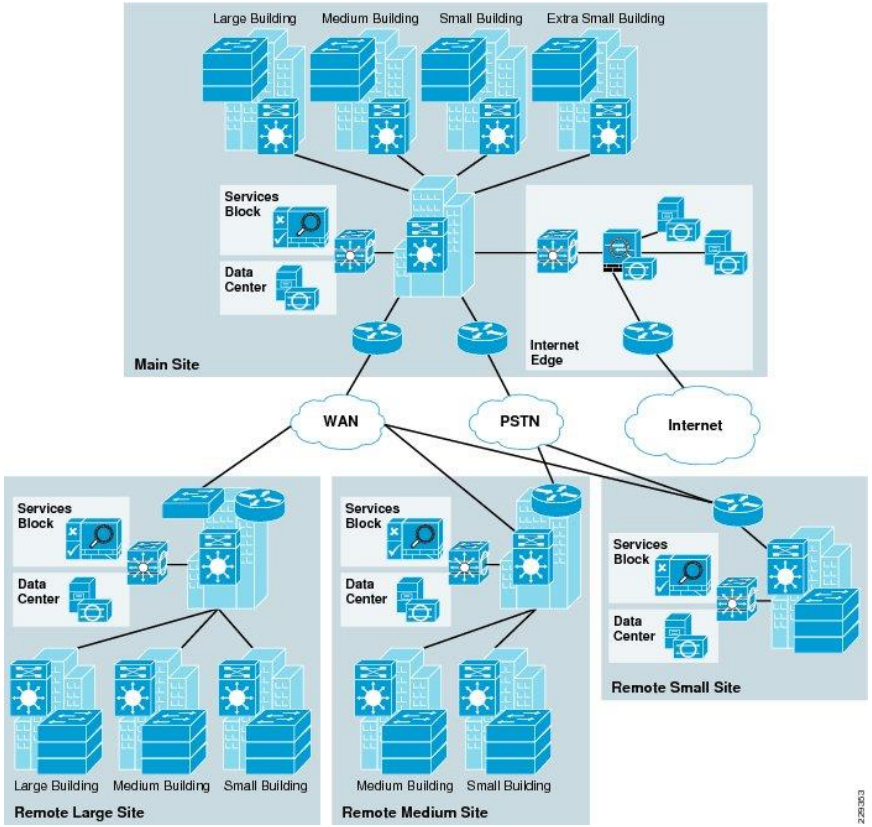
Cisco Software Defined (SD) Secure Access

Евгений Лысенко

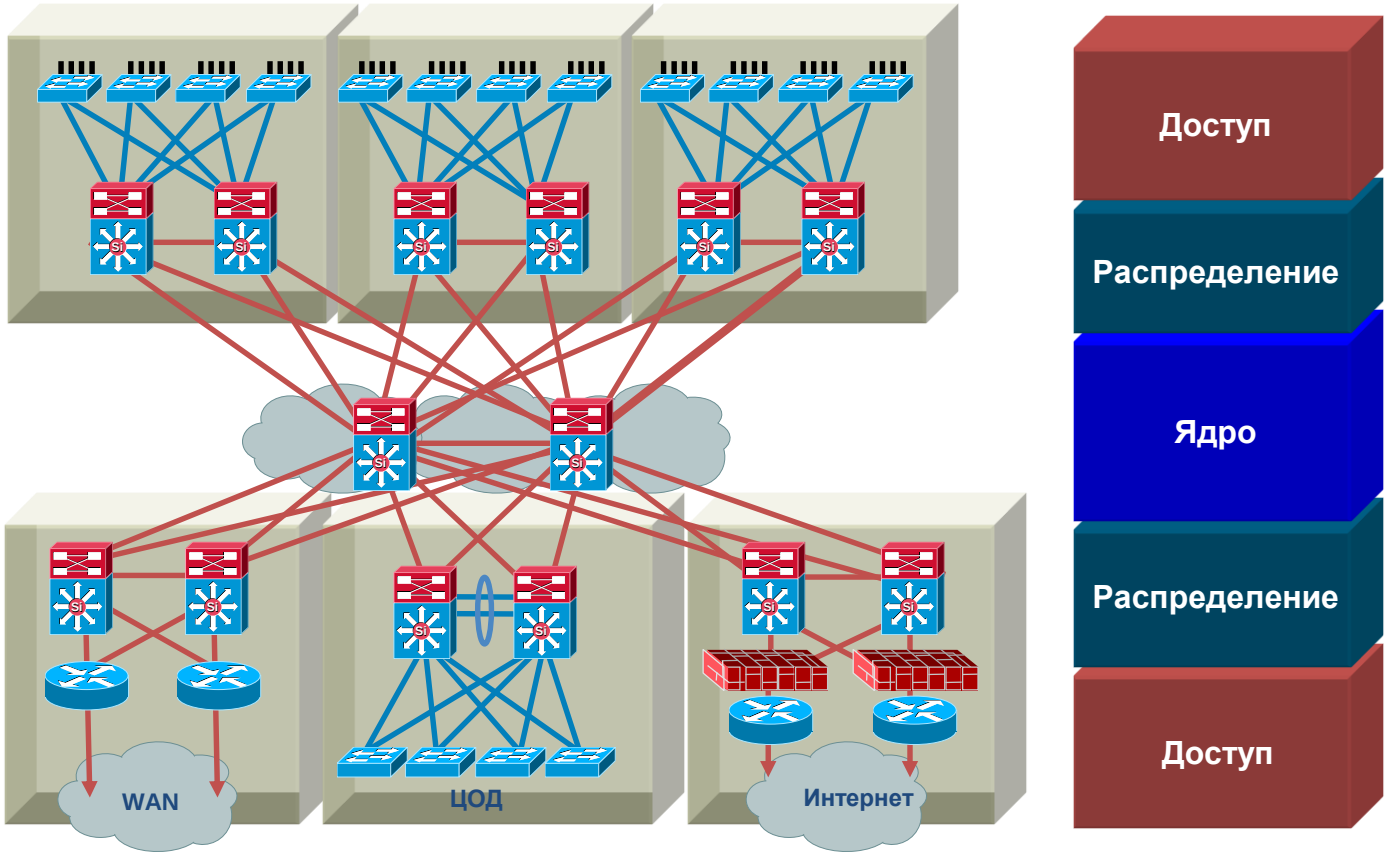
Старший инженер-консультант
Департамент телекоммуникаций
CCNP, CCDP, CCNP DC, CCNA Sec, CCNA Wireless
Evgeniy.Lysenko@it-integrator.ua

Что было раньше?

Example of Computer Network (Enterprise)



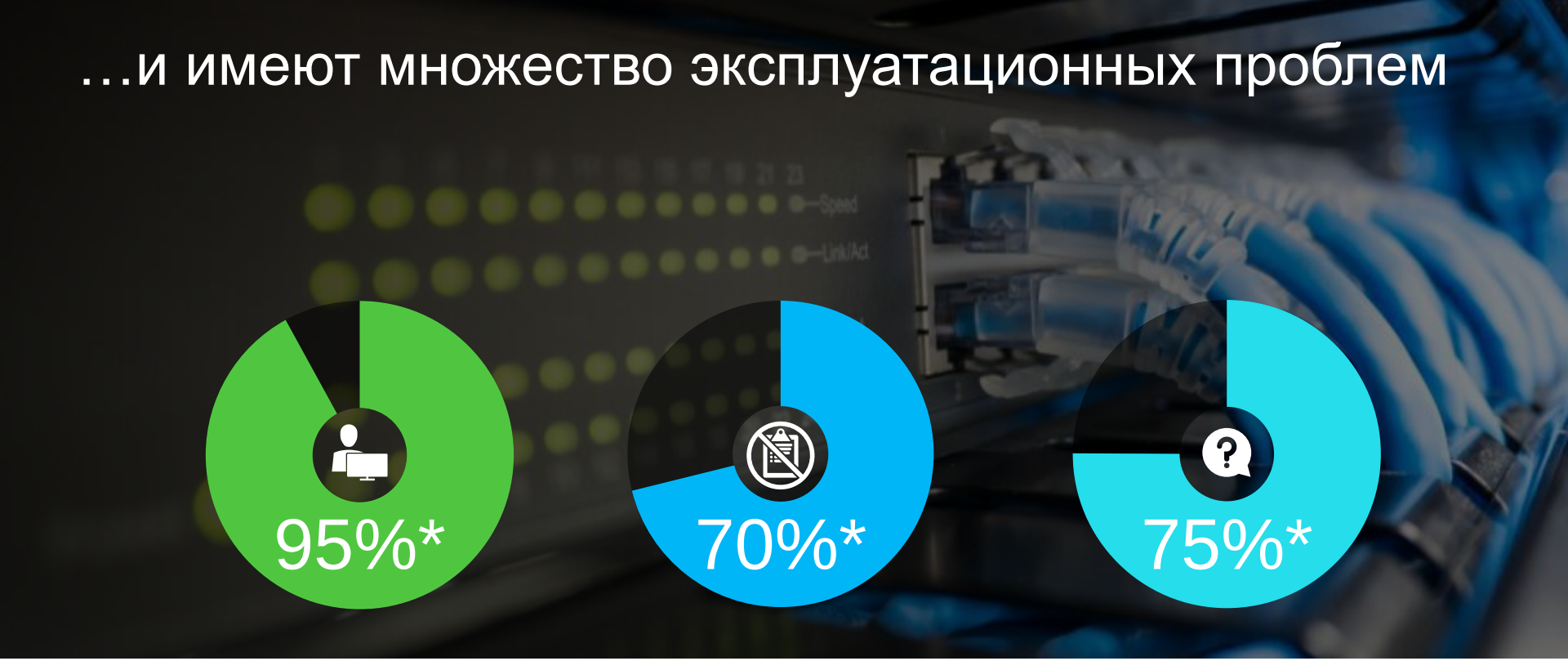
Иерархический кампус



Корпоративные сети сегодня – сложные …

Управление множеством VLAN	Работа с различными сетями	Работа с множеством разных политик - LAN, WLAN, WAN, ЦОД	Масштабирование увеличивает сложность эксплуатации

…и имеют множество эксплуатационных проблем



доля ручного труда при внесении изменений

нарушений политик и правил из-за человеческих ошибок

Операционных расходов приходится на поиск неисправностей и диагностику

Традиционные сети НЕ ГОТОВЫ к быстрым темпам развития потребностей бизнеса

SD-Access

На базе SDN-технологий для кампусных сетей (APIC-EM v2)

Использующий набор продвинутых технологий (VXLAN, LISP, CTS)

Которые спрятаны «под капот» командного центра (DNA-C)

Для упрощения ролевого доступа и сегментации сети (RBAC)

С пониманием контеста доступа и предусловий (CBAC)

Что даст возможность получить больше от сети (Cisco Catalyst)

С меньшим количеством усилий (Cisco Validated Design)

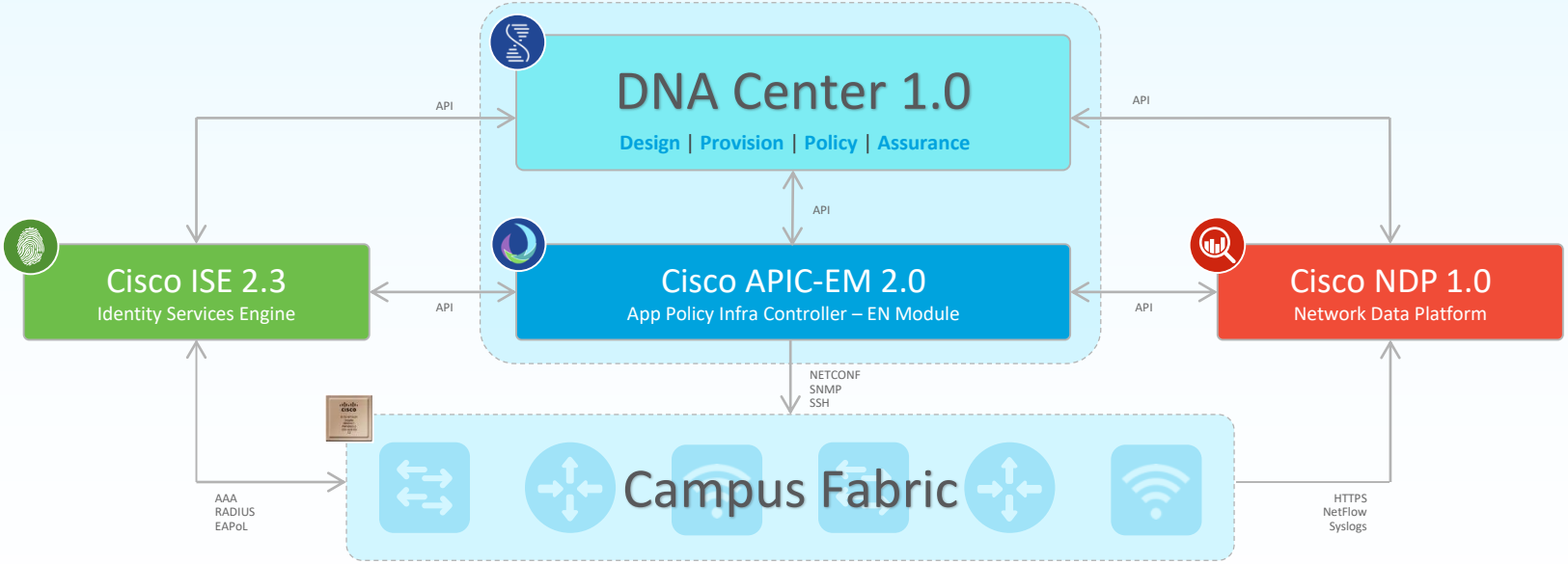
Для кого полезен SD-Access?

1. **Большие ENTERPRISE grade сети**
2. С разпределённой филиальной структурой
3. С требованиями по ИБ (внутренний/внешний compliance)
4. Где есть необходимость автоматизации и упрощения
5. Где есть ограничения количества персонала на обслуживаение
6. Если есть возможность привести оборудование к требованиям
7. Если есть возможность перестроить сеть под новую парадигму

Архитектура SD-Access

SD-Access

DNA Center – Service Components



Cisco Switches | Cisco Routers | Cisco Wireless

Что «под капотом» SD-Access?

❑ **Набор софта:**

- Веб-интерфейс (DNA-C) на базе SDN-контроллера (Cisco APIC-EM v2)
- Cisco ISE для контроля ролевого и контекстного доступа к сети
- NDP для мониторинга
- [опция] StealthWatch для мониторинга (включая ETA) и Rapid Threat Containment (RTC)

❑ **Совместимое железо:**

- Поддержка LISP
- Поддержка VXLAN
- Поддержка SGT enforcement
- Поддержка Campus Fabric
- Поддержка VRF
- **[рекомендуемая опция]** Оборудование созданное с заделом на SD-Access (Catalyst 9k)

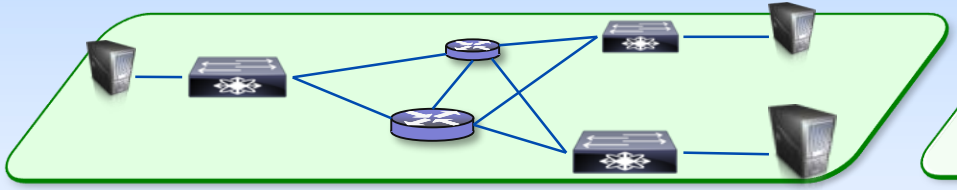
❑ **Cisco Validated Design**

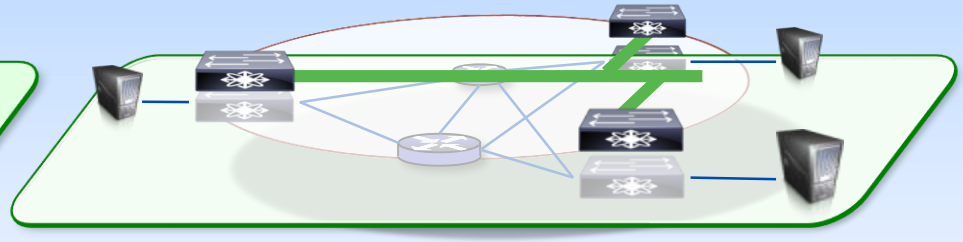
https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/Campus/CVD-Software-Defined-Access-Design-Guide-2017AUG.pdf

Что такое фабрика?

Почему “Overlay”

Разделение шин коммутации и сервисов





Простой транспорт

- Физические устройства и соединения
- Интеллектуальная обработка пакетов
- Максимальная доступность
- Простота и управляемость

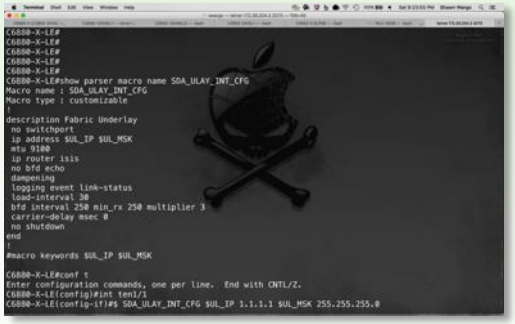
Гибкость виртуальных сервисов

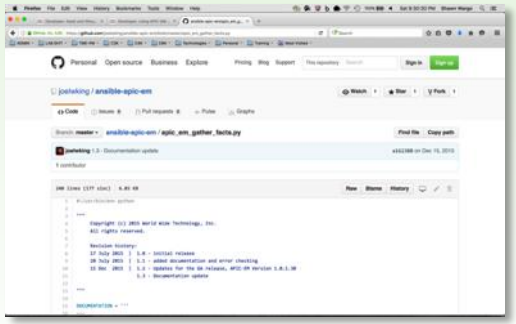
- Мобильность – отслеживание конечных устройств в точках подключения
- Масштабирование – снижение нагрузки на ядро
  - Распределение функций в сторону доступа/границы
- Гибкость и программируемость
  - Снижение числа точек применения усилий

SD-Access

Campus Fabric + Automation & Assurance

Campus Fabric

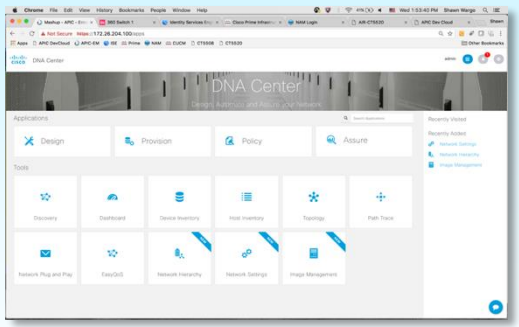




- **SmartCLI Macros**
- Simple User Inputs
- Customized Workflows
- **Box-by-Box Management**

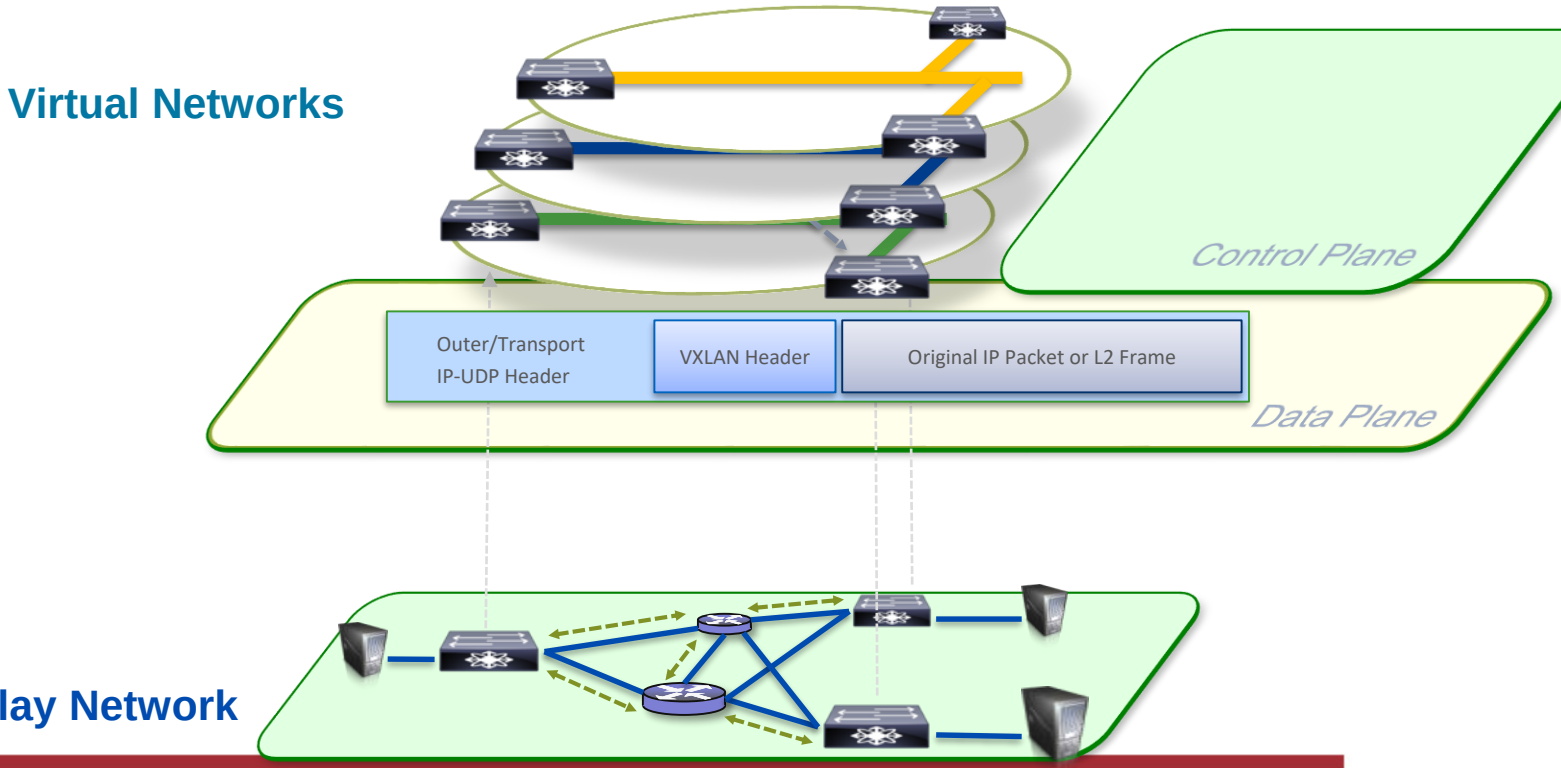
- **Programmable APIs**
- NETCONF / YANG
- Automated Workflows
- **Box-by-Box Management**

SD Access



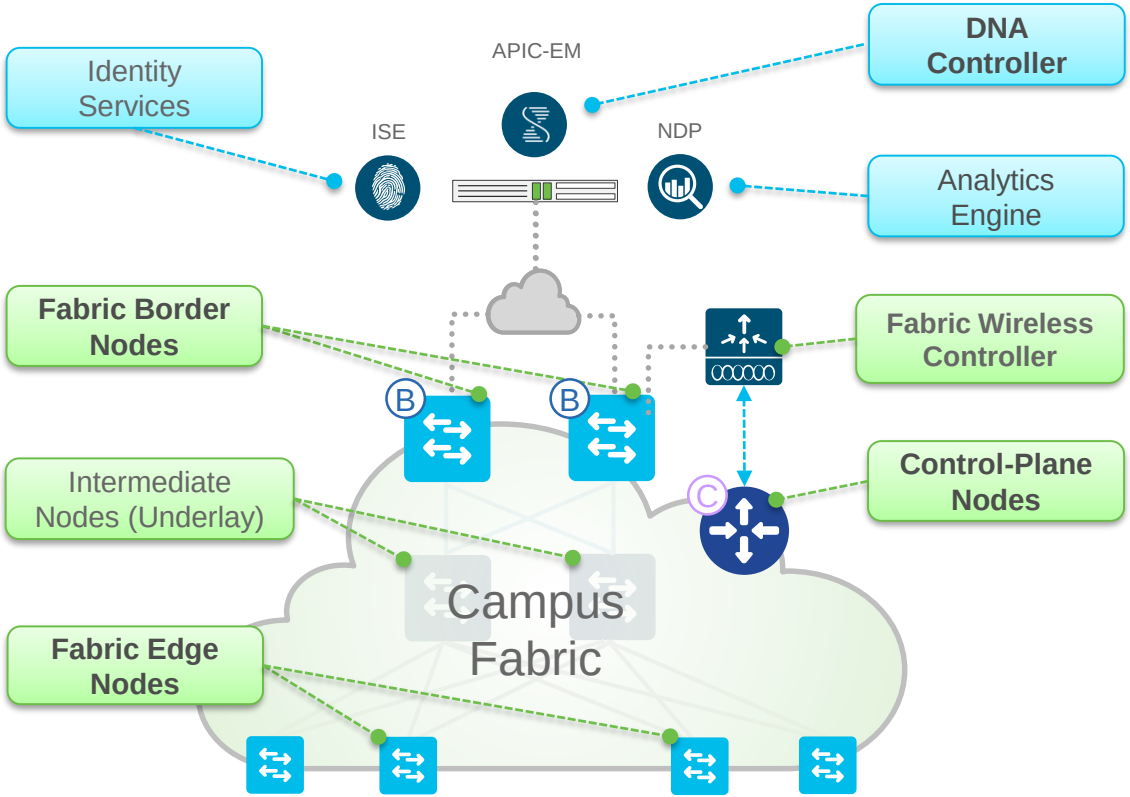
- **DNA Center GUI**
- Cross-App REST APIs
- Automated Workflows
- **Centralized Management**

Упрощение части сети до единой «фабрики»



Из чего состоит фабрика SD-Access?

Fabric Roles & Terminology

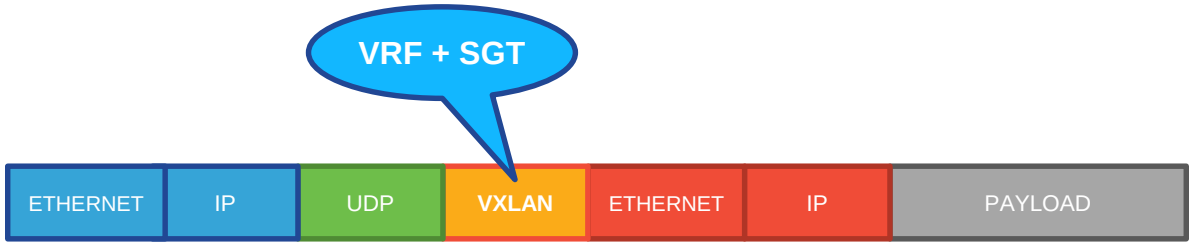


- **DNA Controller** – Enterprise SDN Controller (e.g. DNA Center) provides GUI management and abstraction via Apps that share context
- **Identity Services** – External ID System(s) (e.g. ISE) are leveraged for dynamic Endpoint to Group mapping and Policy definition
- **Analytics Engine** – External Data Collector(s) (e.g. NDP) are leveraged to analyze Endpoint to App flows and monitor fabric status
- **Control-Plane Nodes** – Map System that manages Endpoint to Device relationships
- **Fabric Border Nodes** – A Fabric device (e.g. Core) that connects External L3 network(s) to the SDA Fabric
- **Fabric Edge Nodes** – A Fabric device (e.g. Access or Distribution) that connects Wired Endpoints to the SDA Fabric
- **Fabric Wireless Controller** – A Fabric device (WLC) that connects Wireless Endpoints to the SDA Fabric

SD-Access Fabric

Key Components – CTS

1. **Control-Plane** based on **LISP**
2. **Data-Plane** based on **VXLAN**
3. **Policy-Plane** based on **CTS**

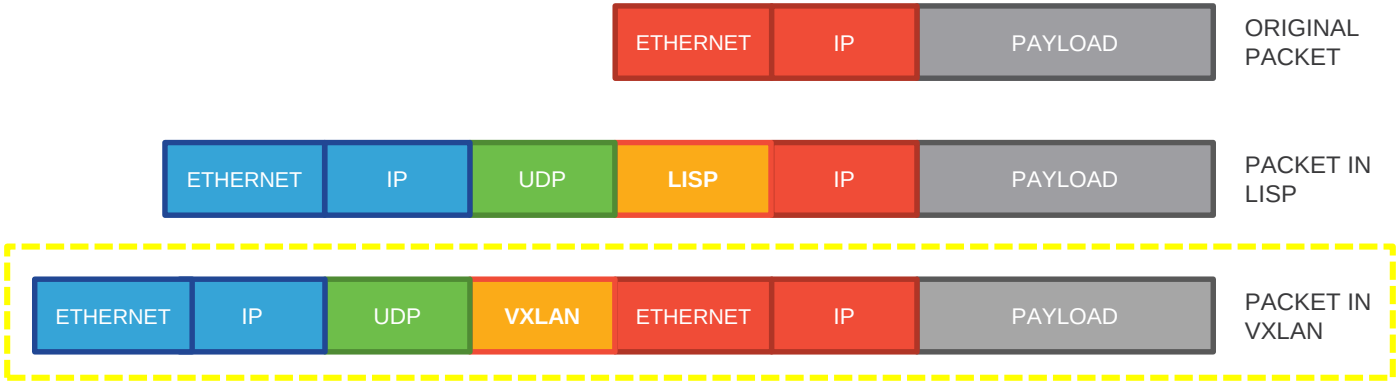


Virtual Routing & Forwarding
Scalable Group Tagging

SD-Access Fabric

Key Components – VXLAN

1. **Control-Plane** based on **LISP**
2. **Data-Plane** based on **VXLAN**

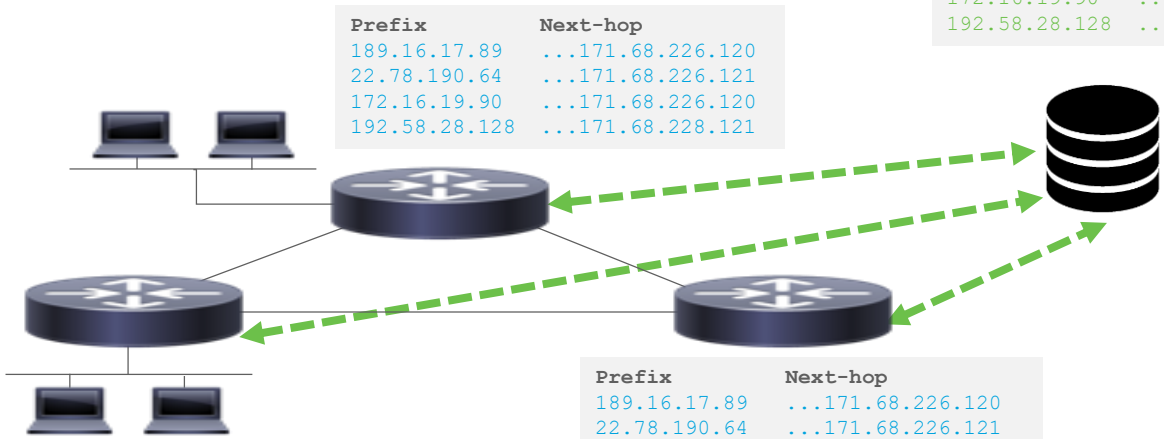


Масштабируемая маршрутизация LISP

LISP DB + Cache

- Меньше таблица и нагрузка CPU
- Разделение Identity и Location

Prefix	RLOC
192.58.28.128	...171.68.228.121
189.16.17.89	...171.68.226.120
22.78.190.64	...171.68.226.121
172.16.19.90	...171.68.226.120
192.58.28.128	...171.68.228.121
192.58.28.128	...171.68.228.121
189.16.17.89	...171.68.226.120
22.78.190.64	...171.68.226.121
172.16.19.90	...171.68.226.120
192.58.28.128	...171.68.228.121



Locator / ID Separation Protocol

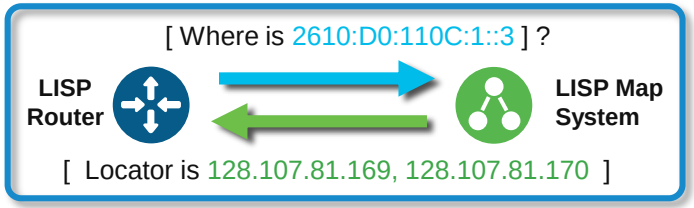
LISP Mapping System

LISP “Mapping System” по аналогии с DNS запросами

– DNS resolves **IP Addresses** for queried **Name** **Answers the “WHO IS” question**

DNS
Name -to- IP
URL Resolution

– LISP resolves **Locators** for queried **Identities** **Answers the “WHERE IS” question**



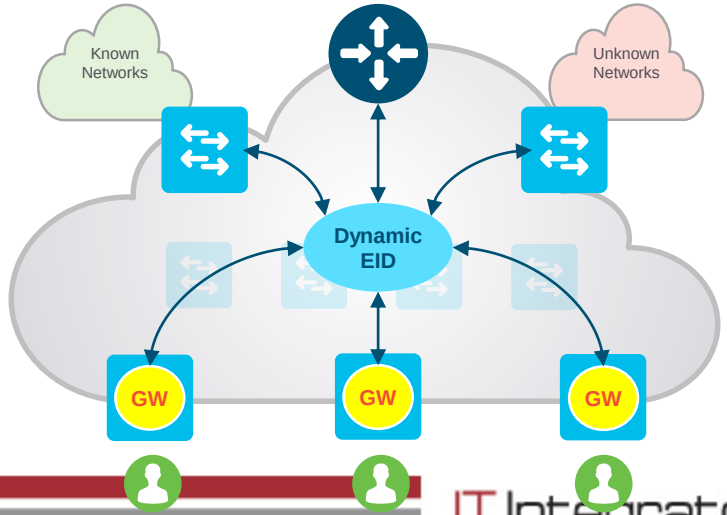
LISP
ID -to- Locator
Map Resolution

Campus Fabric

Endpoint ID Groups – A Closer Look

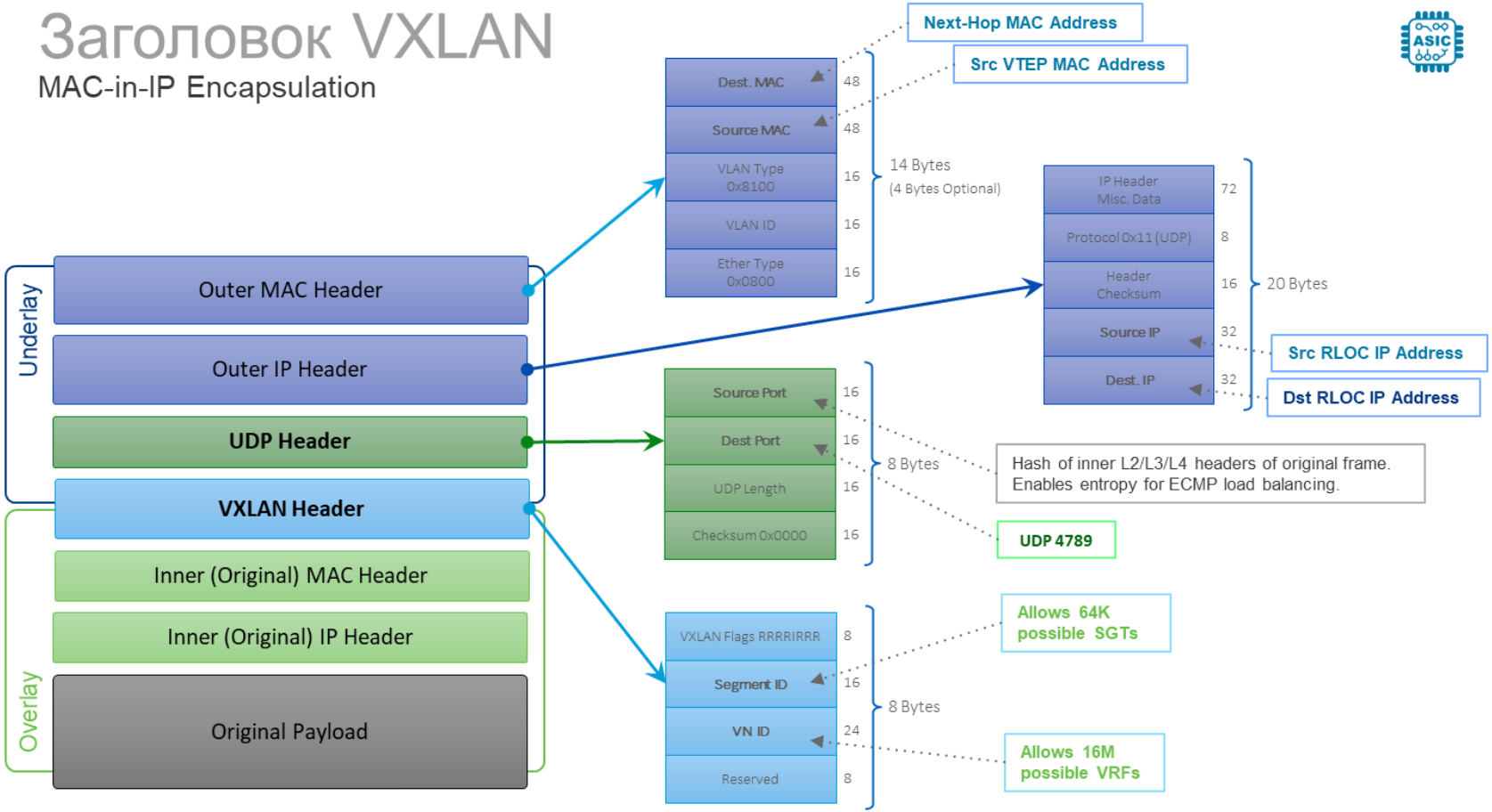
Stretched Subnets allow an IP subnet to be “stretched” via the overlay

- Host IP based traffic arrives on the local Fabric Edge SVI, and is then transferred by Fabric
- Fabric Dynamic EID mapping allows Host-specific (/32, /128, MAC) advertisement and mobility
- Host 1 connected to Edge A can now use the same IP subnet to communicate with Host 2 on Edge B.
- No longer need a VLAN to connect Host 1 and 2 for IP



Заголовок VXLAN

MAC-in-IP Encapsulation

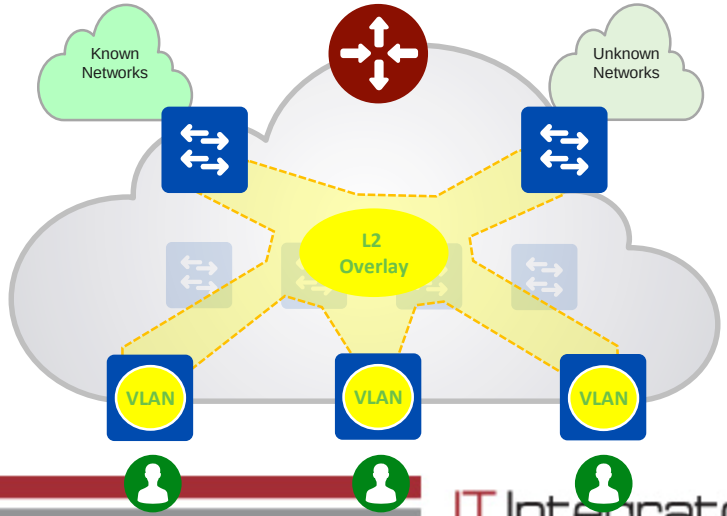


Campus Fabric

Endpoint ID Groups – A Closer Look

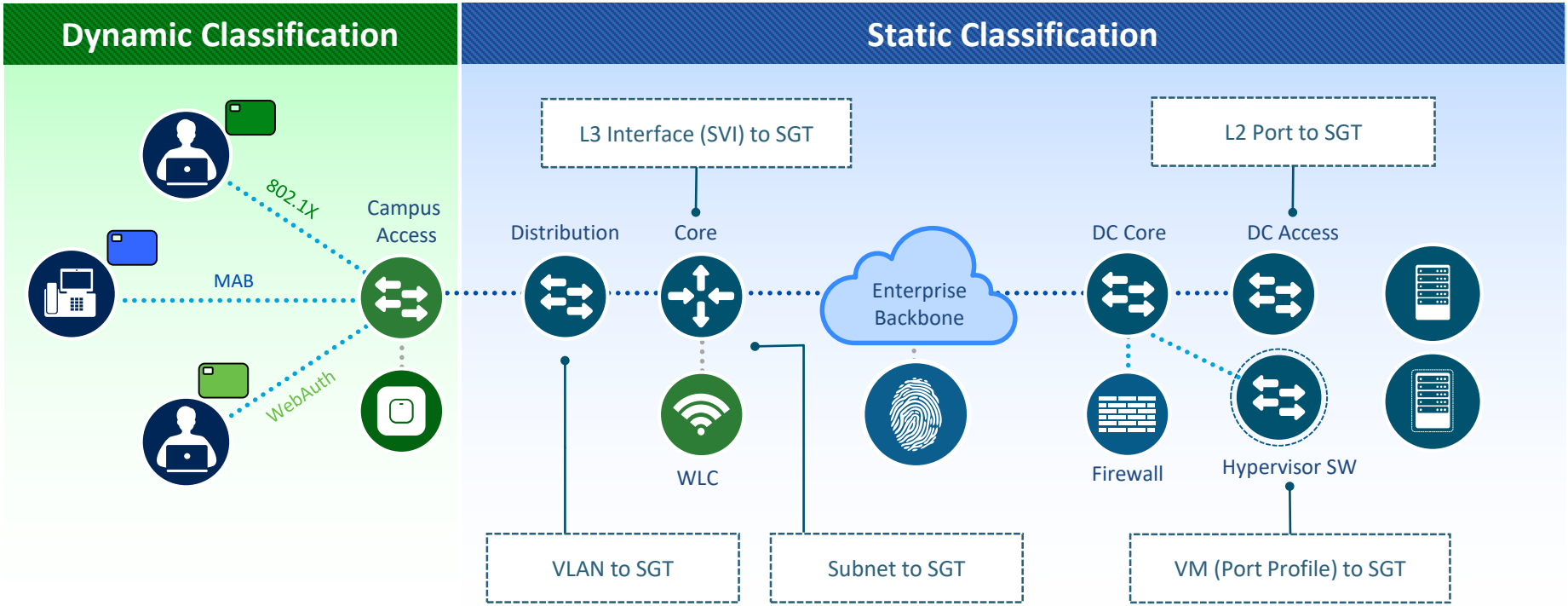
Layer2 Overlays allows Non-IP hosts to connect Broadcast & Multicast

- Similar principle and behavior as Virtual Private LAN Services (VPLS) P2MP Overlay
- Uses Multicast in the Underlay to setup a P2MP Tunnel between remote Fabric Edges.
- L2 Broadcast and Multicast traffic will be flooded to all connected Fabric Edges.
- Can be enabled for specific Host Pools that require L2 service (use Stretched Subnets for all others)



Cisco TrustSec

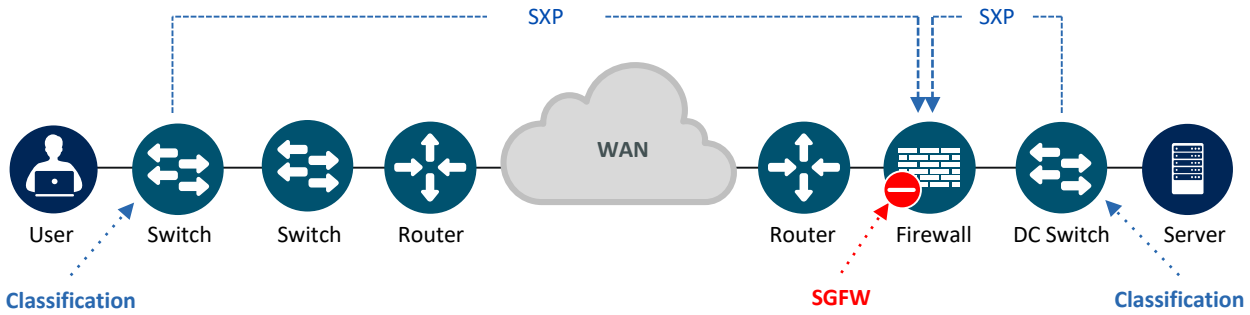
Два способа назначить SGT метку



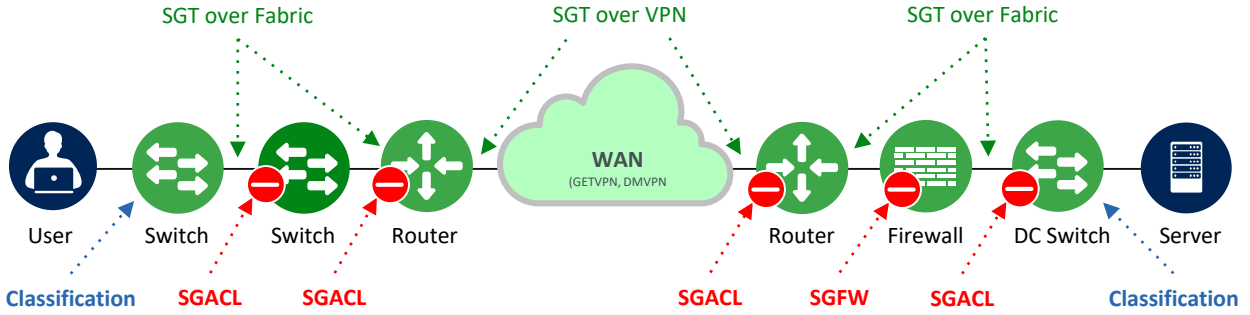
Cisco TrustSec

Распространение и применение политик CTS

Heterogeneous
L2 / L3 Networks



TrustSec Capable
L2 / L3 Networks

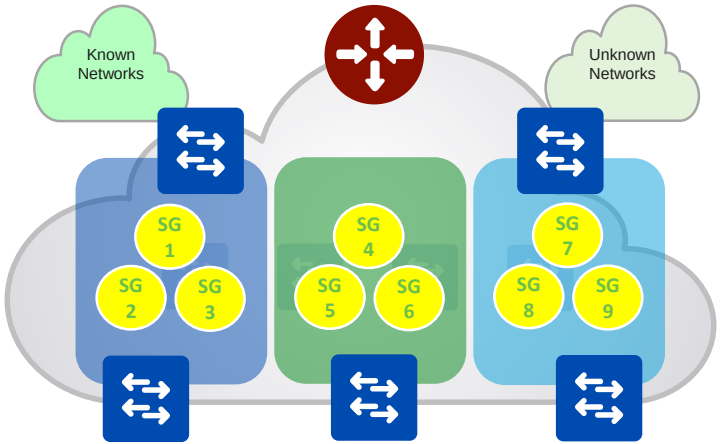


SD-Access Fabric

Scalable Groups – A Closer Look

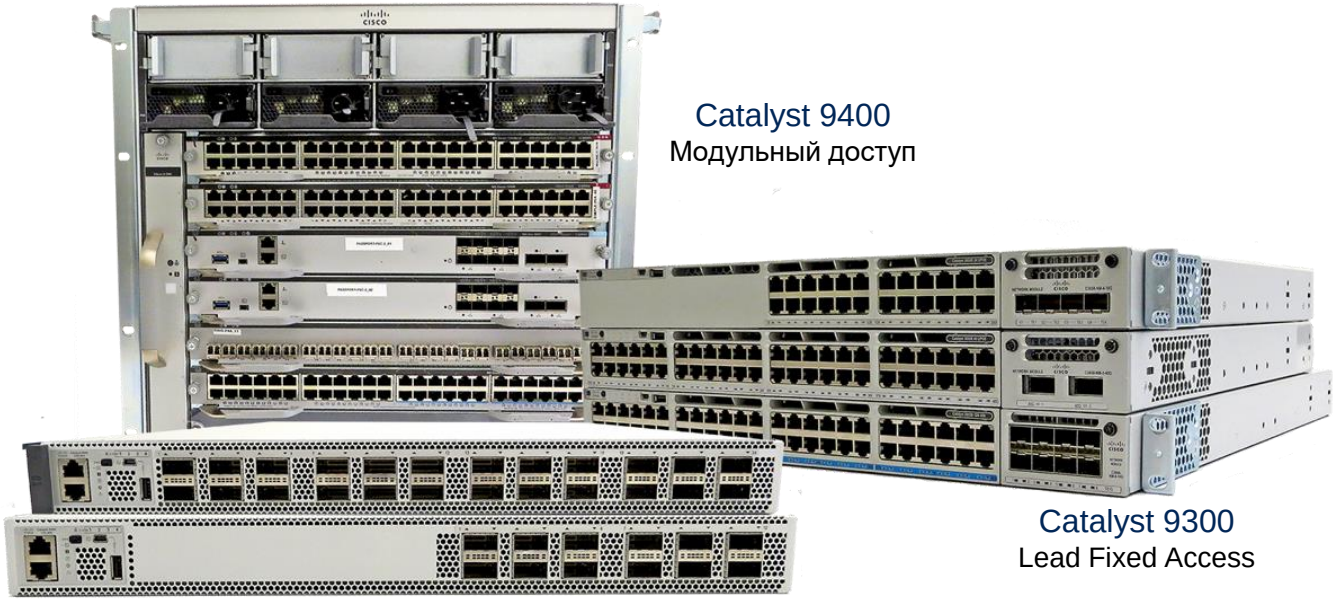
Scalable Group is a logical ID object to “group” Users and/or Devices

- CTS uses “Scalable Groups” to ID and assign a unique Scalable Group Tag (SGT) to Host Pools
- Nodes add SGT to the Fabric encapsulation
- CTS SGTs used to manage address-independent “Group-Based Policies”
- Edge or Border Nodes use SGT to enforce local Scalable Group ACLs (SGACLs)



SD-Access – где поддерживается?

Семейство коммутаторов Catalyst 9K



Catalyst 9400
Модульный доступ

Catalyst 9300
Lead Fixed Access

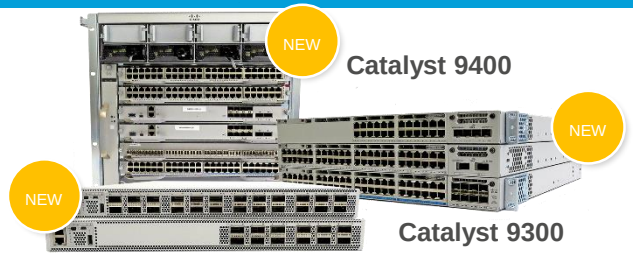
Catalyst 9500
Lead Fixed Core

- UADP 2.0
- Cisco IOS® XE Software
- SD-Access
- x86 CPU and containers
- Encrypted Traffic Analytics (ETA)*
- AES256/MACSEC256*
- Trustworthy systems
- StackWise® Virtual*
- IEEE1588 and AVB*
- NBAR2
- Perpetual/fast PoE
- Model-driven programmability
- Patching/GIR
- Streaming telemetry*

Единое ПО, возможности, лицензирование

SD-Access – поддержка на оборудовании

Switching

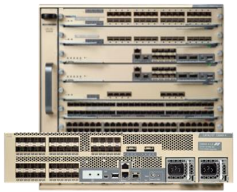


Catalyst 9400

Catalyst 9300

Catalyst 9500

Catalyst 4500E



Catalyst 6K

Nexus 7700

Catalyst 3850 and 3650

Routing

ASR-1000-X

ASR-1000-HX

ISR 4430

ISR 4450

CSRv

Wireless

AIR-CT5520

AIR-CT8540

Wave 2 Aps
(1800, 2800,3800)

Wave 1 Aps
(1700, 2700,3700)*

Subtended Nodes

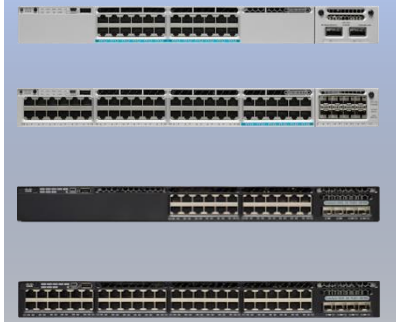
CDB

2960-CX
3560-CX

SD-Access – Edge Node

Подключение клиентов

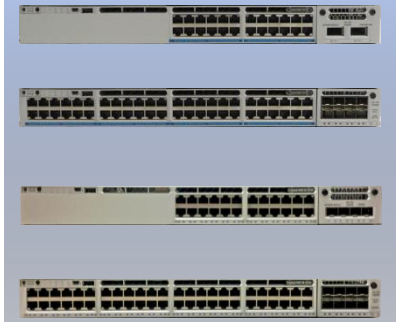
Catalyst 3K



- **Catalyst 3650/3850**
- 1/MGIG RJ45
- 10/40G NM Cards
- **IOS-XE 16.6.1+**

Catalyst 9300

NEW



- **Catalyst 9300**
- 1/MGIG RJ45
- 10/40G NM Cards
- **IOS-XE 16.6.1+**

Catalyst 4K

- **Catalyst 4500**
- Sup8E/9E (Uplinks)
- 4700 Cards (Down)
- **IOS-XE 3.10.1+**

Catalyst 9400

NEW

- **Catalyst 9400**
- Sup1E
- 9400 Cards
- **IOS-XE 16.6.1+**

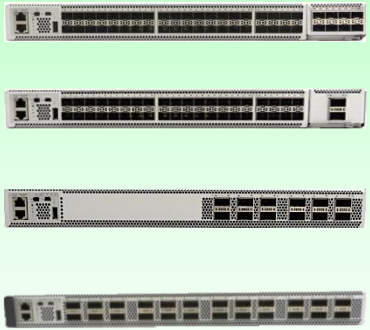
SD-Access – Control-Plane

Catalyst 3K

- **Catalyst 3850**
- 1/10G SFP+
- 10/40G NM Cards
- **IOS-XE 16.6.1+**

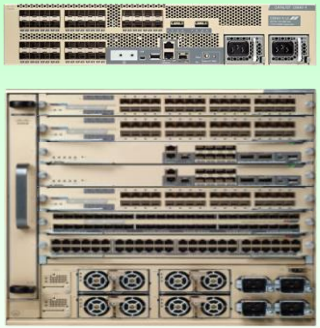
Catalyst 9500

NEW



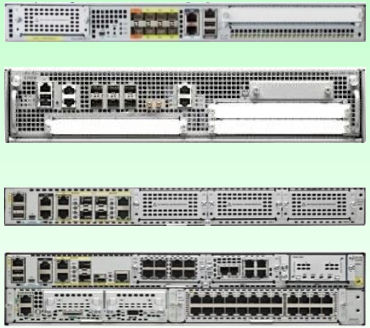
- **Catalyst 9500**
- 40G QSFP
- 1/10G NM Cards
- **IOS-XE 16.6.1+**

Catalyst 6K



- **Catalyst 6800**
- Sup2T/6T
- 6880-X or 6840-X
- **IOS 15.5.1SY+**

ASR1K & ISR4K

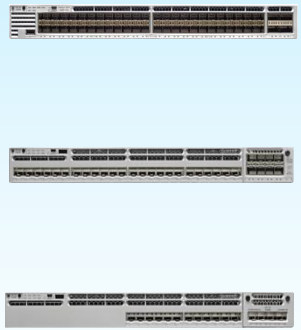


- **ASR 1000-X/HX**
- **ISR 4430/4450**
- 1/10G/40G
- **IOS-XE 16.6.1+**

SD-Access – Border Node

Интеграция с другими доменами

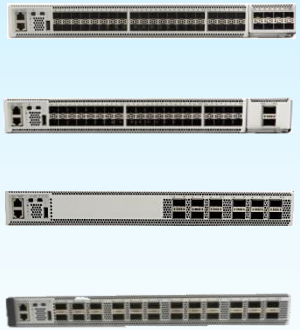
Catalyst 3K



- **Catalyst 3850**
- 1/10G SFP+
- 10/40G NM Cards
- **IOS-XE 16.6.1+**

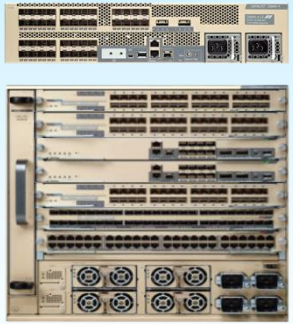
Catalyst 9500

NEW



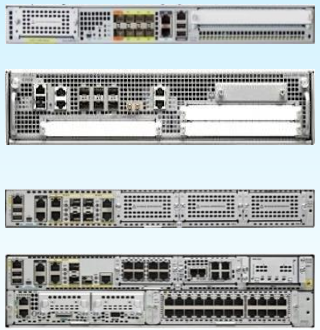
- **Catalyst 9500**
- 40G QSFP
- 10/40G NM Cards
- **IOS-XE 16.6.1+**

Catalyst 6K



- **Catalyst 6800**
- Sup2T/6T
- 6880-X or 6840-X
- **IOS 15.5.1SY+**

ASR1K & ISR4K



- **ASR 1000-X/HX**
- **ISR 4430/4450**
- 1/10G/40G
- **IOS-XE 16.6.1+**

Nexus 7K

- **Nexus 7700**
- Sup2E
- M3 Cards
- **NXOS 7.3.2+**

SD-Access – Fabric Wireless

Подключение беспроводных клиентов

5500 WLC	8500 WLC	Wave 2 APs	Wave 1 APs
			
• **AIR-CT5520** • No 5508 • 1G/10G SFP+ • **AireOS 8.5.1+**	• **AIR-CT8540** • No 8510 • 1G/10G SFP+ • **AireOS 8.5.1+**	• **1800/2800/3800** • 11ac Wave2 APs • 1G/MGIG RJ45 • **AireOS 8.5.1+**	• **1700/2700/3700** • 11ac Wave1 APs* • 1G RJ45 • **AireOS 8.5.1+**

Спасибо
за внимание!