



ния rld2
не
найдена
в файле.

Cisco Software Defined Access

Юрий Довгань
Systems Engineer
ydovgan@cisco.com



Содержание

1

Основные сложности в корпоративных сетях

Предпосылки для программно-управляемых сетей

2

Основные положения

Что такое SD-Access?

3

Построение фабрики

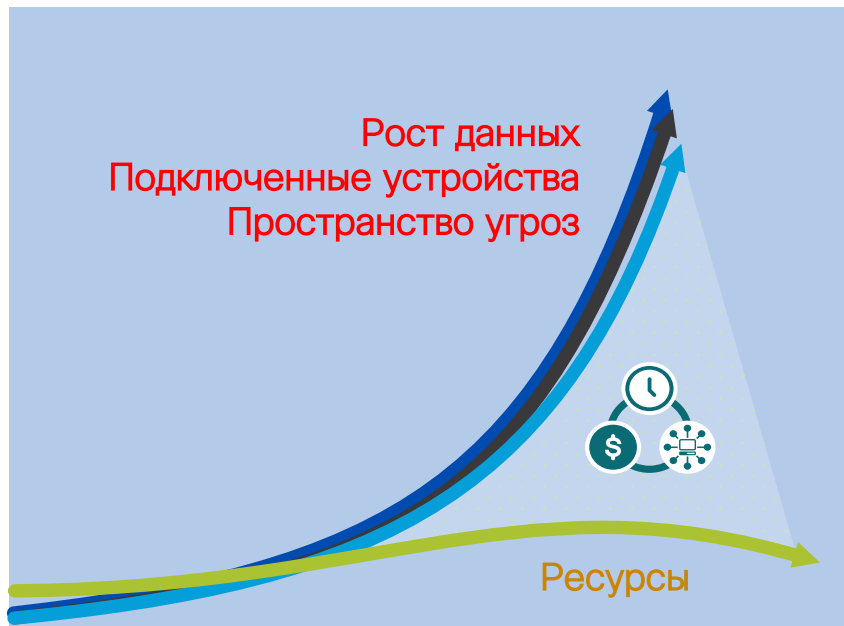
С чего начать?

4

Интегрируем беспроводную сеть

Зачем переходить с централизованной архитектуры на SDA?

Цифровая трансформация – вызов для IT



Тренды цифровой трансформации



Mobility

3.64

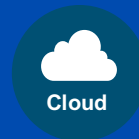
Устройства на
человека



IoT

7.5B

"Вещей"
подключено



Cloud

\$60B

Операционные
расходы на
поддержку сетей

Корпоративные сети сегодня – сложные ...



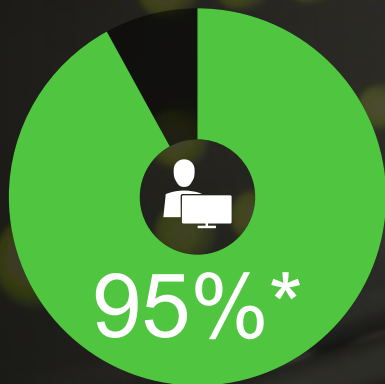
Управление
множеством VLAN

Работа с различными
сетями

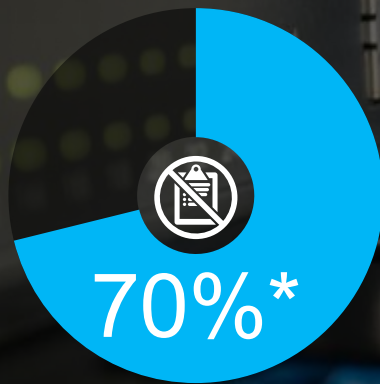
Работа с множеством
разных политик - LAN,
WLAN, WAN, ЦОД

Масштабирование
увеличивает сложность
эксплуатации

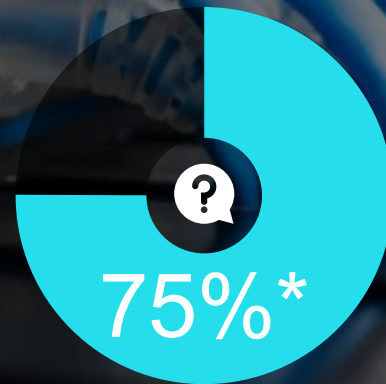
...и имеют множество эксплуатационных проблем



доля ручного труда при
внесении изменений



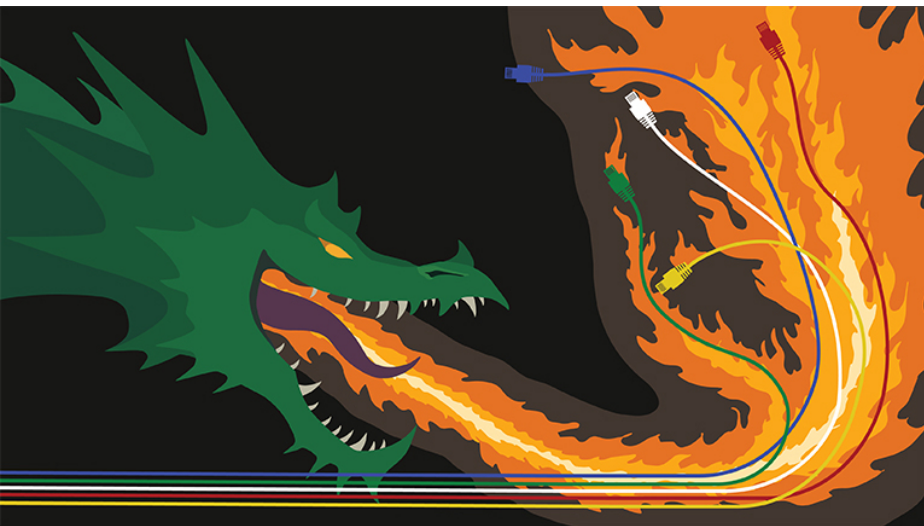
нарушений политик и
правил из-за
человеческих ошибок



Операционных расходов
приходится на поиск
неисправностей и диагностику

Традиционные сети НЕ ГОТОВЫ к быстрым темпам развития потребностей бизнеса

Июнь 2017. Nyetya. Он же Petya-A. Он же Не-Петя



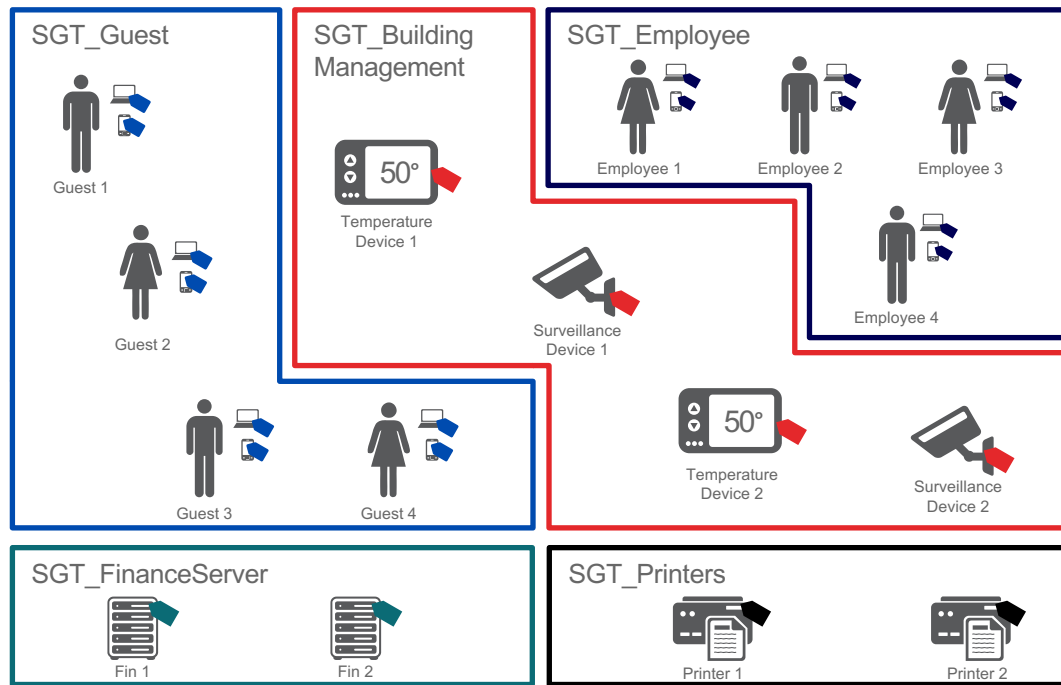
- Использовал доверенный канал бухгалтерского ПО для доставки в организации
- Использовал гибридную методологию распространения
- Шифровал файлы не с целью получения выкупа, а для нанесения урона

Расследование атаки от группы Cisco Talos – The MeDoc Connection

http://www.cisco.com/c/dam/global/ru_ua/solutions/security/ransomware/pdfs/cisco_blog_ransomware_attack_ua_upd4-graphics.pdf

Сегментация сети

- Для любых пользователей и устройств
- В качестве инструмента могут быть **любые сетевые устройства** (файерволы, коммутаторы, маршрутизаторы, WiFi...)



Микросегментация сети

Компьютеры в одной подсети не смогут заражать друг друга

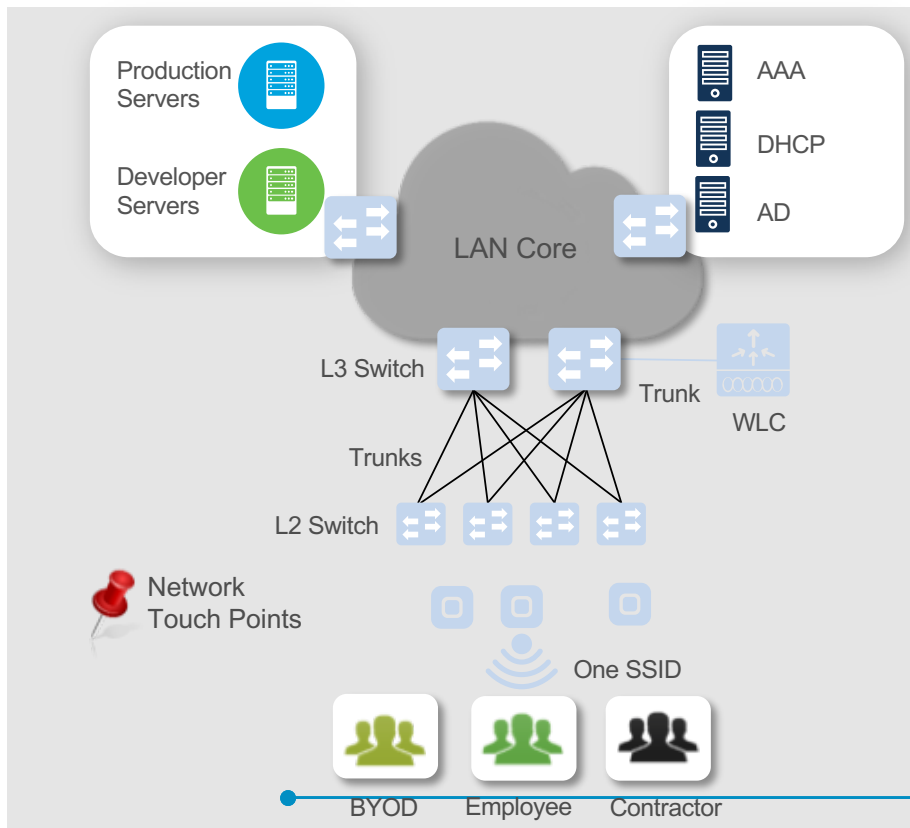


Сложности

- Сложность внедрения
- Сетевая сегментация
- Политики контроля доступа
- Подключение к сети пользователей и устройств
- Медленное устранение неполадок

Типичная проблема (пример на Wi-Fi сети)?

Групповая пользовательская политика - Сегодня



Customer requirements

- Three user Groups
- One single SSID
- Differentiated policies per Group
- Guest segmentation (wired and wireless)

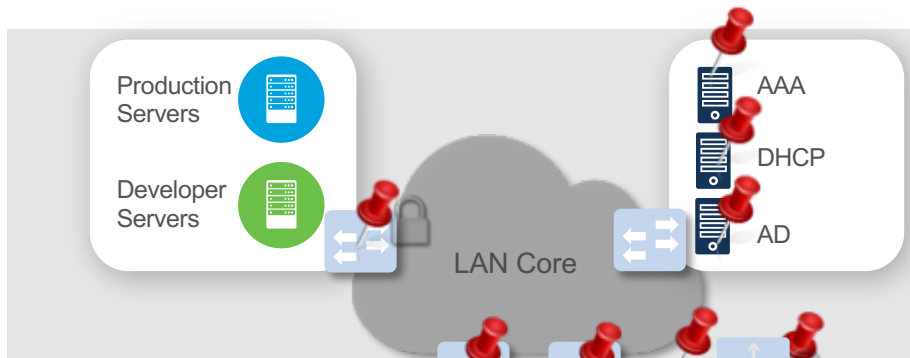
Customer Policy

- Customer Policy requirements:

	Production Serv.	Developer Serv.
Employee		
BYOD		
Contractor		

Типичная проблема (пример на Wi-Fi сети)?

Групповая пользовательская политика - Сегодня



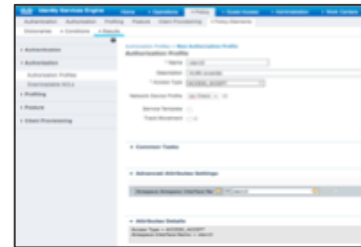
1. Define Groups in AD

2. Define Policies

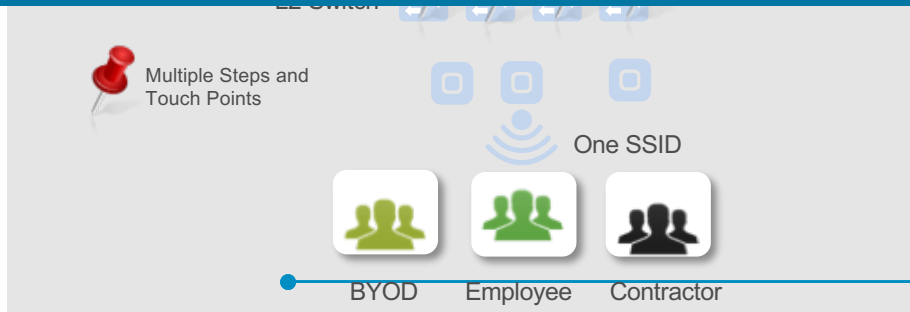
- VLAN/subnet based

3. Implement VLANs/Subnets

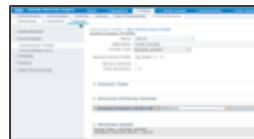
- Create VLANs
- Define DHCP scope
- Create subnets and L3 interfaces
- Routing for new subnets



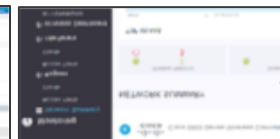
Что, если нам нужно добавить еще одну политику?



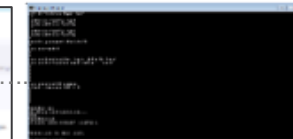
5. Many different User Interfaces



AAA



WLC



Devices CLI

Политики в корпоративных сетях

Модель политик сегодня

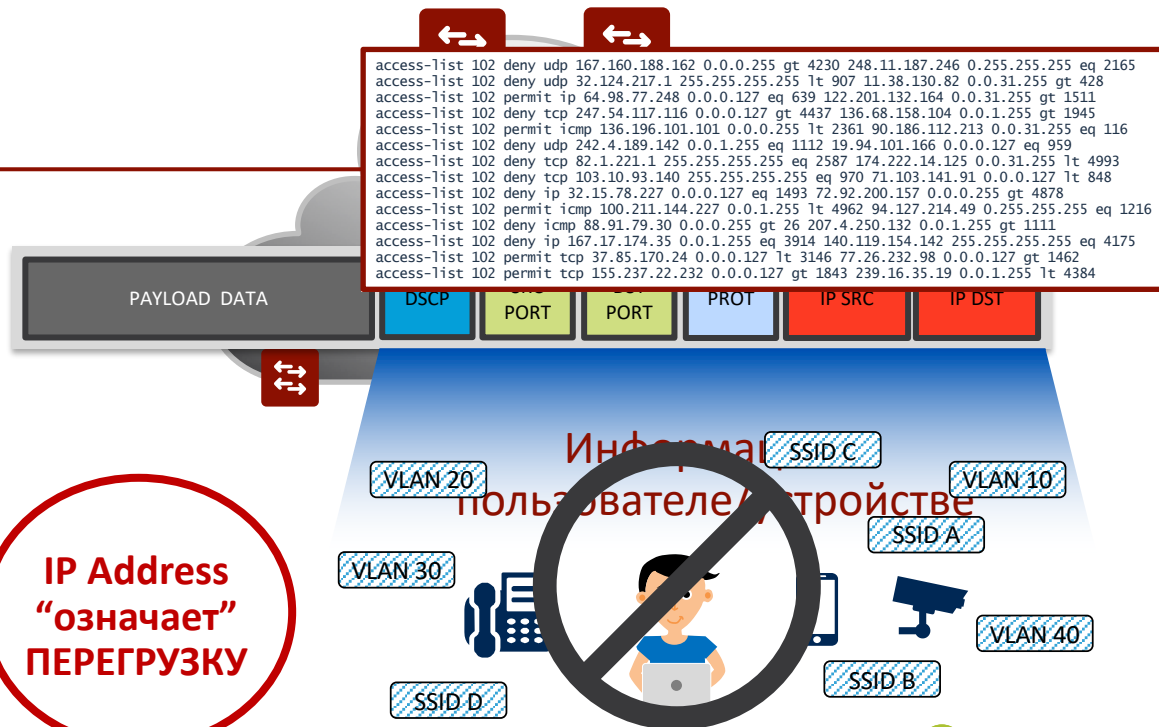
Сетевая политика



IP
АДРЕСА

- Находят тебя
- Определяют тебя
- Ограничивают тебя

IP Address
"означает"
ПЕРЕГРУЗКУ



Но что если ...

... мы можем сделать IP адрес только «**ЛОКАТОРОМ**», и обеспечить **другие методы группировать пользователей/ устройства для применения ПОЛИТИК?**

Основная идея

Если мы “уберем зависимость” между IP-адресацией и политикой, мы можем **существенно упростить** сети и сделать их **намного более функциональными**.

Мы сможем **строить наши сети** более простым способом ...

Внедрять **Политику независимо от сетевых конструкций** (VLAN, IP address)

Осуществлять **Сегментацию** (не применяя MPLS)

Обеспечивать **L2 и L3 гибкость** (без растягивания VLANов)

с помощью Фабрики

... мы можем сделать IP адрес только «**ЛОКАТОРОМ**», и обеспечить другие методы группировать пользователей/ устройства для применения ПОЛИТИК?

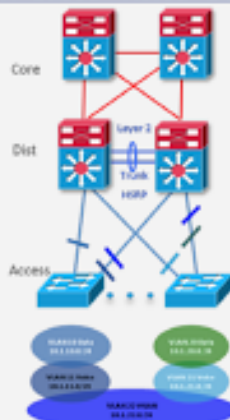
Основная идея

Если мы “уберем зависимость” между IP-адресацией и политикой, мы можем **существенно упростить** сети и сделать их **намного более функциональными**.

Software Defined Access: сетевая фабрика

Эволюция сетей

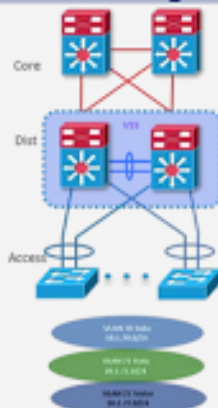
► STP based "Tiered" Design



Classic STP Limitation
50% of all Links not utilized
Complex to Harden

1999 - 2007

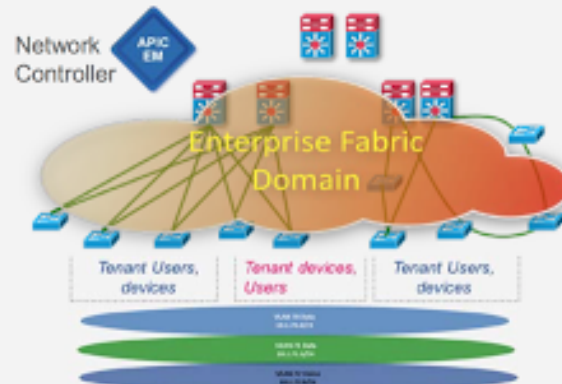
► VSS based Design



No STP Blocked Ports
Full Links Utilization, Faster Convergence
Proprietary two-way Fabric

2008 - 2016

► Standards based Programmable Fabric



No STP blocked ports, L2/L3-ECMP
Standards based programmable VxLAN for L2/L3 services
Automated Underlay with Group based Policies
Designed to handle 802.11ac wave2 and beyond speeds

2017 – next decade

Представляем Cisco Software Defined Access

Что если Вы сможете одновременно обеспечить...

- Сетевую микро- и макросегментацию (без использования MPLS и списков доступа ACL)
- Контроль доступа на основе ролей (без сквозной поддержки TrustSec на всех устройствах)
- Роуминг устройств (без смены IP адреса или расширения L2 домена)

И все это...

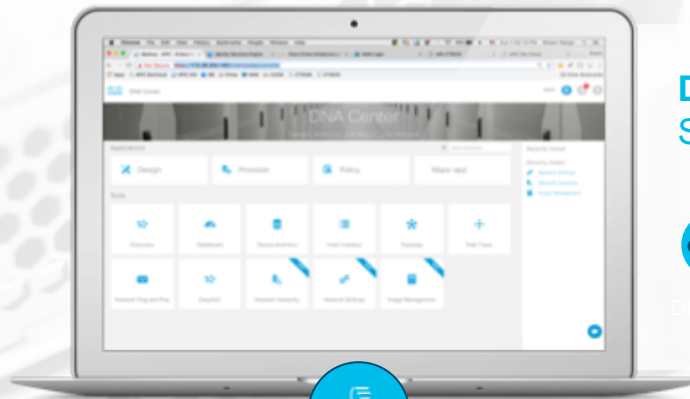
- Одновременно для проводных и беспроводных клиентов
- С автоматизацией внедрения и анализом состояния на основе открытых API
- С использованием простой и проверенной IP-маршрутизации во всей LAN сети

А еще...

- Вам больше не нужен будет Spanning-tree в LAN сети
- На границе сети будет полностью унифицированная конфигурация (с точностью до Loopback)
- А на устройствах ядра-распределения достаточно обычной маршрутизации

DNA Solution

Cisco Enterprise Portfolio



DNA Center Simple Workflows



DESIGN PROVISION POLICY MAPS



DNA Center



Identity Services Engine



Network Data Platform

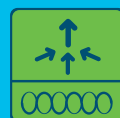
APIC-EM



Routers



Switches



Wireless Controllers



Wireless APs

Что такое сетевая фабрика?

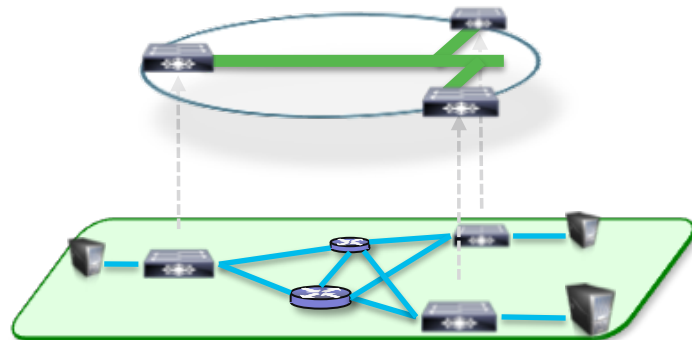
Сетевая фабрика: оверлей

Оверлей (overlay) – это *логическая топология*, используемая для виртуального соединения устройств, построенная **поверх** произвольной физической опорной (*underlay*) топологии.

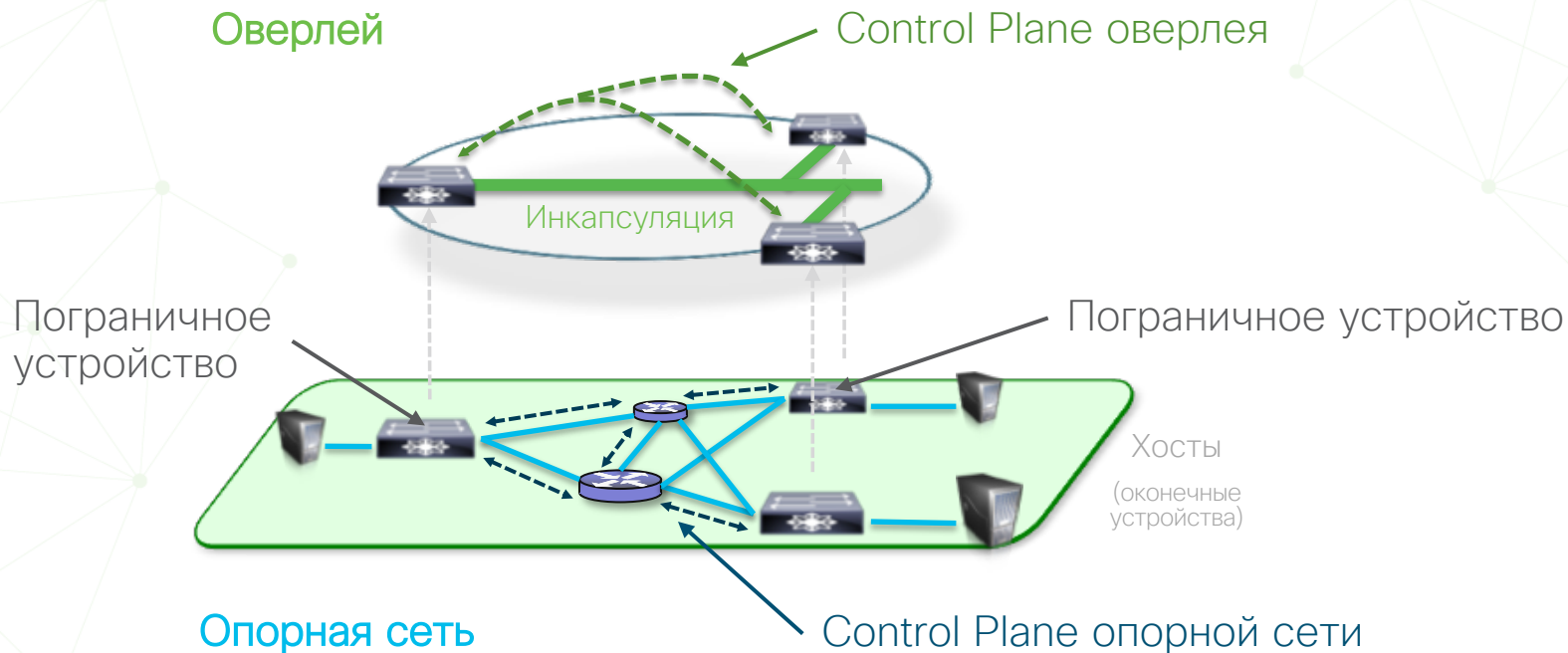
Оверлей часто использует *альтернативные атрибуты* для реализации **дополнительных сервисов**, не обеспеченных опорной топологией.

Примеры оверлеев

- | | |
|----------------|--------|
| • GRE, mGRE | • LISP |
| • MPLS, VPLS | • OTV |
| • IPSec, DMVPN | • DFA |
| • CAPWAP | • ACI |



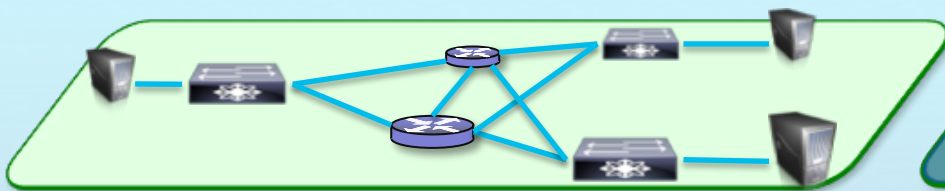
Сетевая фабрика: терминология



Что такое фабрика?

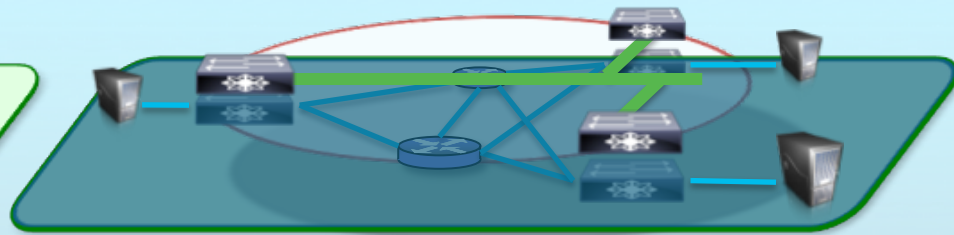
Почему “Overlay”

Разделение шин коммутации и сервисов



Простой транспорт

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

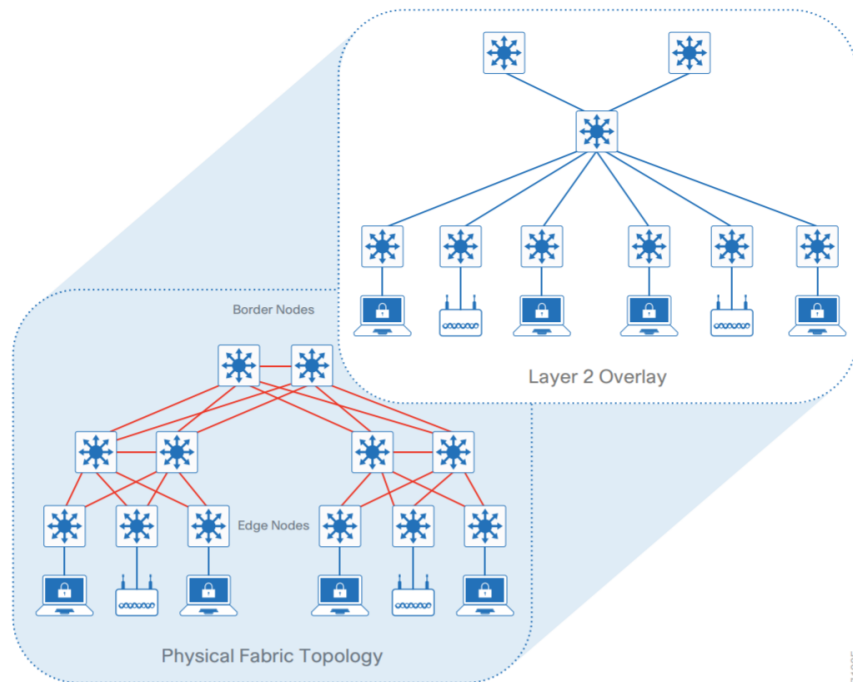


Гибкость виртуальных сервисов

- 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

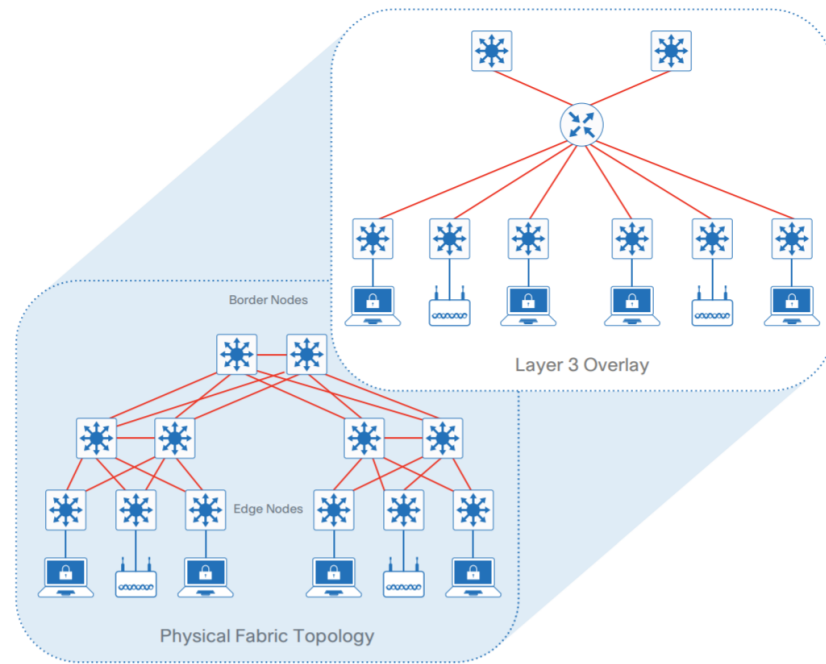
Оверлейный дизайн

Figure 1 Layer 2 overlay—connectivity logically switched



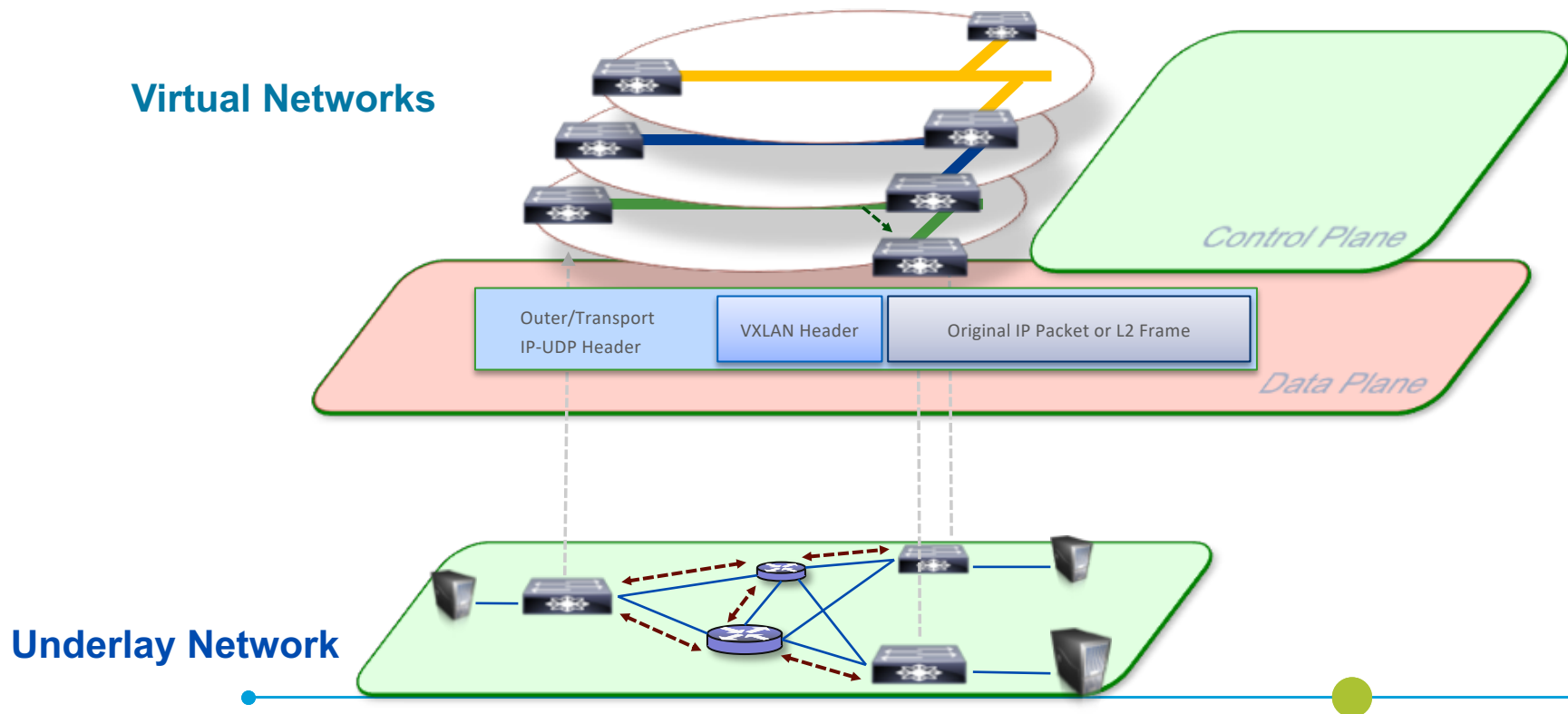
7103F

Figure 2 Layer 3 overlay—connectivity logically routed



7104F

Упрощение части сети до единой «фабрики»



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 на сервере (**DNA-C**)
- [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-2018JAN.pdf>

Какие особенности у SDA фабрики?

Основные компоненты



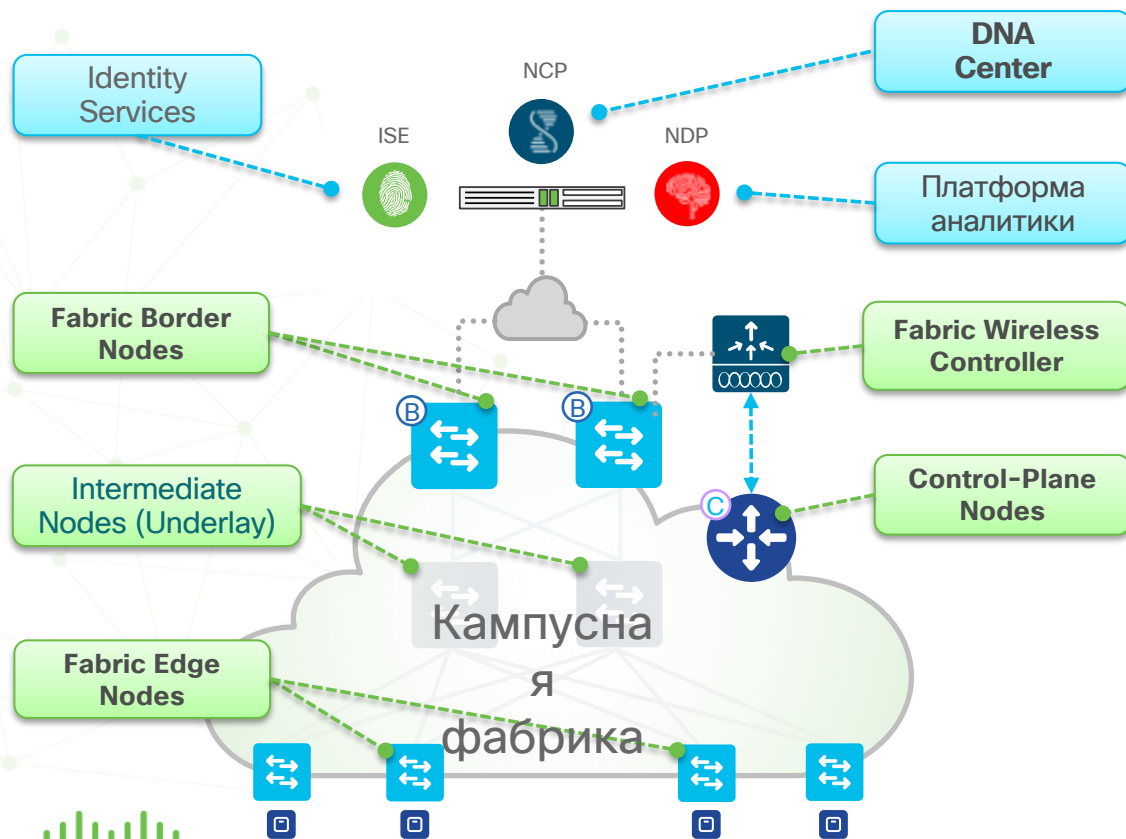
1. **Control-Plane based on LISP**
2. **Data-Plane based on VXLAN**
3. **Policy-Plane based on CTS and VRF**



Key Differences

- L2 + L3 Overlay -vs- L2 or L3 Only
- Host Mobility with Anycast Gateway
- Adds VRF + SGT into Data-Plane
- Virtual Tunnel Endpoints (No Static)
- No Topology Limitations (Basic IP)

SD-Access: роли устройств и терминология

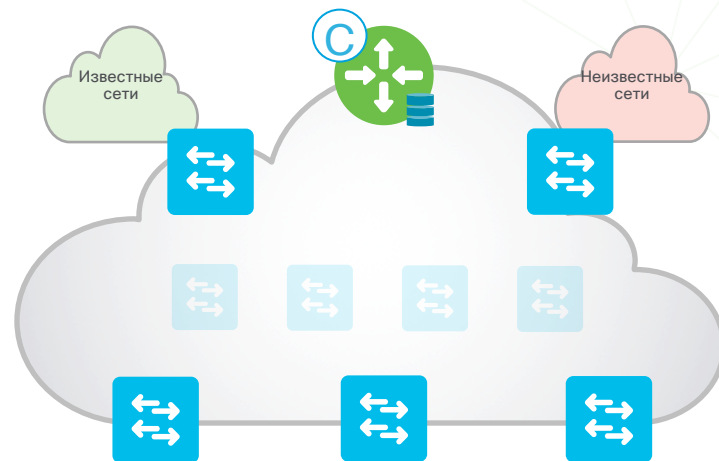


- **DNA Center** – корпоративный SDN-контроллер, обеспечивает GUI, управление и абстракцию сети через API
- **Identity Services** – сервер контроля доступа (ISE) для динамического назначения пользователей по группам и задания политик
- **Платформа аналитики** – реализует мониторинг фабрики, автоматизированный траблшутинг
- **Control Plane Nodes** – ведут учет соответствия клиентских устройств и Fabric Edge Nodes
- **Fabric Border Nodes** – обеспечивают подключение SDA фабрики к внешним сетям
- **Fabric Edge Nodes** – пограничные устройства, подключающие проводные клиентские устройства и точки доступа к фабрике
- **Fabric Wireless Controller** – контроллер БЛВС, работающий в режиме интеграции с фабрикой

Control Plane Nodes: обзор

Control-Plane Node ведут Host Tracking Database (HTDB) для централизованного хранения актуальной информации о местоположении клиентских устройств и префиксов

- Отвечает на вопрос, за какими Edge Nodes находится данный Endpoint ID или префикс?
- Поддерживает разные типы запросов (по адресам IPv4, IPv6 или MAC)
- HTDB получает сведения об Endpoint ID при подключении и/или роуминге от Edge, а также от Border Nodes для “известных” IP-префиксов
- Резолвит запросы от Edge и/или Border Nodes для определения местоположения искомых Endpoint IDs



Control Plane Nodes: элементная база

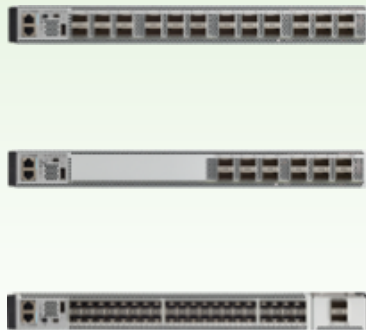
Catalyst 3K



- Catalyst 3850
- 1/10G SFP
- 10/40G NM Cards
- IOS-XE 16.6.2+

Catalyst 9K

NEW



- Catalyst 9500
- 10/40G SFP/QSFP
- 10/40G NM Cards
- IOS-XE 16.6.2+

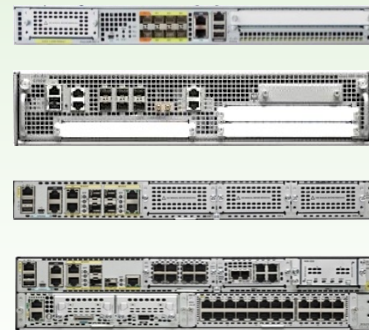
Catalyst 6K*

* Wired Only



- Catalyst 6800
- Sup2T/6T
- 6840/6880-X
- IOS 15.4.1SY4+

ASR1K, ISR4K & CSRv

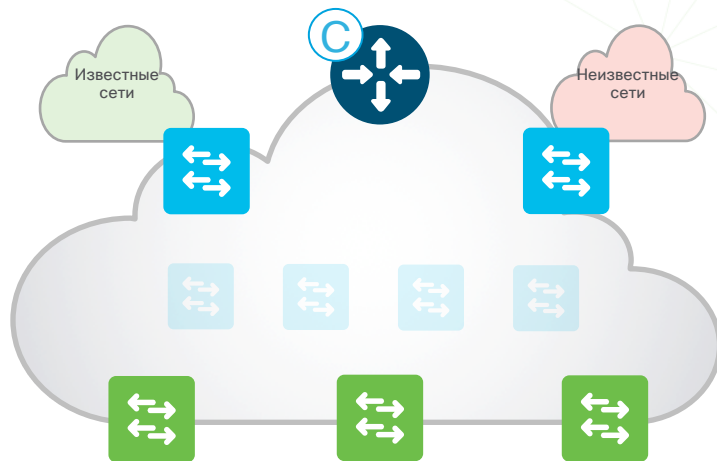


- CSRv 
- ASR 1000-X/HX
- ISR 4300/4400
- IOS-XE 16.6.2+

Edge Nodes: обзор

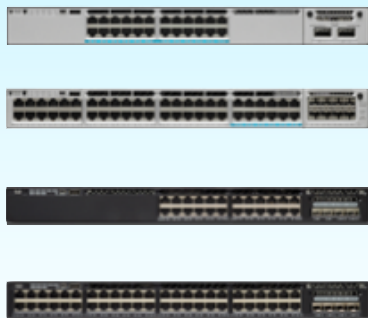
Edge Node обеспечивают подключение пользователей / устройств к фабрике

- Ответственны за применение политик (например, аутентификации/авторизации – статической, 802.1X, Active Directory)
- Регистрируют Endpoint ID (/32 или /128) на Control-Plane Node(s)
- Обеспечивают Anycast L3 Gateway для подключенных устройств (одинаковые IP-подсети на всех Edge nodes)
- Выполняют инкапсуляцию / декапсуляцию трафика для всех подключенных клиентских устройств



Edge Nodes: элементная база

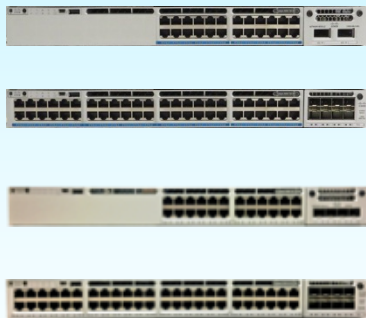
Catalyst 3K



- Catalyst 3650/3850
- 1/MGIG RJ45
- 10/40G NM Cards
- IOS-XE 16.6.3+

Catalyst 9K

NEW



- Catalyst 9300
- 1/MGIG RJ45
- 10/40/mG NM Cards
- IOS-XE 16.6.3+

Catalyst 4K



- Catalyst 4500
- Sup8E/9E (Uplink)
- 4700 Cards
- IOS-XE 3.10.1+

Catalyst 9400

NEW

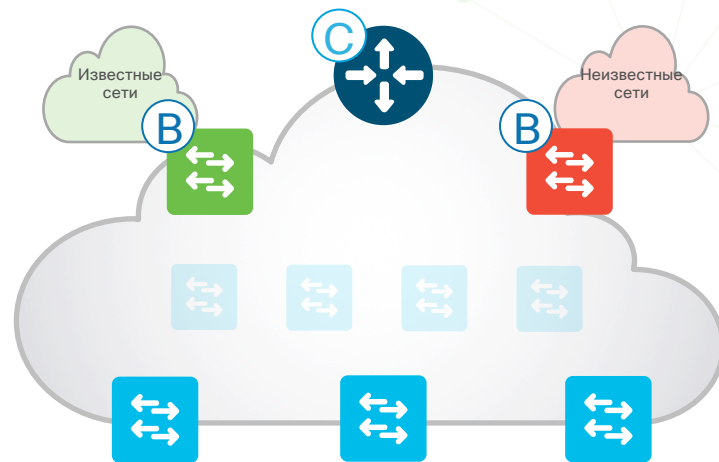


- Catalyst 9400
- Sup1E
- 9400 Cards
- IOS-XE 16.6.3+

Border Nodes: обзор

Border Node – это точки входа / выхода клиентского трафика в фабрику / из фабрики

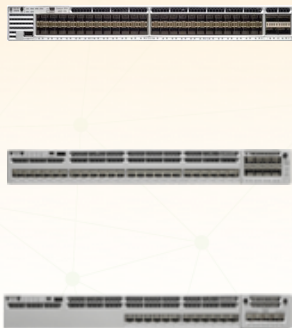
- Существует **2 типа Border Node!**
 - **Internal Border**
Применяются для “известных” маршрутов (как правило, внутри корпоративной сети)
 - **External (Default) Border**
Применяются для “неизвестных” маршрутов (интернет и / или публичные облака)
- А также совмещенная роль **Internal / External**



Border Nodes: элементная база

* External Border Only

Catalyst 3K



- Catalyst 3850
- 1/10G SFP+
- 10/40G NM Cards
- IOS-XE 16.6.3+

Catalyst 9K

NEW



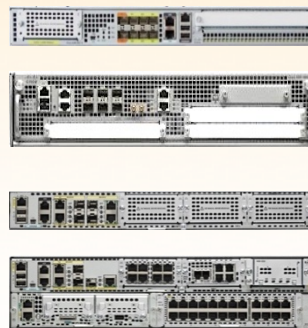
- Catalyst 9500
- 10/40G SFP/QSFP
- 10/40G NM Cards
- IOS-XE 16.6.3+

Catalyst 6K



- Catalyst 6800
- Sup2T/6T
- 6840/6880-X
- IOS 15.4.1SY4+

ASR1K & ISR4K



- ASR 1000-X/HX
- ISR 4430/4450
- 1/10G/40G
- IOS-XE 16.6.3+

Nexus 7K*



- Nexus 7700
- Sup2E
- M3 Cards
- NXOS 8.2.1+

Конструкции фабрики

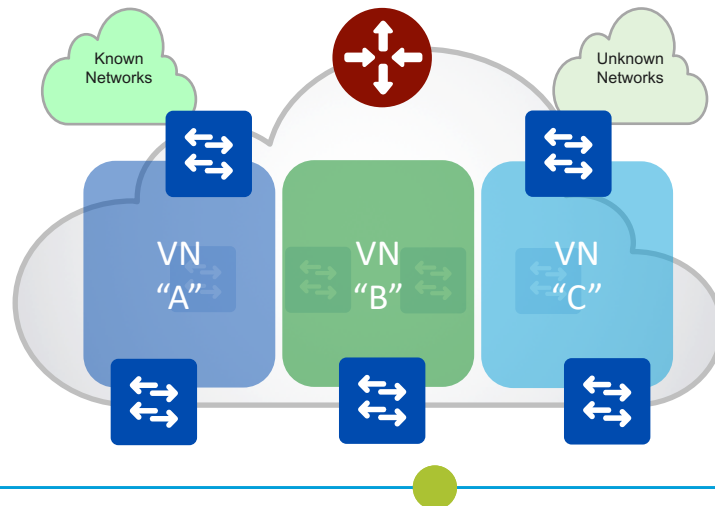
SD-Access Fabric

Virtual Network



Virtual Network: поддерживается отдельная Routing & Switching инстанция для каждой VN

- Control-Plane использует Instance ID для поддержки отдельных VRF топологий (“Default” VRF - Instance ID “4097”)
- Ноды добавляют VNID к инкапсуляции фабрики
- Endpoint ID префиксы (Host Pools) распространяются внутри одной (или более) Virtual Networks



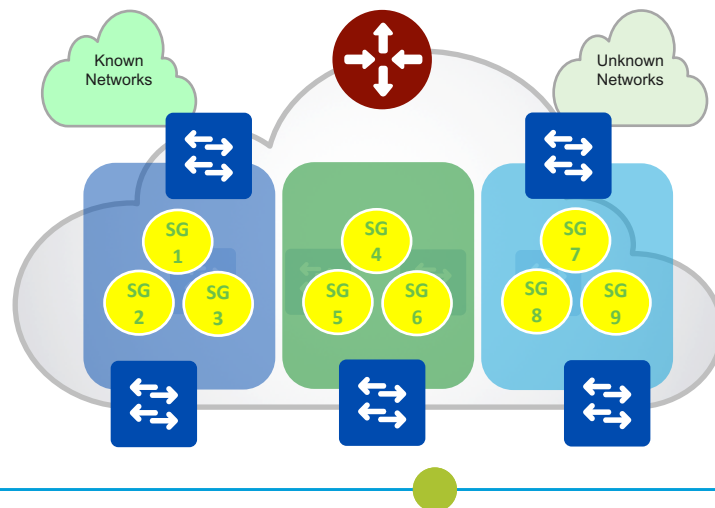
SD-Access Fabric

Scalable Groups



Scalable Group – логический идентификатор “группы” пользователей и/или устройств

- CTS использует “Scalable Groups” и назначает уникальный Scalable Group Tag (SGT) для Host Pool-ов
- Ноды добавляют SGT в инкапсуляцию фабрики
- CTS SGTs используются для управления независимых от адресов “групповых политик”
- Edge или Border ноды используют SGT для применения Scalable Group ACLs (SGACLs)



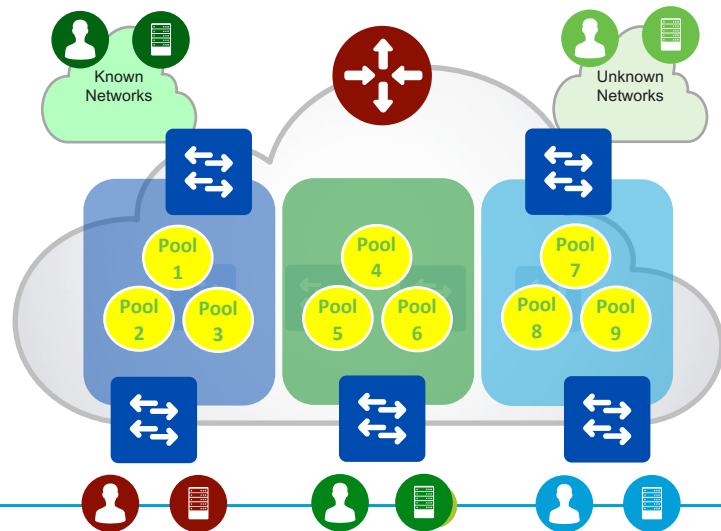
SD-Access Fabric

Host Pools



Host Pool provides basic IP functions necessary for attached Endpoints

- Edge Nodes use a Switch Virtual Interface (SVI), with IP Address /Mask, etc. per Host Pool
- Fabric uses Dynamic EID mapping to advertise each Host Pool (per Instance ID)
- Fabric Dynamic EID allows Host-specific (/32, /128, MAC) advertisement and mobility
- Host Pools can be assigned Dynamically (via Host Authentication) and/or Statically (per port)



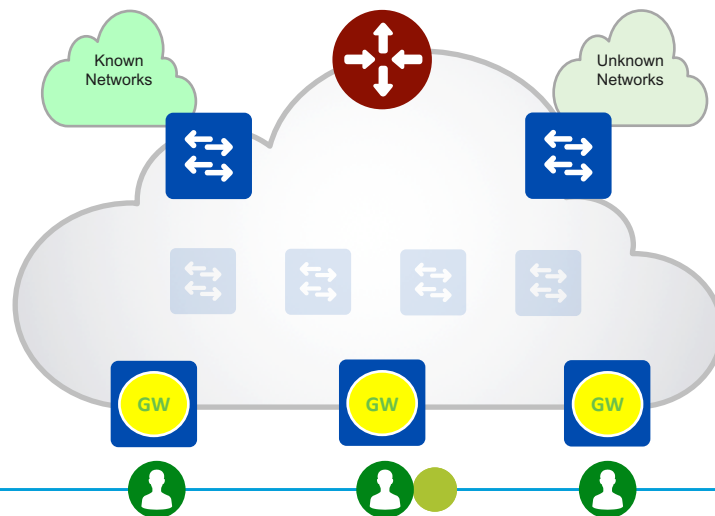
Campus Fabric

Virtual Network– A Closer Look



Anycast GW provides a single L3 Default Gateway for IP capable endpoints

- Similar principles and behavior as HSRP / VRRP with a shared Virtual IP and MAC address
- The same Switch Virtual Interface (SVI) is present on EVERY Edge, with the same Virtual IP and MAC
- Control-Plane with Fabric Dynamic EID mapping creates a Host (Endpoint) to Edge relationship
- If (when) a Host moves from Edge 1 to Edge 2, it does not need to change it's IP Default Gateway!



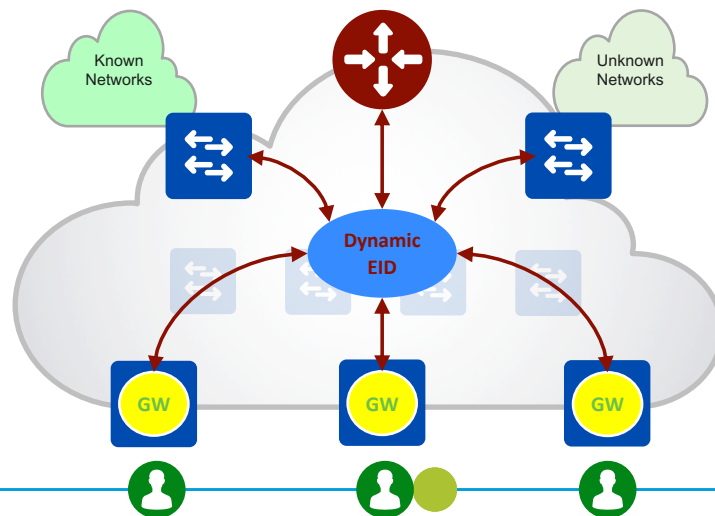
Campus Fabric

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





1. Control-Plane based on LISP



Key Differences

- L2 + L3 Overlay -vs- L2 or L3 Only
- Host Mobility with Anycast Gateway
- Adds VRF + SGT into Data-Plane
- Virtual Tunnel Endpoints (No Static)
- No Topology Limitations (Basic IP)

Locator / ID Separation Protocol

LISP Mapping System



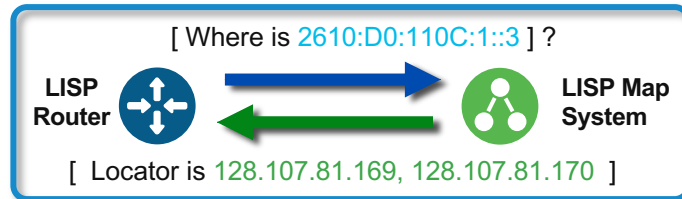
LISP “Mapping System” по аналогии с DNS запросами

- 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**



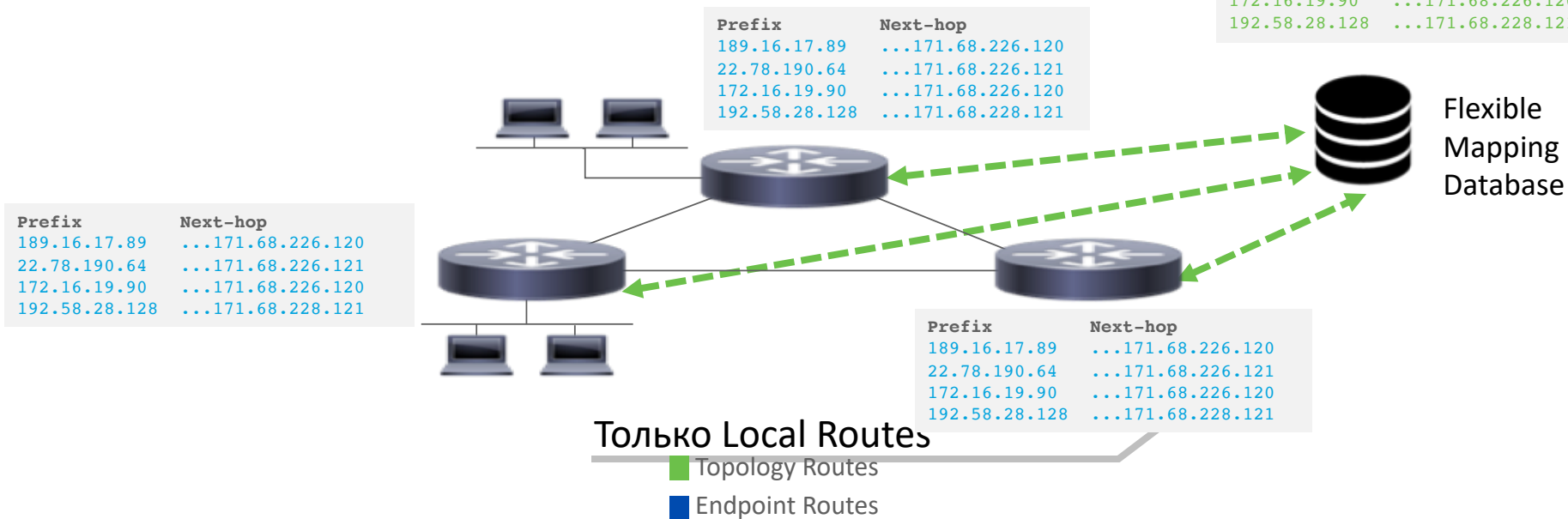
LISP
ID -to- Locator
Map Resolution

Масштабируемая маршрутизация LISP

LISP DB + Cache

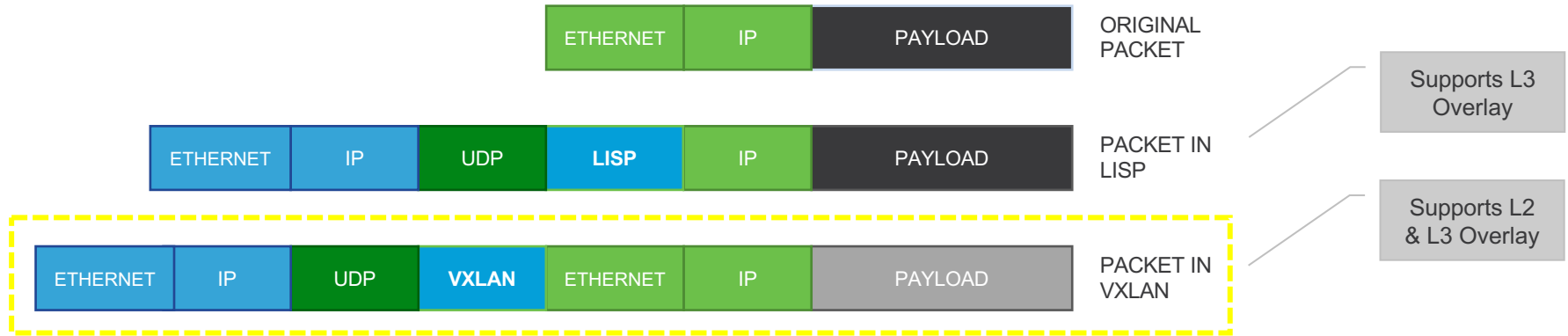
- **Меньше таблица и нагрузка CPU**
- **Разделение Identity и Location**

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



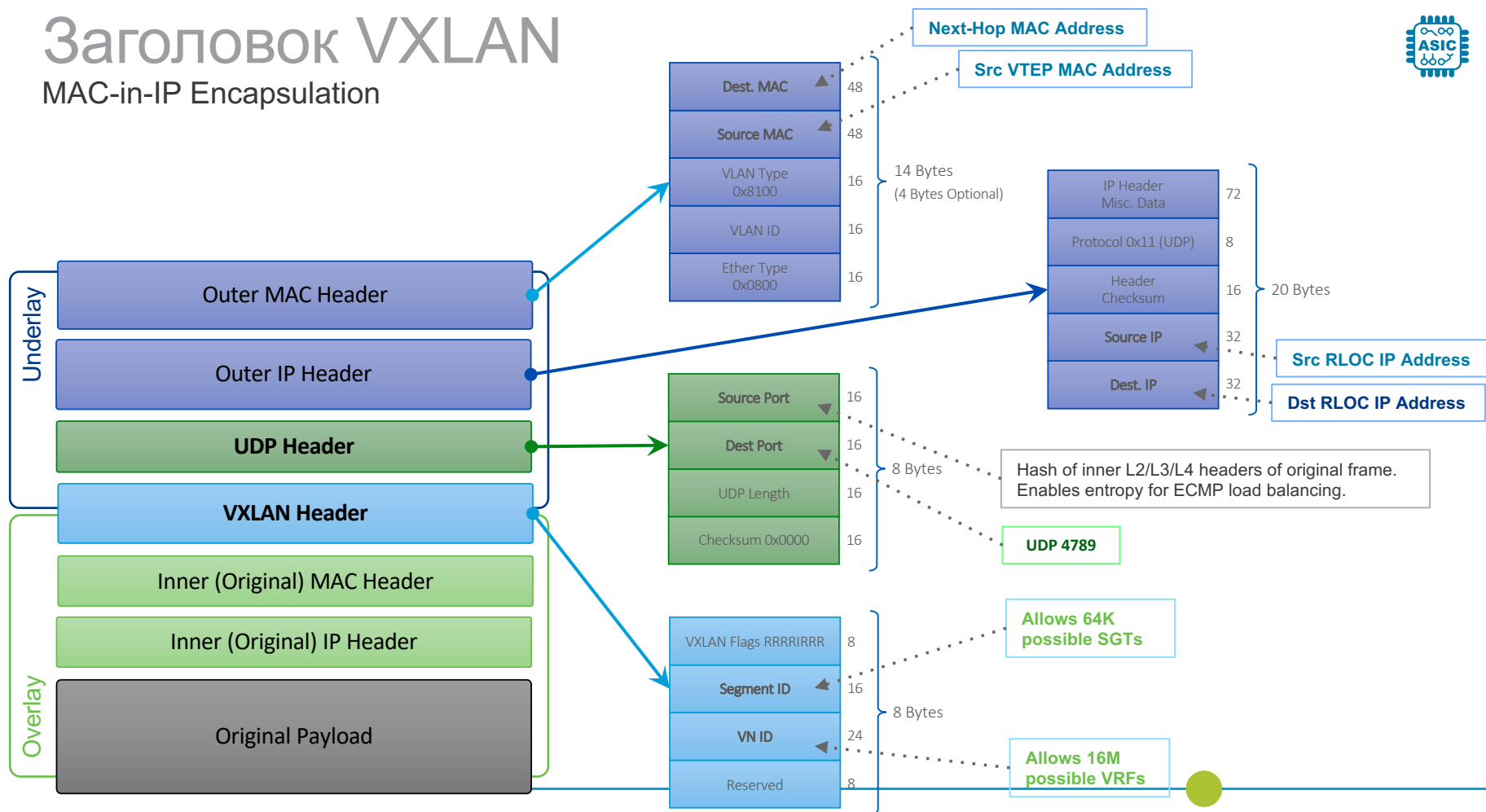


1. **Control-Plane based on LISP**
2. **Data-Plane based on VXLAN**



Заголовок VXLAN

MAC-in-IP Encapsulation



SD-Access Fabric

Key Components – CTS



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

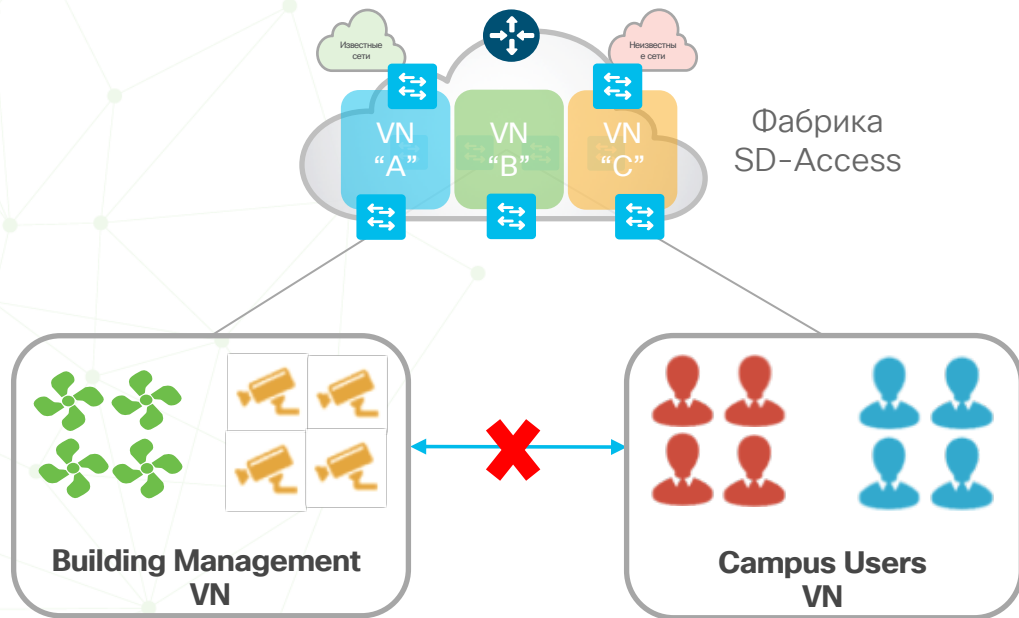


Virtual Routing & Forwarding
Scalable Group Tagging



Политики в SD-Access

Двухуровневая иерархия – макроуровень

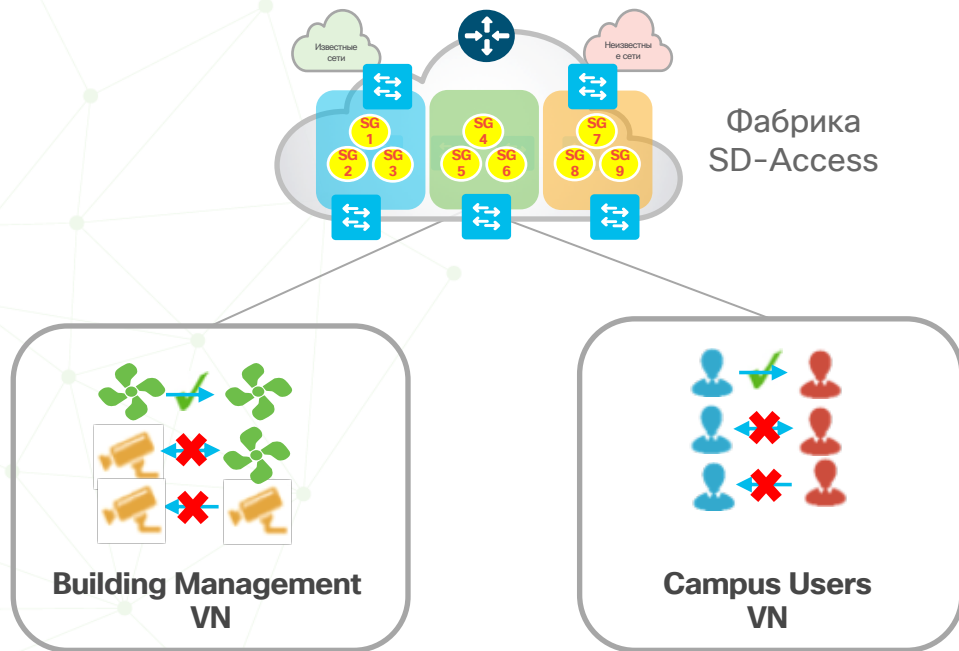


Virtual Network (VN)

Первый уровень сегментации **исключает взаимодействие** между виртуальными сетями. Возможность консолидировать много сетей в едином management plane.

Политики в SD-Access

Двухуровневая иерархия – микроуровень



Scalable Group (SG)

Второй уровень сегментации обеспечивает **контроль доступа на основе ролей** между двумя группами в пределах Virtual Network. Позволяет сегментировать сеть, например по направлениям бизнеса или функциям.

Кратко о Cisco TrustSec



Исполнение политик

Групповые политики
ACLs, Firewall Rules



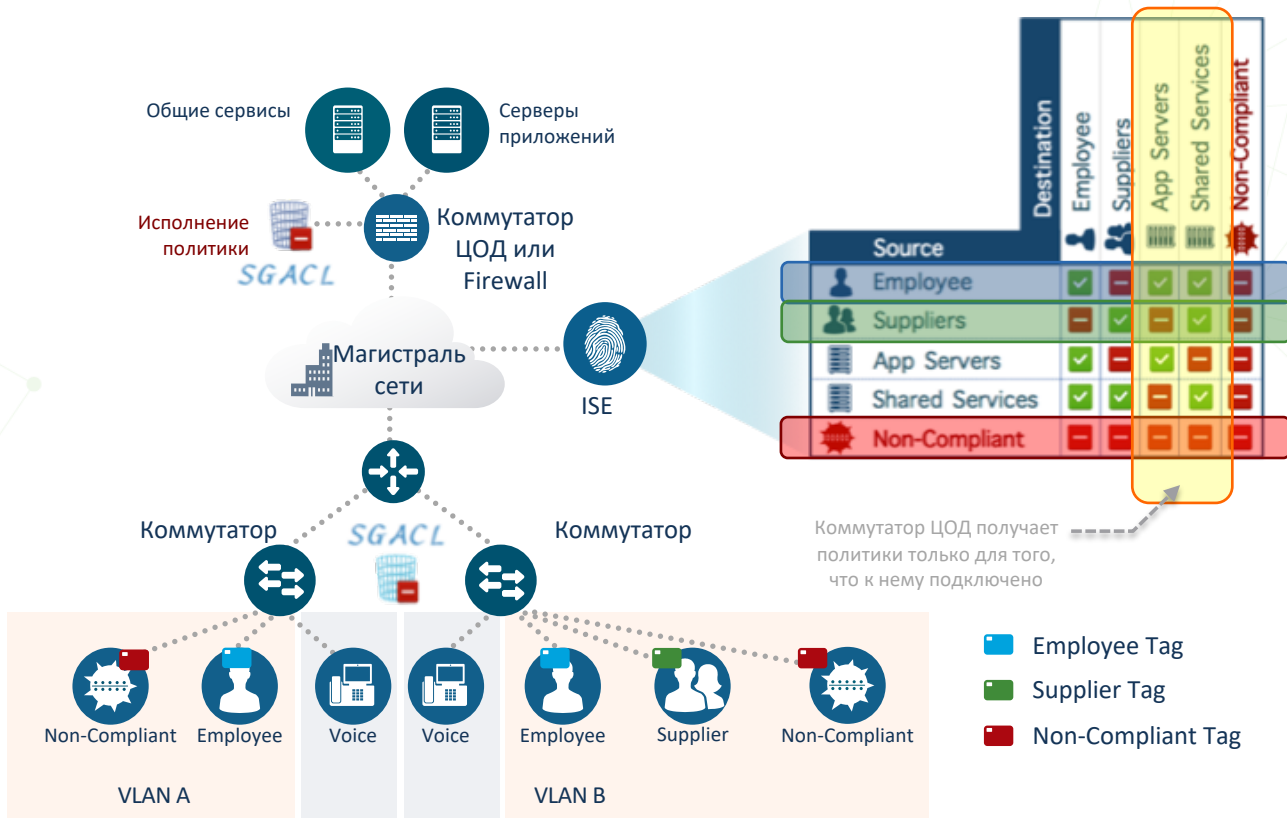
Распространение

Перенос
“группового”
контекста по сети с
помощью SGT



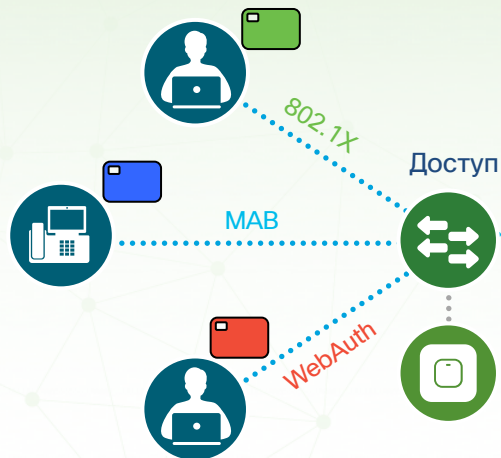
Классификация

Статическая или
динамическая
Назначения SGT

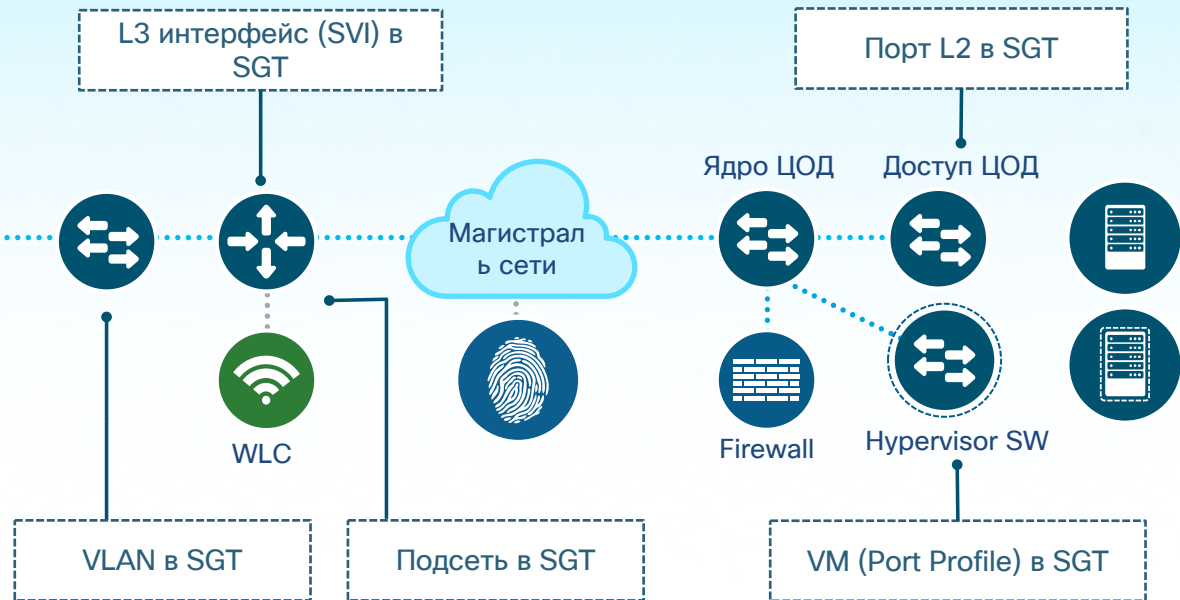


Назначение групп

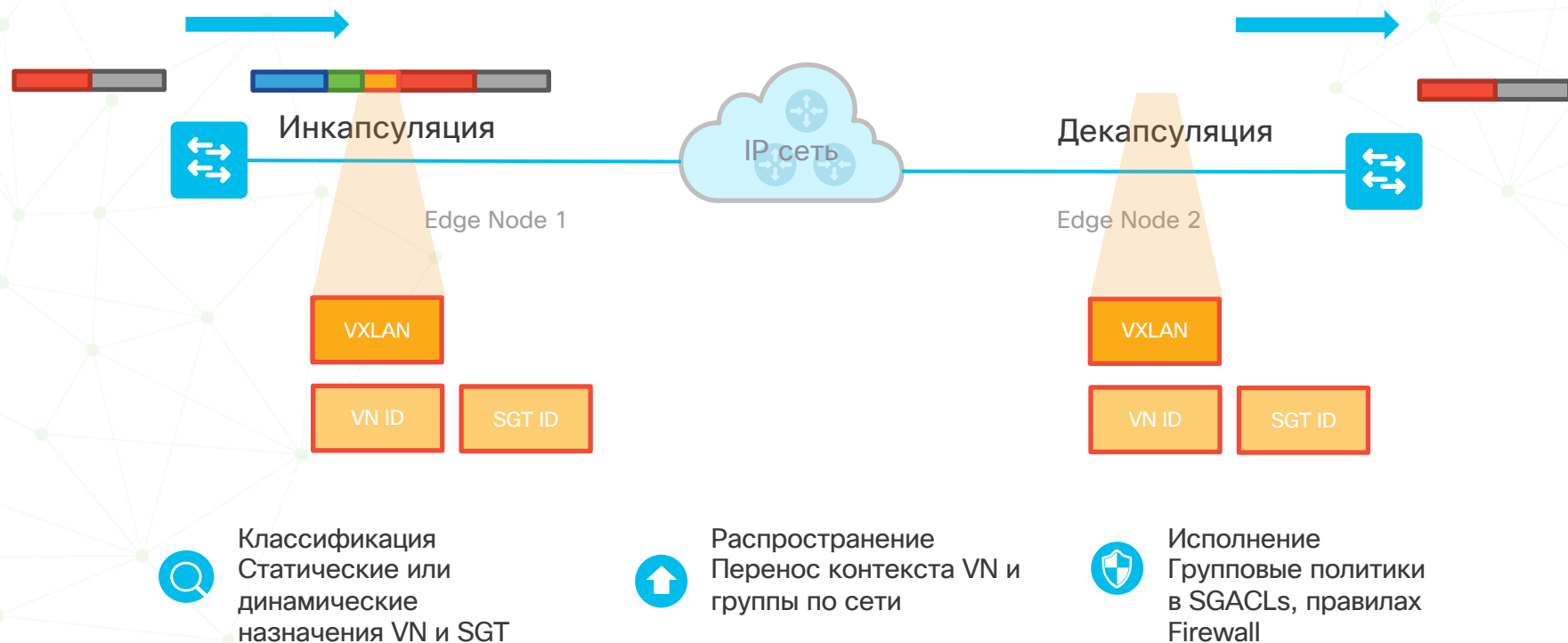
Динамическая классификация



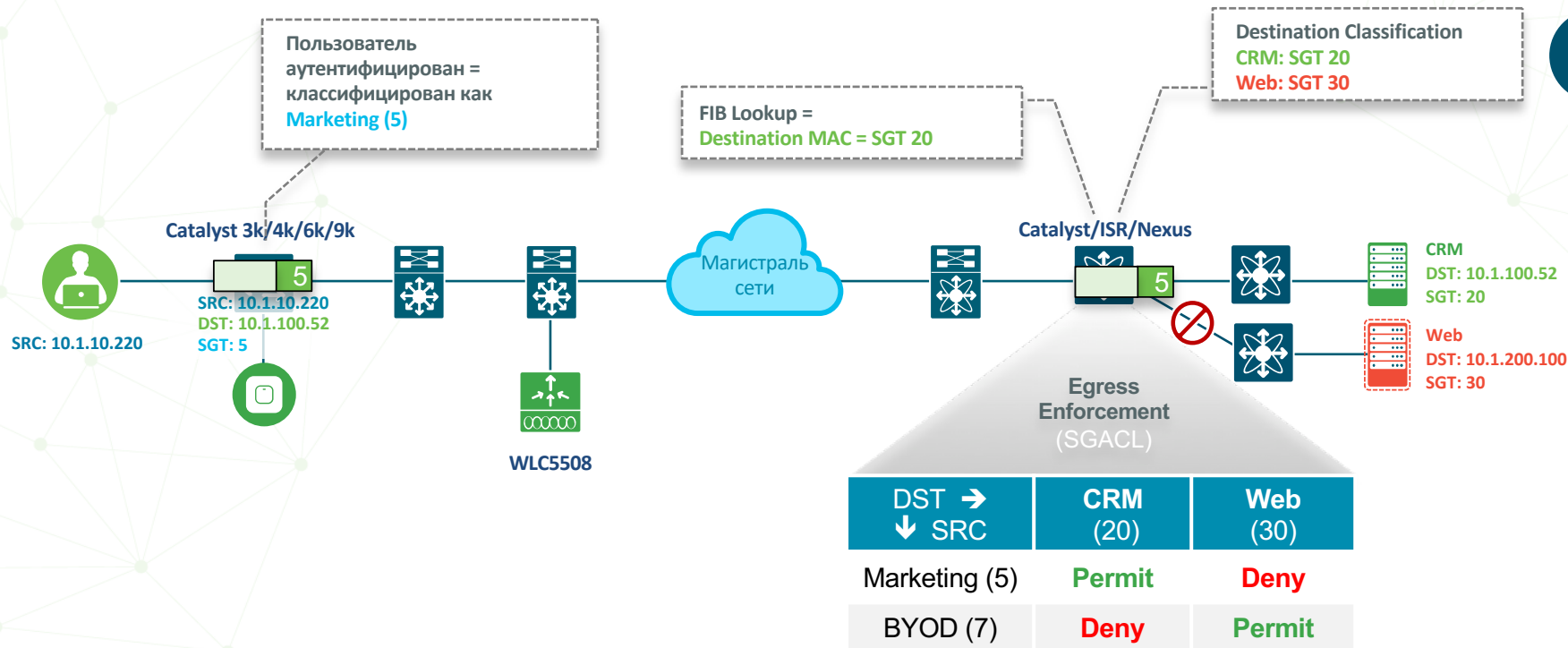
Статическая классификация



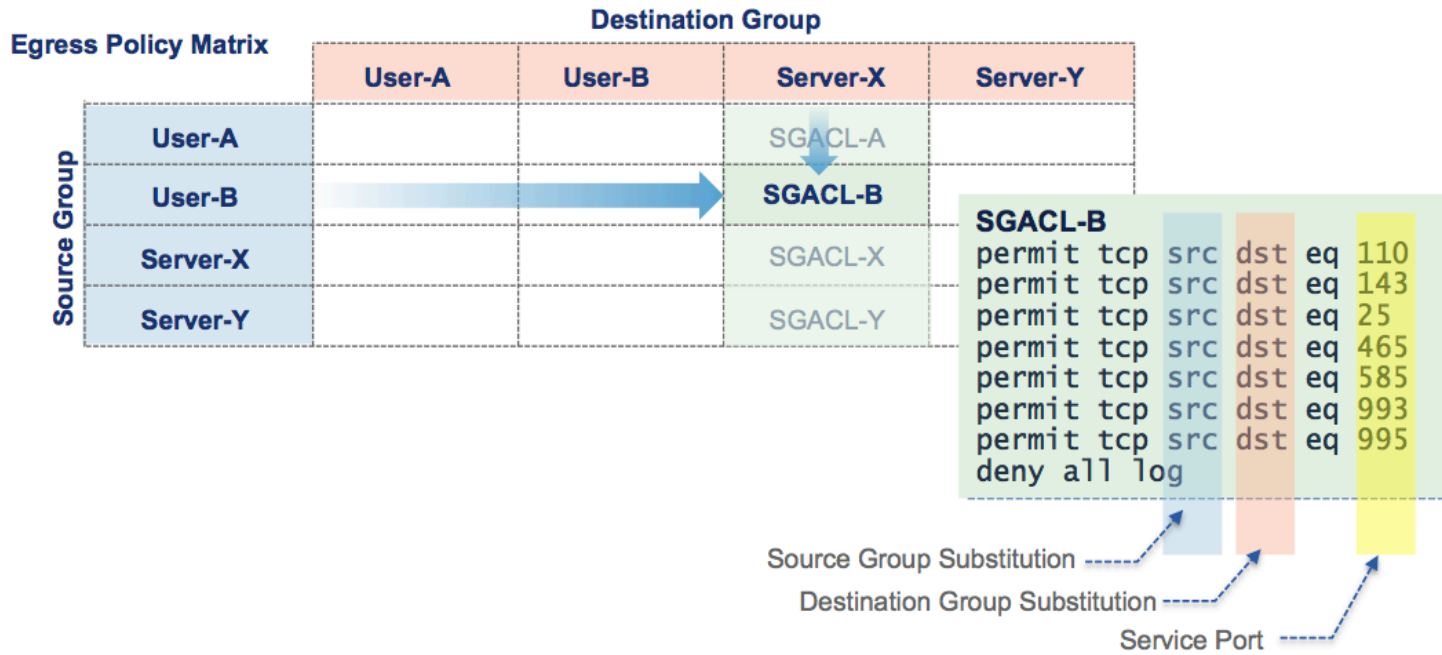
Перенос атрибутов политик по сети



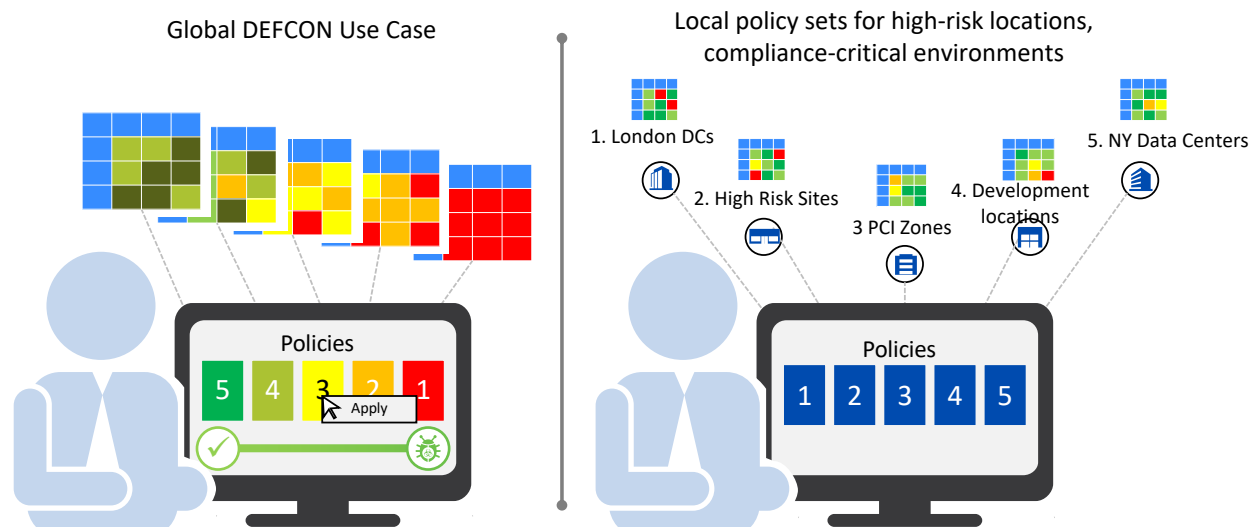
Пример: микросегментация в действии



Scalable Group Access Control Lists



Политики безопасности с учетом уровня угрозы



DEFCON (аббревиатура, англ. *DEFense readiness CONdition* — готовность обороны) — шкала готовности вооружённых сил Соединённых Штатов Америки. Стандартный протокол в мирное время — DEFCON 5. DEFCON 1 соответствует ожиданию немедленной полномасштабной атаки

Политики DefCon для сети



Multiple levels of
policy sets
Applied globally

Standard Policy

Source	Destination							
	LoB 1 Employee	LoB 2 Employee	Partner 1	Partner 2	PCI Server	Shared Apps	LoB 1 Apps	LoB 2 Apps
LoB 1 Employee	✓	✗	✗	✗	✗	✓	✓	✗
LoB 2 Employee	✗	✓	✗	✗	✗	✓	✗	✓
Partner 1	✗	✗	✓	✗	✗	✓	✗	✗
Partner 2	✗	✗	✗	✓	✗	✓	✗	✗
POS Terminal	✗	✗	✗	✗	✓	✗	✗	✗

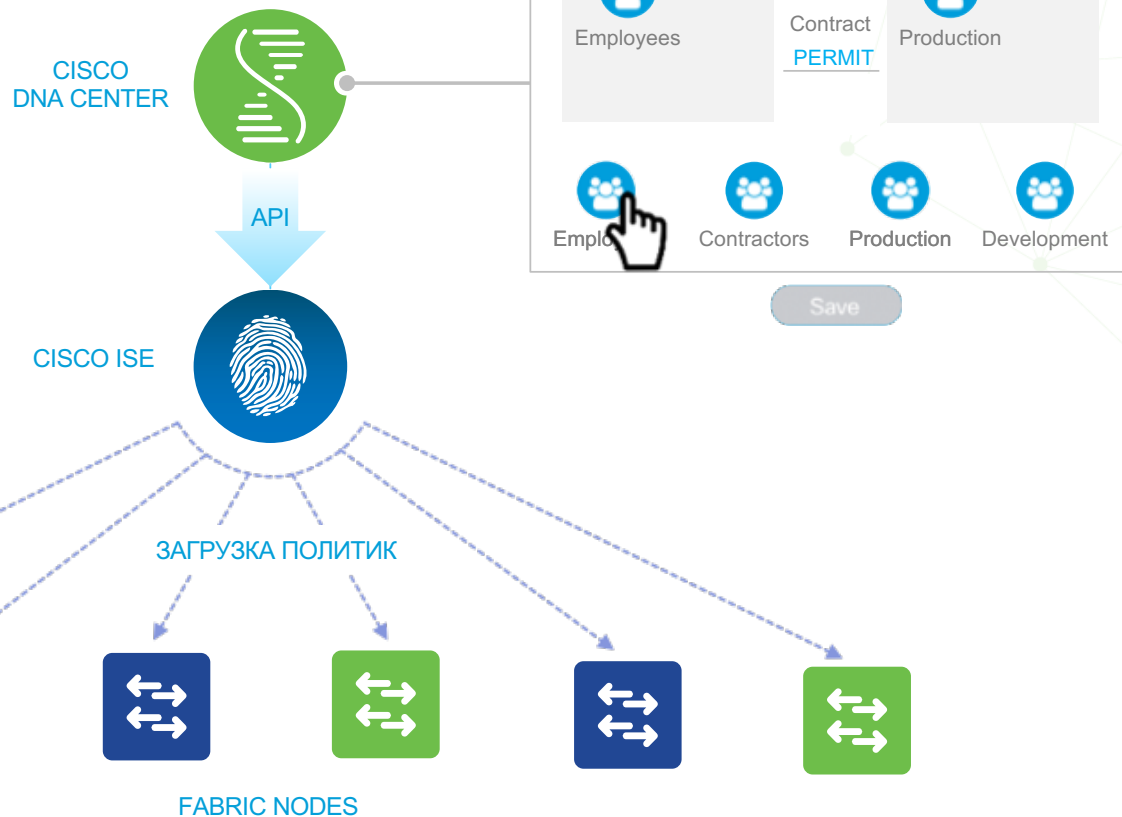


Ограничение
распространения

DEFCON3 Policy

Source	Destination							
	LoB 1 Employee	LoB 2 Employee	Partner 1	Partner 2	PCI Server	Shared Apps	LoB 1 Apps	LoB 2 Apps
LoB 1 Employee	✗	✗	✗	✗	✗	✓	✓	✗
LoB 2 Employee	✗	✗	✗	✗	✗	✓	✗	✓
Partner 1	✗	✗	✓	✗	✗	✗	✗	✗
Partner 2	✗	✗	✗	✓	✗	✓	✗	✗
POS Terminal	✗	✗	✗	✗	✓	✗	✗	✗

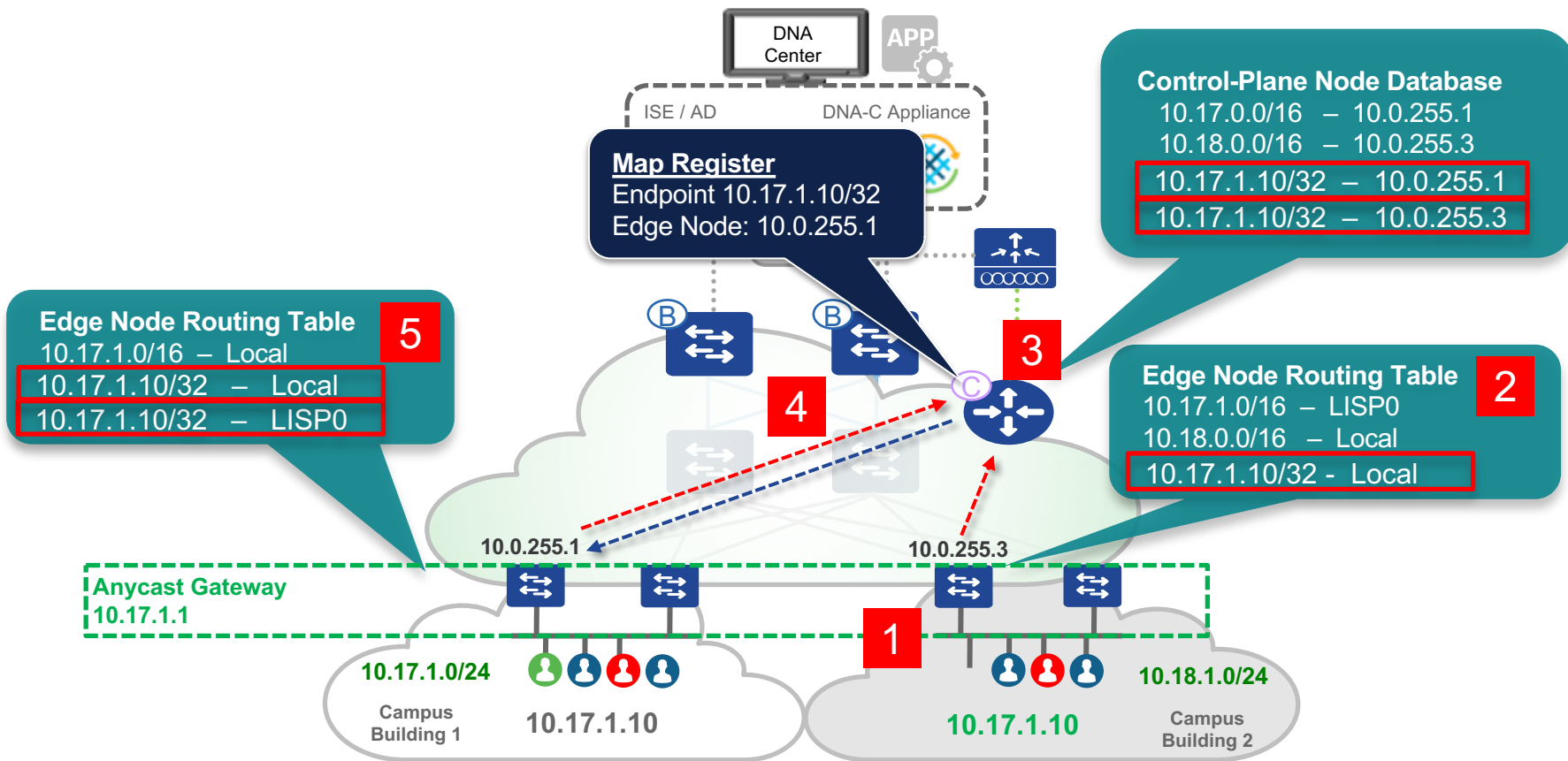
Распространение политик



Wired and Wireless

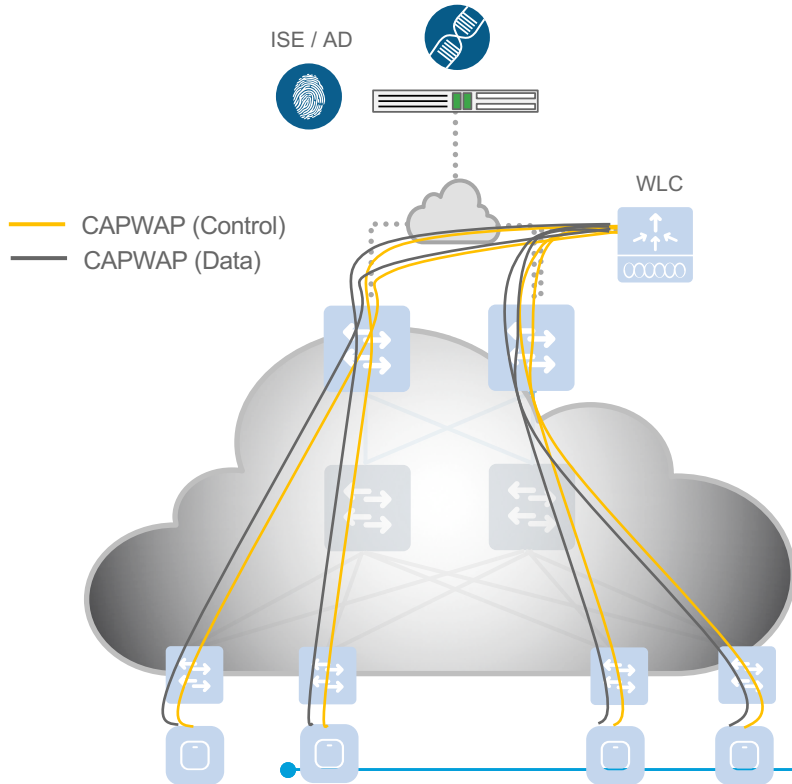
Host Mobility Without Stretching VLANs

Always connect to the same L3 gateway



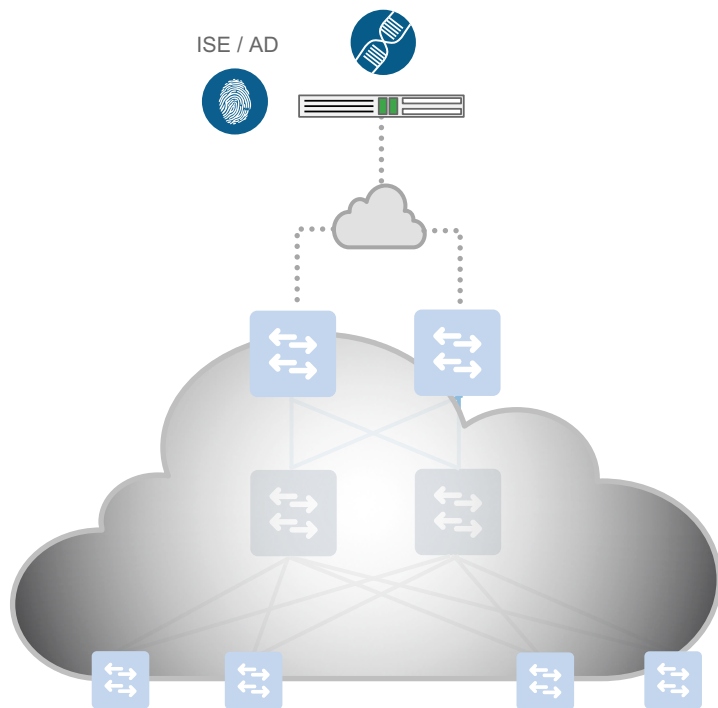
SD-Access — внедряем беспроводную сеть

Централизованная архитектура - преимущества



Simplified operations?	Yes with WLC
Network Overlay?	CAPWAP
L3 roaming across Campus?	WLC as Mobility Anchor
Simplified IP addressing?	WLC as mobility Anchor
Guest traffic segmentation?	Foreign-Anchor

Проводной сегмент: сильные стороны



Segmentation

VRF-Lite, MPLS

Complex ACL capabilities

Scalable TCAMs

Distributed Data Plane

Scalable and
Reliable

Distributed Feature Plane

AVC, NetFlow,

Comprehensive QoS capable

12-class, Queuing

SD-Access Wireless Architecture

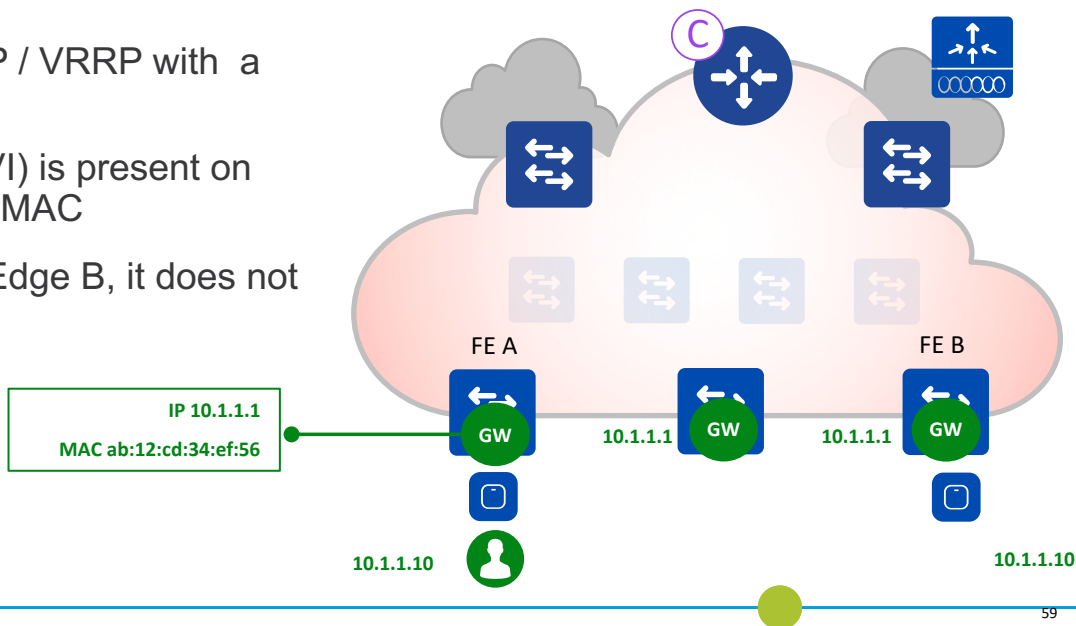
Optimizing the Data Plane: Anycast Gateway – A Closer Look

2

Anycast GW provides a single L3 Default Gateway

Based on Virtual IP address (VIP)

- Similar principle and behaviour as HSRP / VRRP with a shared Virtual IP and MAC address
- The same Switched Virtual Interface (SVI) is present on every Edge, with the same Virtual IP and MAC
- If (when) a Host moves from Edge A to Edge B, it does not need to change it's (L3) Default Gateway!



SD-Access Wireless Architecture

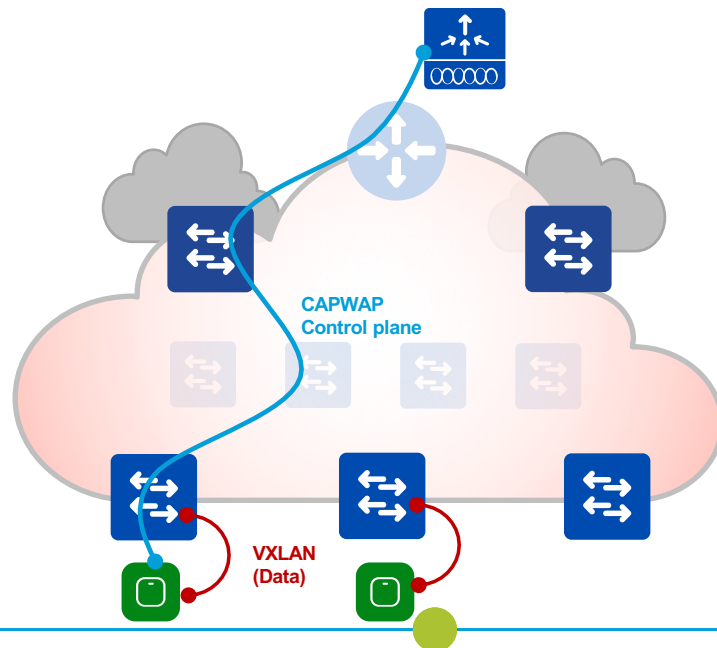
Optimizing the Data Plane: Stretched subnets – A Closer Look

2

Fabric Mode AP integrates with the VXLAN Data Plane

Wireless Data Plane is distributed across APs

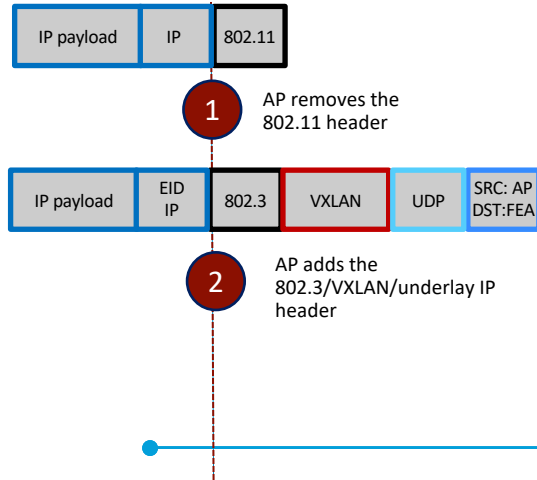
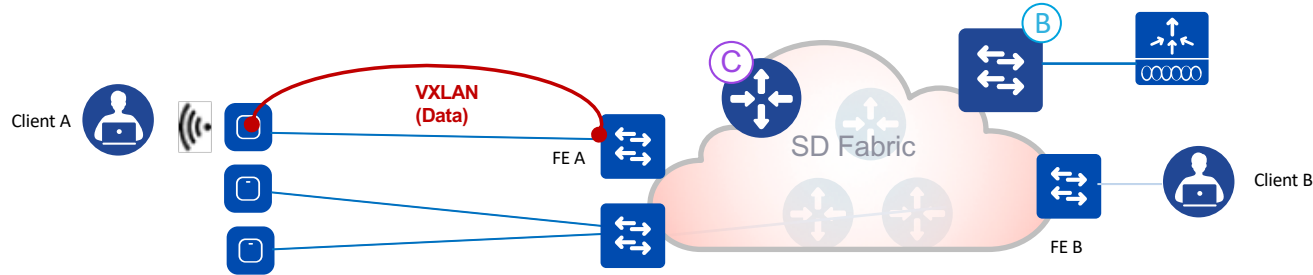
- Fabric mode AP is a local mode AP and needs to be **directly connected** to FE
- CAPWAP control plane goes to the WLC using Fabric
- **Fabric is enabled per SSID:**
 - For Fabric enabled SSID, AP converts 802.11 traffic to 802.3 and encapsulates it into VXLAN encoding VNI and SGT info of the client
 - Forwards client traffic based on forwarding table as programmed by the WLC. Usually VXLAN DST is first hop switch.
- AP applies all wireless specific feature like SSID policies, AVC, QoS, etc.



SD-Access Wireless Architecture

Simplifying policy and Segmentation

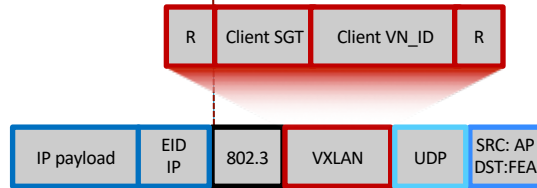
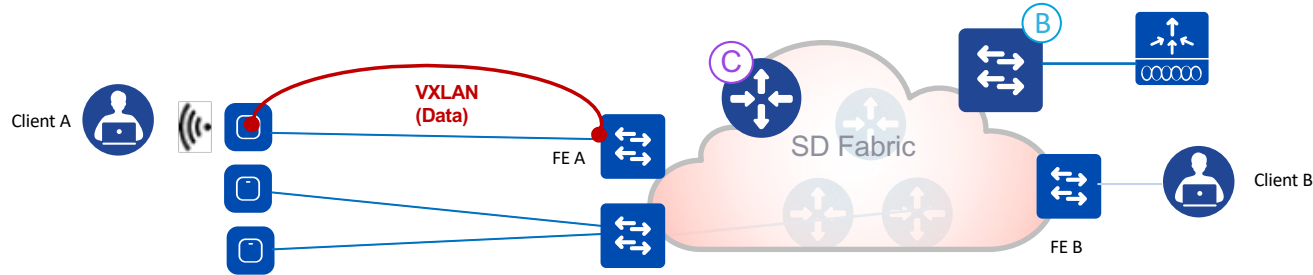
3



SD-Access Wireless Architecture

Simplifying policy and Segmentation

3



2

APs embed the Policy information in the VXLAN header and forwards it

The client VRF is represented by the Layer 2 Virtual Network (L2 VNID)

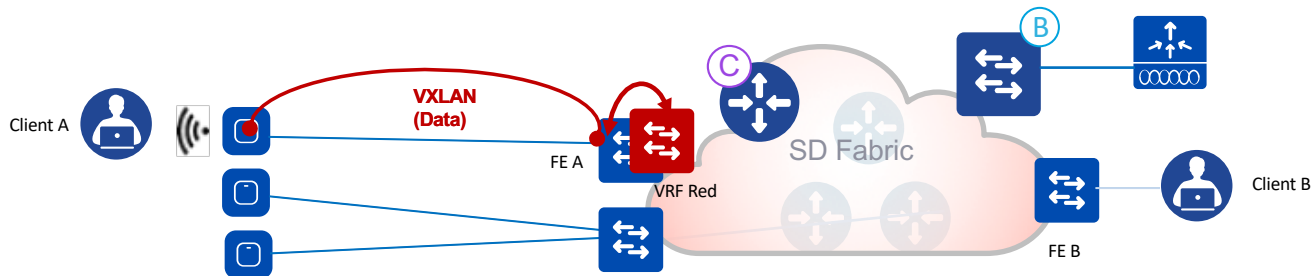
Hierarchical Segmentation:

1. Virtual Network (VN) == VRF - isolated routing Control Plane + Data Plane
2. Scalable Group Tag (SGT) – User Group identifier

SD-Access Wireless Architecture

Simplifying policy and Segmentation

3



FEA does a lookup to CP to locate client B



3

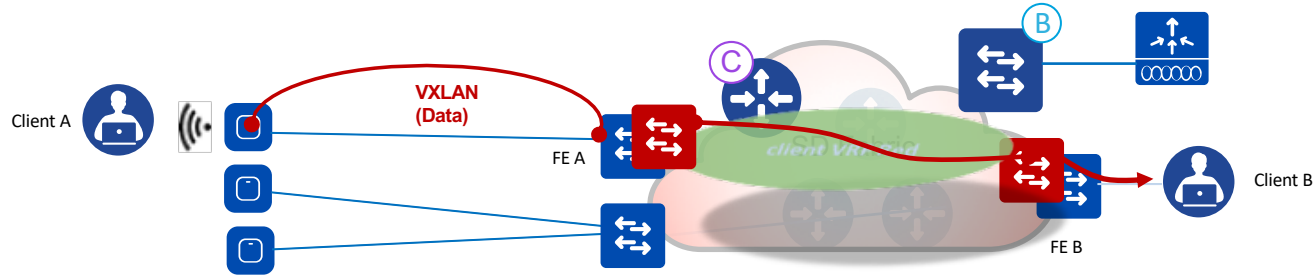
FE decapsulates the VXLAN header, looks at the L2 VNID and maps it to the VLAN and L2 LISP instance.

Then FE A does the lookup and rebuild the VXLAN encapsulates to the destination FE B

SD-Access Wireless Architecture

Simplifying policy and Segmentation

3



Mapped to VRF
SGT policy is applied



4

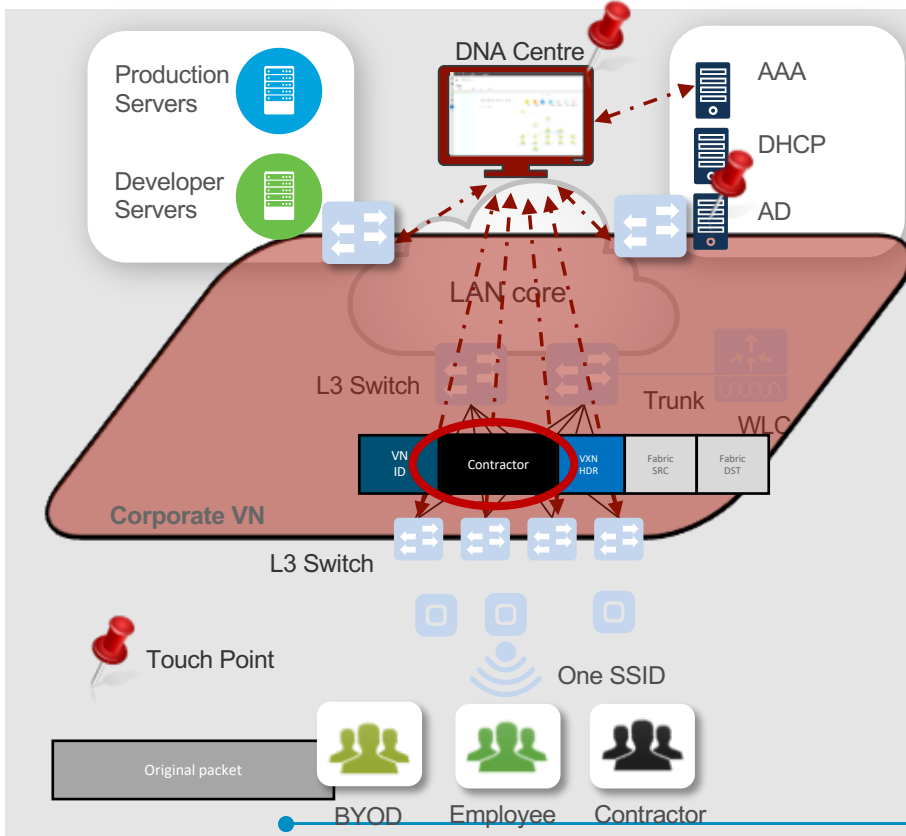
FE removes the outer IP header, looks at the VNID maps it to the VLAN.

Also looks at the SGT and apply the policy before forwarding the packet

Client Policy is carried end to end in the overlay

SD-Access Wireless Benefits

User Group policy rollout



1. Define Groups in AD

2. Design and Deploy in DNA-C

- Create Virtual Network for Corporate
- Define Policies
 - Role/Group based
- Apply Policies
 - SGT based

	Production Serv. SGT 10	Developer Serv. SGT 20
Employee SGT 100		
BYOD SGT 200		
Contractor SGT 300		

3. Upon user authentication, Policy is automatically applied and carried end to end

User Group policy rollout



- Create Virtual Network for Corporate
- Define Policies
 - Role/Group based
- Apply Policies
 - SGT based

One Touch Point



Строим фабрику

SD-Access

Fabric Underlay – Manual vs. Automated

Manual Underlay

You can reuse your existing IP network as the Fabric Underlay!

- **Key Requirements**

- IP reach from Edge to Edge/Border/CP
- Can be L2 or L3 – We recommend L3
- Can be any IGP – We recommend ISIS

- **Key Considerations**

- MTU (Fabric Header adds 50B)
- Latency (RTT of $\leq$ 100ms)

Automated Underlay

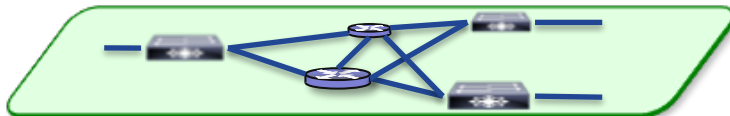
Prescriptive fully automated Global and IP Underlay Provisioning!

- **Key Requirements**

- Leverages standard PNP for Bootstrap
- Assumes New / Erased Configuration
- Uses a Global “Underlay” Address Pool

- **Key Considerations**

- PNP pre-setup is required
- 100% Prescriptive (No Custom)

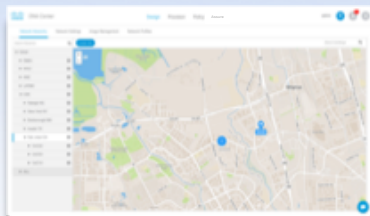


DNA Center

SD-Access 4 Step Workflow

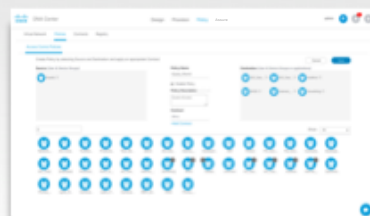


Design



- Global Settings
- Site Profiles
- DDI, SWIM, PNP
- User Access

Policy



- Virtual Networks
- ISE, AAA, Radius
- Endpoint Groups
- Group Policies

Provision



- Fabric Domains
- CP, Border, Edge
- FEW / OTT WLAN
- External Connect

Assurance



- Network Health
- 360° Views
- FD, Device, Client
- Path Traces

Planning & Preparation

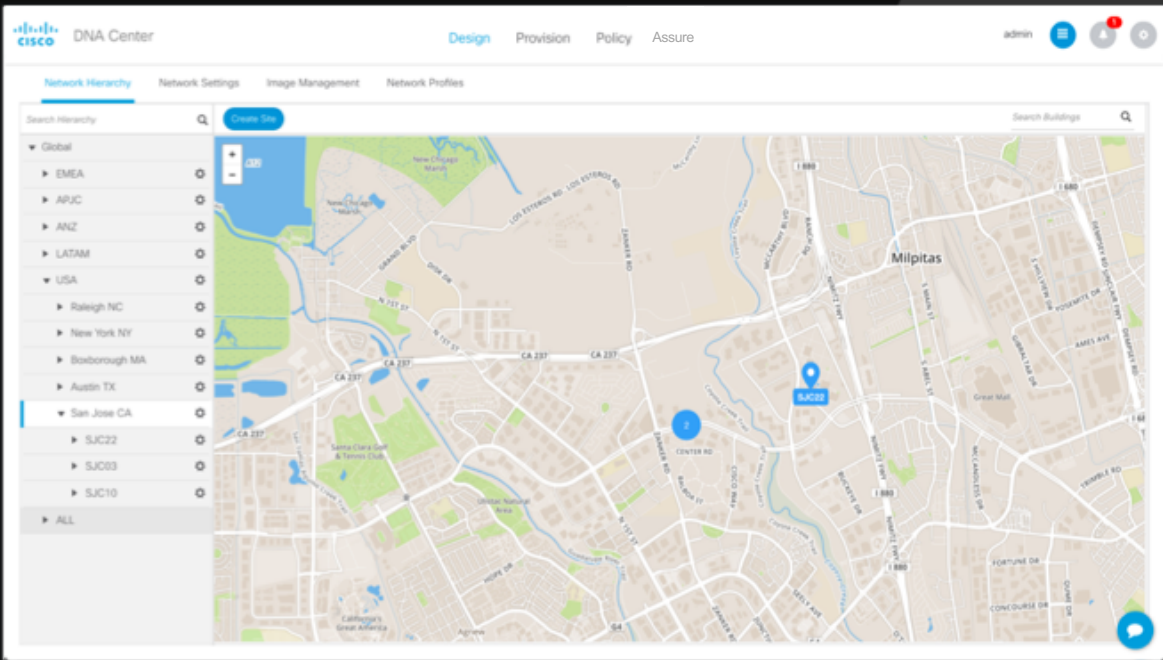
Installation & Integration

SDA - Design



DNA Center

Design, Automate and Assure your Network



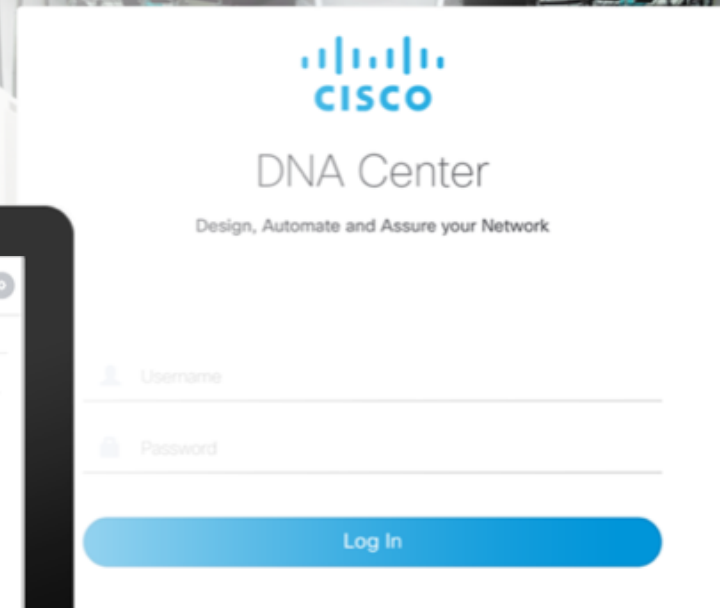
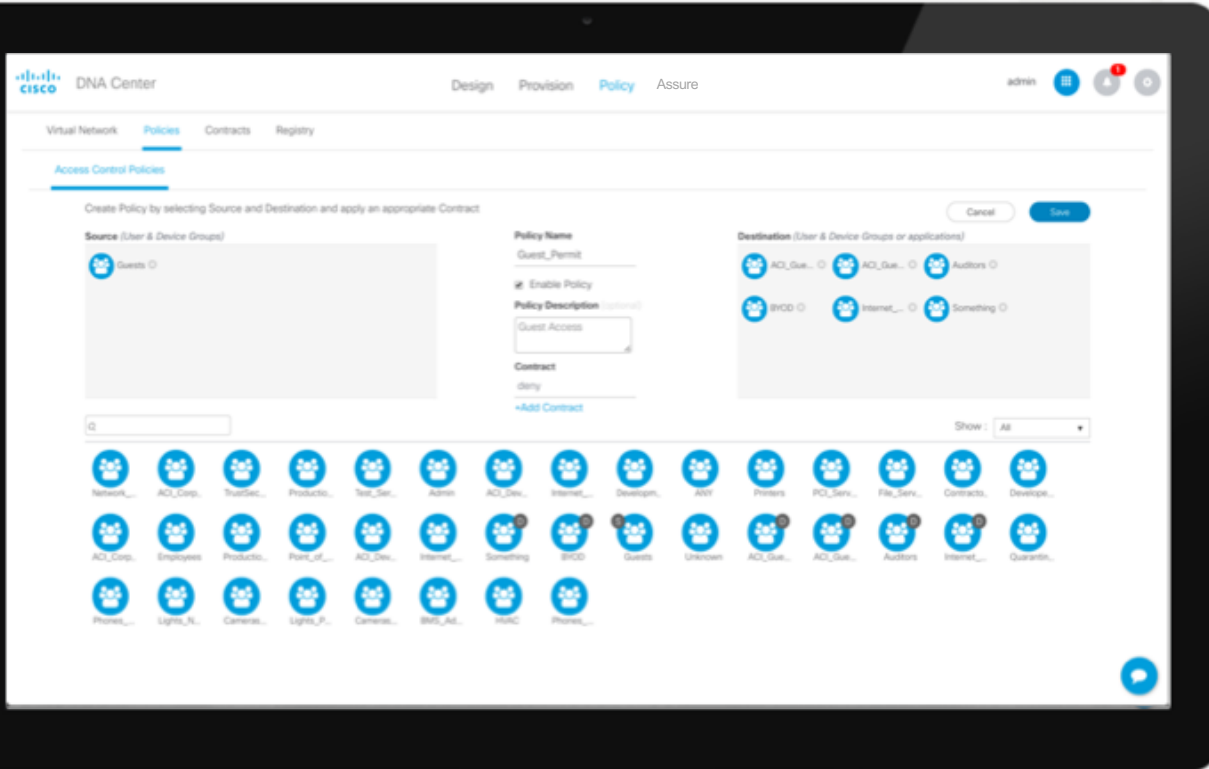
Username

Password

[Log In](#)

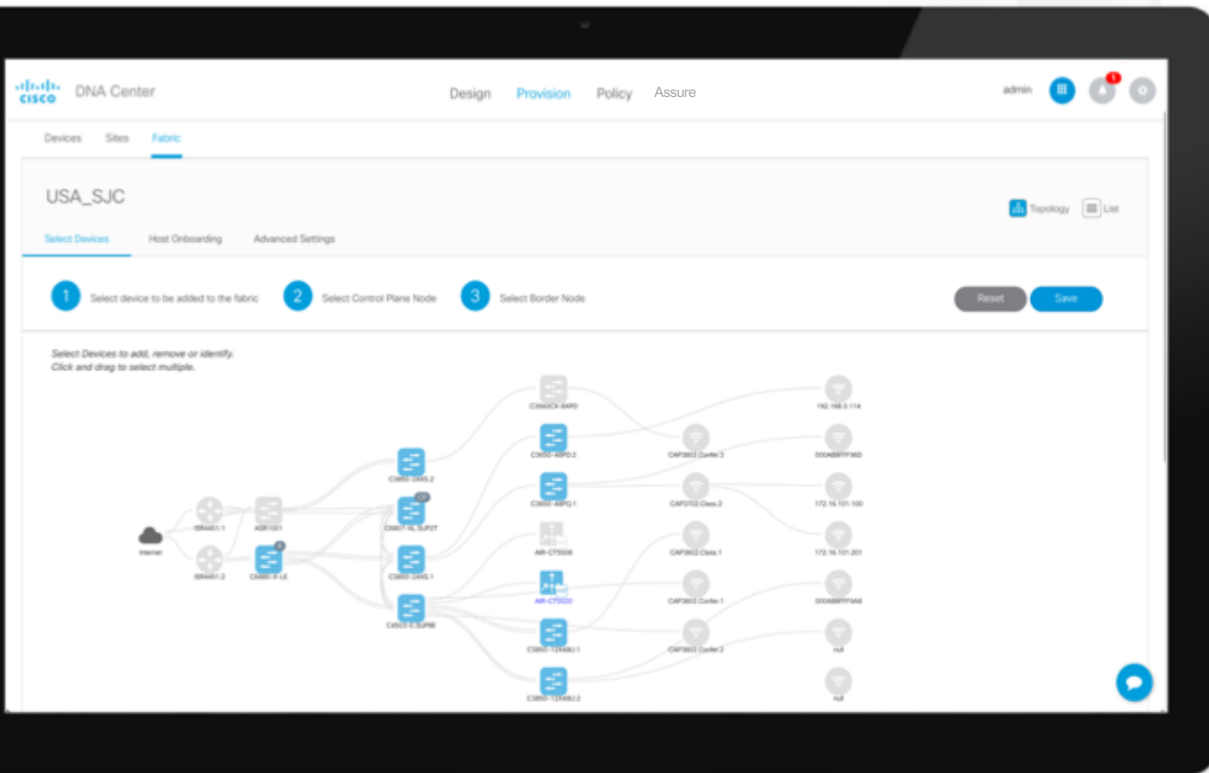
Network Hierarchy
Network Settings
Image Management
Network Profiles

SDA - Policy



Virtual Networks
Access Control
Application Priority
Application Registry

SDA - Provision



DNA Center

Design, Automate and Assure your Network

Username

Password

Log In

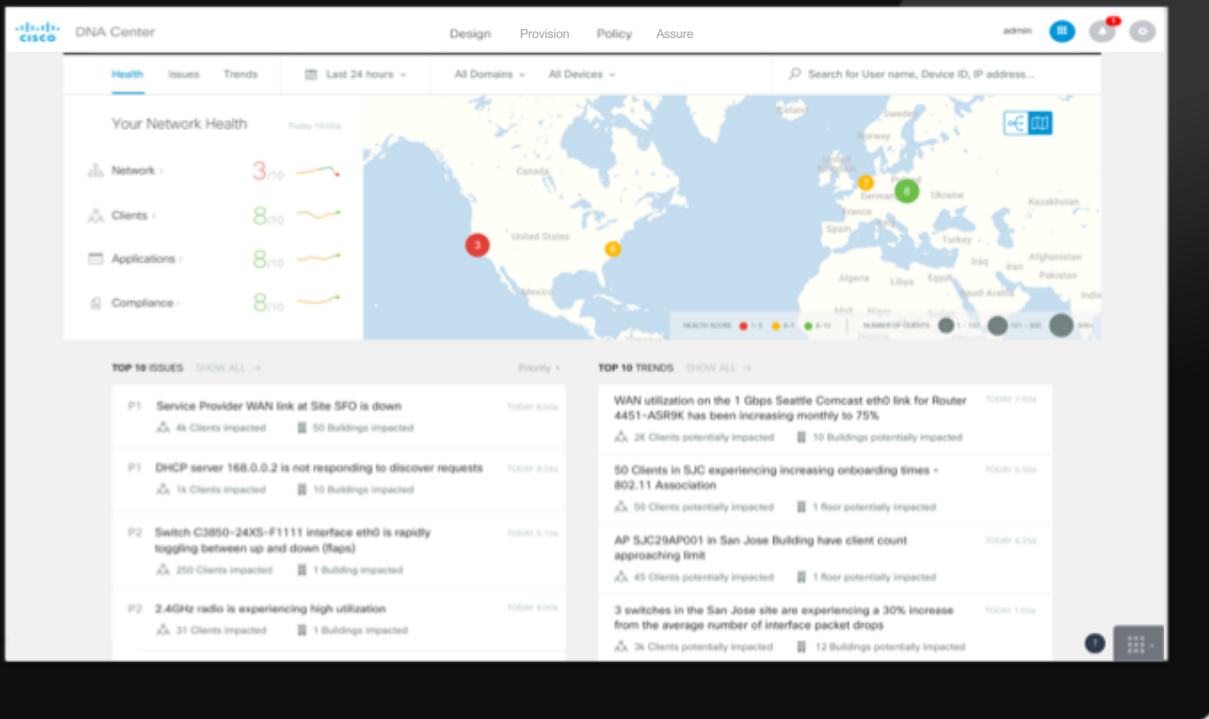
Device On-Boarding
Device Inventory
Fabric Administration
Host On-Boarding

SDA - Assurance



DNA Center

Design, Automate and Assure your Network

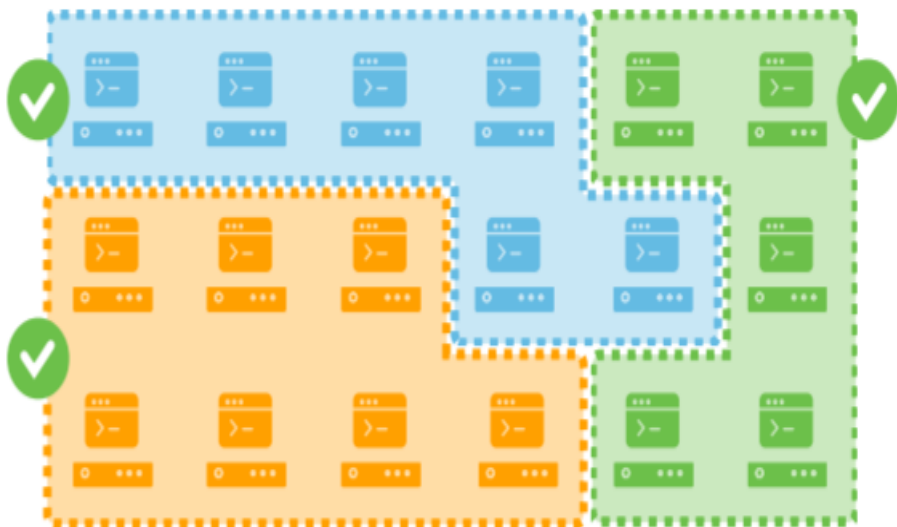


Health Scores
Client 360
Device 360
Application 360
Click to Resolve

Before: Box by Box
Manual | Error Prone



After: Automation
Scalable | Simple



Design

2 hours > 15 minutes

Policy

4 hours > 5 minutes

Provision

5 hours > 5 minutes

2 Hrs.

(Old Method)

- Load correct software images
- Configure console access via serial and SSH
- Define VLANs
- Configure every active interface as a VLAN member
- Configure switch virtual interfaces (SVIs) with IP addresses
- Define network settings for AAA/DHCP/DNS & SNMP
- Define IP Address Pools
- Configure dynamic routing protocol(s) such as BGP, OSPF, and EIGRP
- Verify connectivity to other local switches
- Verify connectivity to local default gateway and/or peer router(s)
- Verify connectivity to core services such as AAA, DHCP, DNS, and SNMP



Design

15 Mins

(New Method)

- Select a Site
- Define network IP pools
- Select the image
- Define network services
- Discover devices

4 Hrs.

(Old Method)

- Configure VRF
- Enable Connection between all devices and ISE
- Enable TrustSec on all devices
- Add TrustSec user access policy on ISE
- Configure and ensure connectivity with auth server(s) from all devices
- Import and export routes between VRFs as needed



Policy

5 Mins

(New Method)

- Add business segmentation
- Add group policy

5 Hrs.

(Old Method)

- Enable 802.1x dynamic host authentication on desired ports of each switch
- Configure static SGT port mapping for any ports not configured with 802.1x
- Configure 802.1x options as needed (closed, open, priority, etc.)
- Add CTS configuration per port
- Configure handoff to DC, WAN etc.
- Import external routes via BGP
- Export internal routes via BGP
- Repeat previous step for all intermediate devices edge and border switch/router



Provision

5 Mins

(New Method)

- Add devices to fabric
- Select the IP pool with authentication options
- Add Border node
- Configure external Connectivity

Comparison of Total Workflow Time

Total Workflow – ONE Device

11

Hours
(Old Method)

25

Mins
(New Method)

Comparison of Total Workflow Time

Total Workflow – **FIFTY** Devices

50

Days
(Old Method)

25

Mins
(New Method)

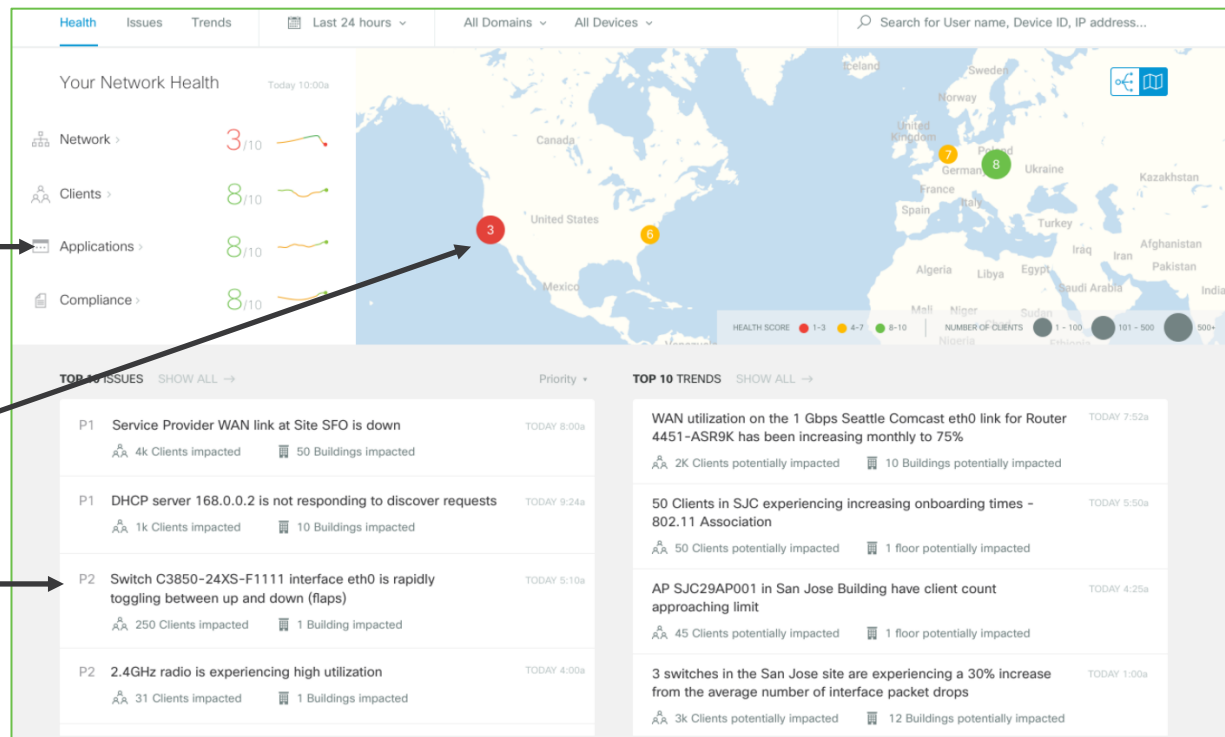
Простота использования : Пример

Главная страница – какие главные проблемы наблюдаются в вашей сети?

Overall health of
your network, clients,
and applications

Where in the world
the most serious issues
are happening

Your top 10 issues
and trends



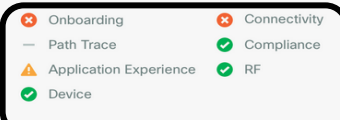
3/10 George Baker

User Name: gbaker Location: San Jose, CA Email: gbaker@email.com

Reliable scoring to assess client health in real-time

Incorporation of diverse network data types

3/10 GeorgeBaker-iphone 9/10 George-macbook



1 Issue (TODAY AT 9:30a)

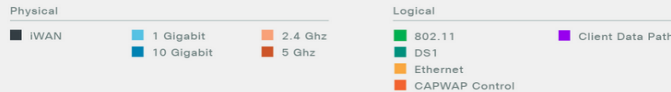
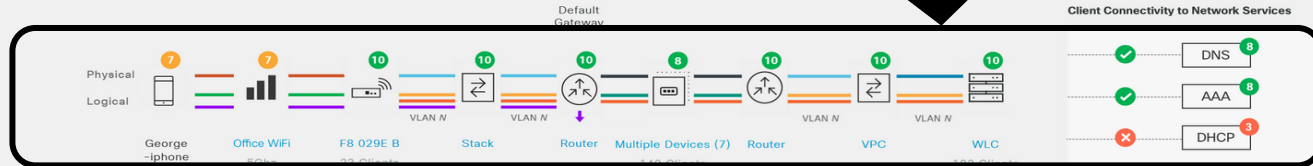
Accurate alerting for fast root cause analysis

Onboarding
DHCP server 168.0.0.2 is not responding to discover requests.

1k Clients impacted 10 Buildings impacted

Live end-to-end visibility brings together multiple data sources at high volumes and speeds

Onboarding
2/14/17 09:58:09
UPDATE



Variety

Velocity

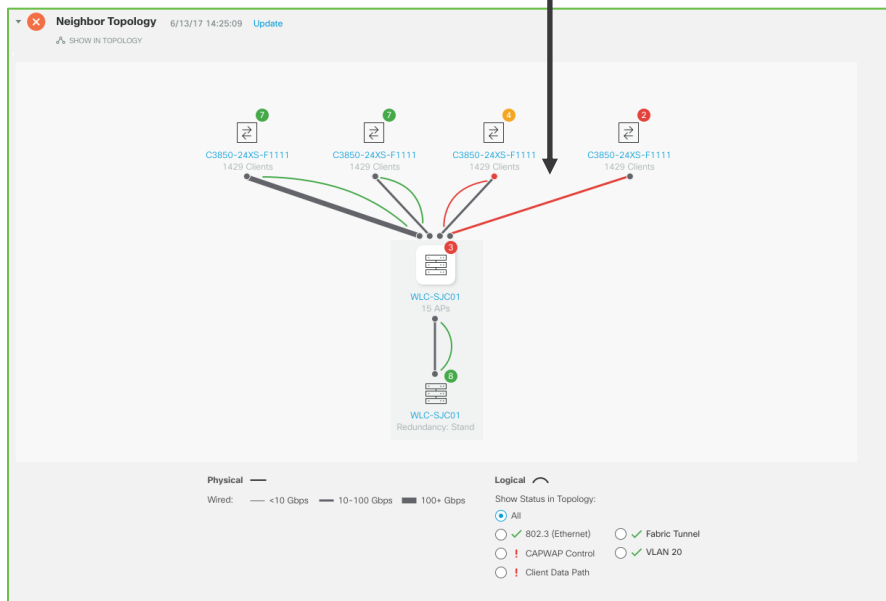
Volume

Veracity

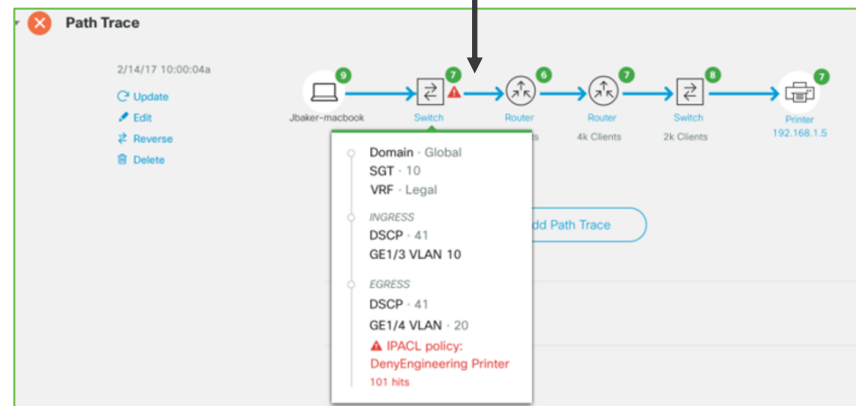
Простота использования : Пример

Мгновенное обнаружение причин проблем с SDA-фабрикой и/или политиками CTS

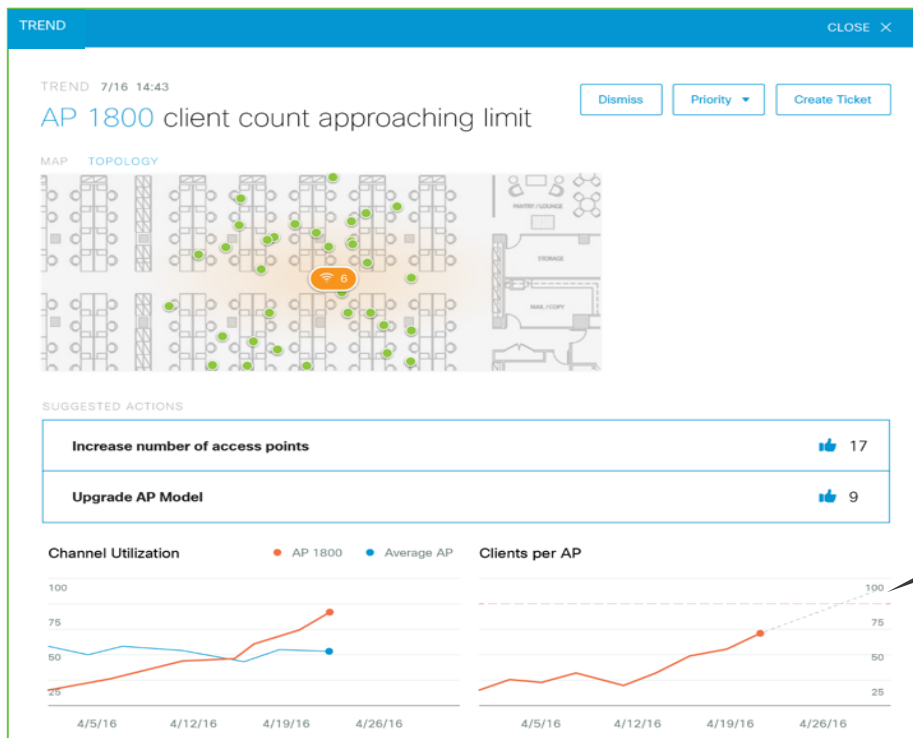
- 1 Quick visual of the fabric overlay tells you where you might have issues



- 2 Assurance-enabled path trace tells you where policies are failing



Анализ трендов



Trend analytics anticipate when a resource will run out of capacity

SD Access. Собираем всё вместе

Support

Solution support (CON-SSSNT)

DNA Center (appliance)

Design + Policy + Provision + Assurance

Лицензии

ISE Base + ISE Plus subscription

Cisco ISE (appliance / VM)

Управление политиками доступа

Подписка на управление с SDN контроллера

DNA Advantage

Сетевое оборудование для фабрики (Catalyst 9k)

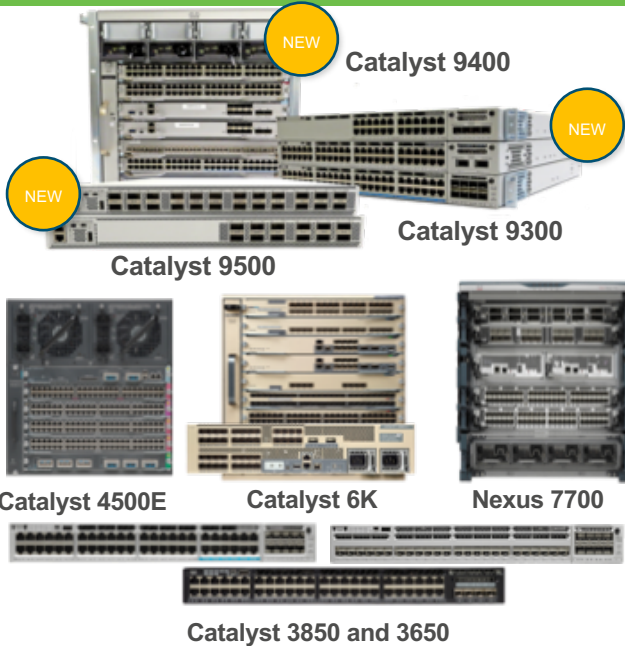
Поддержка: nw fabric, VRF, VXLAN, SGT, LISP

SD-Access – поддержка на оборудовании

Полная защита инвестиций



Switching



Routing



Wireless



Subtended Nodes



Software Defined Access

Полезная литература

Cisco SD-Access eBook:

<https://www.cisco.com/c/dam/en/us/products/se/2018/1/Collateral/nb-06-software-defined-access-ebook-en.pdf>

Software-Defined Access Design Guide

<https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/Campus/CVD-Software-Defined-Access-Design-Guide-2018APR.pdf>

Software-Defined Access Deployment Guide

<https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/Campus/CVD-Software-Defined-Access-Deployment-Guide-2018APR.pdf>

Software-Defined Access Segmentation Design Guide

<https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/Campus/CVD-Software-Defined-Access-Segmentation-Design-Guide-2018MAY.pdf>

Software Defined Access

Полезная литература

Cisco Live 365 Sessions: <https://www.ciscolive.com/global/on-demand-library/?#/>
(search for the session IDs shown below):

- Cisco SD-Access – A Look Under the Hood – BRKCRS-2810
- Cisco SD-Access – External Connectivity – BRKCRS-2811
- Cisco SD-Access – Migration – BRKCRS-2812
- Cisco SD-Access – Monitoring and Troubleshooting – BRKCRS-2813
- Cisco SD-Access – Assurance – BRKCRS-2814
- Cisco SD-Access – Policy – BRKCRS-3811
- Cisco SD-Access – Wireless Integration – BRKEWN-2020
- Cisco SD-Access – DC Integration – BRKDCN-2489



Спасибо! Вопросы?