

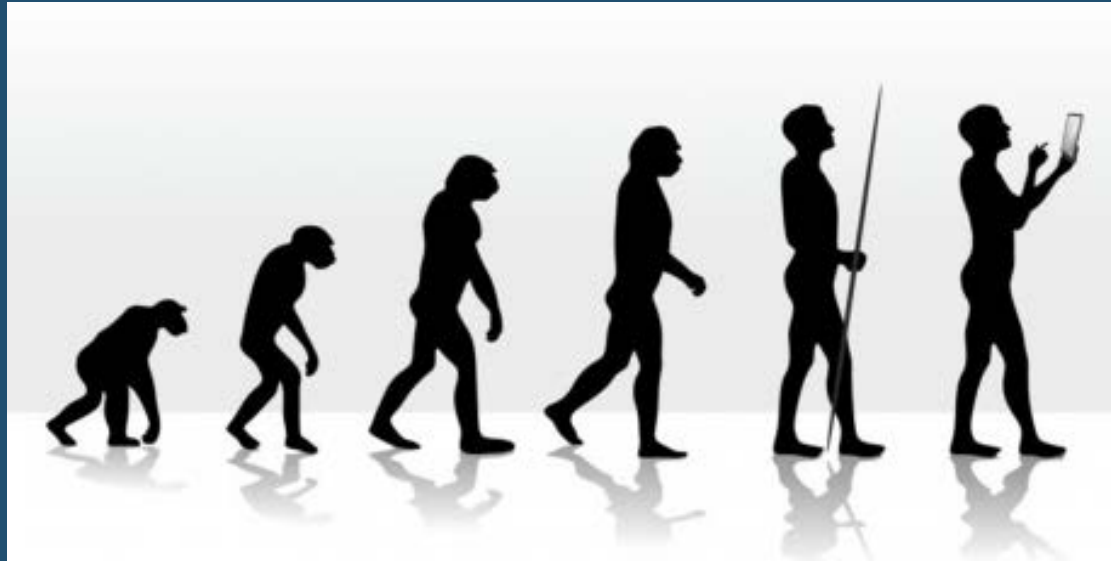


The Network. Intuitive.


Cisco's Next Generation
Enterprise Architecture

Gabriel Slomovitz
Systems Engineer





**Quienes sobreviven no son los más fuertes ni los más inteligentes,
sino quienes se adaptan mejor.**

An aerial view of a city, likely New York City, with a blue overlay. The image is filled with various technology and business icons, including a network diagram, a terminal window, a traffic light, a smartphone, a cloud, and a server rack. The text is centered in the middle of the image.

Digital business moves at the speed of software.
What about your network?

Cost

\$60B

Annually spent on
Network Operations,
Labor & Tools¹



95%
Network changes
performed manually



70%
of Policy Violations are
due to human error



75%
of Opex spent on
changes and
troubleshooting



Operational Diversity

Complexity

3.3B

M2M connections
in 2021



- Mobile-Cloud**
Phones, tablets, wearables
- Digital BMS**
Badging, lighting, HVAC, cameras
- IoT**
Robots, infusion pumps, sensors



Endpoint Diversity

Risk

\$5.3B

Stolen in Ransomware



6 months to detect breach²

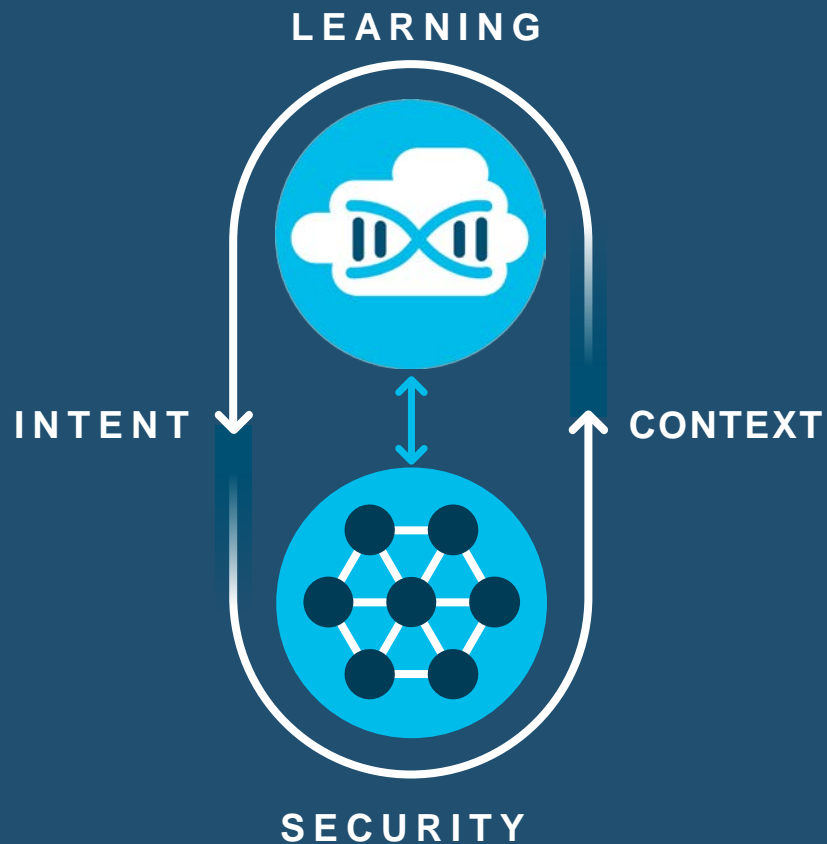
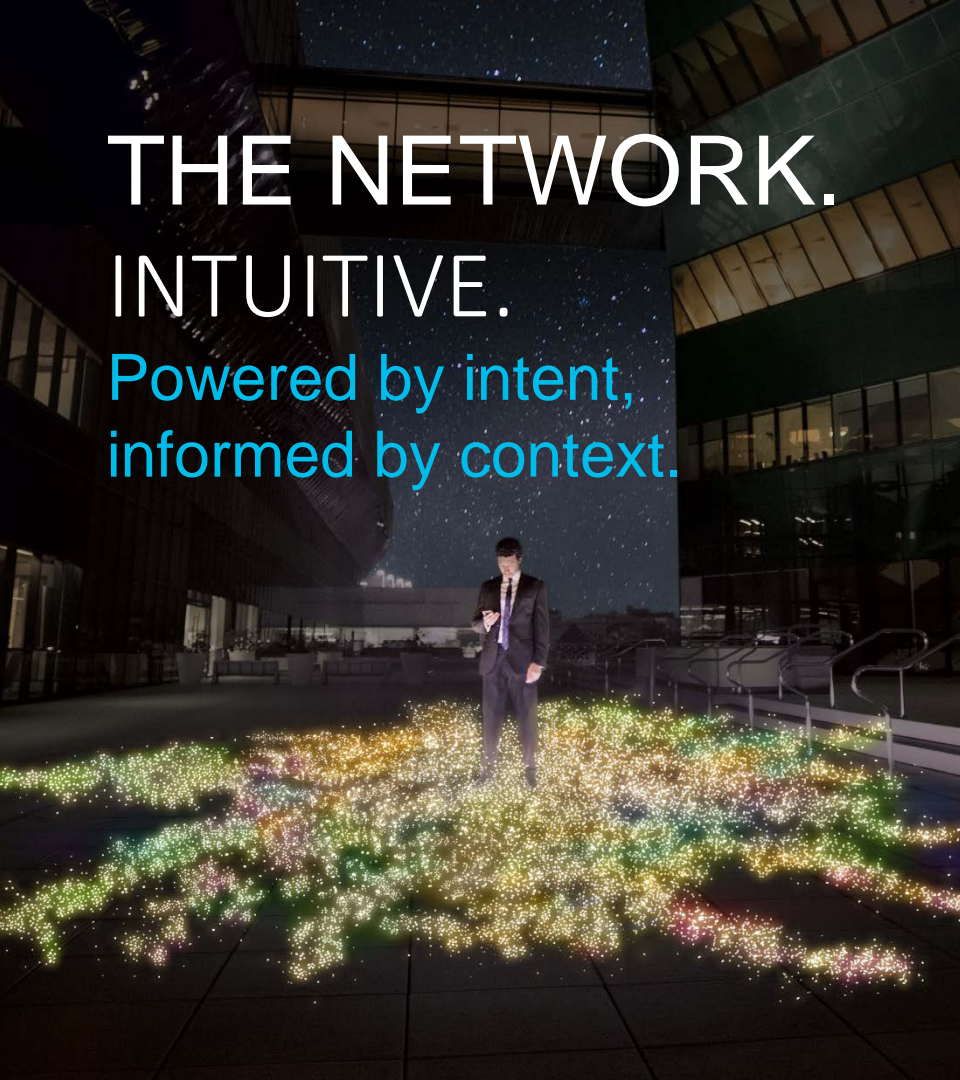
- Mobile-Cloud**
Phones, tablets, wearables
- Digital BMS**
Badging, lighting, HVAC, cameras
- IoT**
Robots, infusion pumps, sensors



Increased Threat Surface

THE NETWORK. INTUITIVE.

Powered by intent,
informed by context.



Intent

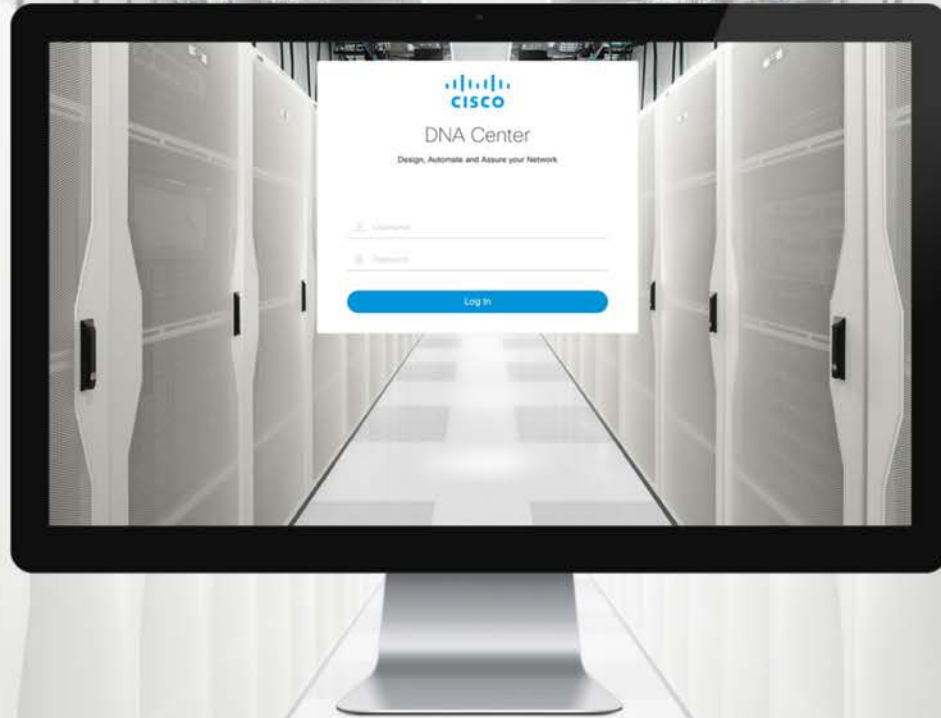
A male athlete in a starting crouch on a track. The athlete is wearing a black and white singlet with red accents and black shorts with red accents. He is wearing white and red running shoes. He is in a starting crouch on a track, with his hands on the ground and his feet in starting blocks. The background is a clear blue sky with some clouds and a distant horizon.

Tell the network *what you want* and let it figure out *how to do it*



Context

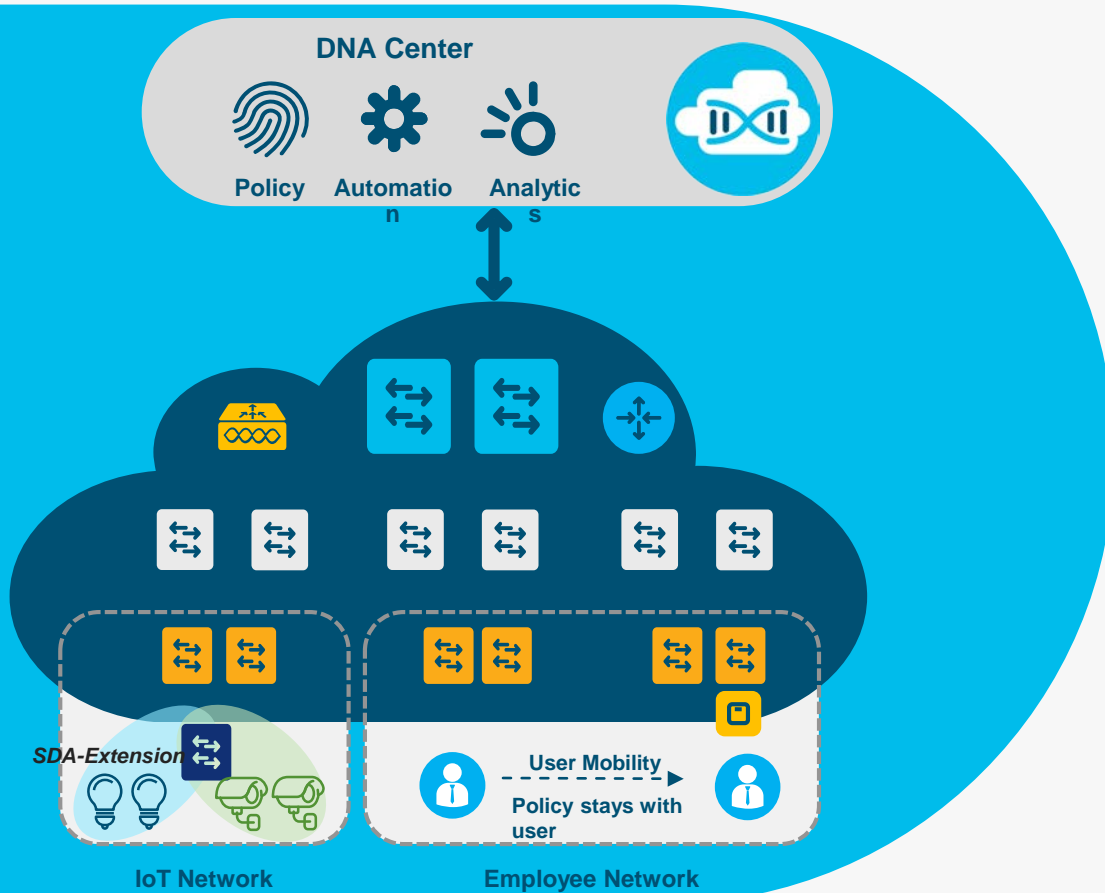
Correlation of *multiple events* giving **deeper insights** with *suggested actions* for **problem resolution**



What is SD-Access?

Software-Defined Access

Networking at the speed of Software!



Identity-based Policy & Segmentation

Decoupled security policy definition from VLAN and IP Address



Automated Network Fabric

Single Fabric for Wired & Wireless with Workflow-based Automation



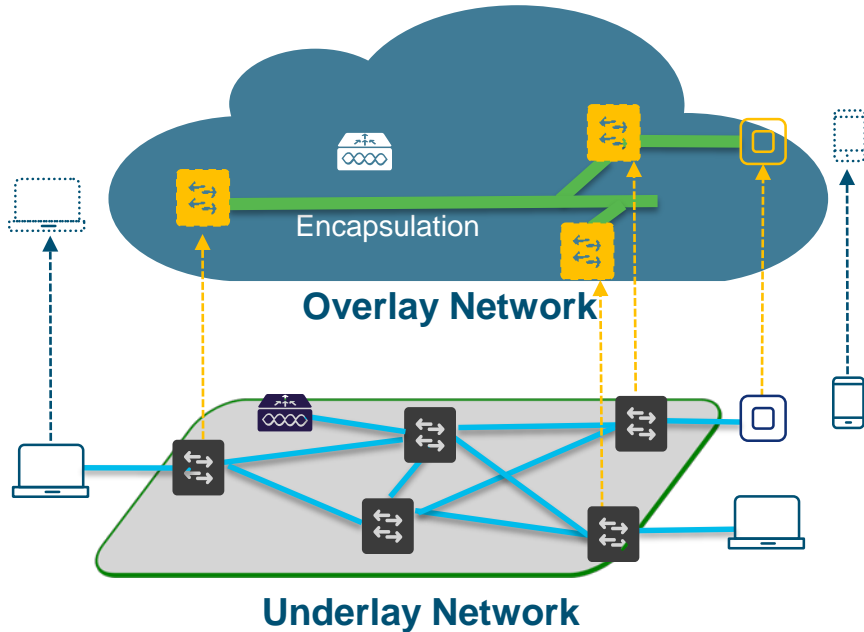
Insights & Telemetry

Analytics and insights into user and application behavior



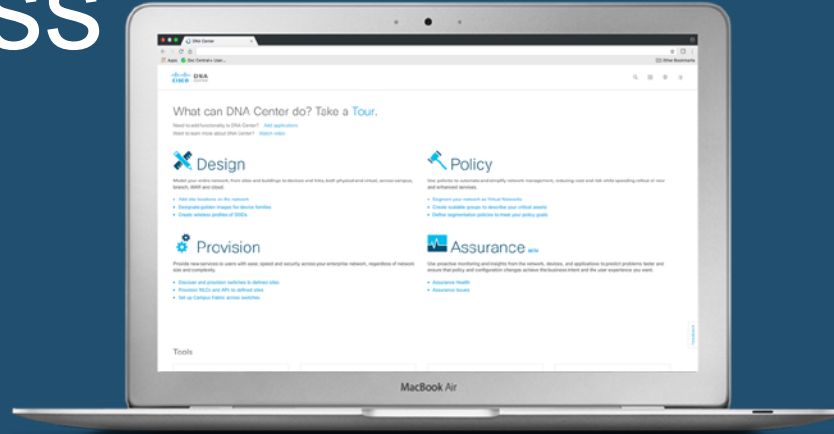
Software-Defined Access

Network Fabric – Normalized Transport for Wired & Wireless



- **Dynamic Logical Topologies with Overlays (Stateless Tunnels)**
- **Traffic for Wired and Wireless is carried inside Overlays**
- **Policy Context is carried inline with Traffic**

SD-Access



Automated
Network Fabric



Policy &
Segmentation



Insights &
Telemetry



Automated **N**etwork **F**abric



Global



Sacramento



San Francisco



San Jose



Building 22



Building 23



Building 24



Floor 3



Floor 2



Floor 1

2

Network Settings
AAA: 10.1.5.1/24
DHCP: 10.2.1.250/24
DNS: 10.1.5.5/24
SYSLOG: 10.1.7.12/24
NTP: 10.5.2.3/24

1

3



Device: Catalyst 9300

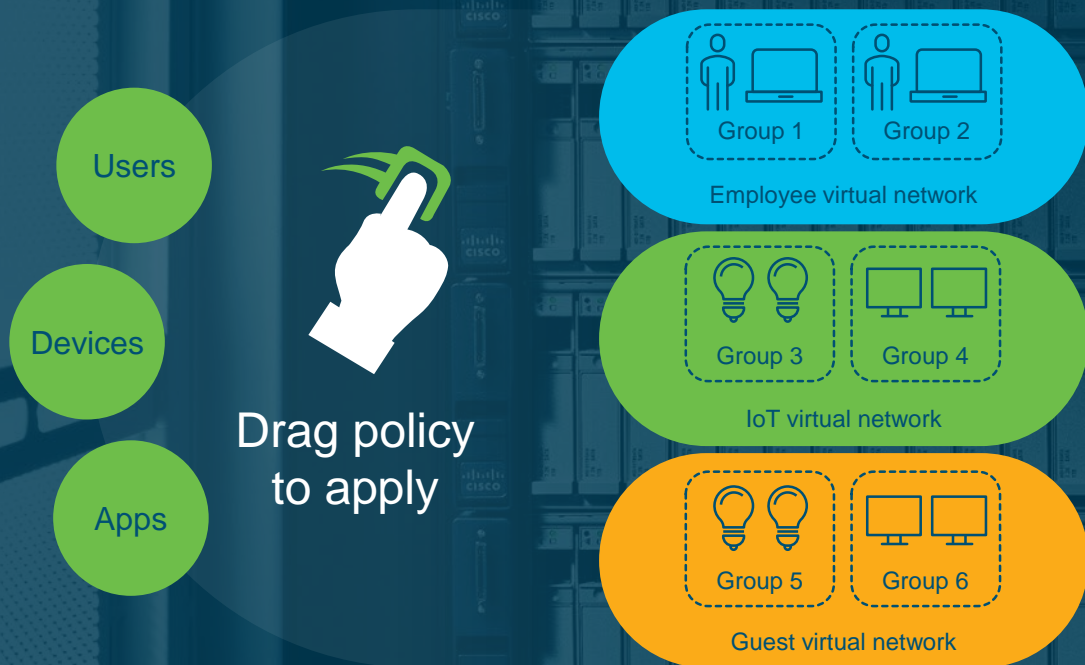


Site Hierarchy and Device Settings



Policy and Segmentation

Secure segmentation and onboarding: Cisco Software-Defined Access



IT simplicity

- No VLAN, ACLs, or IP address management required
- Single network fabric
- Define one consistent policy

Security

- Simplified microsegmentation
- Policy enforcement

Completely automated | Policy follows identity | Reduces lateral threat movement

Seeing and acting on ALL threats

80%

of organizations are victims
of malicious activity*

41%

of attacks used encrypted
traffic to evade detection*



*Source: Ponemon Institute – Hidden threats in encrypted traffic

How do you provide security while maintaining privacy?

Machine learning identifies malware

Encrypted Traffic Analytics



Malware in encrypted traffic



Security AND privacy



Detection: 99.99% accuracy

Infrastructure view of the data



DNA Assurance

Components

Network, Client & Applications

- Health
- 360
- Issues
- Suggested Actions



Health Dashboards

Issues

Open Resolved

Last Occurred Time

Title

Jan 27, 2018 8:42 am

Wireless due to

Jan 26, 2018 7:53 pm

Wireless

Jan 29, 2018 9:05 am

TenGig

Jan 29, 2018 9:05 am

High im

Jan 29, 2018 9:05 am

Fabric

Jan 29, 2018 9:05 am

Fabric

Jan 29, 2018 9:05 am

Fabric

Wireless client took a long time to connect (SSID: LA-Corporate3, AP: LA2-AP1815-33, Band: 2.4 GHz, Site: Global/USA/Santa Monica/Level 1) - Excessive time due to RF issues

Status: Open

Last Occurred: Jan 27, 2018 8:42 AM

Description

This client is taking longer than expected time to connect to 'LA-Corporate3' SSID due to excessive authentication time.

- Onboarding took 48.3 seconds (expected time should be less than 10.0 seconds).

The authentication delay is because the client is slow to respond to authentication messages. The client was connecting to 'LA-Corporate3' SSID on 2.4 GHz radio on 'LA2-AP1815-33' AP in 'Global/USA/Santa Monica/Level 1'. The AP was connected to 'LA1-WLC5520-3' WLC.

Impact

Location:

1 Building

Clients

2 Wireless Clients

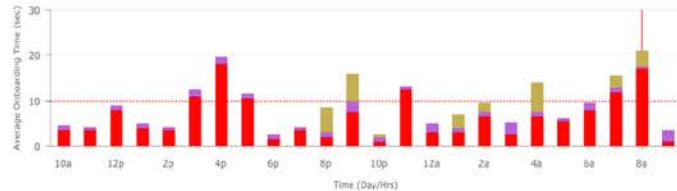
Suggested Actions (5)

- Check whether the client moved during the authentication phase, since a moving client may cause packet losses and retries.

Average Onboarding Times (AP Group: 149b3580-422a-4378-948d-6c1943ae28b2)

Jan 26, 2018 8:42 am to Jan 27, 2018 8:42 am

Show All



802.11 Association Authentication DHCP Addressing Failure Threshold

Impacted Client

Feedback

Health Dashboards

High input/output utilization on interface 'TenGigabitEthernet1/0/2'

Status: Open

Last Occurred: Jan 29, 2018 9:22 AM

Issues

Open Resolved

Last Occurred Time	Title
Jan 27, 2018 8:42 am	Wireless
Jan 26, 2018 7:53 pm	Wireless
Jan 29, 2018 9:05 am	TenGiga
Jan 29, 2018 9:05 am	High in
Jan 29, 2018 9:05 am	Fabric B
Jan 29, 2018 9:05 am	Fabric D
Jan 29, 2018 9:05 am	Fabric B

Suggested Actions (6)

Preview All Run All

- Verify configuration is compliant on this device TO-3850-ACC-1.corp.local and the device on the other side of the link.

 - Check running configuration on the affected interface on network device

sh run int TenGigabitEthernet1/0/2

```

interface TenGigabitEthernet1/0/2
switchport access vlan 100 switchport mode access
ip device tracking maximum 10
load-interval 30
speed 100
end
TO-3850-ACC-1#
                    
```

Success
 - Check port counters on the affected interface on network device

show interface TenGigabitEthernet1/0/2

```

show interface TenGigabitEthernet1/0/2
TenGigabitEthernet1/0/2 is up, line protocol is up (connected)
Hardware is Ten Gigabit Ethernet, address is 6c0d.3026.8082 (bia 6c0d.3026.8082) MTU 1500 bytes, BW 100000 Kbit/sec, DLY 100 usec,
reliability 255/255, txload 1/255, rxload 248/255
Encapsulation ARPA, loopback not set
Keepalive set (10 sec)
Full-duplex, 10000/s, media type is 100/1000/2.5G/5G/10GBaseTX
input flow-control is off, output flow-control is unsupported
                    
```

Success
- Check interface utilization (tx/rx) on both sides of the link.

Run

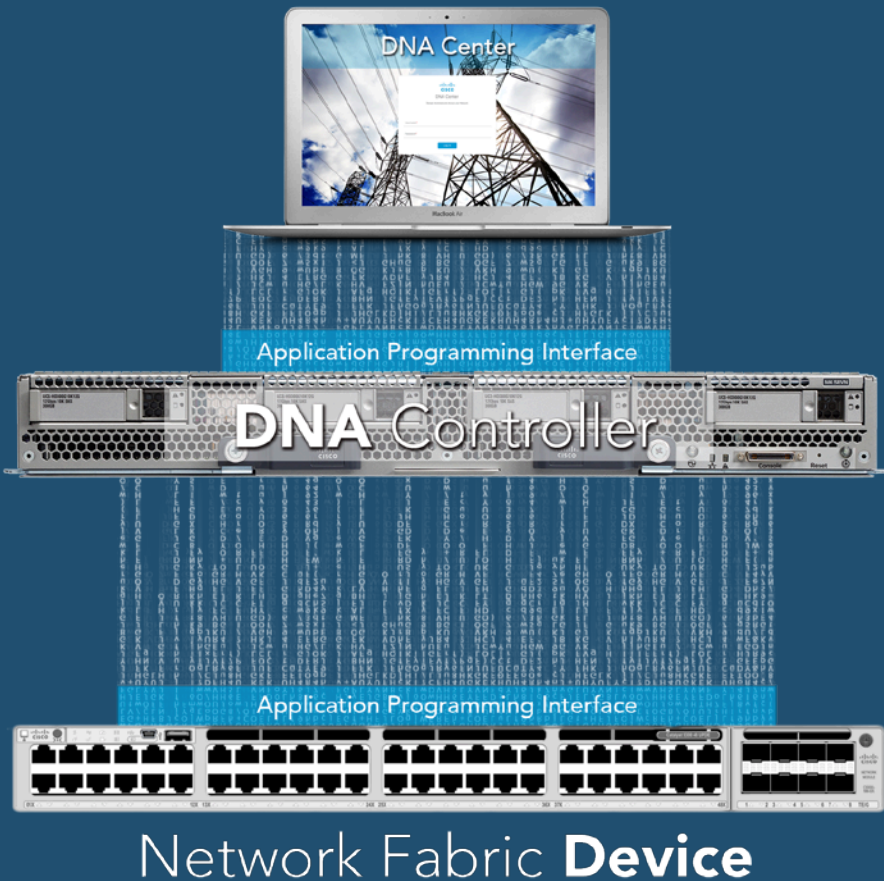
Feedback



Oh,.. one more IMPORTANT point

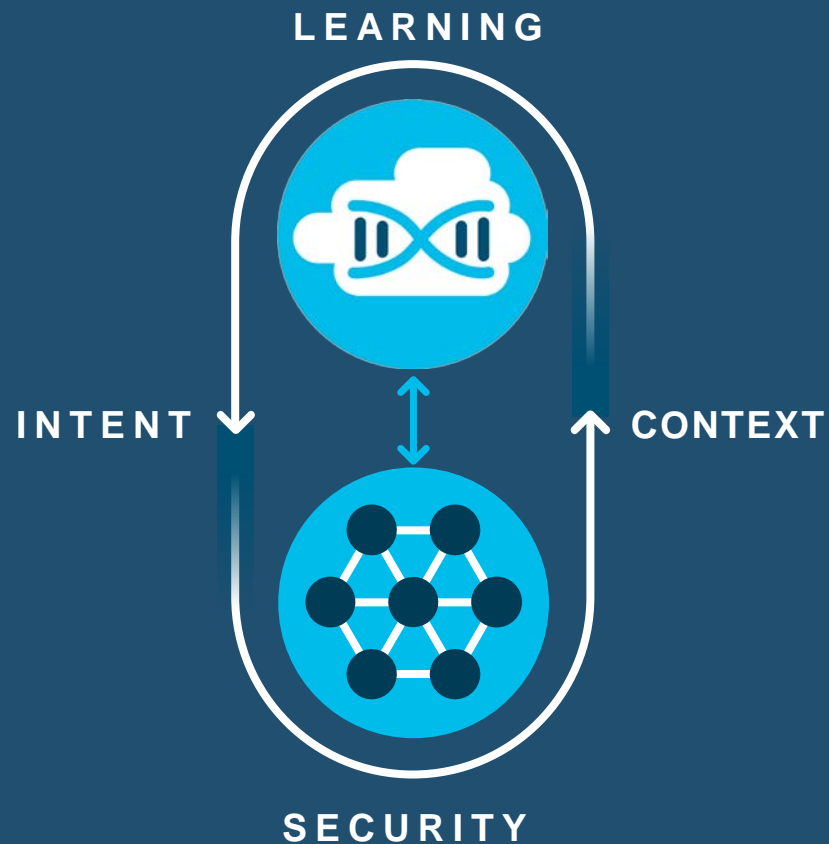
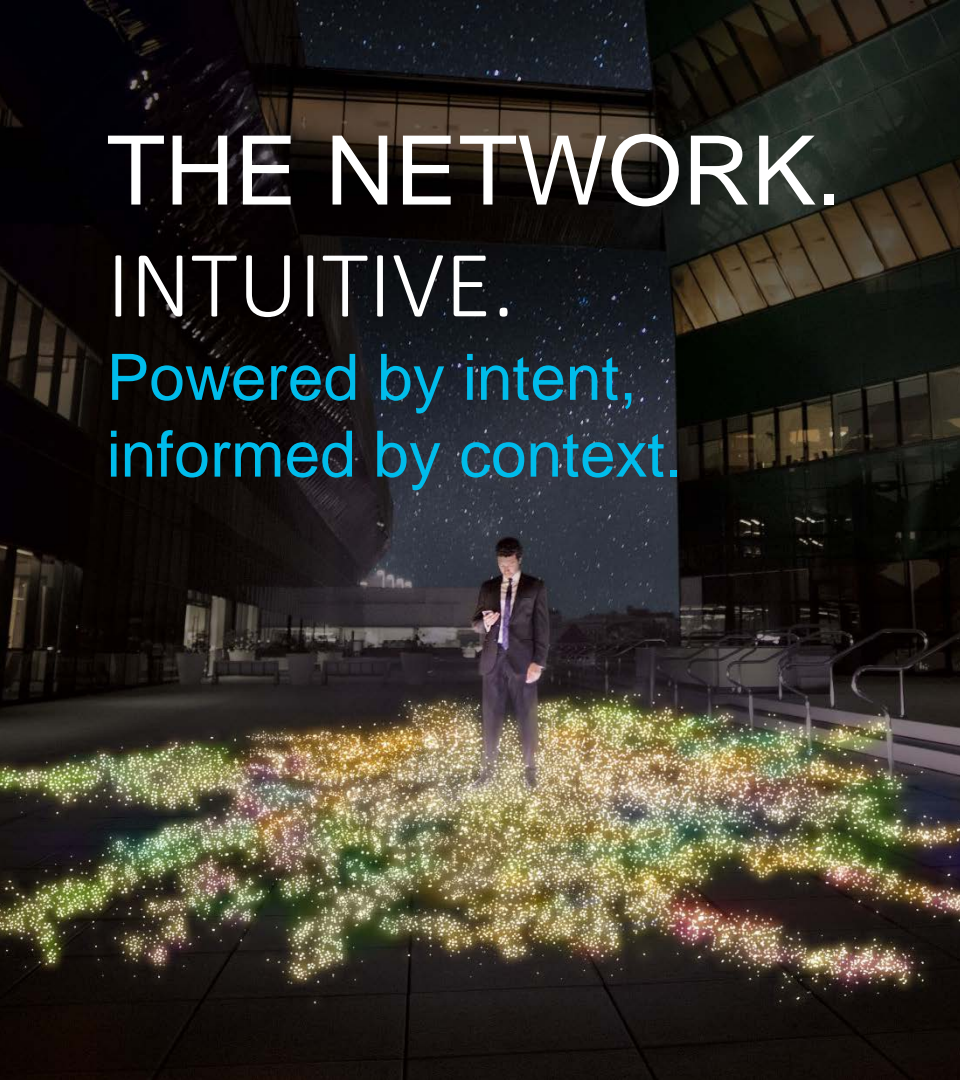
API's

Open Application
Programming Interfaces are
available to be consumed by
our customers and
partners...



THE NETWORK. INTUITIVE.

Powered by intent,
informed by context.





Quienes sobreviven no son los más fuertes ni los más inteligentes, sino quienes se adaptan mejor.

