DNA Analytics and Assurance

Vedran Hafner, vehafer@cisco.com

Cisco's Intent-based Networking

DNA Center

Policy   Automation   Analytics

Learning

Intent

Context

Security

Intent-Based Network Infrastructure

Switching   Routers   Wireless
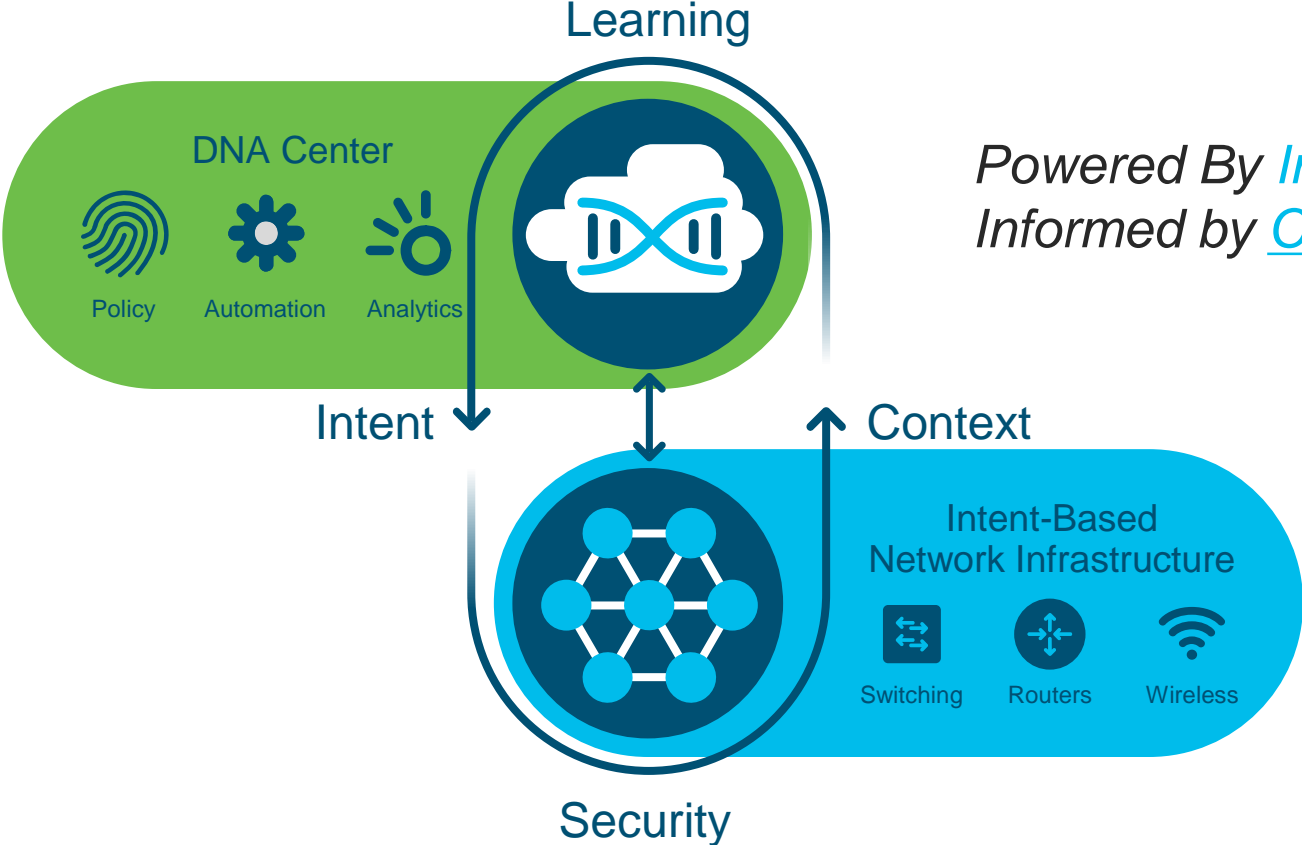
Powered By Intent.
Informed by Context.

Biggest Consumer of IT Time: 43% Troubleshooting

4x
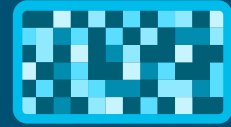
Network operators spend more time collecting data than analyzing while troubleshooting
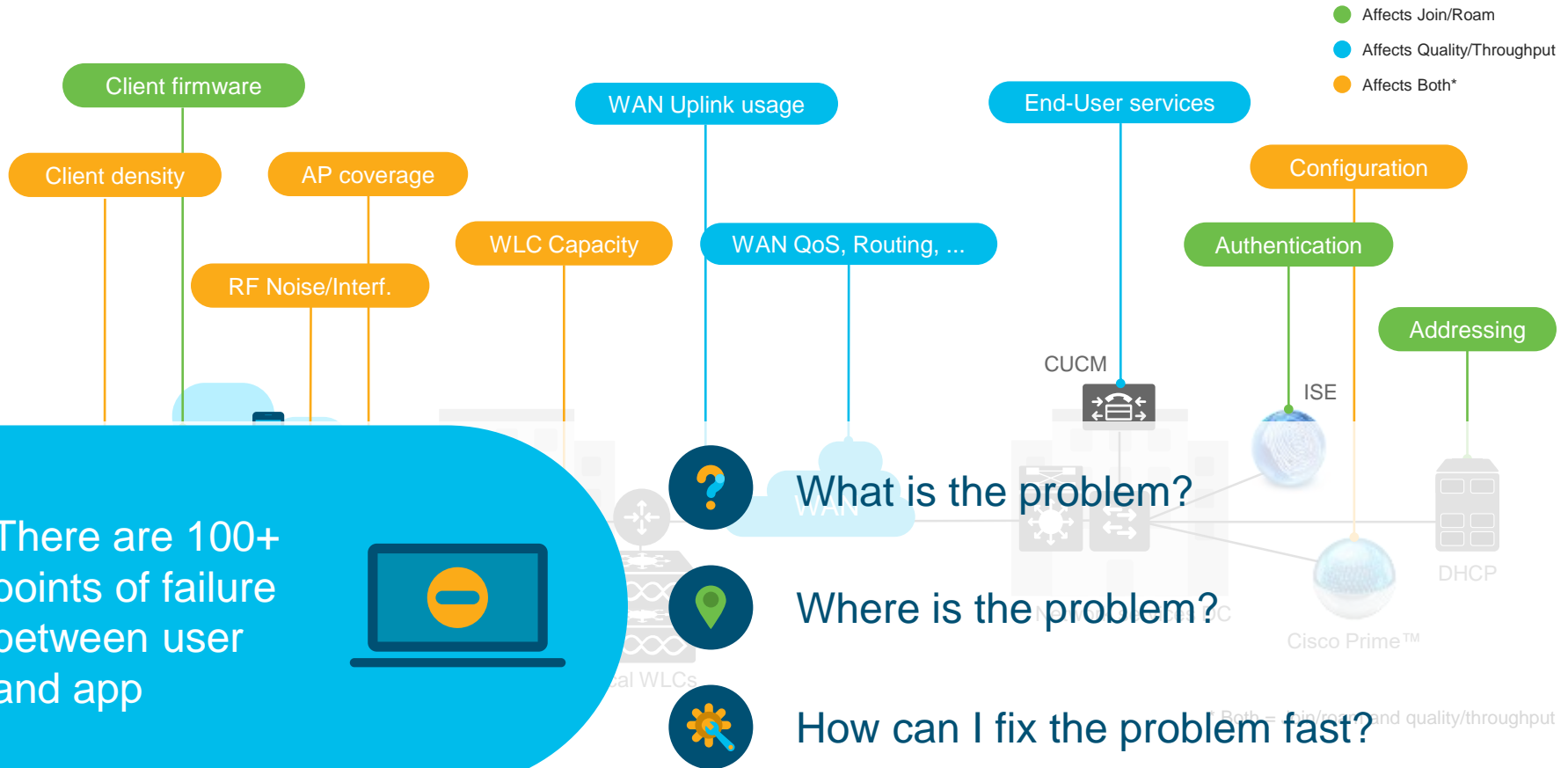
Replication challenge

Troubleshooting an issue can be impossible if IT can't replicate the issue or see the issue as is it happening real time

Slow resolution

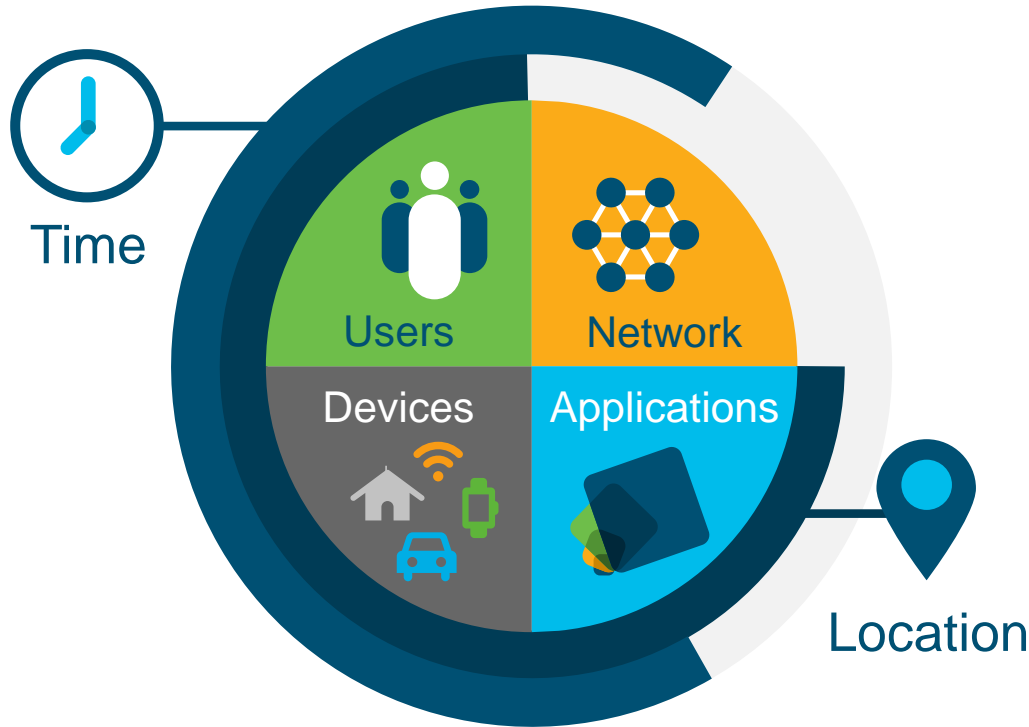Downtime is expense; unplanned downtime cost Fortune 1000 $1.25-2.5B annually

Network Quality is a Complex, End-to-End Problem

Legend:
- 🟢 Affects Join/Roam
- 🔵 Affects Quality/Throughput
- 🟠 Affects Both*

Client firmware

Client density

AP coverage

RF Noise/Interf.

WLC Capacity

WAN Uplink usage

WAN QoS, Routing, ...

End-User services

Configuration

Authentication

Addressing

CUCM

ISE

DHCP

WAN

Cisco Prime™

Local WLCs

There are 100+ points of failure between user and app

❓ What is the problem?

📍 Where is the problem?

⚙️ How can I fix the problem fast?

* Both = join/roam and quality/throughput

CONTEXT MATTERS

In this Environment, Context is Key

Time

Users

Devices

Network

Applications

Location

Cisco Context

360-degree Visibility

+

Data Granularity

+

Historical, Real-time, Future

Rich Context Increase Business Productivity and Frees Up IT Time

Introducing DNA Assurance

End-to-End Visibility

360⁰ view across network

Historical view

Ability to follow the network path

Proactive & Predictive Insights

Proactive to get ahead of the problem

Predictive to stay ahead

Assessment to see impact of changes

Guided Remediation

Today—Remediate with user input

Future—Automated remediation

Transforming network operations through actionable insights and simplicity

Today's tools are limited and do not address network needs

Too Many Tools

Fragmented visibility

Closed interfaces / Silo'd views

Devices queried multiple times

Different protocols/mechanisms

Reactive Systems

Always playing catch up

Not designed for analytics

Inconsistent API architecture

Specialized knowledge required

Limited Insights

Limited data that is not actionable

My report vs your report

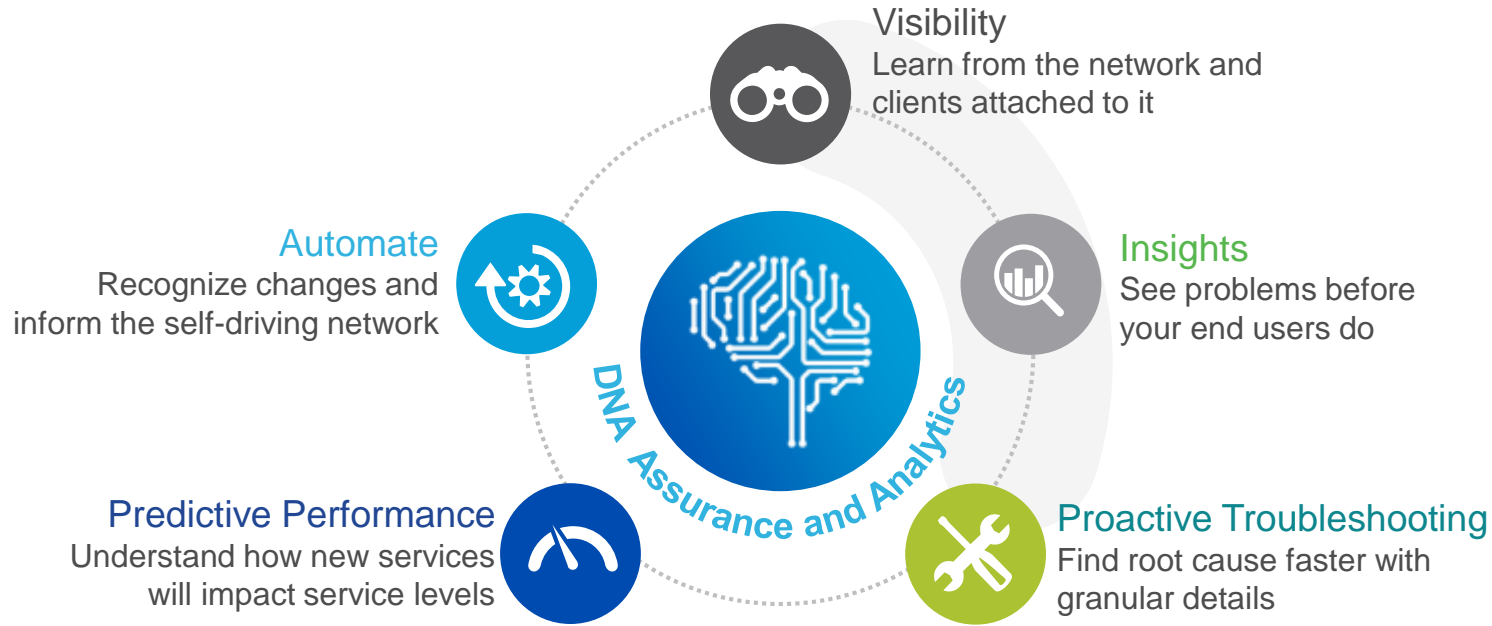No view of state changes

Lacking context or feedback loop

| Rigid | Closed/Proprietary | Lack of Intelligence |

DNA Assurance and Analytics
Converting Data to Business & IT Insights

Visibility
Learn from the network and clients attached to it

Automate
Recognize changes and inform the self-driving network

Insights
See problems before your end users do

Predictive Performance
Understand how new services will impact service levels

Proactive Troubleshooting
Find root cause faster with granular details

DNA Assurance and Analytics

Industry's First Self-Predicting Network Analytics Platform

End-to-End Visibility and Insights

End user **Client** on-boarding and connectivity

Network health and status

Application visibility and performance

APP

CUCM

Mobile Clients

APs

Office Site

Local WLCs

Network Services DC

NMS

DHCP

SFCDC
SNOW
BOX

Cloud Apps
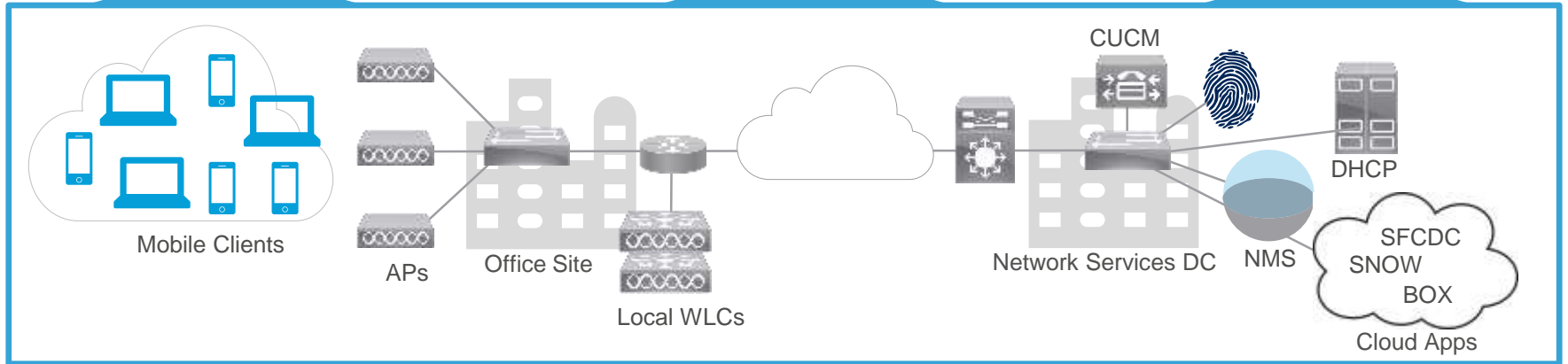
DNA Assurance is part of DNA Center

Automation

Design	Provision	Policy

Design
- Global settings
- Site profiles
- DDI, SWIM, PNP
- User access

Provision
- Fabric domains
- Device on-boarding
- Device inventory
- Host on-boarding

Policy
- Virtual networks
- ISE, AAA, Radius
- Access control
- Application control

Assurance
- Issues and trends
- Performance
- Proactive troubleshooting

Planning, installation and migration

Proactive and predictive network, client and application assurance

Power of Analytics and Automation working in sync
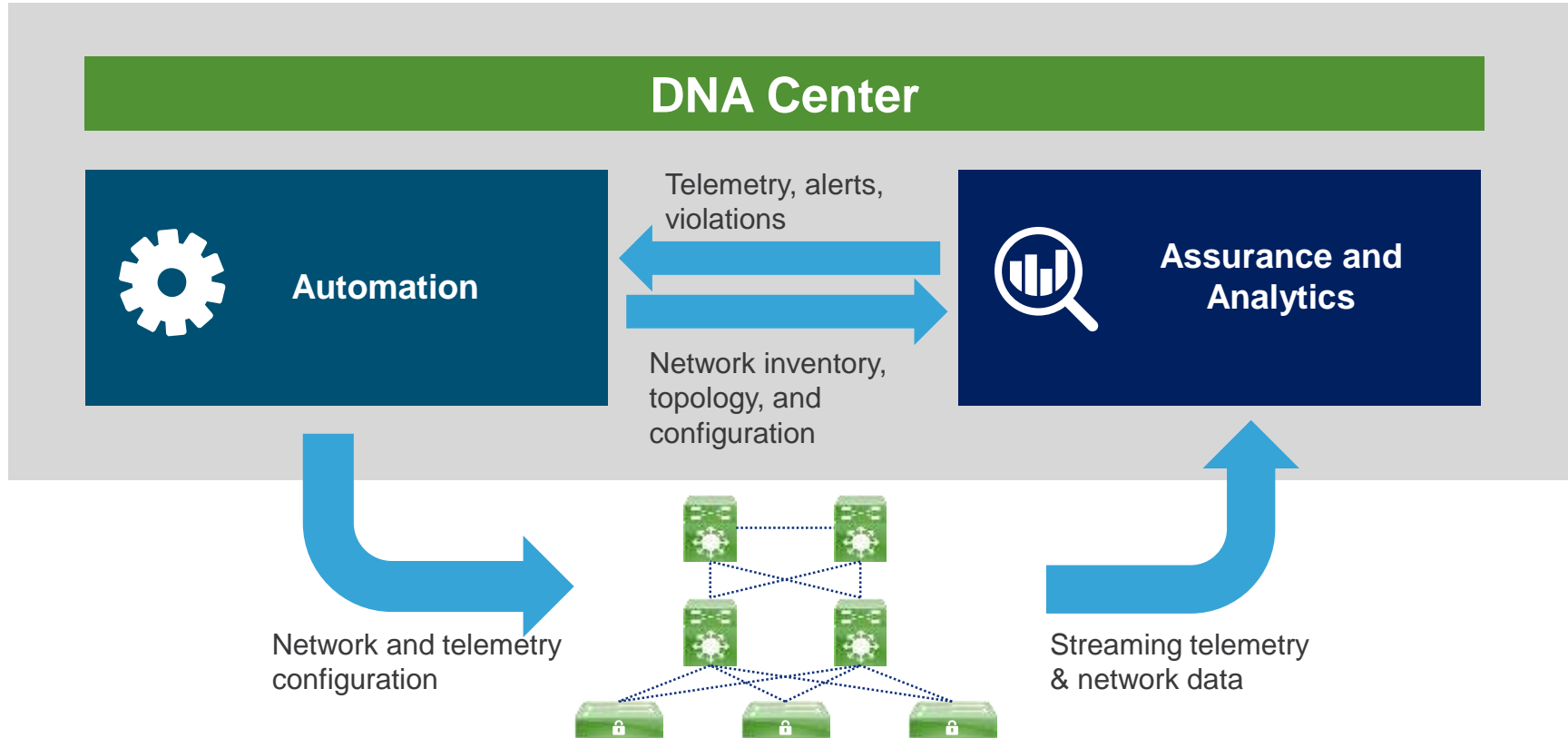
Telemetry Collection

What types of Collection mechanism are used?

Data Type: Users, User Group
Data Source: AD, Cisco ISE
Mechanism: Pull (API)

Data Type: Policy
Data Source: Cisco ISE
Mechanism: Subscription through PxGrid

Data Type: IP Address
Management, Namespaces
Data Source: Infoblox, DHCP, DNS
Mechanism: Pull (API)

Contextual Telemetry Sources

Data Type: Flow, Applications
Data Source: Network Device
Mechanism: Push

Data Type: SNMP
Data Source: Network Device
Mechanism: Pull

Data Type: Wireless
Signaling, Roaming data
Data Source: WLC/AP
Mechanism: Streaming

Data Type: Syslogs, Traps
Data Source: Network Device
Mechanism: Push

Network Telemetry Sources

A singular framework for ingestion

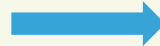# Streaming Telemetry vs. SNMP/Legacy Polling

Traditional Telemetry

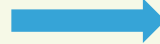SNMP / Legacy data pull methods

Streaming Telemetry

Intent-based Wireless Infrastructure

Streaming Telemetry
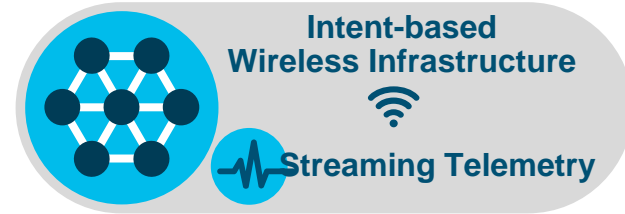
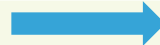| Traditional Telemetry	Streaming Telemetry
Pull based data import	Push based data export
CPU overhead with data crawlers	Low CPU overhead
Data intensive without optimizations	Optimized for Data export (KPI, Events)
No real time notification and false alarms	Notification send seconds after change
Min polling has too many black holes	Reduced delay in management data

Insights: Wireless Use Cases

Client Onboarding

- ✓ Association failures
- ✓ Authentication failures
- ✓ IP address failure
- ✓ Client Exclusion
- ✓ Excessive on-boarding time
- ✓ Excessive authentication time
- ✓ Excessive IP addressing time
- ✓ AAA, DHCP reachability
- ✓ Client Side Analytics (Apple Insights)

Client Experience

- ✓ Throughput analysis
- ✓ Roaming pattern analysis
- ✓ Sticky client
- ✓ Slow roaming
- ✓ Excessive roaming
- ✓ RF, Roaming pattern
- ✓ Dual band clients prefer 2.4GHz
- ✓ Excessive interference

Network Coverage & Capacity

- ✓ Coverage hole
- ✓ AP License Utilization
- ✓ Client Capacity
- ✓ Radio Utilization

Network Device Monitoring

- ✓ Availability
- ✓ Crash, AP Join Failure
- ✓ High Availability
- ✓ CPU, Memory
- ✓ Flapping AP, Hung Radio
- ✓ Power supply failures

Application Performance

- ✓ Sensor Tests:
- • Web: HTTP & HTTPS
- • Email: POP3, IMAP, Outlook Web Access
- • File Transfer: FTP & TFTP
- ✓ Application Experience (Packet Loss, Latency, Jitter)

Insights: Wired Use Cases

Client Onboarding

- ✓ Client/Device DHCP
- ✓ Client/Device DNS
- ✓ Client authentication / authorization

Control Plane

- ✓ Control plane reachability
- ✓ Edge reachability
- ✓ Border reachability
- ✓ MAP server
- ✓ BGP AS mismatch, Flaps
- ✓ OSPF adjacency failure
- ✓ EIGRP adjacency failure

Data Plane

- ✓ Border and edge connectivity
- ✓ Border node health
- ✓ Access node health
- ✓ Network Services DHCP, DNS, AAA
- ✓ Interface High Utilization
- ✓ Interface Flaps
- ✓ Gateway Connectivity
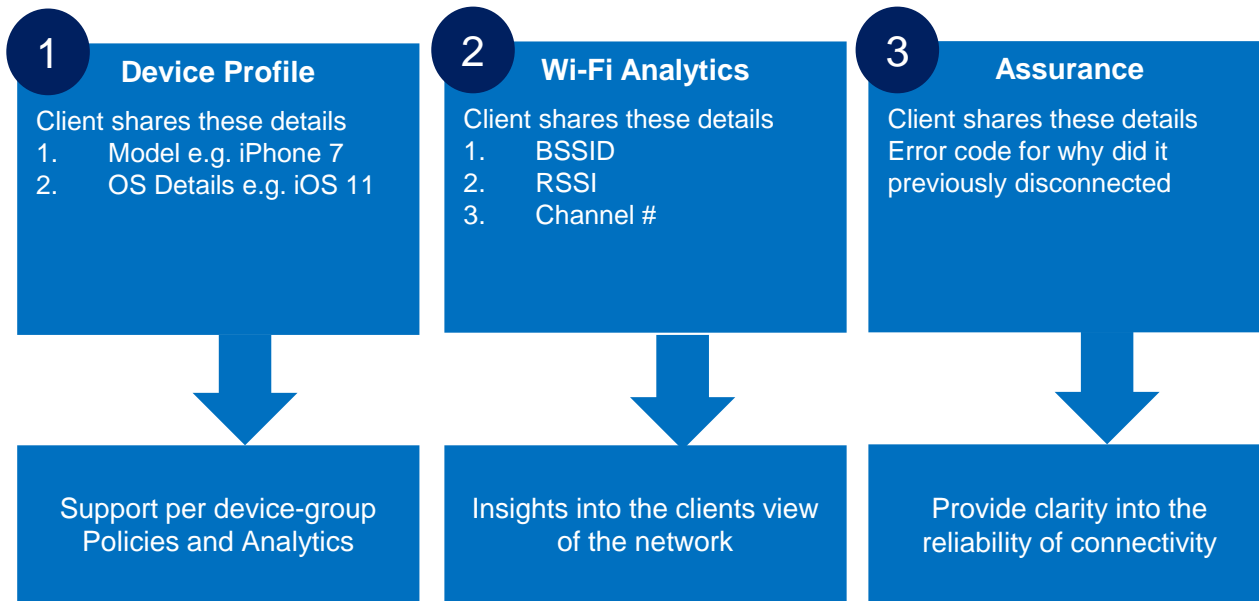- ✓ Application Performance (Packet Loss, Latency, Jitter)

Policy Plane

- ✓ ISE/PxGrid connectivity
- ✓ Border Node policy
- ✓ Edge Node policy
- ✓ SGACL validation

Network Device Monitoring

- ✓ High CPU
- ✓ High Mem
- ✓ High Temp
- ✓ Line-card
- ✓ Modules
- ✓ POE power
- ✓ TCAM Table

Advanced Client Insights– Apple iOS Analytics

1

Device Profile

Client shares these details
1. Model e.g. iPhone 7
2. OS Details e.g. iOS 11

2

Wi-Fi Analytics

Client shares these details
1. BSSID
2. RSSI
3. Channel #

3

Assurance

Client shares these details
Error code for why did it
previously disconnected

Support per device-group
Policies and Analytics

Insights into the clients view
of the network

Provide clarity into the
reliability of connectivity

+

Advanced Client Insights– Apple iOS Analytics

Detailed Client device profile information – device model, OS details

Insights into the clients view of the network – Neighboring Access Points

Provide clarity into the reliability of connectivity – client disassociation details

Capability unique to Cisco Wireless Networks only !!

Proactive Monitoring

Proactive Insights– Wireless Sensors

Test your network anywhere at any time

- ➤ On-Boarding Tests
  - • 802.11 Association
  - • 802.11 Authentication & Key Exchange
  - • IP Addressing DHCP (IPv4)
- ➤ Network tests
  - • DNS (IPv4)
  - • RADIUS (IPv4)
  - • First Hop Router/Default gateway (IPv4)
  - • Intranet Host
  - • External Host (IPv4)
- ➤ Application tests
  - • Email: POP3, IMAP, Outlook Web Access (IPv4)
  - • File Transfer: FTP (IPv4)
  - • Web: HTTP & HTTPS (IPv4)

Sensors act as clients

Access point

R1

Dedicated Sensor AP1800
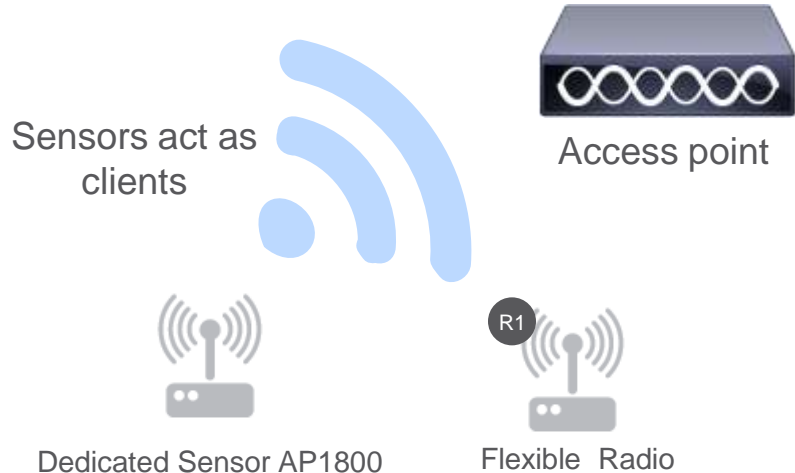
Flexible Radio

Flexible Radio Assignment Algorithm intelligently identifies excessive radios and seamlessly converts those into Sensor mode without client impact

Supported Network Devices

How About Network Platforms?
What All is Supported in DNAC 1.1?

Wireless: 11n, 11ac (Wave 1, 2) AireOS

Type	Hardware
APs	Aironet 802.11n (700, 1600, 2600, 3500, 3600)
	Aironet 802.11ac Wave 1 (1700, 2700, 3700)
	Aironet 802.11ac Wave 2 (1810, 1815, 1830, 1850, 2800, 3800)
WLCs	WLC5520
	WLC8540
	WLC3504
XOR radio and AP as a Sensor	Wave2 APs only
Dedicated Sensor	AP1800s
SDA (Fabric-Assurance)	Only on Wave 1 and Wave 2 APs

Software Releases Supported: 8.5.120 (8.5MR2)

Switching platforms

Hardware
Catalyst® 3650, 3850
Catalyst® 4500
Catalyst® 6500, 6800
Catalyst® 2960, 3560
Catalyst® 9300, 9400, 9500
Nexus 7700

Routing platforms

Hardware
ISR: 800, 1900, 2900, 3900, 4400, 4300, 4200, 1100
ASR 1K
ENCS (5400, 5100)
Virtual: CSR1K, ISRv1K

For more details of HW and SW support, please visit DNAC Device Support Matrix on Cisco.com

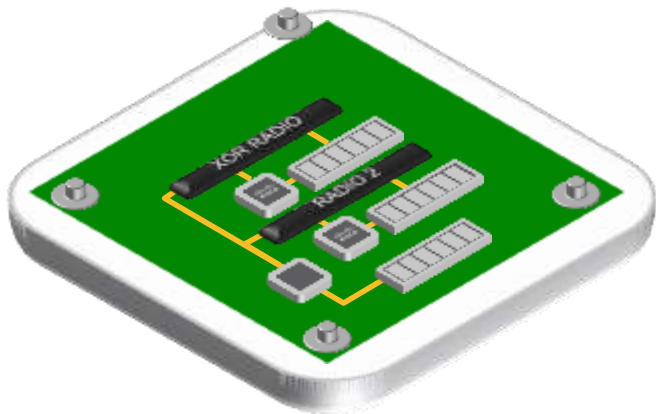# Wireless Sensor Support

Flexible Radio as Sensor (2800/3800)

Dual 5 GHz Flexible Radios
Software defined radios automatically adjust to dual 5GHz

Purpose-built Hardware for Analytics
Flexible radios can to provide simultaneous in-line monitoring to DNA for analytics and insights while serving clients (future)

🟢 5GHz.

XOR RADIO

🟠 2.4GHz.

⚫ Sensor (Client Testing)

Dedicated AP as Sensor

1815/1830/1850 AP

1815

1830/1850

1800s dedicated sensor

- 2x2 with 2 spatial streams
- Multiple powering options:
  - PoE Power
  - USB Type "C" power
  - Direct AC Power Plug
- Integrated BLE

Cisco Aironet 4800 Access Point: Next Generation Purpose-built Analytics Platform with Wi-Fi and BLE Hyper-location

Cisco Aironet® 4800

- Industry leading 4x4 MIMO 802.11ac Wave 2 access points
- Tri-radio, 802.11ac Wave 2, 160 MHz
- Built-in BLE Radio
- Combined Data Rate of 5.2Gbps
- 2 x 5 GHz: 4x4: 3SS supporting
  - SU-MIMO / MU-MIMO
  - Flexible Radio Assignment: 2.4GHz, Dual-5GHz, Wireless Security Monitoring, and DNA-C Assurance
- 1 x 2.4GHz/5GHz for DNA Analytics, Wireless Security monitoring, and Hyperlocation
- Gigabit Ethernet and multi-Gigabit Ethernet (1G, 2.5G, 5G)
- Built-in Hyperlocation Antenna Array 16-elements <3m Acc (median)
- HDX Technology
- USB 2.0
- Analytics enabled, DNA Ready

Redefining Analytics and Location

Health Scores

Site Health Score ＝ *function* (Client Health Score, Device Health Score)

Client Health Score ＝ *function* (Onboarding Score, Connectivity Score)

Client 360

10/10 daphine.blake

Daphine-iPad   Daphine-PC

Device Health Score ＝ *function* (System Health Score, Control Plane Score, Data Plane Score)

Device 360

6/10   AP LA1-AP3802-21   Global / USA / Los Angeles / Level 26

Device Model: AIR-AP3802I-B-K9   IP Address: 10.30.18.12   Software Version: 8.5.107.102

Application Health Score ＝ *function* (Traffic Class, Latency, Packet Loss)

Name	Domain Name	Health	
		Most Recent	Last 24 Hours
All Applications			
disney-web-portal	www.disney.com	10	View
espn-browsing	www.espn.com	1	View

Thank You