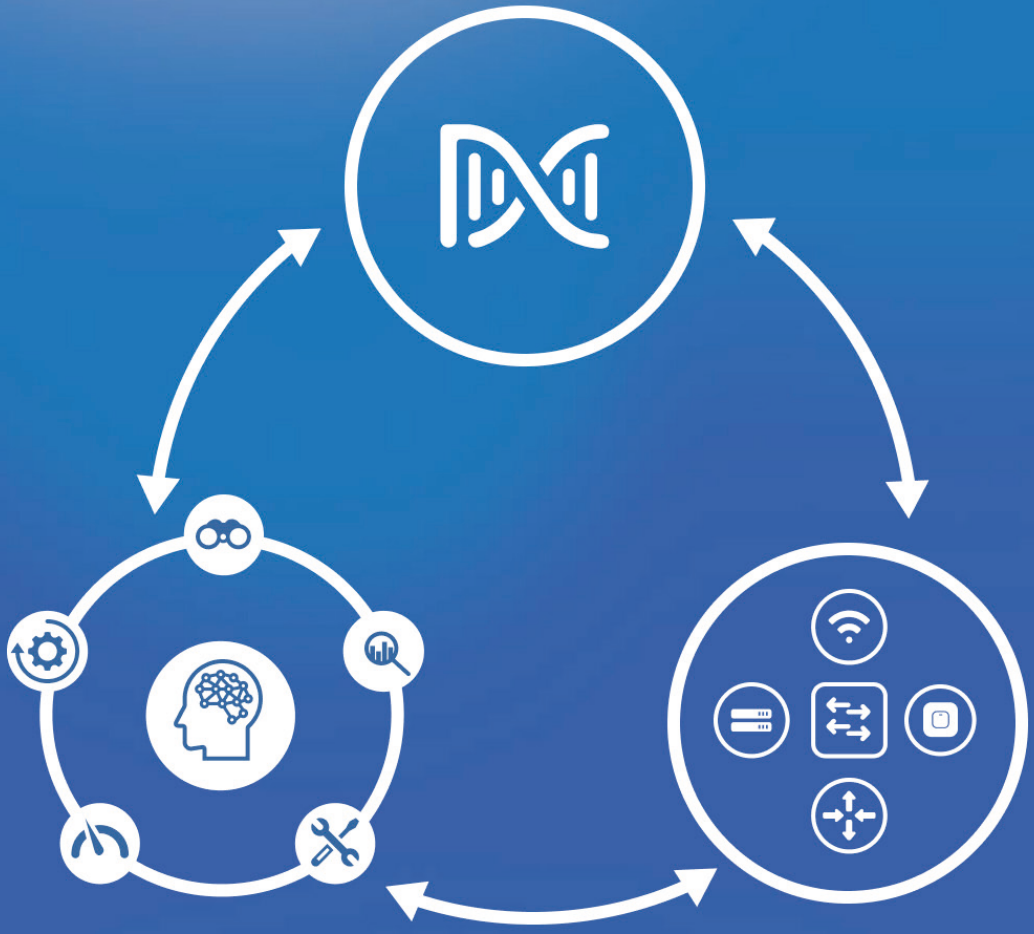
Cisco DNA Assurance

Unlocking the Power of Data



cisco

Cisco DNA Assurance

Unlocking the Power of Data

Table of contents

Preface

Authors

This book represents a collaborative effort between Technical Marketing, Product Management, Customer Experience, Engineering, and Systems Engineering during a week-long intensive session at Cisco Headquarters in San Jose, CA.

- Dave Zacks - Technical Marketing
- Ina Singh - Engineering
- Jeremy Cohoe - Technical Marketing
- Karthik Kumar Thatikonda - Technical Marketing
- Markus Harbeck - Systems Engineering
- Matt Swartz - Customer Experience
- Meghna Muralinath - Technical Marketing
- Min Se Kim - Technical Marketing
- Saurav Prasad - Technical Marketing
- Shyam Sundar Srinivasan - Product Management
- Sumit Patel - Product Management
- Taranpreet Kohli - Product Management
- Tim Szigeti - Technical Marketing

Acknowledgements

A special thanks to Cisco's Enterprise Networking Business Product Management, Engineering, Sales and Customer Experience teams who supported the realization of this book. Thanks to Carl Solder, Ronnie Ray, Greg Dorai, Chandan Mehndiratta, Ramit Kanda, Prakash Rajamani, Kaushik Dam, Philippe Ciampossin, Rakesh Thaker, Jeff McLaughlin, Bipin Kapoor, Joe Bounour, Jonathan Leary, James Mobley, Odysseas Charalambous and Kay Wintrich for supporting this effort. We would also like to thank Sehjung Hah for extending support throughout our journey to make sure that everything worked smoothly (including making sure we were all fed and watered), and Christina Munoz for her exceptional resource organization.

We are also genuinely appreciative to our Book Sprints (*www.booksprints.net*) team:

- Adam Hyde (Founder)
- Barbara Ruhling (CEO)
- Karina Piersig (Operations and Service Design)
- Lennart Wolfert and Henrik van Leeuwen (Illustrators)
- Juan Carlos Gutiérrez Barquero (Technical Support)
- Agathe Baëz (Book Producer)
- Laia Ros (Facilitator)
- Raewyn Whyte and Helen Kilbey (Proof readers)

Laia and the team created an enabling environment that allowed us to exercise our collaborative and technical skills to produce this publication to meet a growing demand.

Organization of this book

This book is structured to keep it informative for multiple personas within the Enterprise. The first few chapters cover Cisco's broader networking vision, how Cisco DNA Assurance fits into it, and the high-level concepts related to Assurance. Chapters in the middle are focused on real-world use cases that Cisco DNA Assurance helps to solve. The closing chapters focus on discussing Cisco DNA Center architecture, recommendations, and best practices.

While readers are highly encouraged to read the book in its entirety to get a complete understanding of Cisco DNA Assurance, here is some high-level guidance which may be useful.

- The big picture for Business Decision Makers Chapter 2, Chapter 3 and Chapter 4
- The practical approach for Technical Decision Makers - Chapters 5 through Chapter 8
- How to get started for Implementors - Chapter 10, Chapter 11 and Chapter 12

Note that this book is not meant to be a substitute for the Cisco DNA Assurance deployment or user guides.

Intended Audience

This book focuses on transforming network operations through actionable insights and simplicity using Cisco DNA Assurance. While network managers, network operators, help desk personnel, problem managers and service managers are likely to reap maximum benefit from this book, other IT professionals can leverage it to understand Cisco's Digital Network Architecture vision and the role of Cisco DNA Assurance in increasing IT productivity by streamlining network operations.

Book Writing Methodology

> *"Write. Rewrite. When not writing or rewriting, read. I know of no shortcuts."*
> *– Larry L. King*

We started writing this book about Cisco DNA Assurance by first acknowledging the reading habits in the *digital era*. Significant time and effort was invested to ensure that the book caters to a wide variety of audiences from business decision makers to technical experts. Assurance, part of the Cisco Digital Network Architecture, is foundational in providing the insights that are needed to effectively operate today's complex networks.

The Book Sprints (***www.booksprints.net***) methodology helped in capturing each of our unique strengths, fostering a team-oriented environment, and accelerating the overall time to completion.

We survived the hundreds of hours of work in writing, reviewing and re-writing the content to present you with a practical book highlighting how Cisco DNA Assurance can change the way you monitor, troubleshoot and assure network operations! Read on!

Setting the Stage - IBN and Cisco DNA

Intent-Based Networking (IBN)

Cisco has pioneered a new approach to network deployment and operation - Intent-Based Networking (IBN). IBN is a completely new approach by which organizations are able to implement, operate, maintain, and grow their networks. IBN is focused on several key outcomes that are critical for organizations today - and tomorrow. These include providing automated, standardized, and simplified design and deployment options for sophisticated network functions and capabilities, and allowing network performance to be continuously optimized to align to the changing needs of the applications that run the business.

To really appreciate the value of the IBN and why it is such a revolution in network design, operation, and use, it is important to review and understand the ways in which Enterprise networks have traditionally been implemented.

Traditional Network Deployment - Overview and Challenges

For many years, networks have been implemented by highly-trained and experienced network operators manually with extensive use of the CLI (Command Line Interface), and in some cases automated by the same individuals using customized scripting. However, even with scripting, the deployment - and subsequent operation - of a large, geographically-distributed network remains a very daunting task for most organizations.

Consider what is needed today to roll out a new application (such as a Point of Sale system) across an Enterprise network, and to prioritize that application appropriately to receive the necessary service level from the network (for example, relative priority vs. other applications competing for such traffic).

Typically, such roll out involves classifying the application traffic in the network (based on IP subnet/addresses and TCP port numbers, for example), and then assigning this traffic to a given queue, based on its relative priority. Sounds simple enough, doesn't it?

But as always, the devil is in the details. Network devices quite often have different queue structures and QoS capabilities complicating the configuration. Add this complexity across many devices in the path, multiply this by the applications involved, and factor in various software versions, and you begin to grasp the magnitude of the problem. And for the next application that comes along? Rinse and repeat. Very time-consuming, very manual, and very prone to human error.

And further consider the issues that then arise if traffic is misclassified across the network at any point. The result would be poor application experience and delays in access to data - very obvious to end-users and severely impacting their productivity. Finding the location in the network where the traffic is being misclassified or tagged inappropriately would be extremely difficult and time-consuming.

It is to address such tasks, which are the life of the network architect, network manager, and network operations staff, that Intent-Based Networking was created. This is just one example of the many challenges that IBN can help to address - and in the following section, we will begin to see the power of IBN in action to address challenges such as this. However, keep in mind that the broad-ranging set of capabilities that IBN brings for Automation and Assurance go well beyond this single use case. IBN in fact not only provides a new set of capabilities, and does so in a very innovative yet simplified fashion - it actually changes the paradigm in network deployment and use. Let's begin to explore how.

Intent-Based Networking - A New Paradigm

What if a network manager had a tool to input which applications were to be prioritized relative to others, and then press a button?

What if that same tool understood the network topology involved and could render the network manager's "intent" - i.e. "it's my intention to prioritize this application vs. this other one when bandwidth is constrained" - into all of the appropriate device-level configurations for all of the various network devices involved?

What if that tool could then distribute those machine-generated configurations automatically onto the network devices without human errors, typos, or scripting?

What if this intent could also be triggered through APIs using external applications?

And what if the same tool could analyze the resulting network deployment and automatically spot issues with application performance and network quality when they arose? What if the tool could then not only alert the network manager to an issue, but actually guide them to the root cause and suggest the appropriate resolution?

In other words, what if a network manager could have their intent translated into action - rapidly and automatically - and be assured that the network was continually performing as it needed to? This is the essence of Intent-Based Networking.

Cisco's solution to the aforementioned QoS example would be Cisco DNA Center's Application Policy combined with Cisco DNA Assurance - an excellent example of the Cisco IBN vision in action. Using Cisco DNA Center Application Policy, a network manager can roll out an entire Enterprise QoS deployment across the network's end-to-end infrastructure with merely a few clicks - with the system (based around the Automation functions in Cisco DNA Center, Cisco's Enterprise controller platform) translating their intent into action, and without the network manager needing to be concerned with the details of individual platform implementations.

And once these capabilities are rolled out, the same Cisco DNA Center can also provide Cisco DNA Assurance functionality to continuously measure whether that stated intent is being accomplished by the network infrastructure, and provide issue identification with remediation if it is not. This set of Assurance capabilities is the focus of this book.

Intent thus applies equally for both Automation and Assurance. Intent-Based Networking serves as the basis for a revolution in network design, operation, and ongoing use. The network will no longer be a bottleneck to the rollout of new applications and services. With IBN, new applications, new network deployment models (such as Software-Defined Access and Software-Defined WAN), and new network devices and services, can very simply be designed, deployed, managed, and updated - in a highly-automated, predictable, and streamlined fashion.

Essentially, IBN allows a network architect to define their “intent”, and then have this rendered into the appropriate set of “actions” to realize that intent within the underlying network infrastructure, in a simplified and standardized fashion. This includes not only the intent associated with automating a set of capabilities, but also the intent to then continuously monitor the network deployment, recognize and respond to trends and anomalies, and continuously optimize the network to maximize the performance of the organization's most critical applications and users.

Cisco Digital Network Architecture, DNA, is the master blueprint for Enterprise network deployments, and provides the framework against which all Cisco products are developed - switches, routers, WLAN controllers, access points, and more. Cisco DNA defines the key attributes and capabilities such products, and the solutions they support, must provide.

The key to realizing the IBN vision is Cisco's Digital Network Architecture, along with Cisco DNA Center - Cisco's controller for the Enterprise network domain.

Let's explore those now.

Cisco Digital Network Architecture (DNA)

Cisco DNA comprises Cisco's overall strategy for Enterprise network design, deployment, and operation. It consists of several major building blocks as outlined below.

Policy

Cisco DNA provides a robust environment within which network architects and managers can define and deploy network-wide policies end-to-end. These could include QoS policies to provide application prioritization, security policies controlling user and service access, or policies for gathering network data for capacity planning and issue identification / remediation. Policies within Cisco DNA are generally expressed at the Intent level and then translated into appropriate device-level configurations via tools such as Cisco DNA Center.

Automation

Automation capabilities enable Cisco DNA to understand the network overall, device families, roles of devices, and topology. Automation realizes the deployment intent that the user has expressed, and translates that into standardized, automated configurations pushed out to network devices. Cisco DNA Center implements simplified, yet powerful, automation capabilities for the Enterprise network.

Analytics and Assurance

Analytics enables Cisco DNA to gather the relevant data from the network, store this in highly-efficient industry-leading databases, and employ smart algorithms to correlate this data. From this, conclusions can be drawn, issues identified, and remediation applied to ensure that the intent specified by the end user is, in fact, being realized. Cisco DNA Assurance allows the network manager to easily consume the vast amount of data generated by the Enterprise network. This data is consolidated and rendered into an easy-to-understand form to identify issues, determine the root causes for those issues, and drive guided remediation efforts as issues are resolved.

Virtualization

Virtualization allows for network services to be deployed on a physical (appliance) or virtual (software) basis, as designated by the network manager. Leveraging virtualization, key capabilities can more quickly be designed, deployed, and managed at various locations across the Cisco DNA-based network system. Virtualization allows for flexibility and enhances deployment speed, making the network deployment - and the organization - more agile.

Programmable Infrastructure

Programmable infrastructure encompasses two important aspects within a Cisco DNA deployment. First, network elements can contain flexible hardware components. An example of this are the Catalyst 9000 switches, which leverage the UADP (Unified Access Data Plane) ASIC (basically, the "heart" of the switch platform). UADP is flexible and can be adapted to new protocols and encapsulations over time via a simple software upgrade. This allows even brownfield devices based on UADP (such as the Catalyst 3850) to be upgraded to support new, market-leading solutions such as Software-Defined Access, allowing new and more advanced capabilities to be implemented in a simplified fashion. In addition, Cisco DNA-capable network devices and functions leverage a set of API (Application Programming Interface) frameworks which enable simplified interaction between devices. Selected sets of these APIs can then be exposed both northbound and southbound from network and management elements, supporting custom use cases and integration of disparate systems.

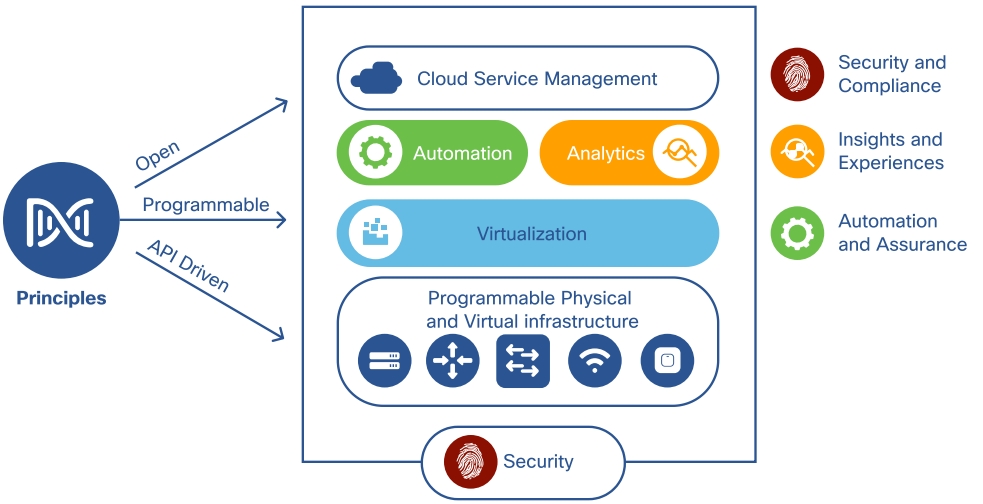
Cloud Integration

Cloud integration allows Cisco DNA functions to integrate with on-premise elements as well as cloud-based components. By leveraging the best of cloud integration and on-premise deployments, Cisco DNA allows the Enterprise to reap the benefits of cloud-based services including simplified integration, rapid deployment, and consistent services across the organization.

Security

Finally, all functions deployed in the network must incorporate a secure approach, both for the devices themselves as well as their method of deployment and use. In today's Enterprise network, an inherently-secure system is key to the continuous operation of the Enterprise. To this end, Cisco's DNA approach incorporates security at every level within the system, and within every device and solution as deployed.

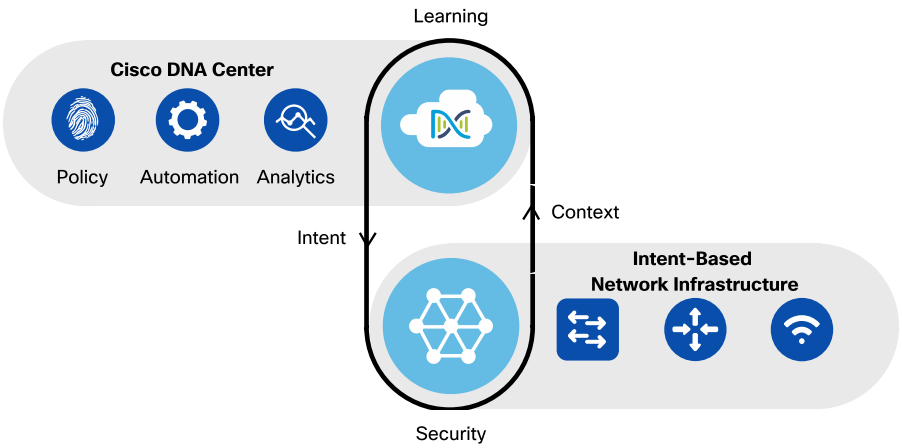
DIAGRAM Cisco Digital Network Architecture



Intent-Based Networking with Cisco DNA

As shown in the following illustration, in the Intent-Based Network system leveraging Cisco DNA, intent is expressed by the network manager into tools such as Cisco DNA Center, which then renders that intent down into device-specific configurations and then pushes these onto the network devices involved with the appropriate level of network-integrated security.

DIAGRAM Intent-Based Networking Overview



Data can then be extracted from those same network devices and analyzed by Cisco DNA Center, which is then leveraged by the network manager to assist in creating a "closed-loop" system of network operation. The system is constantly learning how the underlying network is functioning. Cisco's DNA helps Enterprises prepare for growth and change, in a robust, simple, and scalable fashion.

The solution overall is designated as "The Network. Intuitive", with Cisco's DNA as the foundation for this.

In summary, Cisco DNA provides the framework for the integration, deployment, and operation of next-generation Enterprise networks. Going forward, let's proceed to examine one of the key elements of Cisco DNA associated with Assurance - namely, Cisco DNA Center.

Cisco DNA Center and Cisco DNA Assurance

Introducing Cisco DNA Center and Cisco DNA Assurance

Cisco DNA Center is a key element of the Cisco DNA architecture, providing a controller-based solution for network design, deployment, and ongoing operation.

Cisco DNA Center provides two key sets of capabilities in a single, integrated system: Automation and Assurance. Automation serves to support use cases such as the deployment of Quality of Service (QoS) through the Application Policy framework. Assurance, on the other hand, is focused on extracting data from the underlying network infrastructure. Data such as Streaming Telemetry, NetFlow records, SNMP, and Syslog are collected and correlated, providing key insights into network operations and utilization and enabling a focus on what really matters: the user-to-application experience.

Cisco DNA Assurance is vital to understanding how the network is performing, and answering questions such as:

- Is this application being handled and prioritized across the network as intended?
- Are there any issues with application or network performance that are affecting users, and if so, where and when?

In other words, Assurance helps the Network Manager understand if their intent is being carried out appropriately in the network. It also allows for faster response to any issues that may occur, by utilizing machine-based data collection, correlation, and simplified issue reporting.

Both Automation and Assurance are key parts of Cisco's Intent-Based Networking vision. However, Assurance is the primary focus of this book. Knowing the capabilities that Cisco DNA Assurance offers, and then getting hands-on and trying Assurance out,

will enable a much better understanding of how IBN operates and how it can be deployed.

To that end, the challenges with Enterprise networks today are now reviewed, and how Cisco DNA Center and Assurance help to address those challenges. After this, some of the IT customer roles that might leverage Cisco DNA Assurance within an organization are briefly discussed, followed by a detailed examination of many of the components and capabilities that make up Cisco DNA Assurance and enable its sophisticated set of functionalities. And finally, multiple use cases are delved into in detail to show Cisco DNA Assurance in action.

So read on! The journey into the world of Cisco DNA Assurance, a key pillar of Cisco's Intent-Based Networking vision, begins now.

Why Do We Need Assurance?

Customers wishing to delve into the world of Assurance may want to start with a simple question or two: “Why do I need Assurance in my network?" as well as "What problems does Assurance solve?”

Good questions! The text in this chapter will address the key issue in both of these questions: "What value can Assurance provide?"

This question is answered by examining some of the key issues in Enterprise networks today, and reviewing how Cisco’s Assurance capabilities help address these issues. Assurance provides visibility for users and applications, deeper insights into network issues, and drives actionable outcomes for the business.

To appreciate what Assurance provides, let's start by examining today's Enterprise network - its importance, its issues, and the challenges it faces.

The Importance of the Enterprise Network

Today’s Enterprise network is critical to the proper functioning of the organization.

Stop and think for a minute about what runs over the Enterprise network infrastructure today. Various applications, user communities, and numerous types of devices attach to the network. Over the last several years, everything has become network-attached and this trend is not only continuing, it is accelerating. No longer are just PCs attached to the network to access business applications, email, and web-based applications. Today, everything from IP phones, IP cameras, to door locks and badge readers - and much more - are in use, with many of these services being business-critical.

In addition, more IoT devices are being attached to the network every day, including integration of HVAC (Heating, Ventilation, and Air Conditioning) systems, POS (Point of Sale) terminals, lighting systems, elevator controls, and more. All of these services are

being attached to, and are becoming dependent on, the Enterprise network infrastructure. Looking to the future, this will likely only increase in the diversity and volume of applications.

Many of these functions are vital to the overall operation of the organization. The Enterprise network is the key element that ties all of these functions together. However, as a critical organizational asset, the Enterprise network today also faces many challenges. These include:

- **Increasing reach:** Many organizations today are extending their networks into "non-traditional" areas and deployments. Whether this means deploying networks in cruise ships, casinos, underground mining sites, or other areas, the Enterprise network today is called into service well beyond the traditional carpeted office spaces of the past. As the reach of the Enterprise network grows, so does the need to rapidly identify and resolve network issues in a wide variety of deployment scenarios.
- **Increasing complexity:** Driven by the need to support more and more functions, the network has also become increasingly complex for many organizations. Whether integrating QoS capabilities for enhanced application experience, embracing Network Virtualization to assist with integrated security, or providing connectivity in many non-traditional network locations, the Enterprise network has become ever more complex. Network managers today are being challenged to keep up.
- **Increasing level of threats:** The Enterprise network faces many threats from both internal and external sources. Network-based attacks can appear and spread very quickly and can have a severe impact on the business. Given the criticality of the functions accessed over the network, providing rapid visibility into such threats, or blocking them in the first place, is top-of-mind for many network managers.

In short, the Enterprise network today is **business-critical** for many organizations and is likely to be even more so in the future.

Given this, many organizations would like to have greater visibility into their networks, more insights into how their applications are performing, and a clearer picture of the actual experiences of end users and customers.

Today, a large portion of IT budgets are focused on network operations, with the majority of that spend focused on providing better visibility and troubleshooting. That said, many organizations today still feel they lack the insights into the operation of their network that they wish they had.

The widely-distributed network systems of today are a Big Data problem on steroids! Too many Syslog messages, SNMP data and NetFlow records... just to name a few. As the network becomes more complex and integrates more and more users, devices, and applications, this issue becomes ever more acute.

Many Enterprises today need a level of visibility greater than that provided by traditional NMS (Network Management System) tools. One of the challenges of NMS tools is not that they provide **too little data** on network performance – in many cases, it is that they provide **too much data** ... far too much data, from too many diverse sources, for a network manager to absorb, integrate, and take action on. The data is neither interpreted nor correlated which makes it in many cases impossible to consume.

What is needed is not more data, rather, it is **insights** into actual network operation – insights that are actionable to help drive outcomes for the business.

What is the network manager to do? How can he or she not only keep pace but also get ahead of the curve - moving from a reactive approach to a more proactive stance in improving the operations of the Enterprise?

Good questions. Let's proceed, and examine first a few more details about the challenges with traditional NMS approaches, and then move on to review how Cisco DNA Assurance changes the paradigm - providing Enterprises with greater visibility and control of their critical network environments, and simpler, more rapid, and more accurate service for their end users, customers, partners, and applications.

Challenges with Traditional NMS

Traditional network management systems (NMS) have many limitations that render them insufficient to meet the needs of today's enterprise networks along with business needs. For example:

- NMS systems often rely on legacy polling-based protocols such as Simple Network Management Protocol (SNMP). These protocols place heavy loads on the network to gather data, both in terms of CPU cycles and network bandwidth.
- The SNMP Management Information Base (MIB) is often polled to obtain a single Key Performance Indicator (KPI), which results in significant inefficiency.
- It is up to the operator to know which KPIs are of interest and where to find them. Furthermore, the operator needs to interpret the data, to discern if that individual KPI value is "good" or bad". If the values are "bad" then the operator needs to decide what to look for next in order to troubleshoot the issue to its root cause.
- Finally, resolution may be contingent on the issue actually happening at the time the network operator is troubleshooting, which may not be the case, especially for intermittent wireless client issues.

Managing network operations via NMS tools is becoming increasingly untenable for IT departments. This challenge is exacerbated by myriad inconsistent and incompatible hardware and software systems and devices. Furthermore, troubleshooting network, client, or application issues is a complex problem that can often involve dozens of points of failure between the user and the application. These network troubleshooting challenges include:

- **Data collection**: Network operators spend four times longer collecting data than they do analyzing and troubleshooting it, especially without knowing when the data was relevant to the issue being investigated.

- **Replication**: It is extremely difficult for network operators to troubleshoot issues that are not manifesting when they begin troubleshooting, which may be minutes, hours, or days after the reported event. When operators are unable to detect or replicate the issue they are unable to effectively investigate it further.
- **Time to resolution**: Some network quality issues require many hours to identify the root cause as well as to implement a resolution.
- **The network is to blame**: The network is often blamed first as the cause of the problem, but in many instances, it is not at fault. Network operators spend considerable time proving the network's innocence.

These are some of the challenges that Cisco DNA Assurance helps to solve.

Introduction to Cisco DNA Assurance

Cisco DNA Assurance changes the paradigm by which Enterprises approach the thorny issues of maintaining their network, troubleshooting issues as they arise, and planning for future growth.

Assurance integrates rich contextual data from many sources. It provides correlation and summarization, driving simplified and actionable insights for the overworked network manager. When the network manager encounters a problem today, he or she is presented with a screen with many data points and has to search for the needle-in-the-haystack to determine what the issue is. With Cisco DNA Assurance, they would instead be able to rapidly identify the actual root cause of a network issue, and would be provided with guided remediation for accurate issue resolution. To do this, Cisco DNA Assurance leverages time-series databases, sophisticated analytics, and machine learning.

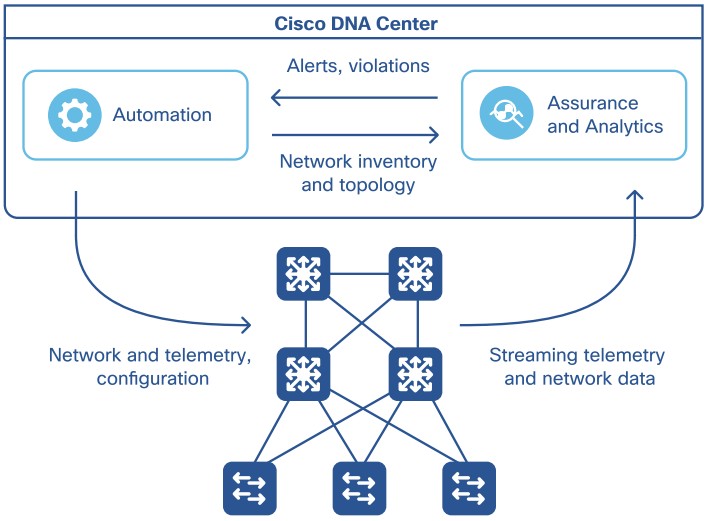
Using Cisco DNA Assurance, network managers get a bird's-eye view of the current operating state of the entire network. Rather than presenting the network manager with hundreds of data points, many KPIs from network devices and applications are rolled up into easily-consumed and color-coded "**health scores**". This assists the network manager to easily zoom in on areas that need focus while continuing to monitor areas of the network that are operating normally.

Assurance provides visibility to the actual experiences of the users and applications across the network end-to-end. This frees up the time available to the organization's operations team to focus on the bigger picture and helps to move the overall Enterprise network forward and achieve the larger goals for the business. In addition, Cisco DNA Assurance also provides device-level visibility for Apple devices via iOS Analytics, leveraging Cisco's strategic partnership with Apple.

Cisco DNA Center provides a "closed loop" system. Automation drives new capabilities into the network infrastructure in a simple, predictable fashion, while Assurance

extracts data from the network to determine how well it is performing for the applications, users, and devices. This is illustrated in the following figure.

DIAGRAM Cisco DNA Center Overview



By encompassing both wired and wireless networks, legacy deployment models, and new Software-Defined Access options, Cisco DNA Assurance addresses organizations of many types and sizes, anywhere along their Intent-Based Networking journey.

It is also important to note that Assurance is only at the beginning of its life cycle. Some of the new and exciting areas that are already supported by Assurance are outlined in this book. Many more capabilities are coming in the future within Cisco DNA Center. Watch this space! Assurance will be evolving, innovating, and maturing for some time to come.

Cisco DNA Assurance - Changing the Paradigm

Cisco DNA Assurance is different from a traditional NMS, and changes the paradigm by up-levelling the overall solution to a far simpler, elegant, and yet more powerful set of capabilities.

Assurance incorporates advanced elements and provides sophisticated capabilities, including the following items of note:

- **Big Data Engine:** Cisco DNA Assurance incorporates advanced analytics that provide sophisticated processing of network issues, leveraging data from multiple sources to arrive at a deeper level of insight into network operations. The cutting-edge Big Data analytics functionality within Cisco DNA Assurance processes data from many points to provide the operator with a more comprehensive picture, and allows them to arrive at a more rapid, accurate assessment of any issues or areas of concern that need to be addressed.

- **Data Sources**: Cisco DNA Assurance ingests data from many sources, including network devices such as routers, switches, wireless LAN controllers (WLCs), access-points (APs), and sensors. In addition, contextual sources such as client devices, IP Address Management (IPAM) servers, authentication servers, application servers, and so forth are also ingested. Such external data sources enrich the context of network telemetry data, providing deeper insights to the network operator.

- **Correlation Engine**: Cisco DNA Assurance “connects the dots” by mapping relationships between associated data points. For example, a NetFlow record would include a source IP address, as well as the application that generated the traffic. But on its own, it does not answer the question of: "Which user generated the traffic?" However, an IPAM server could map the source IP address to a Media Control Access (MAC) address of the client device. Then, an authentication server, such as Identity Services Engine (ISE), can map the MAC

address to an individual user. In this manner, specific application flows can be connected to specific users, and these views are presented in context to the network operator.

- **Time Series Database**: Cisco DNA Assurance is based on a unique database. This not only holds all of the data from the network, but correlates it in a time series such that the network manager is able to "zoom back", allowing them to understand the network conditions, as well as the user and application experience, at that point in time. By being able to "time travel" back to the point where an issue occurred, network operators are freed up from the time-consuming (and often frustrating) task of having to re-create network issues. They can gain much more insight into what their users and applications were experiencing.

- **Streaming Telemetry**: Cisco DNA Assurance ingests model-based streaming telemetry from network devices, allowing these devices to “push” alerts when a given KPI has crossed a pre-defined threshold. This allows for faster response times to events, lowers overall device CPU impact, lowers bandwidth requirements, and thus improves overall scalability.

- **Machine Learning**: The integration of machine learning functionality takes analytics to the next level by allowing patterns of network operation to be determined, trend lines drawn, and conclusions reached, based on sophisticated ML algorithms. Given the vast amount of information which can be gathered from a large Enterprise network - many gigabytes or even terabytes per day - machine learning approaches have a very significant role to play in taking this large mass of data and allowing the network manager to be presented with clear outcomes and actionable insights.

- **Health Scores:** With so many data points being offered to a network operator, from so many sources, how can the simple question of "How is a network / device / application / user performing?" be answered? Cisco DNA Assurance introduces the concept of "health scores" - simplified metrics that roll up a variety of relevant KPIs into a single number that represents how "healthy" the service or endpoint involved is. For example, an application is experiencing more than normal end-to-end delay across the network path. In this case, the

application continues to function, but its health - its ability to provide appropriate service for end users - is impacted. In such an event, the health score would be marked to a lower value (say, 8 out of 10 on a sliding scale), indicating in an easy-to-absorb fashion that an out-of-profile condition exists, and that corrective action may be necessary.

- **Issues:** By correlating multiple metrics together, Cisco DNA Assurance presents the network manager with issues to guide them to areas of the network which may need attention. Issues can come in a variety of levels of priority, based on their impact to the overall operation of the organization, site, or network devices involved. This allows a more rapid determination to be made as to which challenges may need to be addressed first, without the network manager becoming lost in a morass of detail. This permits the network manager to be more responsive to the business, and resolve such issues more quickly and accurately.

- **Guided Remediation:** Sometimes the steps to take to resolve a issue are not necessarily straightforward. Several steps or options may exist to determine not only the root cause, but how to remediate the issue and restore normal network operation. Cisco DNA Assurance provides an integrated capability for guided remediation, helping to lead the network operator through a series of steps to resolve many common issues. By integrating insights, issues, health scores, and more, network operators can resolve issues more quickly, and return the network to normal service more rapidly. This allows many issues to be resolved without having to escalate to second or third-level support personnel. In many cases, this can also be done without accessing the network element directly (for example, via CLI), using instead an API integration into the Help Desk tools in use.

- **Proactive Monitoring:** It is advantageous to be able to stop a problem before it even occurs. Cisco DNA Assurance provides several key capabilities to enable the network manager to be proactive and not reactive. For example, if wireless sensors are deployed in the network, Cisco DNA Assurance can monitor these sensors and alert the network manager when wireless conditions change or degrade - even before users have observed or reported any issues. Intelligent Capture allows network operators to "sniff" wireless traffic remotely - without

having to go onsite and replicate transient issues. Intelligent Capture also analyzes packet streams for common wireless issues, such as authentication failures, and assists the network operator to diagnose and identify the root cause of such problems.

All of the above shows the power of combining Assurance and Automation into a single platform - Cisco DNA Center - and serves to illustrate how Cisco DNA Assurance, and its rich set of capabilities, changes the paradigm of how Enterprises can gain greater visibility into, and control over, their network deployments.

Now let's proceed to explore some of the key concepts of Cisco DNA Assurance, such as Issues, Health Scores, and more.

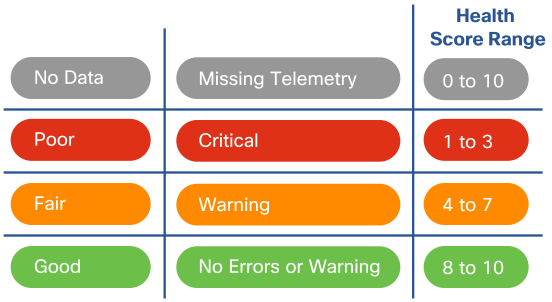
Cisco DNA Assurance - Core Concepts

Health Scores

Traditional network management solutions present the network operator with many disparate elements of raw data that the operator is expected to review, analyze, troubleshoot and remediate. The fact is that network operators often spend more time collecting data than analyzing it during troubleshooting. Cisco DNA Assurance aims to reduce this burden by abstracting this complexity into an enriched and intuitive composite metric - a Health Score.

Cisco DNA Assurance monitors several Key Performance Indicators for clients, network devices, and applications. In turn, it computes a Health score for each client, network device, and application that is being monitored. A Health score is a smart amalgamation of KPIs associated with the performance of client, network device, and applications. Health scores are colored to reflect the alert level that warrants attention from the network operator, as shown in the following diagram.

DIAGRAM Health Score Range



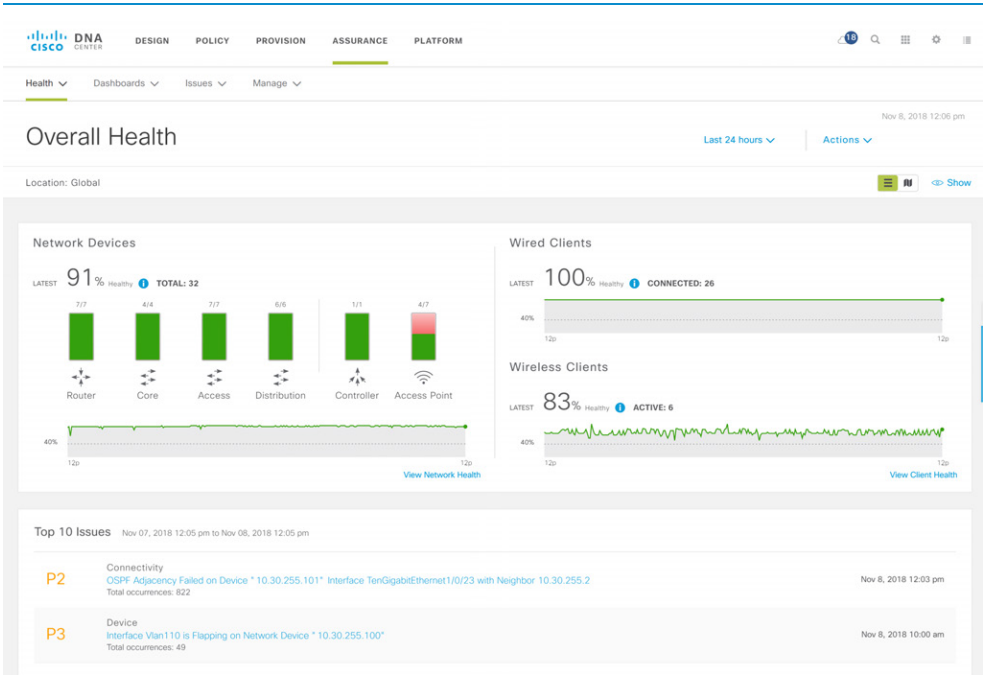
By abstracting raw data into a single health score based on the most important metrics, Cisco DNA Assurance allows the network operator to focus on the problem areas and find the root cause quickly through intuitive workflows.

Health Scores are summarized in the Health Dashboard in Cisco DNA Assurance in an actionable form, with drill-down workflows to quickly get to the 360 Views that provide additional details if the Network Operator needs to get more information.

Overall Health

The Overall Health Dashboard provides a high-level overview of how the network and client devices are performing, along with a view of Top Ten issues that require attention from the network operator. From here, the network operator can further drill down into Network or Client Health for a more detailed view of how the network infrastructure and the clients are performing, as shown in the following diagram.

DIAGRAM Cisco DNA Assurance – Overall Health Dashboard

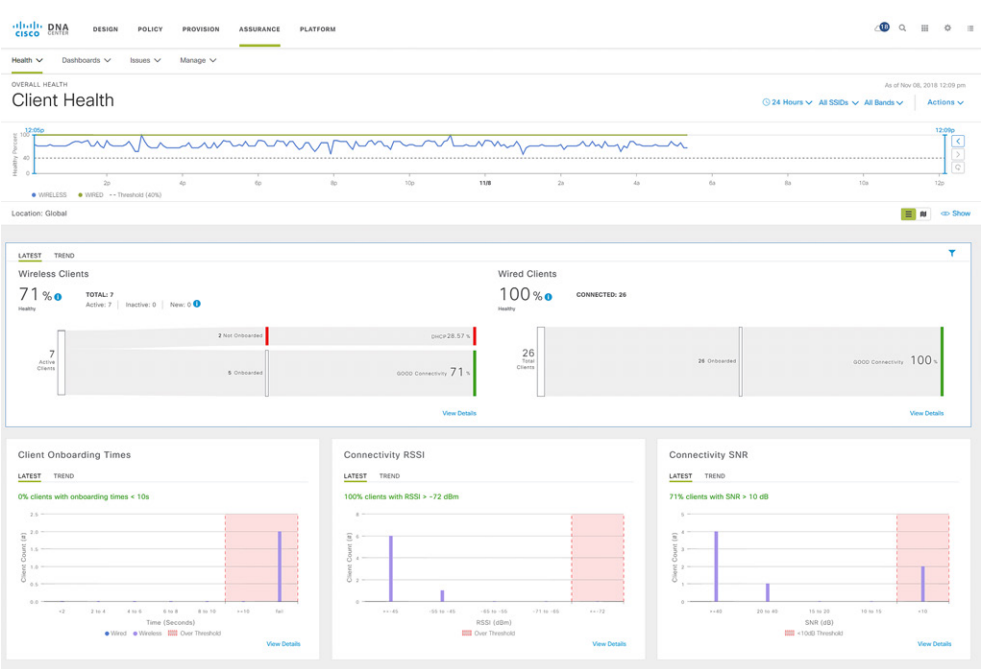


Client Health

Individual client health scores are computed based on initial onboarding, as well as the persistent connectivity experience. The Client Health Dashboard provides an analytical summary of how well clients are able to connect to the network, and once they are connected, shows how their connectivity experience has been.

The overall Client Health Score is based on the number of healthy clients divided by the total number of clients based on client type (wired or wireless). The Client Health Dashboard is illustrated in the following diagram.

DIAGRAM Client Health Dashboard showing Onboarding and Connected analytics



Network Health

Individual network device health scores are computed based on System, Data Plane, and Control Plane Health.

Switches and Routers

The Switch and Router Health Score is the minimum sub-score of the following parameters:

- System Health - memory utilization and CPU utilization.
- Data Plane Health - link errors and link status.
- Control Plane Health - for Fabric devices, includes reachability to the Fabric Control Plane node.

Access Points

The AP Health Score is the minimum sub-score of the following parameters:

- System Health - memory utilization and CPU utilization.
- Data Plane Health - link errors, radio utilization, interference, noise, and air quality.

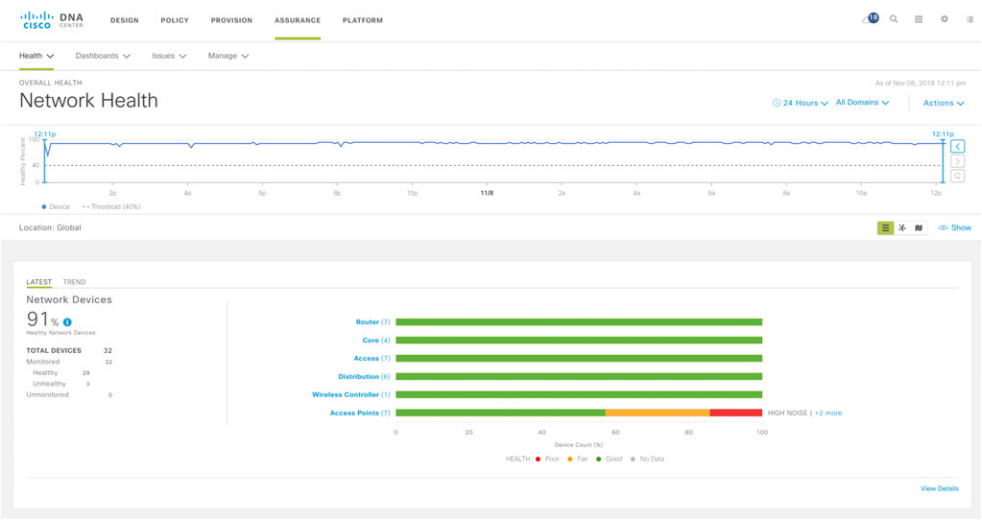
Wireless LAN Controllers

The Wireless LAN Controller Health Score is the minimum sub-score of the following parameters:

- System Health - memory utilization, free timers, and free memory buffers (MBufs).
- Data Plane Health - Work Queue Element (WQE) pools, packet pools, and link errors.
- Control Plane Health - For Fabric WLCs, includes reachability to the Control Plane node.

The Overall Network Health is a percentage computation of healthy devices divided by the total number of devices by type that are being monitored by Cisco DNA Center, as shown in the following diagram.

DIAGRAM Network Health Dashboard

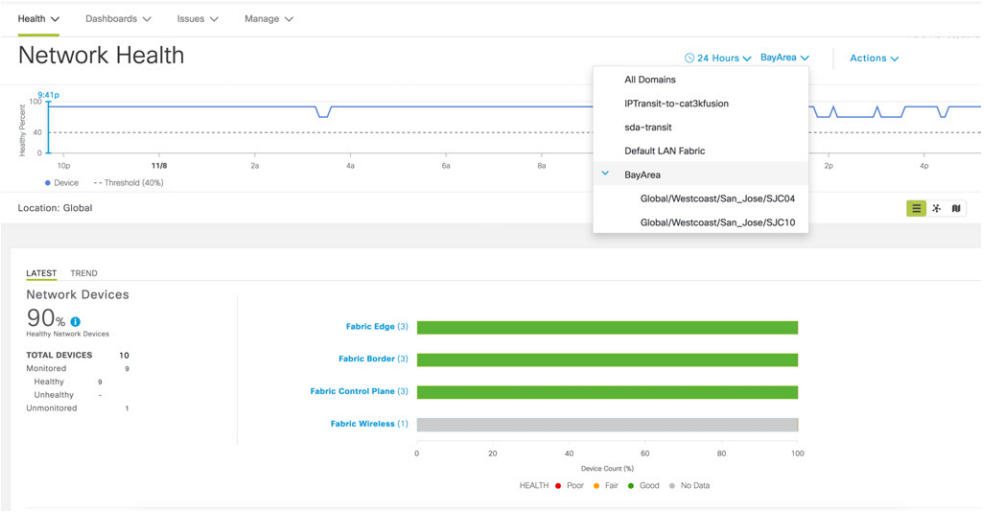


SD-Access Fabric Network Health

Cisco DNA Assurance provides Network Health for Software-Defined Access (SD-Access) Fabric deployments.

Cisco DNA Assurance provides granular visibility at both the Fabric Site and Domain levels by aggregating the health across individual Fabric sites as shown below. This provides the individual health score per Fabric Domain and Site.

DIAGRAM SD-Access Fabric Health Dashboard



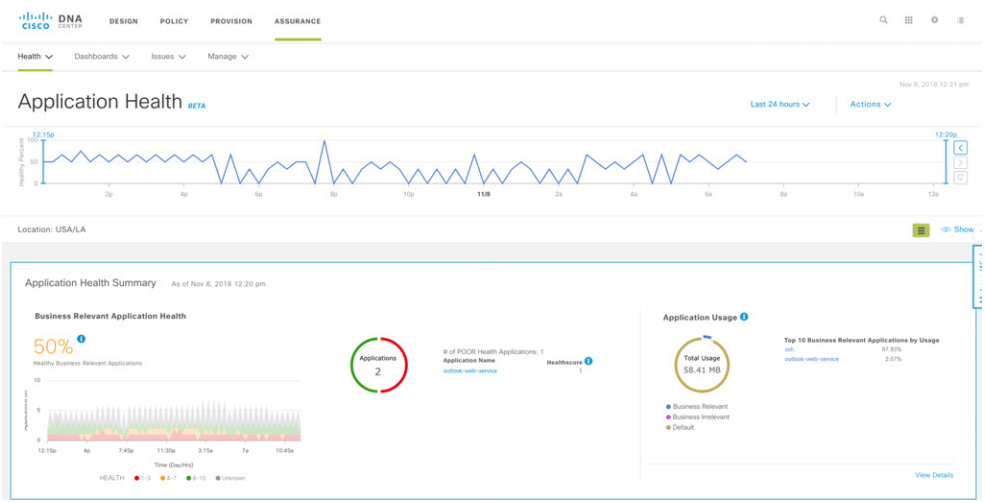
Application Health

Cisco Application Experience allows the network operator to monitor the health of applications. Application health is calculated based on the application's qualitative metrics, such as packet loss and network latency.

Metrics are monitored from both clients and servers via ART (Application Response Time). Application Experience leverages NetFlow records exported by ISR, ASR and CSR routers. Based on the nature of an application it will be classified as Business Relevant, Business Irrelevant, or Default. The classification is based on the use of the NBAR2 (Network Based Application Recognition) capability within the router.

The Application Health Score is the percentage of the number of healthy business-relevant applications divided by the total number of business relevant applications, and is computed over a 15-minute interval. This is shown in the following diagram.

DIAGRAM Application Health Dashboard



In summary, Cisco DNA Assurance provides a full view around the health statistics for networks, clients, and applications. This provides the network manager with an ability to review the performance of the Enterprise network using a variety of different "lenses", and assists in more rapidly drilling down into any issues or problem areas that may exist. The use of health scores permits the network manager to easily understand the most critical aspects of network operation, distilled from a huge amount of underlying data, in a simplified fashion.

Issues

Cisco DNA Assurance provides both system-guided and self-guided troubleshooting. Multiple KPIs are correlated to determine the root cause of the problem, and then possible actions are provided to resolve the problem. The focus here is on highlighting an issue rather than monitoring data.

Cisco DNA Assurance generates issues using thresholds and rules defined by many Cisco wireless and wired experts, TAC engineers, and Escalation support, based on more than 30 years of learning. In future, the power of Machine Learning will allow the evolution from static to dynamic thresholds, such that issues will only be triggered when the respective KPIs go beyond the normal baseline for the specific environment.

Issues are categorized into 3 broad types:

1. Client-related issues.
2. Network-related issues.
3. Sensor-driven issues.

Issues that typically have a network-wide impact are flagged as critical when multiple clients or many devices are affected. The priority, issue category, issue description, and the number of occurrences is displayed in the Top Ten Issues panel on the Executive Dashboard. When an individual issue is selected, the issues panel expands to provide additional details and allows the user to review and understand more data points, including impact and suggested actions for resolution.

The criticality of the issue is also marked according to issue priority, based on severity and impact:

- P1 is a Critical issue in network operations.
- P2 is a Major issue impacting multiple clients or devices.

- P3 is a Minor issue with localized or minimal impact.
- P4 is an Informational issue that may not necessarily be a problem, however addressing P4 issues could optimize network performance and prevent further problems.

All priority levels can be escalated to a higher priority (for example from P3 to P2) indicating a higher impact if network conditions should change. These priority levels are dynamic and can be modified by the administrator.

Let's now look at each of the issue categories in greater detail, and also walk through some of the examples of the most commonly occurring issues across each of the categories.

Client-related Issues

Client issues fall into several categories including Onboarding, Connectivity, RF, DHCP, AAA, Apple iOS Client, and Mobility Failures.

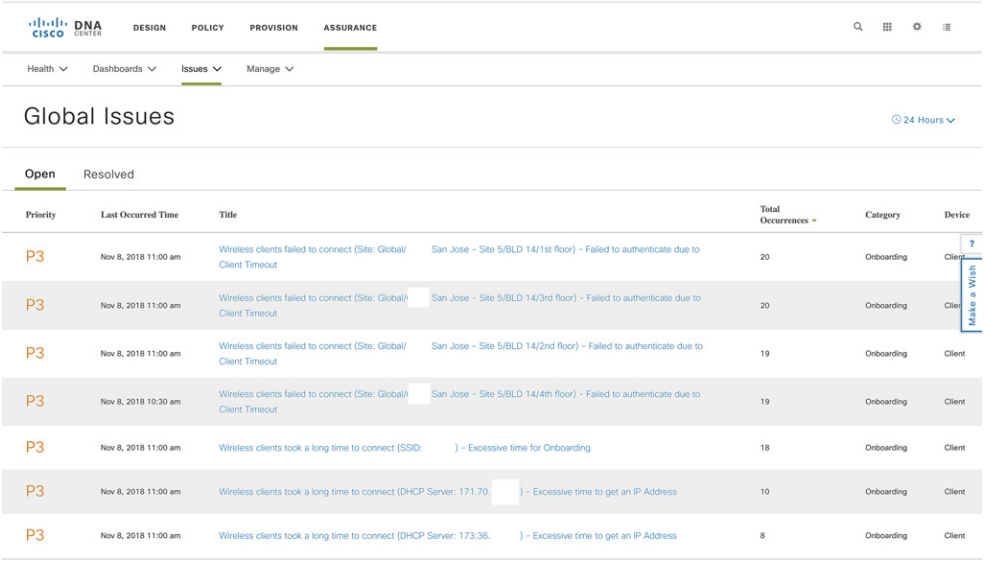
Some of the most commonly occurring client-related issues are:

1. Client failed to onboard due to client timeout.
2. Client is experiencing poor RF conditions.
3. Client is roaming slowly.

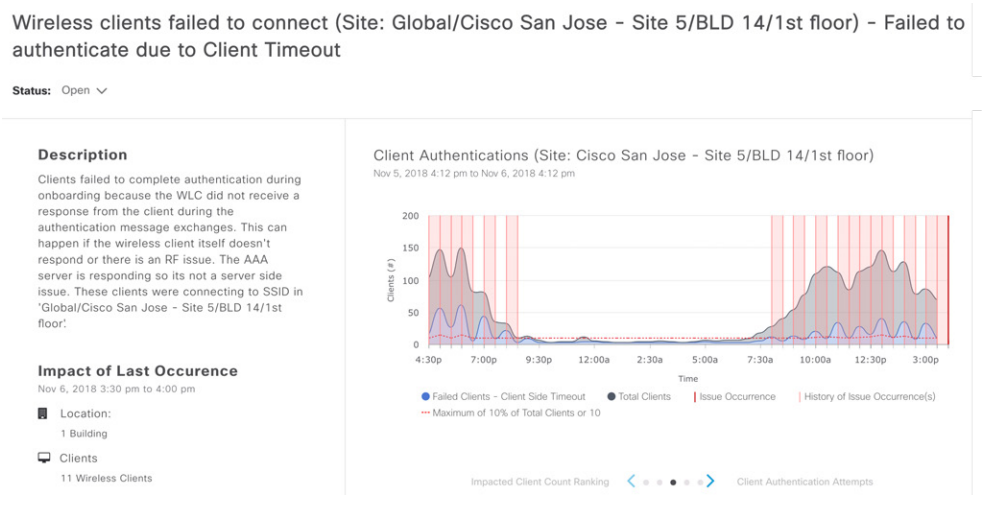
The following issue workflow shows how the network operator can assess the issues at hand, and resolve the problem using Cisco DNA Assurance analytics and suggested actions.

Issue Workflow: Clients failed to onboard due to client timeout

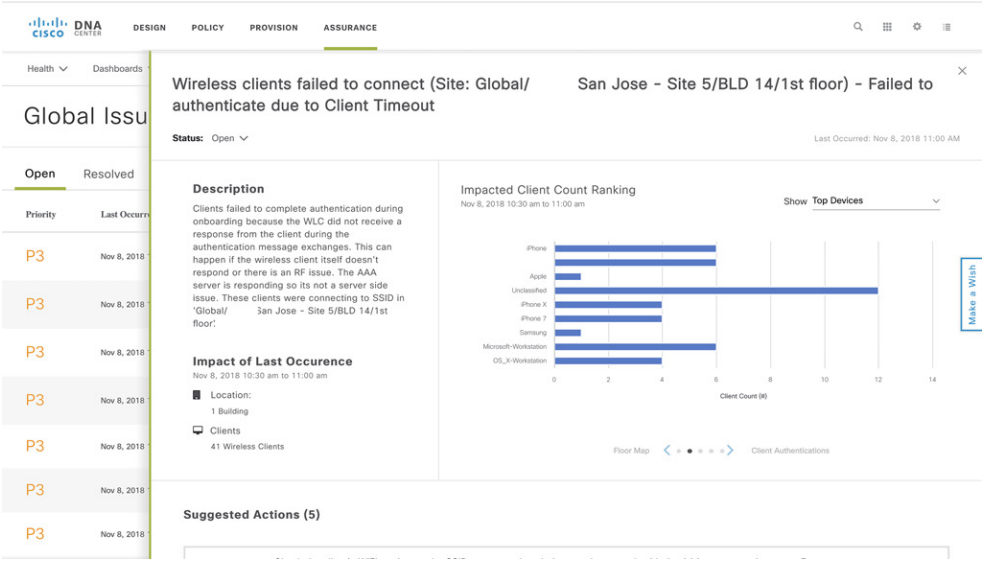
Step 1: Critical issue identified on the Top Ten Issue panel on the Executive Dashboard



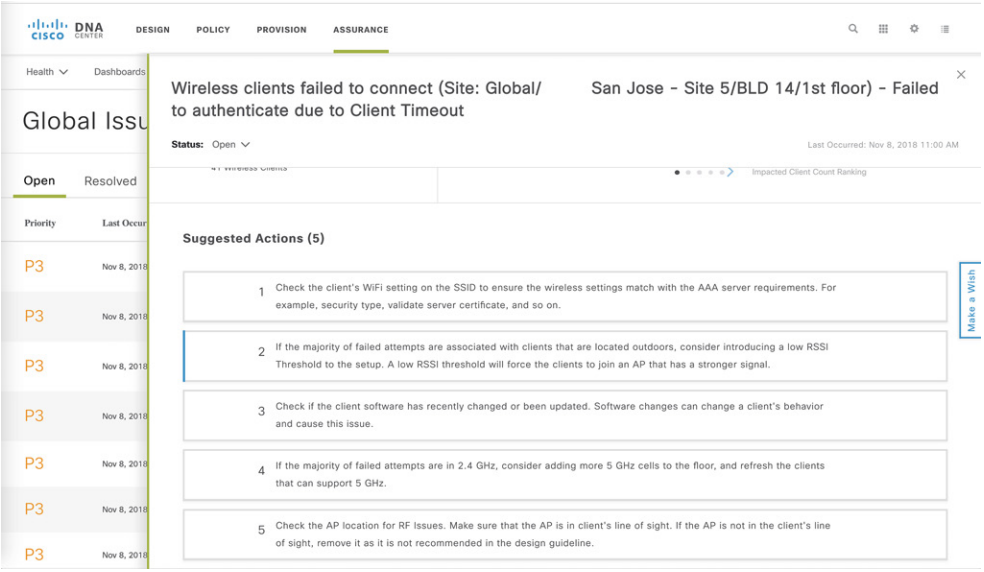
Step 2a: Analyze the issue with detailed analytics for clients impacted, location, and performance metrics



Step 2b: Drill into the issue for further details



Step 3: Follow the suggested actions to troubleshoot and resolve the issue



By following the above client workflow, the network operator was able to far more easily identify the issue, scope the impact, and drive the issue resolution in a timely fashion.

Network-related Issues

Network issues affect devices such as switches, routers, WLCs, access points, and sensors. Typically, network device issues affect multiple clients or users that are attached to, or through, that network device.

Some of the most commonly occurring issues are:

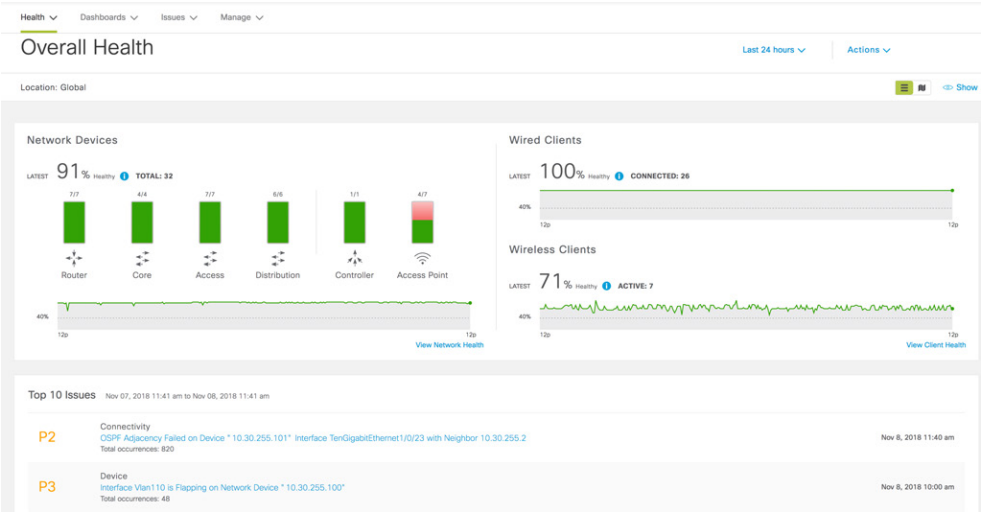
- Routing protocol adjacency failure.
- High TCAM, CPU or memory utilization.
- Link failures or high interference.

The following issue workflow shows how the network operator can assess such issues and resolve them using Cisco DNA Assurance analytics and suggested actions.

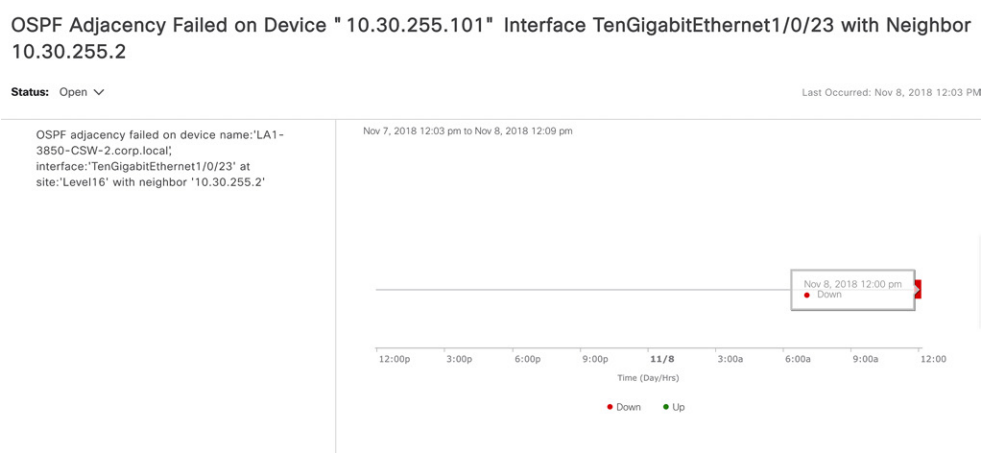
Issue Workflow: OSPF Adjacency Failure

In this scenario, a switch has lost its neighbor relationship to its upstream device on a specific interface because of a routing protocol adjacency failure. The switch is providing streaming telemetry to Cisco DNA Assurance so an alert can be generated. This adjacency failure issue affects the clients that are attached to the switch.

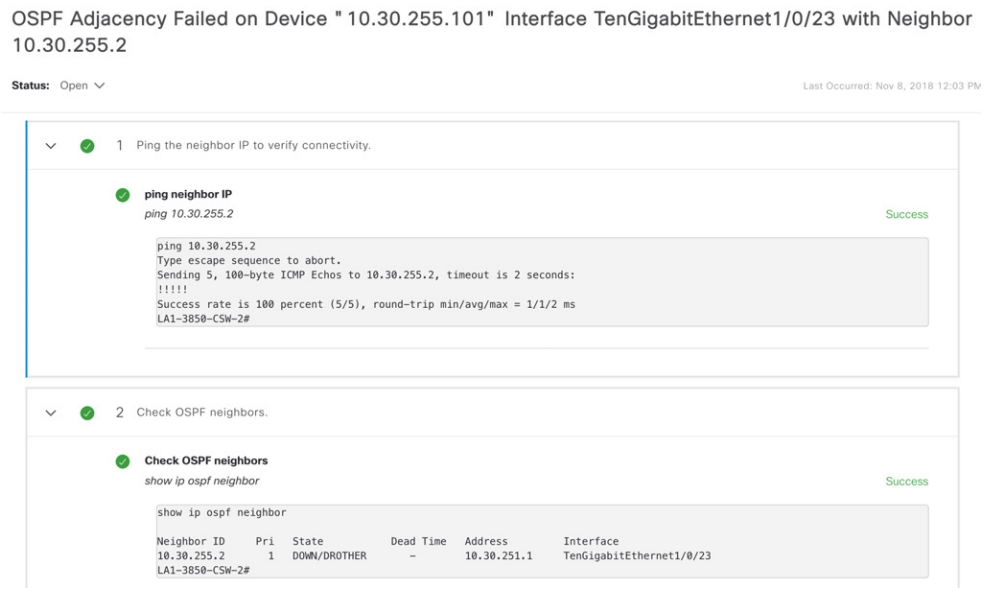
Step 1: Critical issue identified on the Top Ten Issue panel on the Executive Dashboard



Step 2: Analyze the issue with detailed analytics showing what time the issue occurred



Step 3: Follow the suggested action to troubleshoot and resolve the issue

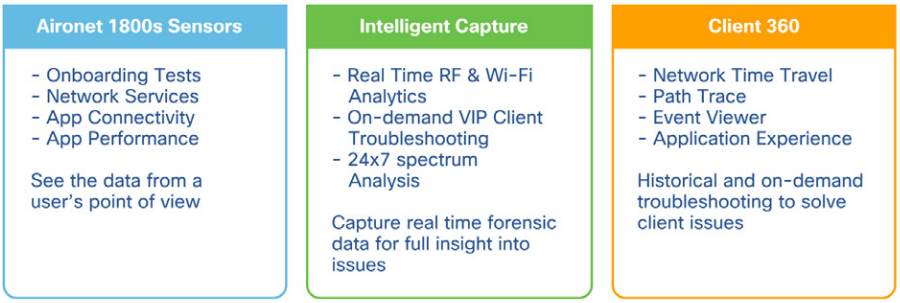


Cisco DNA Assurance displays additional options to run CLI commands on the network device through Cisco DNA Center. This helps network operators determine the root cause of this particular issue and remediate it.

Cisco DNA Assurance Tools

Cisco DNA Assurance addresses not just reactive network monitoring and troubleshooting, but also the proactive aspects of troubleshooting the network, client, application and services. Following are the key capabilities offered by Cisco DNA Assurance that can allow network operators to troubleshoot the issues efficiently across the network and ensure faster turnaround time.

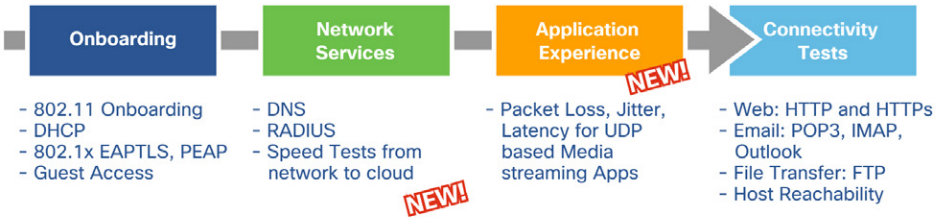
DIAGRAM Assurance Capabilities



Aironet 1800s Sensors

A sensor emulates an end user to help troubleshoot the wireless network, applications, and network services, allowing network operators to monitor network SLAs. The following tests are supported on the 1800s sensors:

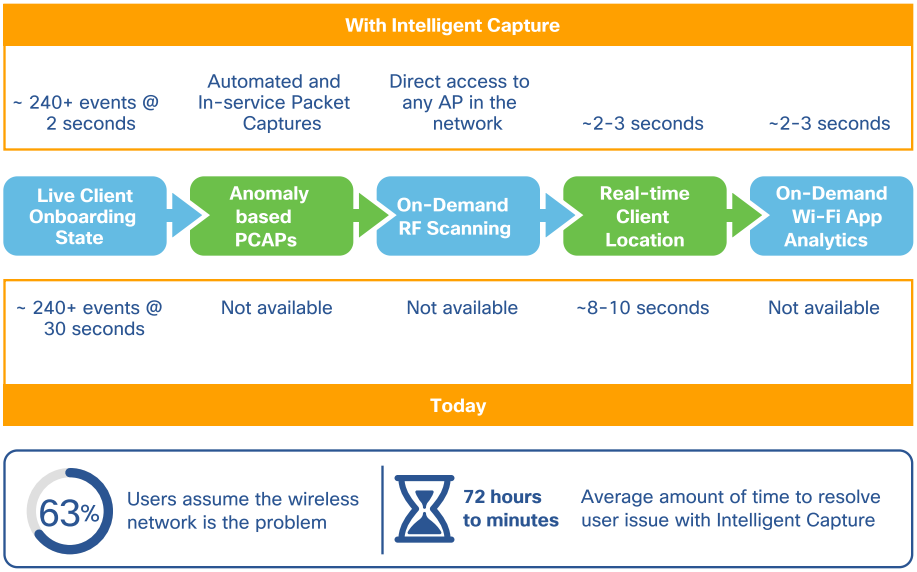
DIAGRAM Aironet 1800s Sensor - Feature Overview



Intelligent Capture

Uses targeted packet capture and radio scanning techniques to proactively find and resolve wireless problems with Onboarding, interference, and poor performance, allowing the network operator to drive faster and more accurate troubleshooting and issue remediation.

DIAGRAM Intelligent Capture - Feature Overview



Client 360

Allows the network operator to view device or client connectivity from any angle or context. Client 360 views include information on topology, throughput, and latency from different times and with different applications.

Additional functions available via Client 360 views include **Network Time Travel** - this allows the network operator to "go back in time" and see the cause of a network issue with all of the data captured at that time period, rather than trying to re-create the issue in a lab or the customer network. **Path Trace:** Provides the network operator with a visualization of the path of an application or service from the client through all devices and to the server, with connectivity statistics for each hop.

The views and tools within Cisco DNA Assurance are continuing to evolve with a focus on providing the network manager and operator with an ever-greater insight into the performance of their networks, applications, and users. The tools available within Cisco DNA Assurance are crucial to drive faster problem identification, root cause and remediation.

Machine Learning-Driven Insights

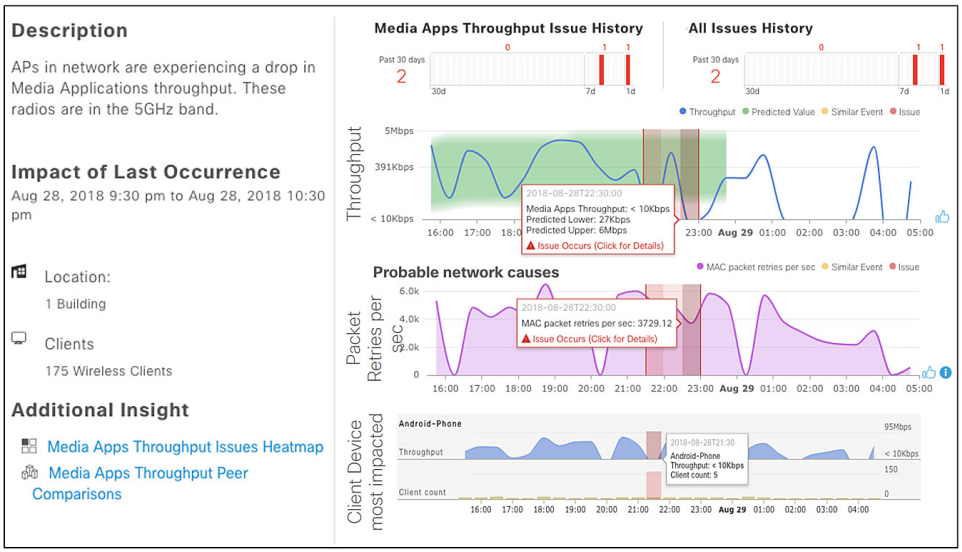
Cisco DNA Assurance leverages a Big Data architecture which makes use of Machine Learning algorithms, refined using Cisco's deep knowledge of networking, in support of advanced capabilities and use cases such as:

- Cognitive Analytics.
- Network Insights.
- Network Heat Map.
- Peer Comparison.

Cognitive Analytics

This capability utilizes complex compute models to detect anomalies across diverse datasets. It provides insights to the network manager by generating issues with highlighted patterns of interest that fall outside of the normal baseline. In the diagram below, the green band indicates the normal baseline for this KPI (throughput), while the red bars indicate deviations from that baseline.

DIAGRAM Issue Detection using Cognitive Analytics

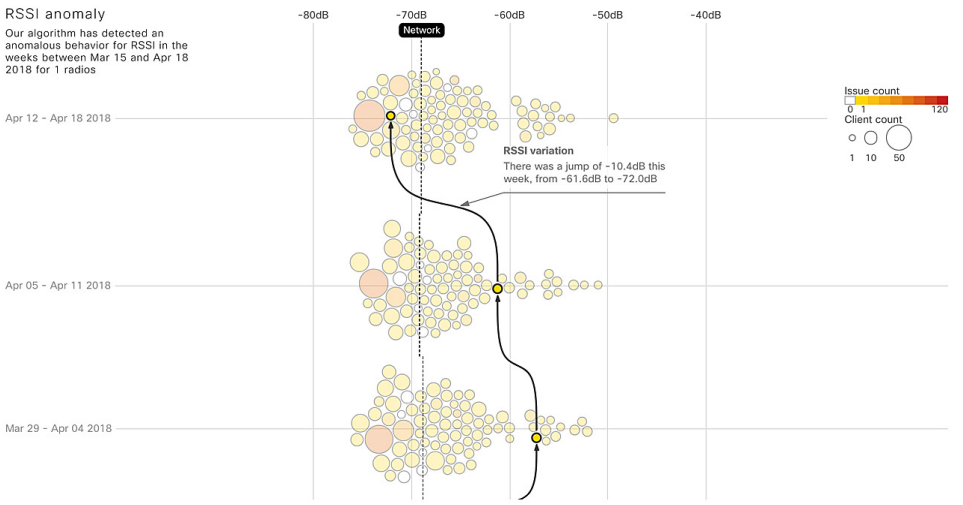


Network Insights

Network Insights provides a long-term trend analysis tool which highlights deviations of specific KPI behaviors over a monthly time window. The KPIs are aggregated over weekly windows and if the algorithm determines that one or more of the monitored KPIs has had a significant deviation over time, it will trigger a network insight. The insight will highlight how the specific KPI has changed over time as well as compare it to similar entities present in the network.

In the diagram shown below, the RSSI (Received Signal Strength Indication) values are compared across weekly boundaries, and a deviation from that baseline as noted is documented via the Network Insights tool for review by the network manager.

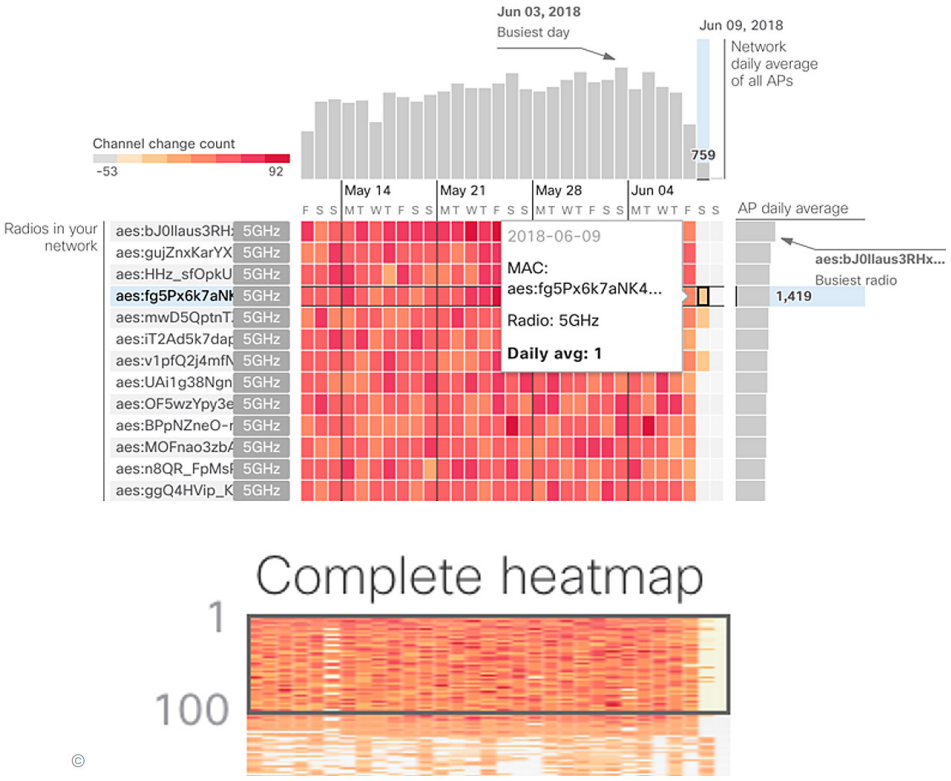
DIAGRAM Network Insights - RSSI



Network Heat Map

Network Heat Map is a tool which performs KPI comparisons within the network. The operator picks a KPI for a particular network entity and visualizes how that KPI compares across the rest of the network. The heatmap allows for the network operator to compare differences on the same day and over time to easily spot network hotspots over time.

DIAGRAM Network Heat Map

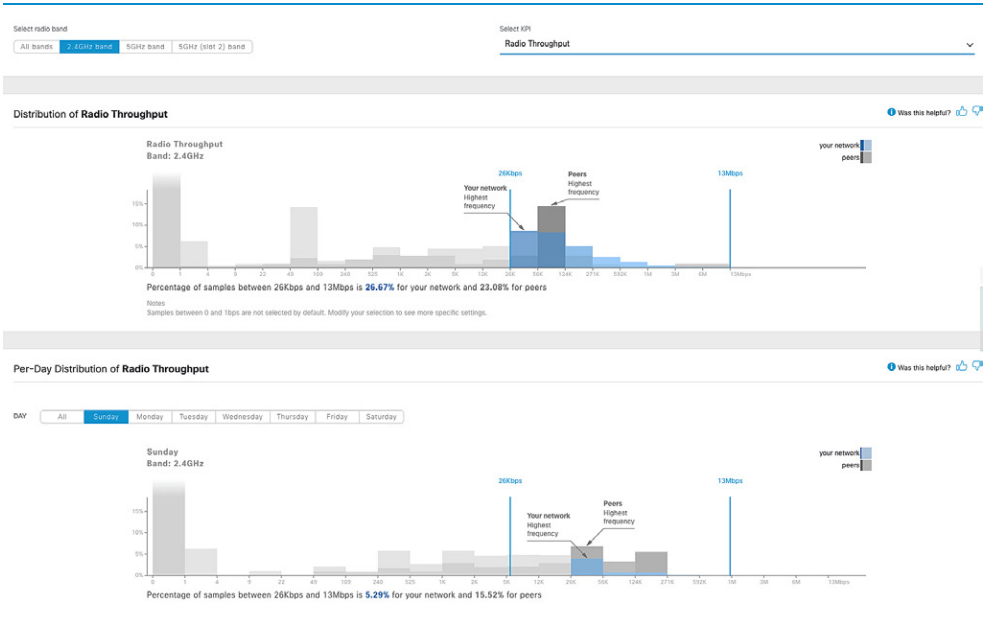


Peer Comparison

The Network Heat Map performs comparisons of entities within a customer network, but the Peer Comparison allows for a comparison of similar entities and KPIs across other customer networks. This allows customers to see how their network is performing in comparison to similar network environments elsewhere.

Note, all machine learning data is anonymized before leaving the on-premise Cisco DNA Center appliance. The Peer Comparison function is optional for use, and must be specifically configured and enabled by the network manager if desired.

DIAGRAM Peer Comparison with Anonymized Data



Users of Cisco DNA Assurance

Roles and Personas

Several key roles within the network team will use Cisco DNA Assurance to resolve issues and enhance business agility. Let's explore these roles to better understand what these roles are and how they interact.

Network Architect

The network architect has the task to decide on how best to implement the network to meet the overall organizational goals. This includes (but is not limited to) selecting equipment vendors, network platforms, overall technical approaches, and design criteria to meet these goals. For example, a network architect may be the one that specifies an MPLS VPN, SD-Access, and/or SD-WAN approach to the network design to meet the stated goals around:

- Network-integrated security and segmentation.
- Network redundancy to assist in driving continuous operations.
- Integrated network monitoring and analysis to help in supporting the network system over the anticipated lifetime of the deployment.

Network Manager

The network manager is most concerned about how the network is deployed and operated on a day-to-day basis. As the person most exposed to ongoing daily network operation, he or she is often the one who is most knowledgeable about the network deployment as a whole. This includes the attributes, issues and challenges faced by the network, and the way it might be improved over time as organizational goals move, as requirements change, or as new applications appear. In smaller to mid-sized deployments, the network architect and network manager may be the same individual, while in larger deployments these are typically separate. The network manager is key to the ongoing operation of the network, working in conjunction with one or more network operators, help desk, or service and problem management personnel.

Network Operator

The network operator is typically "closest to the ground" in the network deployment, often being the person (or persons) tasked with troubleshooting escalation issues as they arrive from the help desk and chasing these problems to resolution. The network operators are often the ones that are "in the firing line" and are the ones most intimately familiar with the network equipment - its daily use, detailed operation, and normal (or abnormal) operating states and issues. Appropriate interfacing of network operations with the network management and help desk staff is crucial to the proper ongoing operation of the network, and has much to do with how responsive and professionally-managed the network appears to the end users of the network.

Help Desk

The Help Desk is the "first point of contact" in the network, processing trouble tickets, providing first-level analysis of problems and issues, and driving escalation of issues requiring deeper investigation. A responsive Help Desk can make a huge difference as to end-user satisfaction and appropriate timely problem resolution. Help Desk personnel escalate issues to the network operators as needed, and potentially higher to the network manager in the case of severe, widespread, or systemic issues.

Service Manager

The service manager is interested in delivering a service for the customer to improve the business. As an example, the manager for the network access service is responsible for onboarding new users, providing them access to the network, IP Telephony, etc. The service manager monitors the service health and relies on the operations team to ensure that any associated SLAs are met. A near-real-time view is absolutely critical for service management. Incidents and unplanned outages have an impact on the available services and so need to be monitored and controlled.

Problem Manager

The problem manager is part of escalation team, and typically owns such escalations. The goal of the problem manager is to find the root cause of the issue involved, document the issue, and have a plan for future avoidance of the problem. Obtaining a complete 360-degree view of an incident and driving towards root cause analysis of the associated problem helps to improve the overall problem management process. Problem management will feed back into network operations helping to close the loop as issues occur and are in turn identified and resolved.

Cisco DNA Assurance Value Proposition

Each member of the teams noted above benefits in a very specific way from Cisco DNA Assurance. The use of Cisco DNA Assurance will markedly enhance the various processes in many network deployments, and can rapidly become a critical element in the daily life of all of the personnel, and all of the roles, noted above. Several examples of how Cisco DNA Assurance assist these roles are provided in the various Use Cases that are documented in the following sections.

Network Operations - A Day in the Life

What does a typical day in the life of a network manager and operator look like? What challenges do they face every day? Which interruptions happen as their day progresses? And, most importantly, how does Cisco DNA Assurance help them in their day-to-day life?

As different organizations operate their networks in very diverse ways, the example used here will consider a large enterprise network. Within the Network Operations Center, or NOC, operators monitor the backbone and core networks servicing the various subsidiary network building blocks. The network consists of multiple distribution blocks with attached access layer switches hosting the wired and wireless devices in each location. In this example, the network comprises approximately 400 switches, 2,000 APs and 15,000+ users with a variety of devices, including laptops and smartphones, as well as supporting building management systems, wired endpoints, and Point of Sale terminals.

The NOC staff is responsible for maintaining the network, managing software upgrades on network devices, and handling standard change management tasks. Complex changes often involve personnel from the network architecture team, and in these situations, the NOC only monitors the network and assists in further troubleshooting.

Examining the Network Operations team more closely, there are several important SLAs and KPIs to take into account:

- The network SLA is 99.99% per month (4m 23s downtime) for the core and 99.7% (2h 11m 29s downtime) for the access layer.
- The NOC handles second-level support including incidents that are escalated from the Help Desk (first level).
- The NOC monitors trending in the network and provides this data to the architecture team for future network capacity planning.

- Standard changes are the NOC's responsibility, including provision of access ports and VLANs.

The NOC team is typically a small group of employees who work in shifts to ensure 24-hour coverage. This may include second- or third-level escalation, which is covered by the architecture team. With these parameters in mind, let's examine a day-in-the-life of the NOC team without - and then with - Cisco DNA Assurance.

Let's start with a scenario with *no* Cisco DNA Assurance:

On Monday morning at 6:00am, the morning NOC shift arrives and receives a handover briefing about the nightly events from the previous shift. Overnight, there were two open tickets in the network. These are Priority 3 and will be handled by the incoming NOC team during the day. A total of ten standard changes are also on the list for the day shift, all planned to be fulfilled within specific time windows. These are all standard changes which follow established procedures.

At approximately 9:00am, the network monitor is still green. As users begin to arrive at work and attach to the network, the NOC team receives multiple tickets in their incident queue from users complaining about not being able to connect to the network.

The network monitor remains green using the NMS tools in use, and thus all should be well from the network operator's point of view. However, users are reporting login issues at an increasing rate. The NOC team starts investigating and while this is happening, also determines that a previously-planned change window for one of the changes begins soon. Per the NOC's standard operating procedure, an incident has priority over a planned change, so the NOC team needs to postpone the change in order to concentrate on the login issue. They check the network state for the locations the incidents were reported from, but do not recognize any obvious network anomalies. As per NOC procedure, they then assign the open trouble tickets to the Active Directory queue, since that team is responsible for user authentication and login. Unfortunately, these tickets only contain the information that no malfunction in the network was detected, and that multiple users are complaining of login issues.

At approximately 11:00am, the incident for the described issue comes back to the NOC from the Application group. What happened in the time in between? The NOC team forwarded the issue to the AD queue, that team forwarded it with no findings to the server queue, who then forwarded it to the application queue. The applications team could not find any problem and forwarded the issue back to the NOC, still not having anything in the report to point to the root cause of the issue. By this time, two hours have already passed and the organization is no closer to determining the root cause of the issue and repairing the underlying problem. At this point, further escalation starts and a problem manager becomes involved since more and more users are not able to log in to the network and cannot perform their daily tasks. The problem manager gets everyone together at a table to troubleshoot the problem together ... Pause!

Is this situation familiar? In this case, every group fulfilled the SLA of their incident queue, yet nobody solved the issue. Certainly users are still unhappy since they cannot log in and they cannot perform their job functions effectively.

Now, assume that the same incident occurred but Cisco DNA Assurance was in place:

Back to Monday morning, 9:00am. A few users are calling the Help Desk and reporting that they are unable to log in. Since the user data is available in Cisco DNA Assurance, the Help Desk operators can identify the users and access their respective Client 360 views to assess the problem. Once there, they can see that wireless users are not receiving IP addresses via DHCP. This indicates a problem with client onboarding, more specifically the authentication and IP addressing process.

Now the power of Cisco DNA Assurance comes to the forefront. A view of the issues, the impacted locations, and the number of users affected are shown in an easy-to-consume fashion. Assurance indicates that users are experiencing an authentication issue caused by RADIUS failures, and a list of all the impacted users is displayed. Cisco DNA Assurance also suggests the correct remediation action to solve the problem - in this case, the Active Directory server is not responding. At this point, the incident can be filled with all of the information extracted and summarized by Cisco DNA Assurance,

and can be forwarded to the AD queue for further troubleshooting, also indicating that the network is behaving as expected. It's not the network!

Cisco DNA Assurance allows the network operators to have a single source of truth as it correlates all of the necessary information and helps identify the root cause of the issue at hand. It also helps the network operator to isolate the incident in real time. In this case, the process required only a few minutes, still allowing time for the planned change (that previously had to be deferred) to be fulfilled. Cisco DNA Assurance freed up the network operators' time by delivering the information they needed to get to the root cause of the problem, and providing the necessary action that needed to be taken to resolve it.

To summarize, by using Cisco DNA Assurance, the concept of Intent-Based Networking is extended to network analytics as well as to automation. The network operators are placed back in the position of supporting the network proactively rather than operating in a reactive mode. This further creates confidence in the network for all parties involved. The network manager, the various network decision makers, and of course the most important parties involved - the end users of the network - can all carry on without being impacted.

To provide a more in-depth view of Cisco DNA Assurance, the next section will explore some of the key use cases that involve solving critical problems across both wired and wireless infrastructure.

Use Case:
Client Experience

Client Onboarding

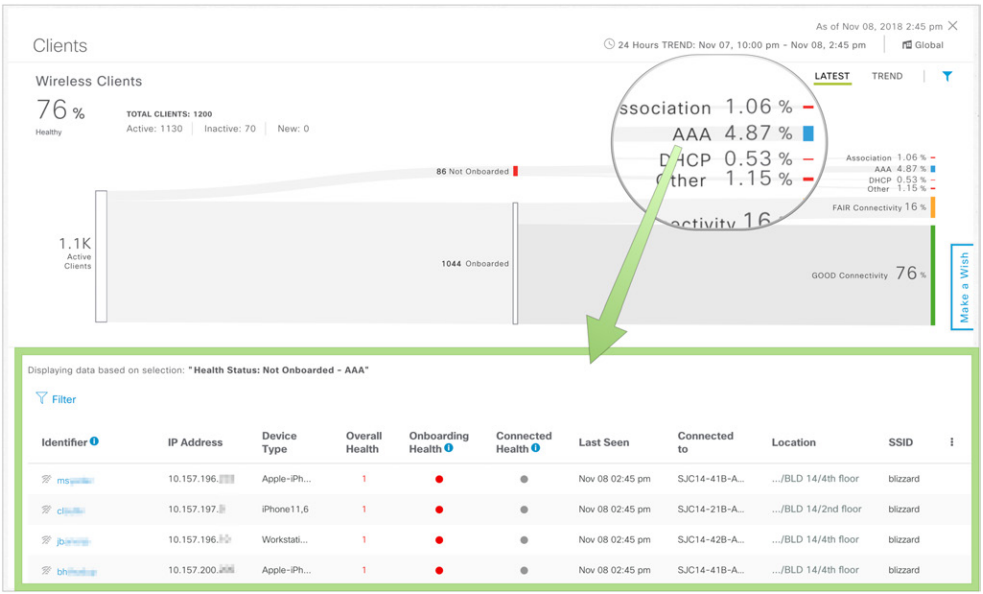
Use Case 1: Wireless client failed to associate due to client timeout

At 11:40am, Larry the network operator receives a new ticket via ServiceNow indicating the San Jose site has many clients failing to onboard to an SSID. Looking at Cisco DNA Assurance, he finds that a critical issue has been created on the Executive Dashboard stating the **"Client is failing to onboard due to frequent authentication failures."**

Understanding the workflow followed by Larry is key to solving this critical onboarding issue. Cisco DNA Assurance utilizes streaming telemetry from the network infrastructure that provides excellent visibility to client onboarding issues. Larry logs into Cisco DNA Assurance and navigates to the Client Health Dashboard. Using the Sankey chart displayed, he is able to understand that many clients are failing to onboard at the San Jose site due to authentication failures.

The Sankey chart shows the different stages of onboarding and connectivity. Each Sankey chart element is interactive so when an item is selected, the client table is updated. From there, Client 360 can be easily accessed.

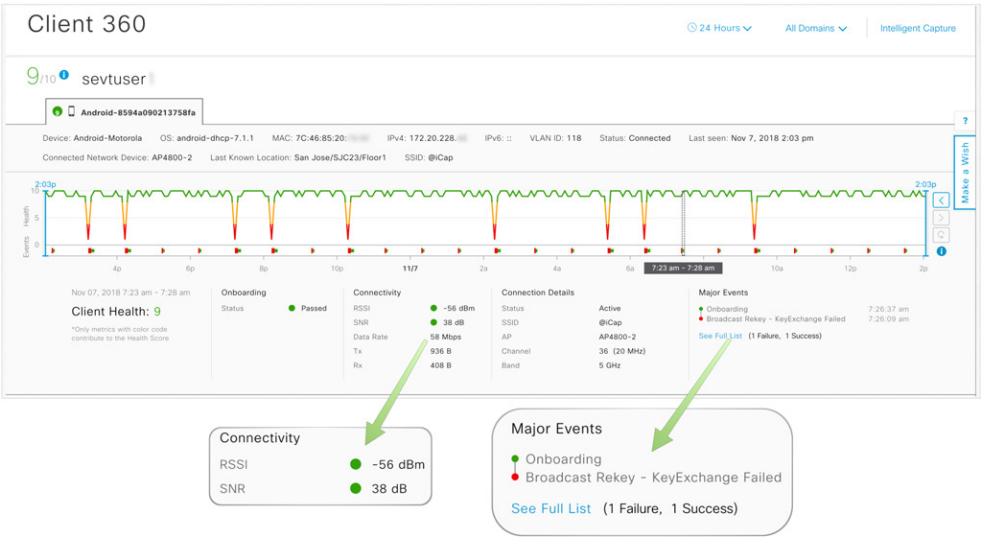
DIAGRAM Client Health Dashboard with Wireless Client Sankey chart



Larry then selects the client and goes into Client 360 to understand the historical behavior and to find the root cause of the problem. He starts with the Time Travel option to go back in time and identify the time and stage of onboarding at which the client has failed.

The top lines of the Client 360 display show the RF details while the bottom line shows onboarding events. The RF signal level is displayed in the Connectivity tab - this indicates the problem is not with RF connectivity, as a strong signal of -56 dBm is present along with a Signal to Noise Ratio (SNR) of 38 dBm. Both of these KPIs are represented in green, which indicates there is no problem. The "Major Events" section shows the results of onboarding events, where a red "Broadcast Rekey" icon is displayed, indicating a potential problem.

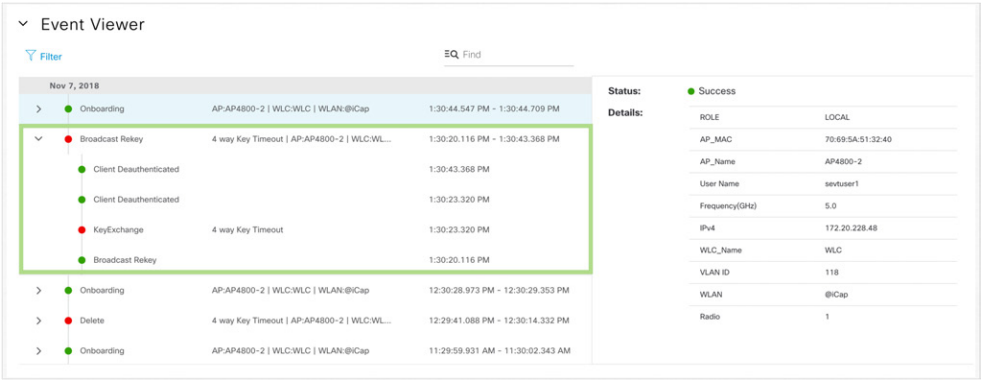
DIAGRAM Client 360 showing Broadcast Rekey failures



Larry then goes into the Event Viewer to identify more details of the onboarding failure that have been reported. There are a variety of problems that can happen at the device driver, supplicant, network, or network service level, including the RADIUS and DHCP services. The onboarding stage is one of the most critical in terms of wireless connection troubleshooting, so detailed step-by-step onboarding analysis for all clients is available. The Event Viewer provides full visibility into wireless client onboarding.

While examining the Event Viewer further, Larry is able to observe that the Broadcast Rekey, which is required as part of the WPA2 security standard, is failing due to a "4 way Key Timeout" error.

DIAGRAM Client Onboarding Failure Event - KeyExchange Failure on Broadcast Rekey process



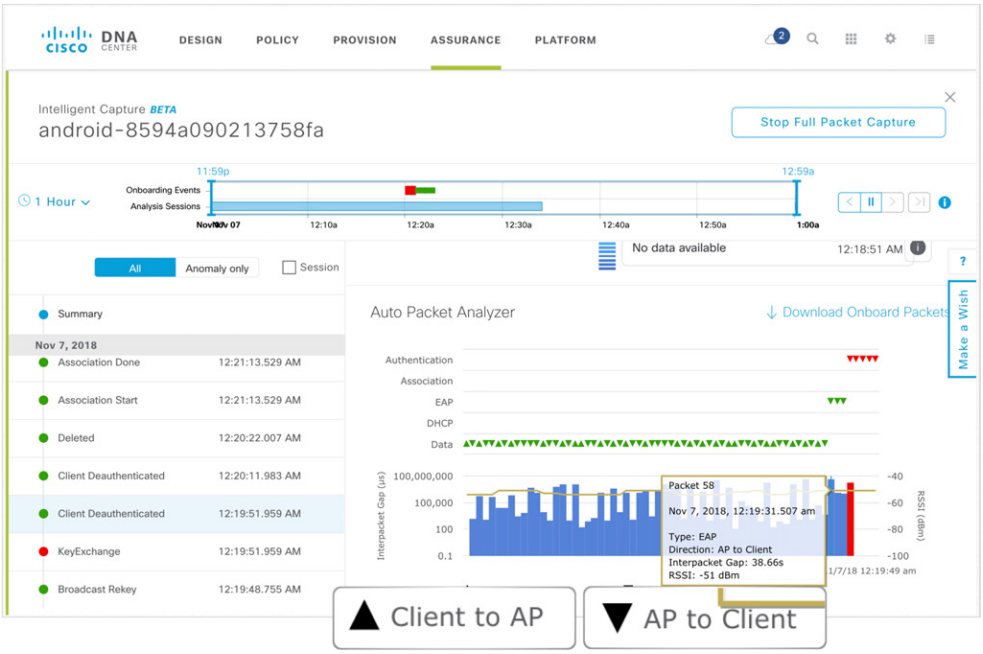
Using the Client Health Dashboard and Client 360 views, Larry is able to identify the "who" and the "what" of the issue involved. However, he is still interested to know the "why". These issues are happening more frequently, impacting this client's overall onboarding experience.

To identify the root cause, Larry utilizes the Intelligent Capture capabilities of Cisco DNA Assurance for that client, and reviews the location and RF coverage. This again helps to confirm that poor RF signal is not the reason behind the onboarding failures.

DIAGRAM Real-time Correlation of Client Onboarding, Location, and RF Environment

Next Larry zooms into the onboarding failure events and reviews information from the Auto Packet Analyzer that shows details for each onboarding event. This includes handshake information between the AP and the client. This allows Larry to identify the delay, timeout, and re-transmission for each onboarding step. The up and down arrows indicate the direction of the packets between AP and client.

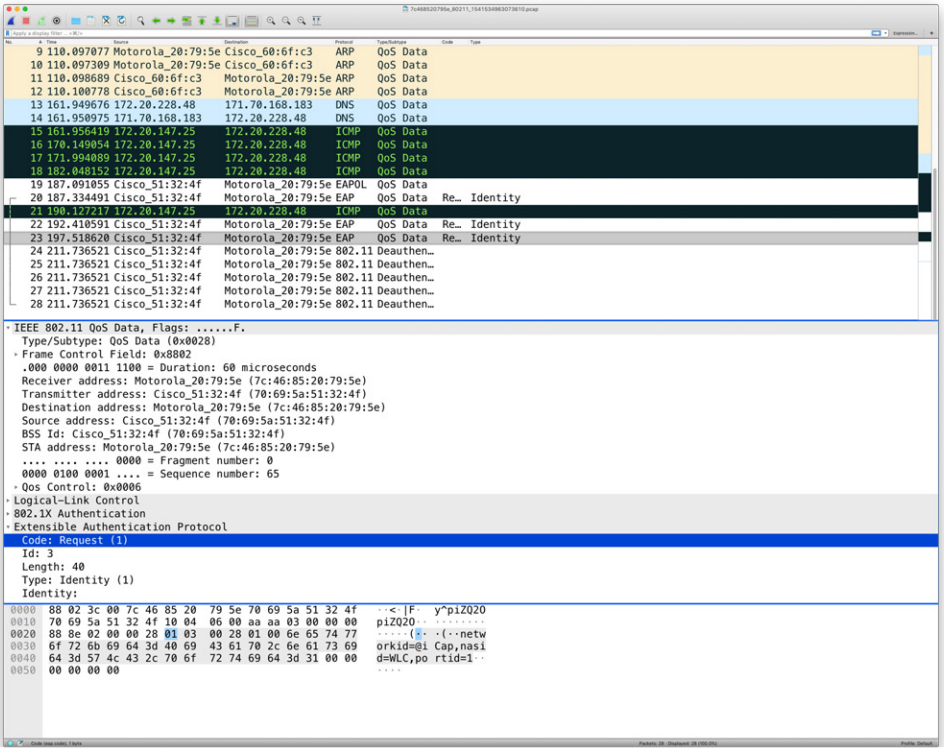
DIAGRAM Onboarding Packet Analyzer Analysis



When leveraging Intelligent Capture, Larry downloads to his laptop the onboarding packets that are associated with the failure. When analyzing the PCAP file, he observes repetitive KeyExchange requests from the AP which are part of the Authentication process. When there is no reply from the client after repeated attempts, the AP deauthenticates the client. By using the packet analyzer tool, Larry is able to conclude that this failure is happening because of a client device driver issue.

Network operators can share the PCAP file with other analysts as required and can use any packet analyzer tool for offline analysis.

DIAGRAM Wireshark Packet Capture Analyzer



Key Cisco DNA infrastructure elements (WLCs and APs) used in this use case are:

- AireOS 8.8 or IOS XE 16.10.1 Wireless LAN Controller Software.
- Access Points 2800, 3800 and 4800 series providing Intelligent Capture.
- Connected Mobile Experience (CMX) 10.5 for location tracking.

Client Connectivity

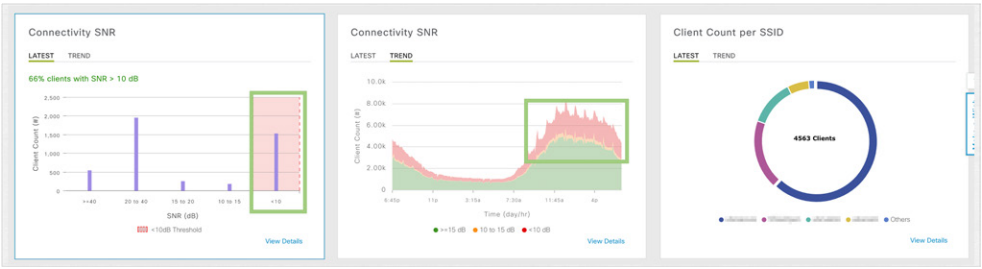
Use Case 1: Wireless client failed to roam due to high interference

At 12:30pm, network operator Larry receives another ServiceNow ticket. There is a new venue on the San Jose site where a large conference is happening, with a high density of users connected to the network. He finds that a global issue has been created on the Executive Dashboard in Cisco DNA Assurance, where the "**Client is failing to associate while roaming due to high interference.**"

Once the client has successfully onboarded, the important aspects that may impact connectivity include RF coverage, client density, interference, and roaming. The network architect aims to design the network to ensure optimum coverage and density and to offer the best-in-class experience to clients. This particular venue has not been properly designed with High-Density wireless in mind. There are also several sources of interference, including wireless projectors, printers, security cameras, and some other IoT devices.

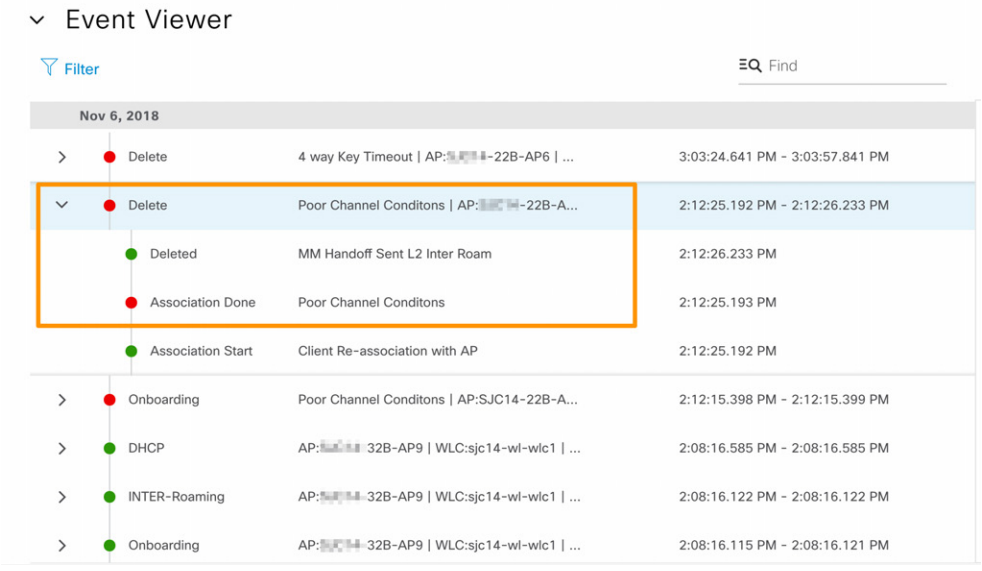
Larry now has the difficult job of assessing the impact of the current issue, identifying the root cause, and ensuring end users receive the right experience. He logs into Cisco DNA Assurance to begin diagnosing the issue. He starts with the Client Health Dashboard to assess the RSSI and SNR and review client density information. Since the SNR is low and the client count is high, this indicates a high amount of interference. The Connectivity SNR dashlet provides the list of specific clients that are experiencing poor connectivity, as shown by the red area on the dashlet. Low SNR can result in poor wireless experiences including frequent roaming, disconnection, delay, and jitter.

DIAGRAM Connectivity Dashlets showing SNR Metrics



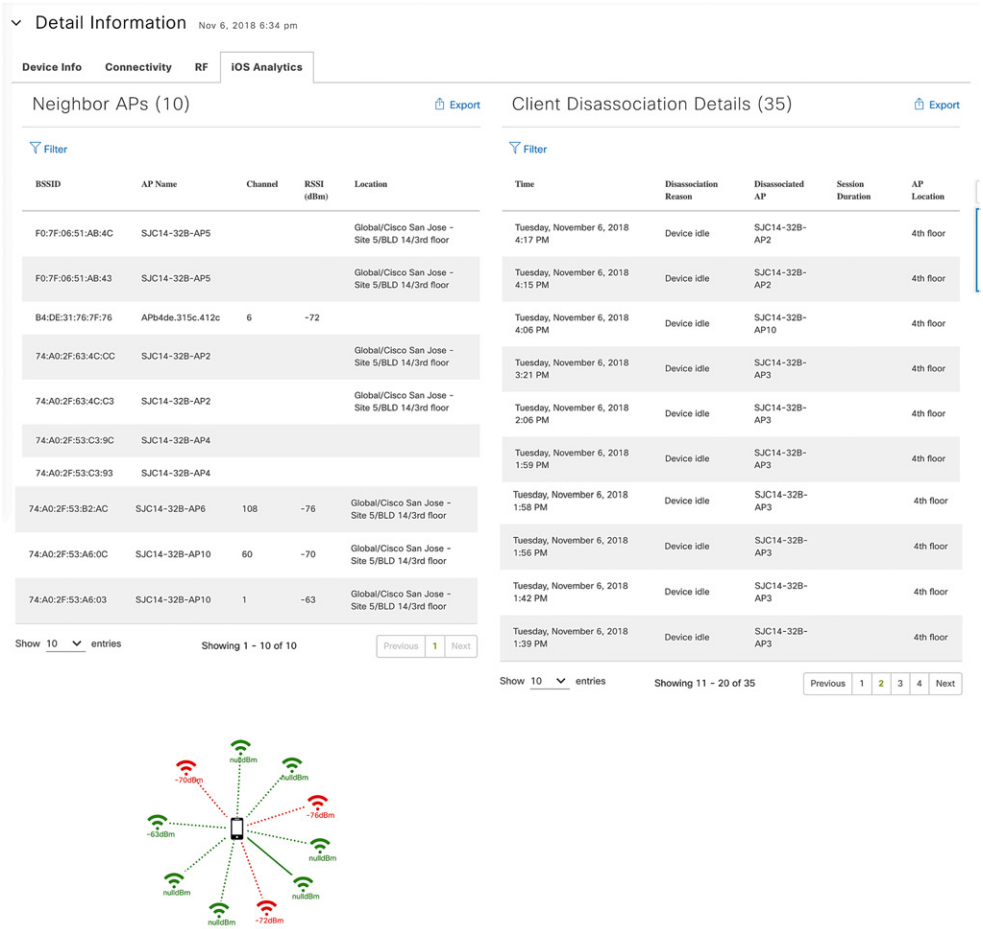
Larry can now go into Client 360 and correlate the high interference with the roaming failures shown in the Network Time Travel view. The Event Viewer in the same Client 360 shows Poor Channel Conditions as the reason for the failure.

DIAGRAM Event Viewer showing Poor Channel Conditions



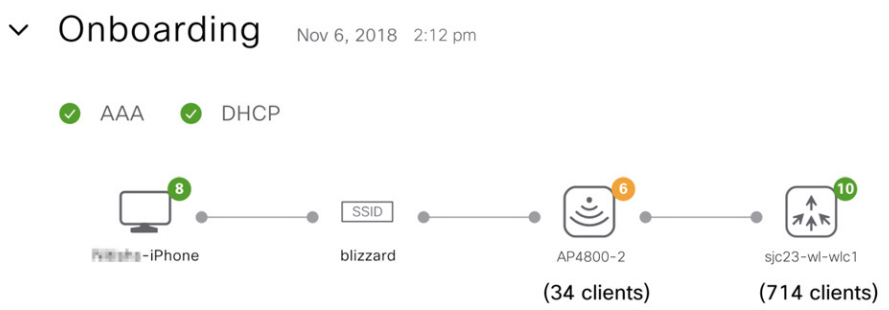
As this is an Apple iOS client device, Larry leverages the iOS Analytics capabilities within Client 360 to identify the reasons for disassociation while the client is roaming. This is the wireless client's perspective that only Cisco DNA Assurance can offer because of Cisco's exclusive partnership with Apple. This additional telemetry that the iOS device provides to Cisco DNA Assurance includes the AP Neighbor List and the client's view of RSSI. The iOS device details, including version and hardware information, are also provided, along with any disassociation details. This does not require any agents or configuration on the iOS device.

DIAGRAM Apple iOS Client Report



Since the coverage offered to the client seems to be acceptable, Larry now looks at the Onboarding Topology via Client 360. This helps to identify the AP that the client is associated with and also displays the health of each element in the path.

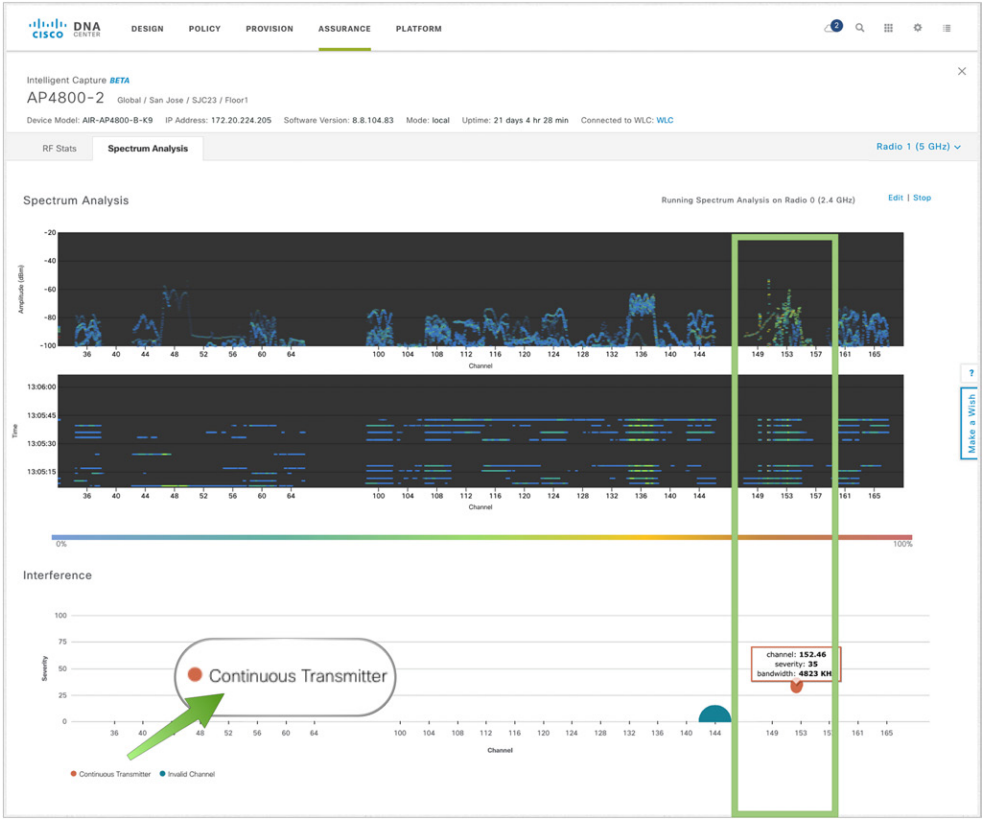
DIAGRAM Onboarding Topology



The Client Health Score is 8, but AP Health Score is 6, and there are 34 clients associated to the AP. The WLC has a Health Score of 10 and has 714 clients associated. The AP's reduced Health Score also impacts the other 33 clients. The onboarding topology is provided for all client types including both wired and wireless.

Since the health of the connected AP is 6 or "fair" due to high interference, Larry uses the spectrum analyzer capability within Intelligent Capture to analyze the RF spectrum and view any potential sources of interference. He concludes that the client is experiencing poor connectivity due to high channel utilization. He also identifies some additional interference that is a continuous transmitter on channel 153.

DIAGRAM Spectrum Analyzer View

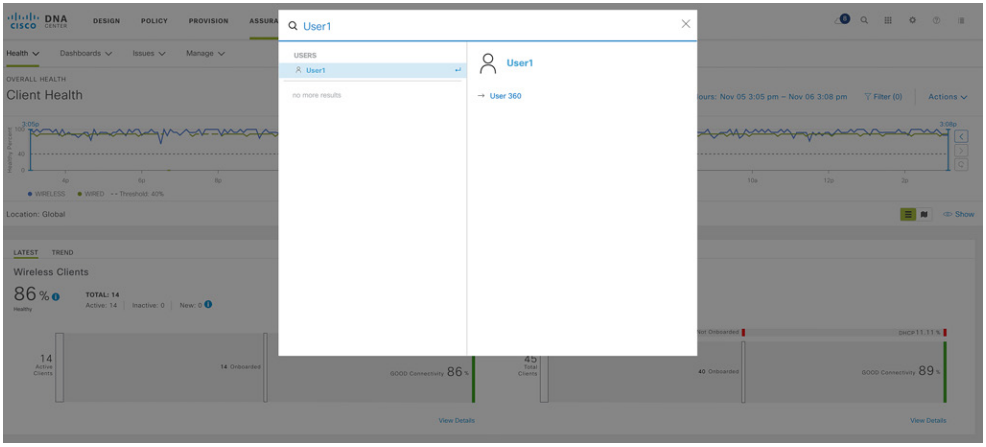


The Spectrum Analysis view shows the spectrum in a waterfall view. The interferer's center frequency and severity index based on duty cycles and power level is also displayed. This is powered by CleanAir technology in AP2800, 3800 and 4800 and the Spectrum Analyzer view is supported in Local, Flex and Monitor mode access points.

Use Case 2: Wired user cannot print due to an ACL

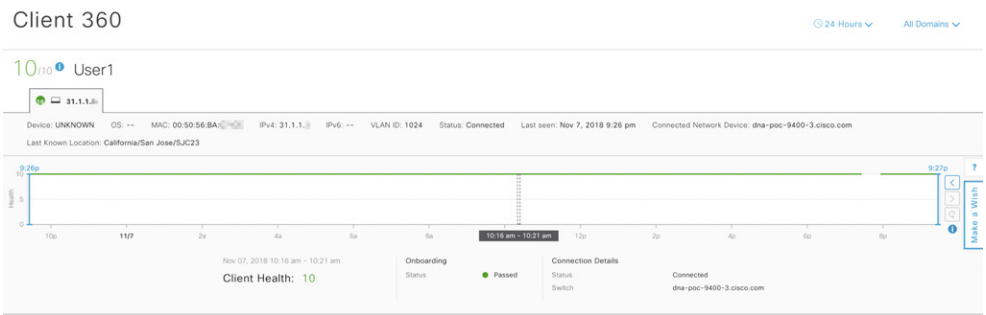
At 2:00pm, Larry receives yet another ticket, this time from a wired user who is unable to print from their desktop at headquarters to a network printer in a branch office. Larry starts by searching for the client username in Cisco DNA Assurance, in this case "User1". Through integration with ISE, Cisco DNA Assurance automatically correlates the wired client username with the device IP, operating system and version details. Larry selects Client 360 to troubleshoot the problem further.

DIAGRAM Global Search



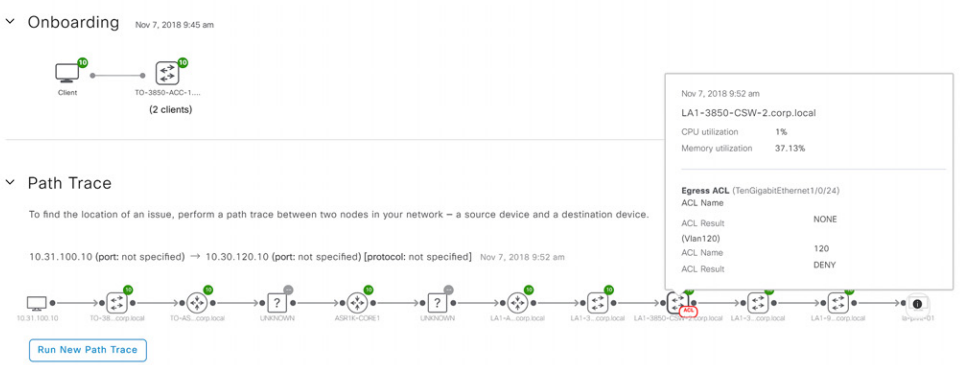
Once in Client 360, by looking at the health chart, Larry gets an overview of how the desktop device has been performing over time. By hovering over the health chart, he is provided with operational details such as onboarding and connectivity status. The wired client view provides a similar workflow and 360 view as that provided for wireless clients.

DIAGRAM Client 360 View



Since the desktop has a perfect 10 out of 10 health score, Larry suspects that the problem could be related to the network. He runs a Path Trace to do a hop-by-hop trace from the desktop to the printer in order to isolate a potential network problem. The Path Trace provides hop-by-hop visibility with ACL network service reachability validation. Path Trace also shows interface details including port number, VLAN ID, and QoS details per hop.

DIAGRAM Path Trace between Two Devices



Cisco DNA Assurance provides the ability to analyze the ACLs that are configured along the path, which helps Larry to quickly identify that there is an ACL misconfiguration on one of the switches (a Catalyst 3850). He can now assign the ticket to the security team for resolution.

Use Case:

Network Assurance

Network Monitoring

Networks have grown in complexity and there can be multiple points of failure between clients and applications. To be able to troubleshoot and fix problems quickly, it is important to understand which layer or domain the issues are seen in.

Cisco DNA Assurance makes proactive monitoring of networks simple through the concept of ongoing monitoring and health scores. Health scores are summarized through Health Dashboards by providing visibility across the different layers of the network. Cisco DNA Assurance supports both real time and historical troubleshooting. For real time troubleshooting, it offers tools such as Intelligent Capture and Path Trace. The time travel capability offered by Cisco DNA Assurance allows network operators the ability to go back in time and analyze problems that occurred in the past.

Use Case 1: Network monitoring using the Network Health Dashboard

Matt, the network manager at Acme Corporation, uses the Health Dashboards to quickly understand the critical areas in the network that need attention. This helps him to plan the work for his team.

Using the Network Health Dashboard, Matt gets an overview of how their network infrastructure is performing across different domains. The common reasons for certain devices having poor or fair health scores are highlighted in the summary section. If required, he can drill down to get the actual list of devices impacted, by clicking on the domain name. He notices that some of their distribution and access switches are experiencing poor health, and he asks Larry, a network operator in his team, to check it out.

DIAGRAM Network Health Dashboard

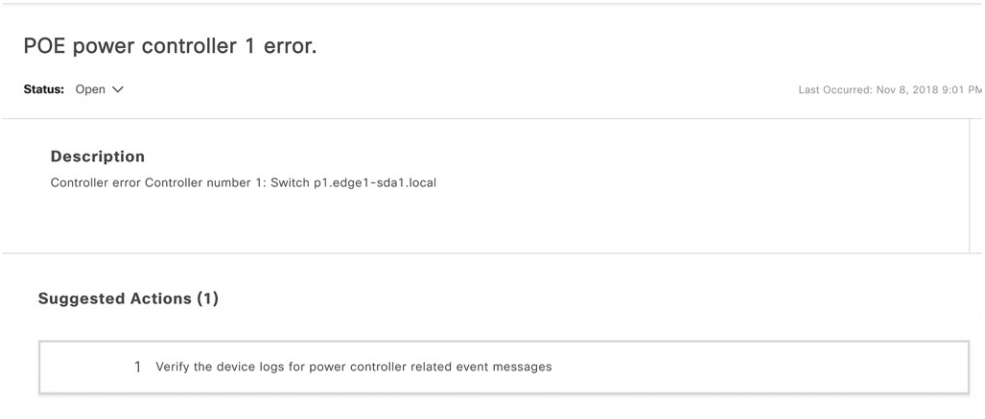
When Larry received this request, he was actually already in the middle of examining another switch issue that he had noted on the Network Health Dashboard around PoE power management for a few other switches. Let's see what he was doing there, before he went into troubleshooting the issue that came over to him from Matt.

Use Case 2: Power management for PoE endpoints

For Larry, the network operator, one of the most common issues that he tackles is to manage power for their PoE endpoints on the switches. This requires the switch to maintain power allocation for the ports and adjust the power budget to PoE-powered devices as required. Cisco DNA Assurance monitors the operation of the PoE power controller on the switch through the network telemetry sent from it.

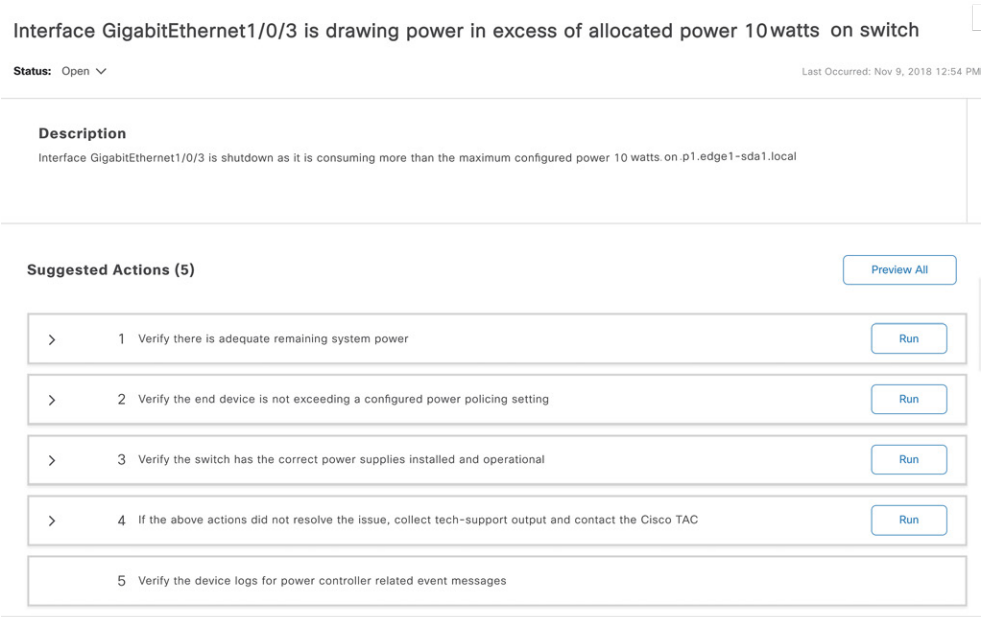
When Larry picked one of the access switches that had poor health and went to the Switch 360 view, he noticed a PoE controller error.

DIAGRAM PoE Power Controller Issue



In addition, Larry also noticed an issue in Switch 360 that one of the ports connecting towards end devices exceeded the allocated power, which explains why the power controller was reporting an error. In this case, he makes a note for himself to examine the PoE power draw for the associated device, and then switches over to the troubleshooting task that came to him from Matt.

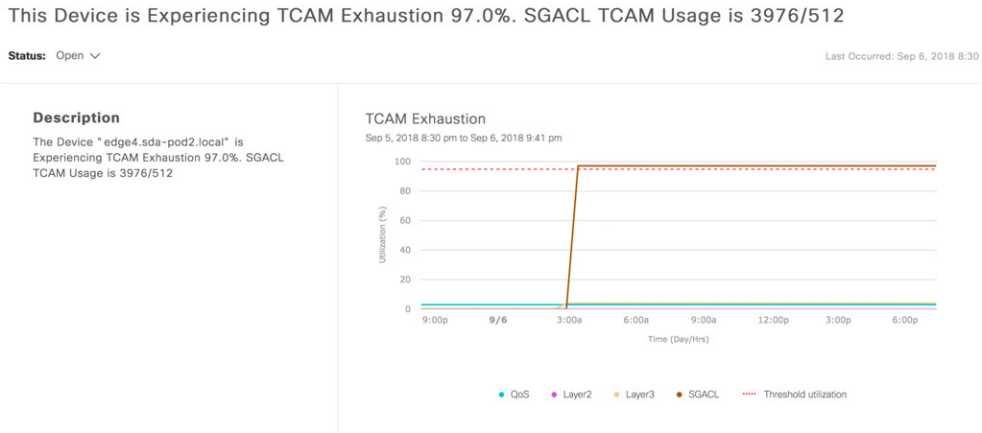
DIAGRAM PoE Power Overdraw



Use Case 3: TCAM utilization monitoring for capacity planning

Nancy, another network operator, monitors the distribution and core switches to ensure that their current network design is able to support the ongoing demands imposed by the company's growing head count. Nancy periodically checks Cisco DNA Assurance's Global Issues to understand if there are issues related to network capacity. She notices that a switch has reached 97 percent of its TCAM utilization and that Assurance has raised an issue for it.

DIAGRAM High TCAM utilization



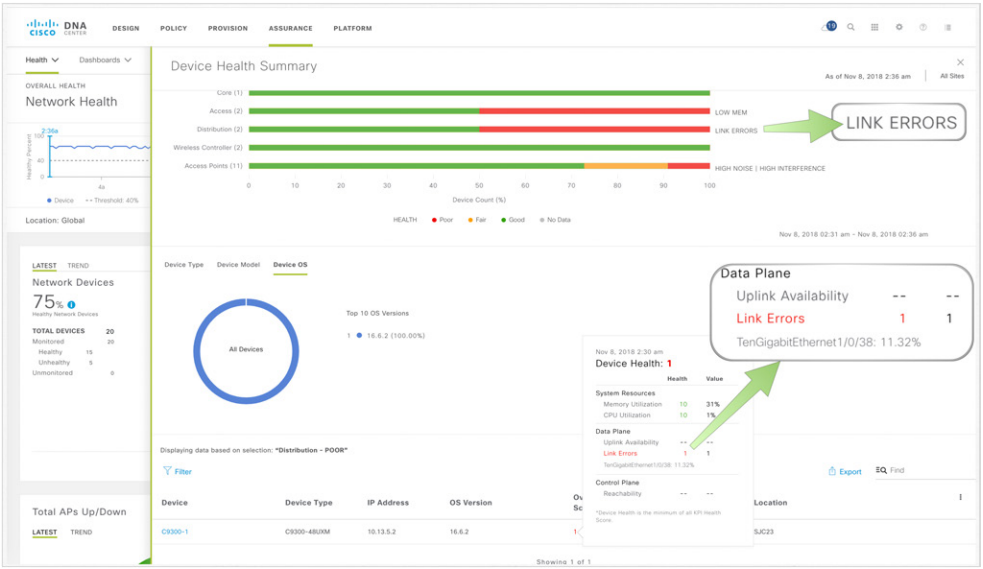
In this case, she notes that the TCAM utilization has spiked suddenly, not growing on a gradual basis as it would if it was related to organic headcount growth. Nancy further notes that this issue is indicating a problem with SGACL (Security Group Access Control List) TCAM utilization, which points towards a problem with the site's security implementation. She therefore raises a ticket with Acme's security team to further root cause the issue.

Network Troubleshooting

Use Case 1: Troubleshooting network devices with persistent Interface Errors

Larry starts on the issue assigned to him by Matt by looking at the Network Health summary and sees that high interface errors are impacting health. Cisco DNA Assurance monitors interface errors as part of the data plane KPIs that comprise the health computations for network devices. An issue is raised when interface errors are persistent over a period of time.

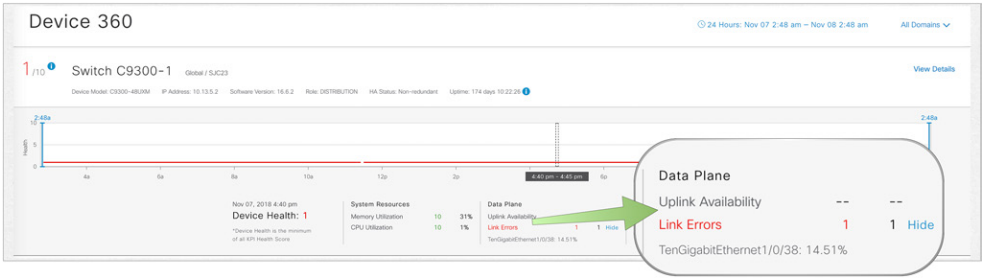
DIAGRAM Network Health Panel Highlighting Link Errors on Device with Low Health Score



Larry gets the list of switches with poor health scores by clicking on the red section of the line chart. Hovering over the health score displays more details about the key KPIs that are monitored for the specific device. From here, Larry drills down to troubleshoot a specific switch by clicking on the name of the switch to get into Device 360.

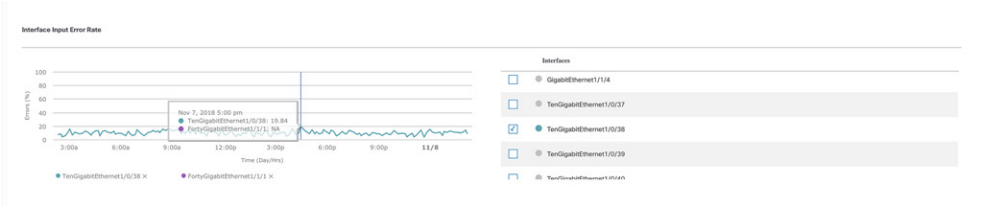
In the Device 360 view Larry can get a quick summary of when the problem started, and how long it has been observed, by looking at the health trend line. This helps him identify which interface has errors. In this case, the interface in question has a 14.51% error rate.

DIAGRAM Device 360 Identifies Interface with High Errors



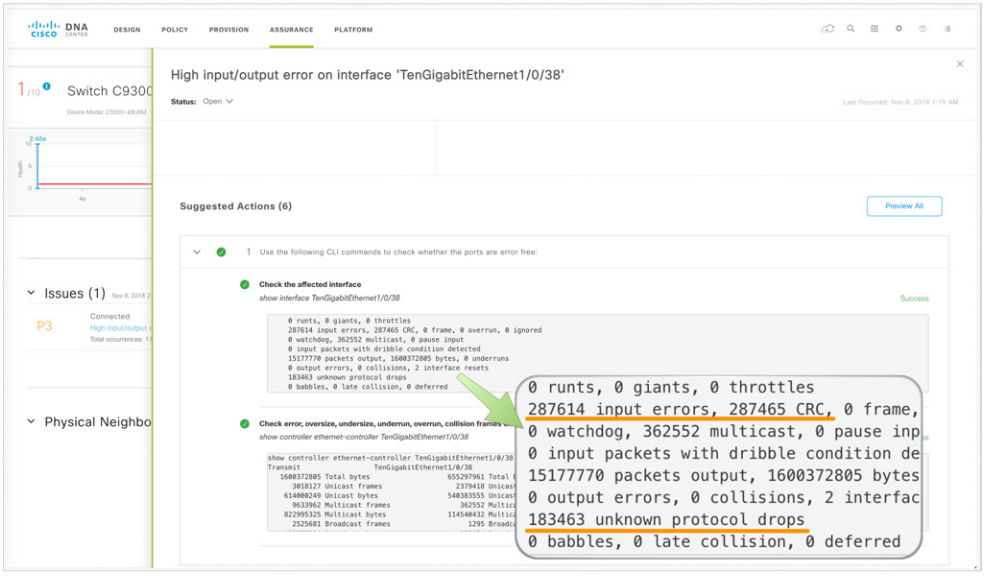
Once the interface is known, Larry looks at the interface error KPI charts to see how the error value is trending.

DIAGRAM Interface Error KPI Chart



Since the interface errors are seen consistently, he also finds an issue raised for this in Device 360. He then leverages the integrated command runner capability of Cisco DNA Assurance to identify the root cause.

DIAGRAM Link Error Issue with Command Runner to run the Diagnostic Check

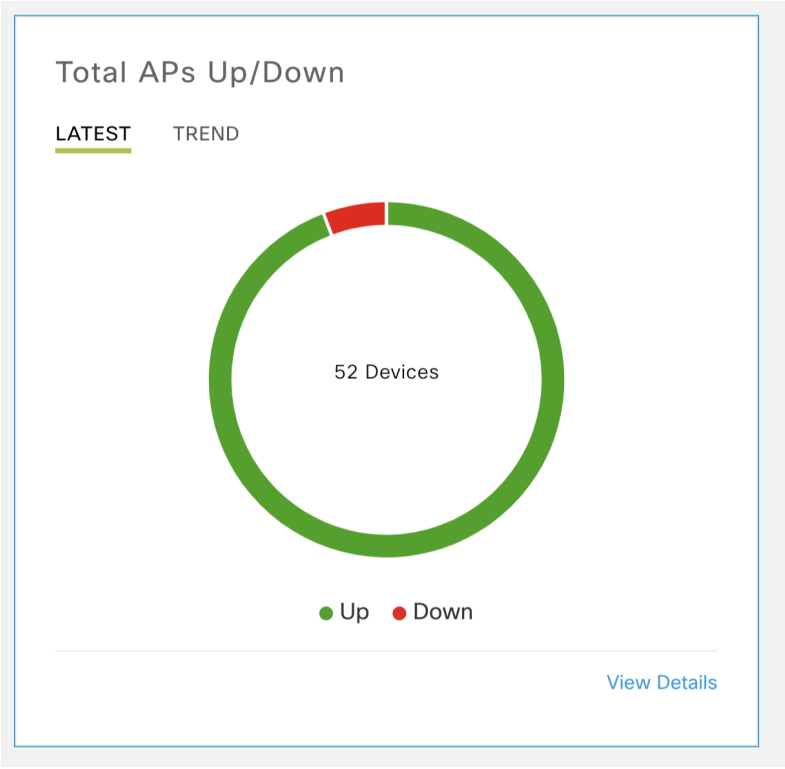


In this case he notes a high CRC error count which is likely to be caused by a failing optic or a cabling issue. He dispatches a technician to the device to swap out the components.

Use Case 2: Troubleshooting APs that are operationally down

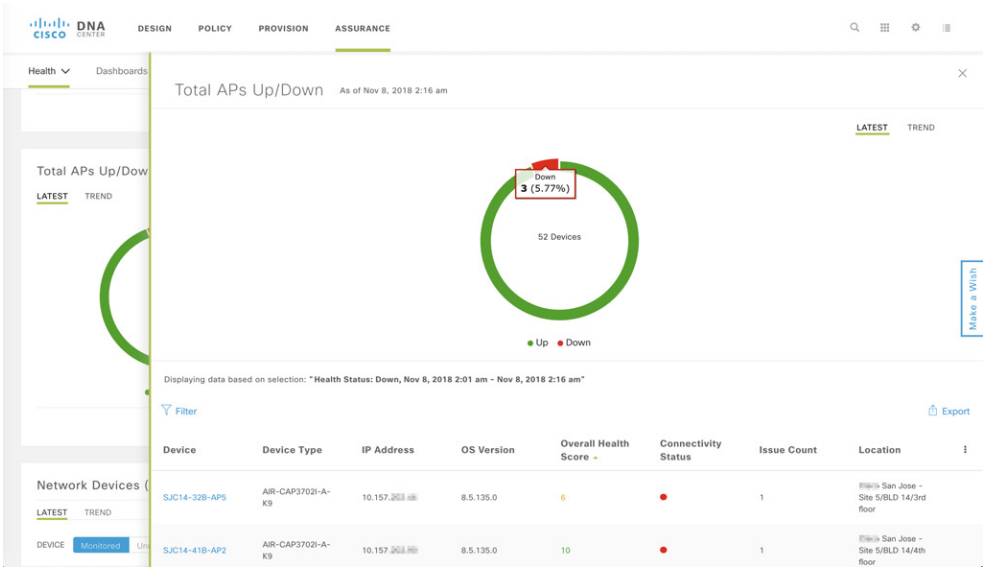
Nancy knows that Cisco DNA Assurance tracks the operational status of APs and provides visibility into AP flaps and AP disconnects. She starts by monitoring the Network Health Dashboard's "Total APs Up/Down" dashlet to understand AP status at any given time.

DIAGRAM Total APs Up/Down Dashlet in Network Health Dashboard



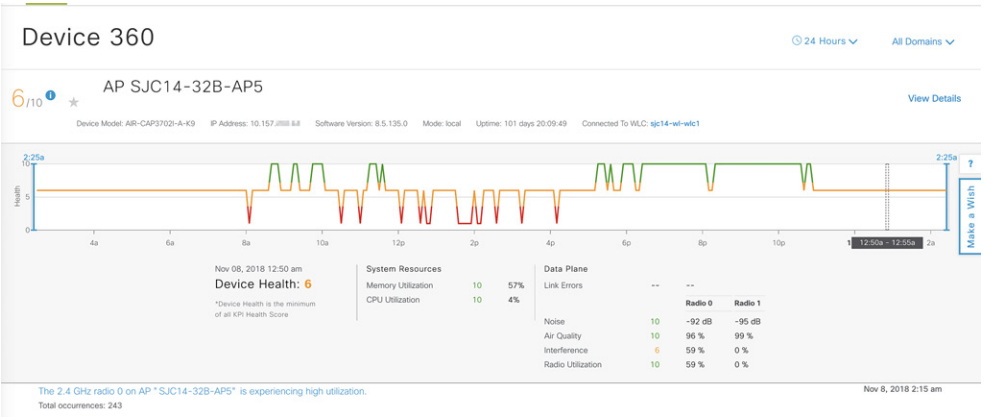
She can then quickly get the list of APs that are down by clicking on the View Details link in the dashlet. The drilldown view lets her analyze whether the problem is seen on a specific floor, which could be because of a closet switch issue.

DIAGRAM APs Up/Down drilldown highlights list of AP Down devices



Since it does not appear to be a switch issue, Nancy then decides to troubleshoot a specific AP that is down by clicking on the AP name to launch Device 360. From the Device 360 view, Nancy understands which WLC the AP was last associated with when the AP went down, and how many clients were last connected to that AP. The health trend line in Device 360 provides her with a quick summary of how the AP was performing over that period of time.

DIAGRAM Device 360 View with Health Trend: AP Encountered High Interference



Nancy observes that the Interference seen by this AP is at a high value (59%), and concludes that this is likely to be related the continuous issues seen with this AP.

Use Case:
Application Assurance

Application Experience

Once clients are successfully connected to the network, their primary concern is application experience - how quickly they can access desired applications, and how reliable the connection is.

Application Assurance offers a quick way for network operators to triage whether the application issues are on the network side or server side.

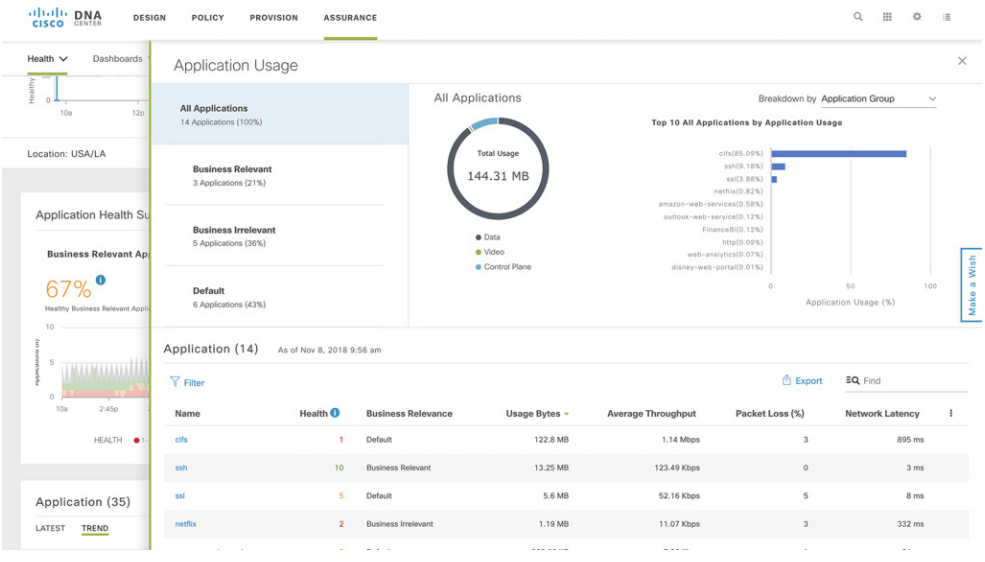
Cisco DNA Assurance uses the NBAR2 engine on IOS XE-based network routers to classify applications into Business Relevant, Business Irrelevant and Default categories. For each application, relevant quantitative and qualitative parameters such as throughput, latency, packet loss and jitter are monitored, and a composite Health Score is computed to indicate how well the applications are performing.

Use Case 1 : Proactive monitoring of Application Experience

Nancy monitors the Application Health Dashboard to understand the performance of business relevant applications. Application Health Dashboard gives her visibility into which business relevant applications are experiencing poor health. She also gets insight into how well the Application (QoS) policies are performing. Top Applications by Usage provides insight into which applications are being used the most and what is the mix between Business Relevant vs Irrelevant vs Default apps.

The Application table in the Dashboard shows quantitative metrics such as Usage and Throughput, and qualitative metrics such as Packet Loss, Network Latency and Application Latency, for each of the applications monitored by Cisco DNA Assurance.

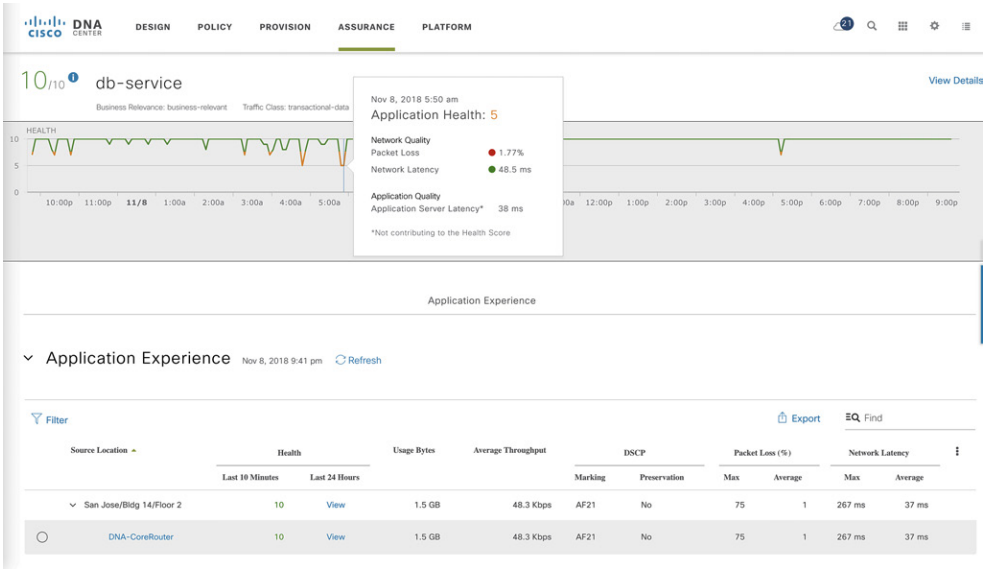
DIAGRAM Application Health Dashboard



Nancy gathers qualitative metrics for each of the applications and drills down into App 360 for detailed troubleshooting if required.

On the App 360 Dashboard, Nancy uses the Time Travel chart to get a summary of how the application has been performing over time. For more insight on the application flow across sites she uses the Application Experience table.

DIAGRAM App 360 Dashboard with Time Travel Chart

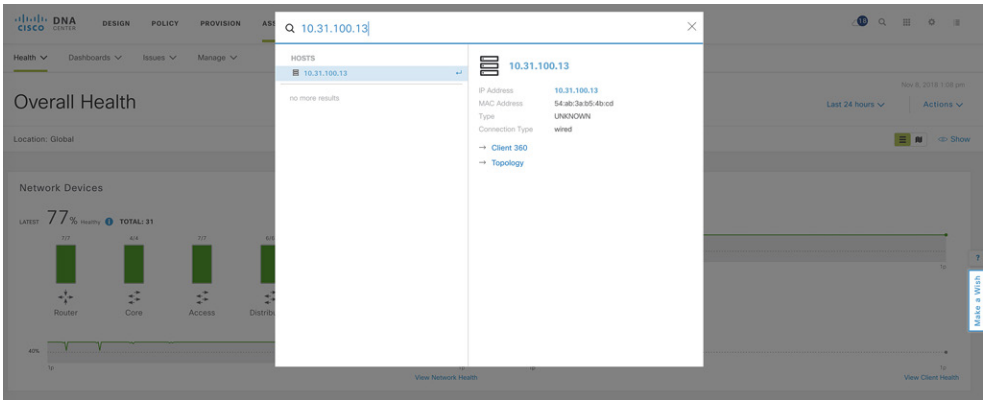


In this case, Nancy is able to observe that the application is experiencing a packet loss rate of 1.77%, which is likely to impact end-user experience with this app. She therefore proactively raises a ticket on the issue to be investigated by her team. She was able to do this before any end user actually had to call into the Help Desk to complain about a problem.

Use Case 2 : Troubleshooting a poor application experience reported by a user

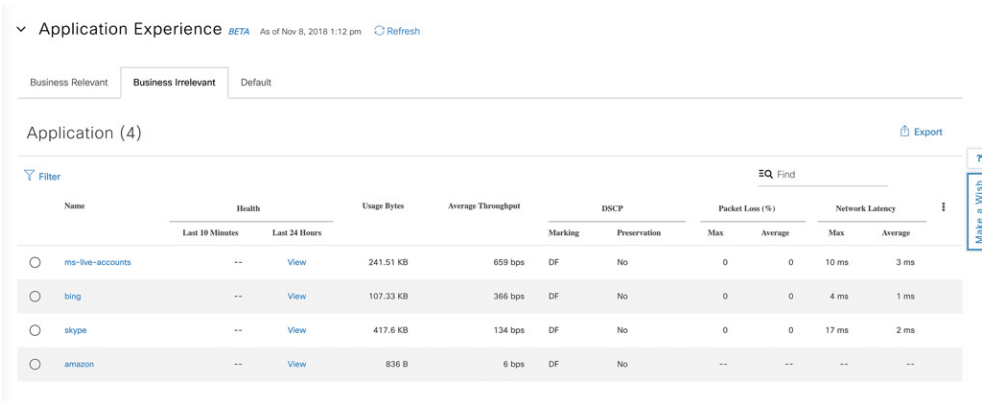
At 3:30pm, network operator Larry is assigned to work on an issue reported by a user concerning poor Skype for Business (S4B) call quality from her wireless phone. Larry searches for the user with her IP address on the Cisco DNA Assurance global search. He uses the Client 360 Dashboard to view her experience of the network.

DIAGRAM Global Search using Client IP Address



Larry checks to confirm there are no issues reported by Cisco DNA Assurance for that user related to poor application performance. Since there are none reported, he then checks the Application Experience table in Client 360 to get insight into all the applications that were accessed by the user, and takes a look at the qualitative metrics for each of these apps.

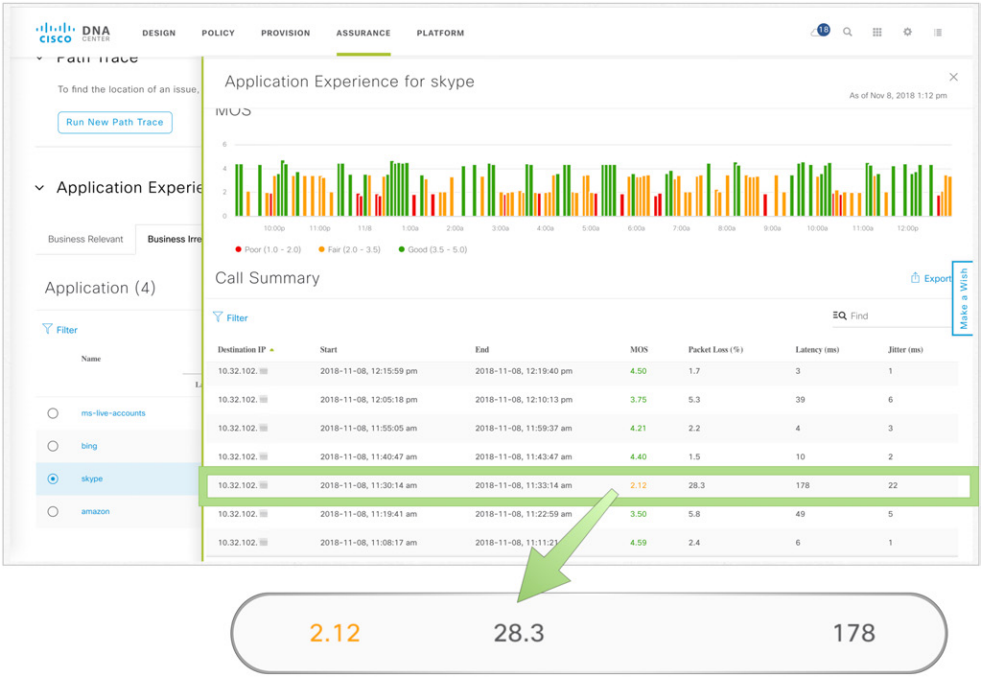
DIAGRAM Client 360 Application Experience



Larry notices that the user had indeed used the S4B application, and decides to drill into the application to analyze the experience. For applications such as S4B, Cisco DNA Assurance provides visibility into individual call records, and a Mean Opinion Score (MOS) for each call through deeper integration with the S4B Server.

Larry observes that the MOS for the calls over a period of time has been intermittently alternating between low and fair. He finds latency and packet loss are high when the MOS reading is low. For example, he can see that the MOS is 2.12 (out of 5) when there is 28.3% packet loss and 178 msec of jitter.

DIAGRAM Skype for Business view with detailed Call Detail Record (CDR), MOS, and Latency



At 4:40pm, he attaches a screenshot of the network metrics for S4B for this user and escalates the ticket to his Level 2 network operator, Nancy. In the next section we will see how Nancy uses Intelligent Capture with Cisco DNA Assurance to further troubleshoot this problem.

Use Case: Proactive Monitoring and Troubleshooting

Intelligent Capture Troubleshooting

Use Case 1: Troubleshoot application experience using Intelligent Capture

Nancy picks up the ticket that got escalated by Larry and clicks on the Client 360 view link in the ticket to contextually launch into the troubleshooting view for the client that raised the ticket.

She quickly verifies Larry's findings around performance, and understands that the poor quality problem with the S4B voice calls are due to high network latency and packet loss. She starts by examining the wireless characteristics of the client using Intelligent Capture to determine whether the problem is related to wireless issues or the rest of the network infrastructure.

DIAGRAM Wireless Application Experience Analytics using Intelligent Capture

Intelligent Capture helps Nancy conclude that the problem is on the wireless side (as indicated by the high rate of packet loss) and she therefore focuses on troubleshooting the AP to which the user was connected.

Sensor Based SLA Monitoring

At 3:00pm on Monday afternoon, network manager Matt receives a call from the CIO informing him there would be a company wide executive workshop in the San Jose conference center, with representatives joining from all over the world via WebEx, the following week. The Chairman and the CEO will also be present in the workshop, and will be local to San Jose. The CIO has given a strict mandate to Matt to make sure that all wireless and application services are offered with 100% uptime for this venue. Obviously, this is a big event and Matt calls for his entire team to meet on Tuesday. Network operator Nancy is asked to present a plan and she recommends using Cisco's 1800s Aironet Active Sensor for testing the network environment for the workshop.

The 1800s sensor can simulate a wireless client and run periodic wireless tests to ensure that the network is up and adhering to committed SLAs. The 1800s sensor is a compact device that can run simulations to test wireless coverage, network services (DHCP, DNS, etc), client onboarding and application performance. This active sensor is ideal for validating client performance and network availability for any mission-critical environment.

Matt approves Nancy's proposal and the network team puts together a plan to deploy the 1800s sensors at the San Jose site. Nancy is planning to test the following services using the 1800s sensor to validate wireless service quality:

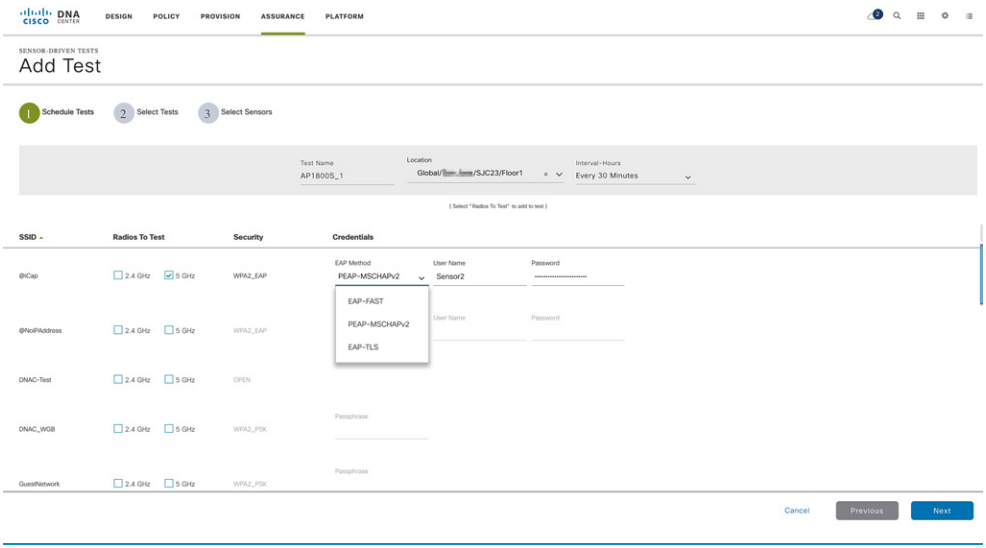
1. Client onboarding.
2. Application performance.
3. Network reachability.

Nancy is planning to commission 25+ Cisco 1800s sensors for the San Jose site. Provisioning the 1800s sensor is very simple using Cisco's Plug and Play application within Cisco DNA Center.

Use Case 1: Persistent onboarding failures happening at particular locations

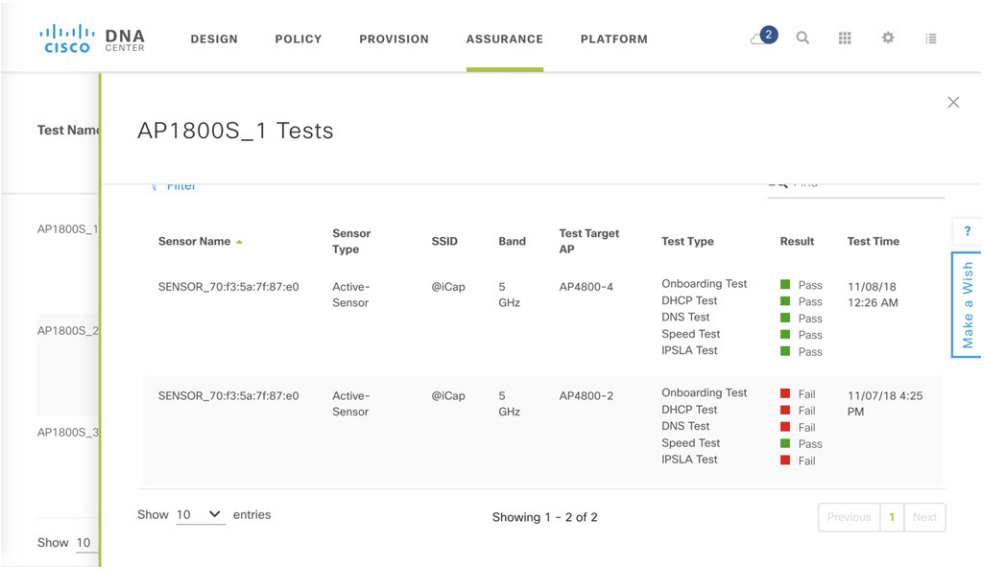
Nancy has scheduled onboarding tests on the 1800s sensor. These tests will be run across all of the APs in the vicinity of the conference center where the workshop will be conducted. These tests will be scheduled to run every thirty minutes to provide a trend assessment on a daily basis through the rest of the week. Nancy plans to set up a very quick onboarding test using the Cisco DNA Center Sensor page.

DIAGRAM Sensor-Driven Tests



Once the tests are executed, Nancy can analyze individual test outcomes for the San Jose site.

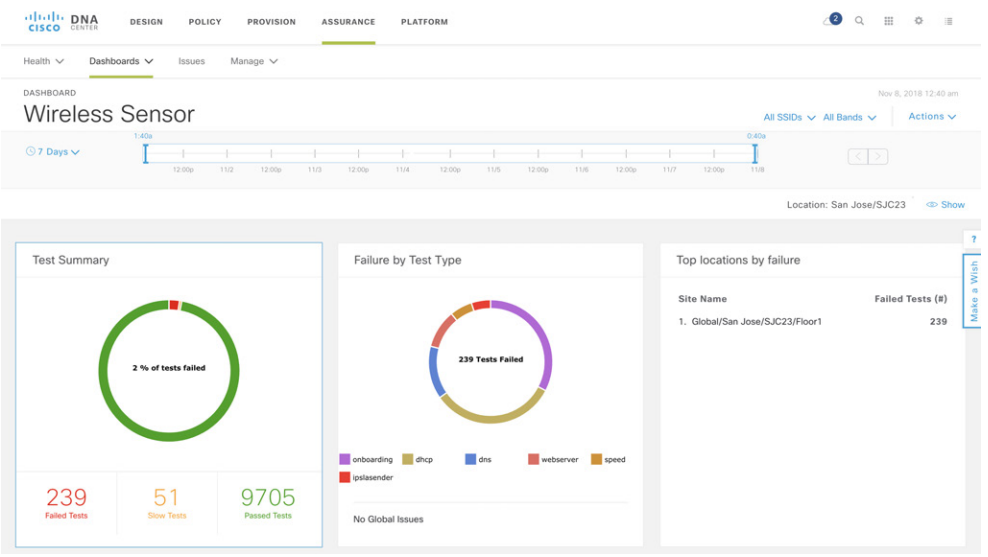
DIAGRAM Scheduled Sensor Test Results



As can be seen, there were a number of test failures, especially onboarding, DHCP and DNS. It appears that unless these failures are corrected, they will exhibit themselves on the day of the workshop. Nancy uses the Sensor Dashboard to compare the performance of onboarding against the company's historical benchmark.

Based on her analysis, Nancy decides to deploy local AAA servers at the San Jose site to mitigate onboarding failures. On Friday, she can view tests and associated results for the week on the Sensor Dashboard.

DIAGRAM Sensor Dashboard



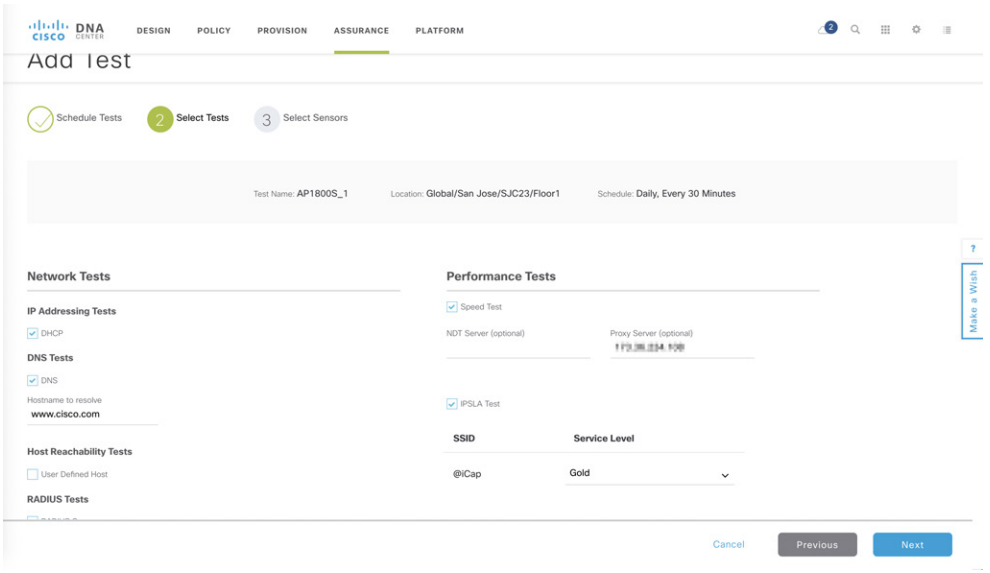
Use Case 2: Audio failures reported from certain locations at the San Jose site

Similar to onboarding, Nancy had also scheduled IP SLA and Speed tests between the sensor and Network Diagnostic Tool (NDT) server. The NDT server reports upload and download speeds, and attempts to determine what potential issues are likely to limit the speed of a cloud based application such as S4B. IP SLA, on the other hand, measures the qualitative performance of a simulated media streaming application between the client and the wireless network.

Nancy schedules IP SLA and Speed tests to run periodically (every thirty minutes) on a different set of 1800s sensors so that they can run in parallel to the onboarding tests. She can review test results and gauge any issues that are likely to impact application

performance. Similar to the setup for the onboarding tests, she sets up IP SLA and Speed tests.

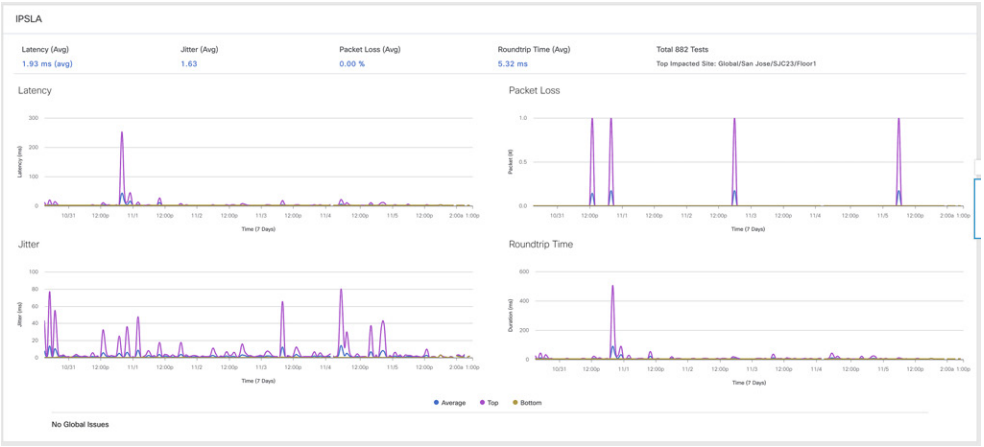
DIAGRAM Performance Tests (Speed and IP SLA) using Sensors



Speed tests provide cloud application performance insights, and IP SLA testing can be used to validate VoWiFi service readiness using UDP-based IP SLA probes.

A couple of hours later, Nancy uses the Sensor Dashboard to compare the SLA of application performance at the San Jose site against the company's historical benchmark. Based on the test results, she decides to enhance the QoS tag for Webex, and lowers the priority of other business-irrelevant traffic flowing through the WAN.

DIAGRAM Sensor IP SLA Test Results (Latency, Jitter, Packet Loss and Round Trip time)



Based on the proactive information that these sensor tests provided, Nancy is able to be more proactive in terms of preparing the site for the conference, and so to reduce the possibility of issues once the conference starts.

Fabric Monitoring

Monitoring SD-Access Fabric networks is critical. The network operators must be able to know if an issue presented to them is in the underlay or in the overlay portion of the Fabric. Cisco DNA Assurance provides proactive monitoring of SD-Access Fabric networks. This helps the network operators to further troubleshoot and resolve any issues that may arise rapidly and efficiently.

Use Case 1: Troubleshooting wired underlay connectivity issues in an SD-Access Fabric environment

Acme Corporation set up an SD-Access Fabric environment in their new office a few days ago and things are working quite well.

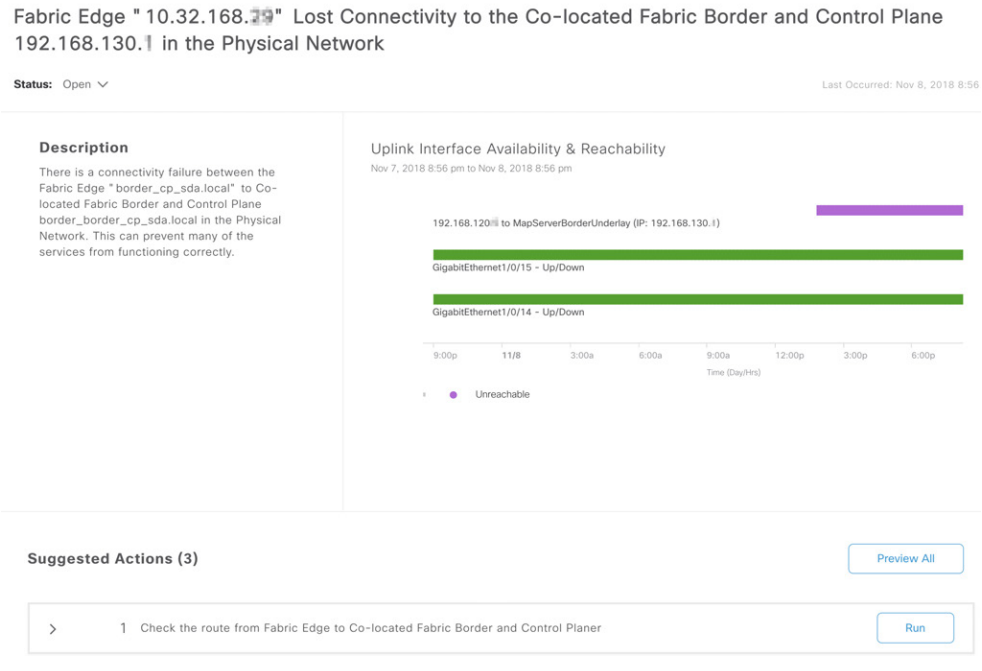
Network operator Nancy understands that in a Fabric environment, connectivity to Fabric Border and Fabric Control Plane nodes are very important for providing a seamless experience to the clients connected to the network. Cisco DNA Assurance proactively monitors reachability to Fabric Borders and Fabric Control Plane nodes from Fabric Edge nodes, and raises issues should the connectivity be impacted.

Nancy starts her day by monitoring the Network Health Dashboard, looking at the Fabric view. The health of Fabric devices is summarized based on their role - Fabric Edge, Fabric Border, Fabric Control Plane, and Fabric Wireless. When a Fabric Edge device loses connectivity to the Fabric Border or Fabric Control Plane, the health of the Fabric Edge node is flagged as poor (red) in the Network Health Dashboard.

When Nancy sees Fabric devices with poor health, she clicks on the Fabric Edge label to drill down and look at all the Fabric Edge devices that are experiencing any challenges. She notices that a Fabric Edge device in their new office is experiencing poor health, and clicks on the device to drill down into the Device 360 view.

In Device 360, Nancy analyzes the health trend of the switch to understand when the connectivity to the co-located Fabric Border / Control Plane (which takes place in the underlay) was lost. She also notices that Cisco DNA Assurance raised an issue when it detected the connectivity loss, and she uses the suggested actions capability to assist in identifying the root cause.

DIAGRAM Fabric Issue in Underlay



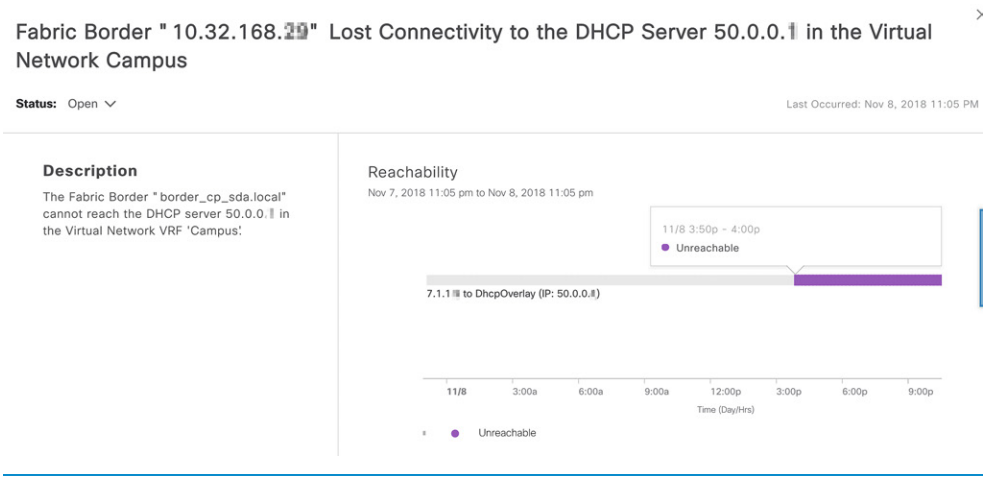
In this case, Nancy knows that she needs to focus her efforts on analyzing the Border / Control Plane connectivity from this Fabric Edge. Again, she is able to do this proactively before any users may have called in to report a problem.

Use Case 2: Troubleshooting wired overlay connectivity issues in an SD-Access Fabric environment

Nancy understands that in a Fabric environment, monitoring overlay connectivity is vital. She knows that all network services must be accessible to clients and end devices that are residing in Virtual Routing and Forwarding (VRF) instances in the SD-Access Fabric. Acme has a Data Center where all these shared network resources are located, such as DHCP and DNS. Cisco DNA Assurance proactively monitors reachability to these shared network services from the Fabric Border nodes, and raises issues should connectivity become impacted.

In the Device 360 view, she analyzes the health trend of the switch to understand if there have been any issues in the past 24 hours. Finally, she scrolls down and notices that Cisco DNA Assurance raised an issue when it detected a connectivity loss, and she uses the suggested actions capability to identify the root cause.

DIAGRAM Fabric Issue in Overlay



Again, Nancy is able to do this before any end users may have called in to raise a ticket, thus being more proactive in terms of addressing any underlying problems, and guiding her team to a faster resolution.

Cisco DNA Center Architecture

Overview

Cisco DNA Assurance is a key application that is built on top of Cisco DNA Center. Cisco DNA Assurance has been reviewed in some detail, so it is now time to delve deeper into Cisco DNA Center itself. The focus is on how Cisco DNA Center is structured, the capabilities it provides, and how it is able to support such a rich variety of services.

Networks are heading into challenges of exploding scale in end points, users, clients and applications. As the Internet of Things, Virtual Reality and Artificial Intelligence become more widely deployed, it will become extremely challenging to manage the networks with traditional systems in use today. The change in growth and capability of networks, users and applications will be dynamic. Network designers of today should be looking for a system architecture that is flexible and can be scaled up by adding more resources as required. Next Generation Enterprise Architectures should ensure that the following goals are met:

- Ability to scale up by adding additional resources to existing systems.
- Ability to visualize the whole end-to-end network at once regardless of network size.
- Intuitive User Experience (UX) that simplifies network operations.
- Ease-of-use in adding new networks, next-generation clients and applications.

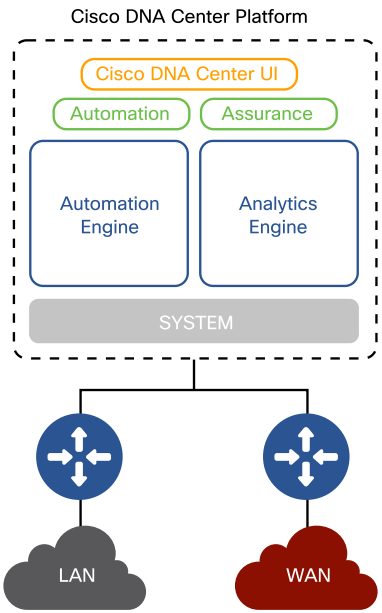
Cisco DNA Center offers a scalable and modular design that is based on a best-of-breed micro services architecture which can scale horizontally to meet the growing demands of Enterprises.

Cisco DNA Center is divided into modular components to carry out specific tasks. The major components include:

- System.
- Network Controller Platform.
- Network Data Platform.

As shown in the following diagram, the Cisco DNA Center applications consisting of Assurance and Automation (including Software-Defined Access) all leverage the scalable architecture of Cisco DNA Center.

DIAGRAM Cisco DNA Center Architectural Overview



System

Cisco DNA Center leverages a micro services-based architecture that hosts micro services in containers. Each physical node of Cisco DNA Center may not be exactly similar to each other in terms of micro services hosted in that node. By keeping the physical node and hosting of services independent of each other, the architecture allows the logical Cisco DNA Center system to operate while the physical system may have faults. Micro services can run independently in containers, and can be 1:1 or N:1. Each container / pod is allocated with resources of CPU and memory. As more and more physical resources (CPU, memory) are added to the pool of the logical system, the number of micro services can grow horizontally in order to serve larger number of users and applications or serve a larger network.

"**System**" refers to a series of infrastructure packages which are responsible for managing the underlying micro services. The System components within Cisco DNA Center help operators with managing system tasks such as upgrades, backup, restore, and monitoring.

Network Controller Platform

Network Controller Platform is one of the essential core packages of Cisco DNA Center. It is built to support Day 0, Day 1 and Day N automation workflows for network management and monitoring. The Network Controller Platform includes the Network Information Database, policy and automation engines, and the network programmer.

The automation engine has the ability to discover the network infrastructure and periodically scan the network to create a single source of truth that includes network device details, software images running on the systems, network settings, site definitions, and device-to-site mapping information. This also includes the topology information that maps the network devices to the physical topology along with the detailed device-level data.

The policy engine provisions various policies across the Enterprise network for Quality of Service, application experience, access control, and other policies. It provides an abstraction layer for the entire Enterprise network using the service and policy framework and leveraging device-specific data models. This module is responsible for the provisioning of network devices.

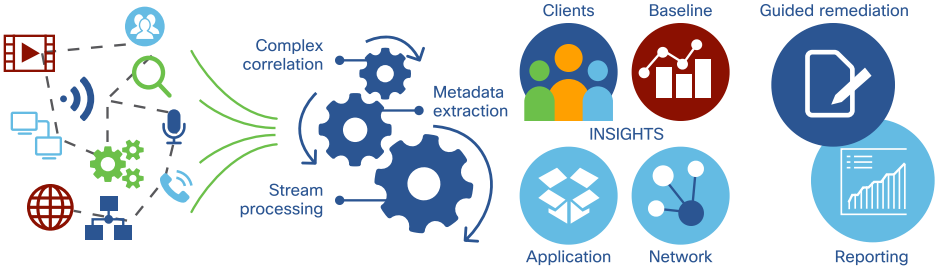
The Network Information Database stores any data that is used by the Network Controller Platform. Part of the Network Information Database, such as network topology and device information, can be exchanged with Network Data Platform for contextual analysis and correlation.

Network Data Platform

Big Data is a term used to describe large of amounts of complex data sets from different sources assimilated to reveal patterns and trends that can be used to address business concerns.

Network devices periodically send structured and unstructured data to network data collectors. Analyzing and correlating large amounts of data from different network points to show actionable insights is challenging. Storing exponentially growing amounts of data can quickly become wasteful and expensive even for small-to-medium sized networks. With the ever-increasing number and types of devices onboarded, as well as the expanding number of applications in use, aging network monitoring protocols such as SNMP and Syslog are no longer adequate to monitor the health of the network. Newer streaming protocols exist that are capable of sending large data streams at faster rates. Security is top-of-mind for many network managers today when collecting and exporting network information. Providing network administrators a window into the state of their network, and enabling them to make decisions that grow their network, are of key importance.

DIAGRAM Network Data Platform



The goal of the Network Data Platform is to convert Big Data coming from different data sources and correlate that information to generate actionable business insights. Network Data Platform is based on a comprehensive micro services-based analytics and stream processing engine. This engine provides a distributed, high performance, scalable data collection and aggregation framework to provide near real time network insights and proactive troubleshooting. Furthermore, this engine also empowers advanced use cases around IT Operations Analytics (ITOA), IT Service Management (ITSM), and Security.

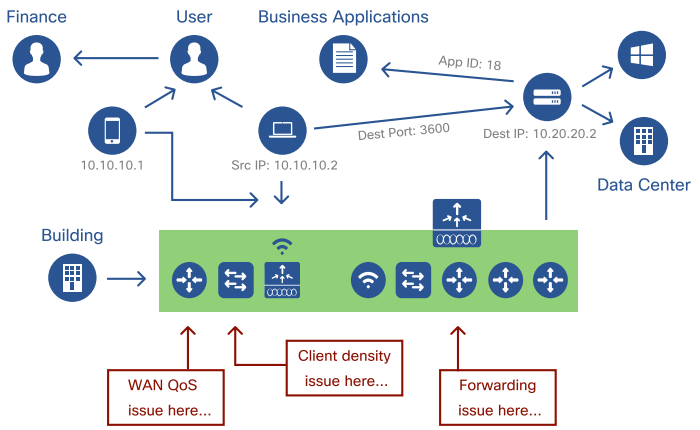
Functional Aspects

Cisco DNA Center drives innovation and simplicity over and above traditional monitoring tools by focusing on generating correlated insights. Cisco DNA Assurance collects multiple data sources for devices, applications, users, and endpoints, and then applies advanced analytics algorithms to uncover issues and suggest options for remediation. Cisco DNA Center uses unique network graph technology developed by Cisco that draws from a combination of data sources to allow for contextual correlation.

Contextual Correlation

Context helps capture and model interactions and relationships between entities and actors on the network. The Network Data Platform within Cisco DNA Center has the ability to continually enrich, aggregate, correlate, and analyze network data in near real-time. Think of this as the Big Data Engine storing the state of the network in the database while making the same available for reviewing and analyzing by Cisco DNA Assurance at some point in time in the future.

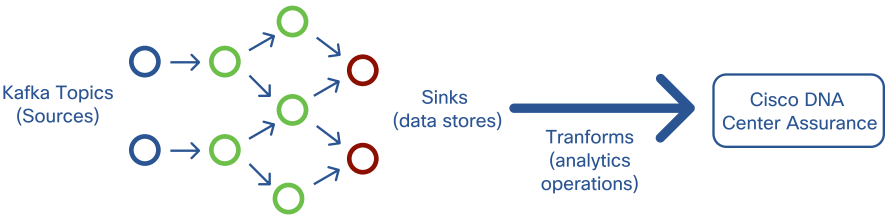
DIAGRAM Graph Data and Contextual Correlation



Time Series Analysis

A time series is a set of data points collected at an equally spaced time interval for creating Cisco DNA Assurance KPIs across networks, devices, clients, applications, and security. With built-in mathematical functions, statistical models and aggregation frameworks, the Big Data Engine sends this data to northbound applications such as Cisco DNA Assurance to create unique insights.

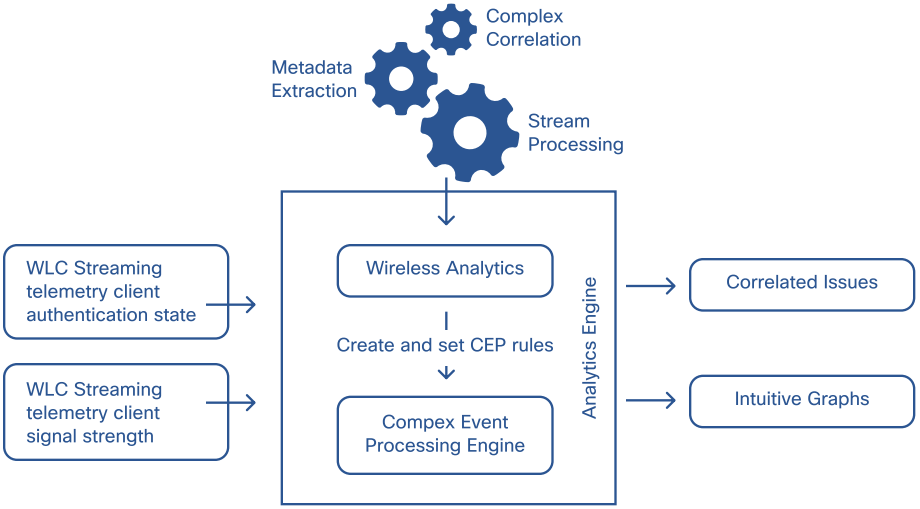
DIAGRAM Time Series Analysis



Complex Event Processing

Complex Event Processing multiplexes data from various data sources to infer events of interest or patterns. Derived patterns then trigger notifications for anomalies detected, or store the information for further processing prior to rendering the insight on the Cisco DNA Assurance Dashboard. The value of Complex Event Processing is rapidly identifying events of significance and alerting on these in near real-time.

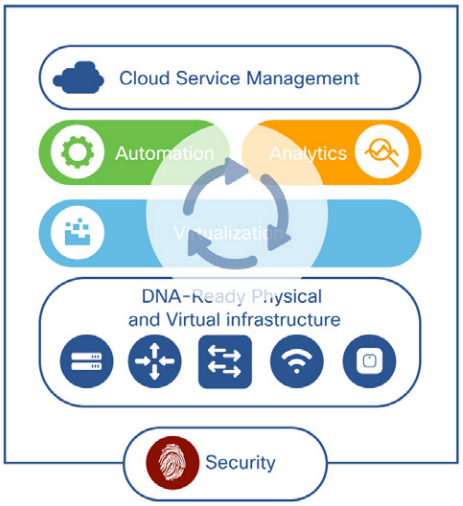
DIAGRAM Complex Event Processing



Closed Loop Remediation

In Cisco DNA Center, the role of the Automation platform is to translate the business intent as expressed by the network manager into network policies and configurations, while the role of Assurance is to monitor the network devices to ensure that everything is working as per the business intent. As shown in the following diagram, this creates a closed-loop system for use by the organization.

DIAGRAM Closing the Loop



Whenever network administrators roll out a change through Automation, they can leverage Assurance to monitor whether, and how, the change is positively or negatively impacting the network operations for the organization, and whether or not the business intent is met.

In a similar way, when Assurance detects an anomaly in the network, Network Administrators have the ability to leverage Automation to take corrective action to restore the intent. Going forward, many of these corrective actions will be automated through Assurance and ITSM workflow integrations.

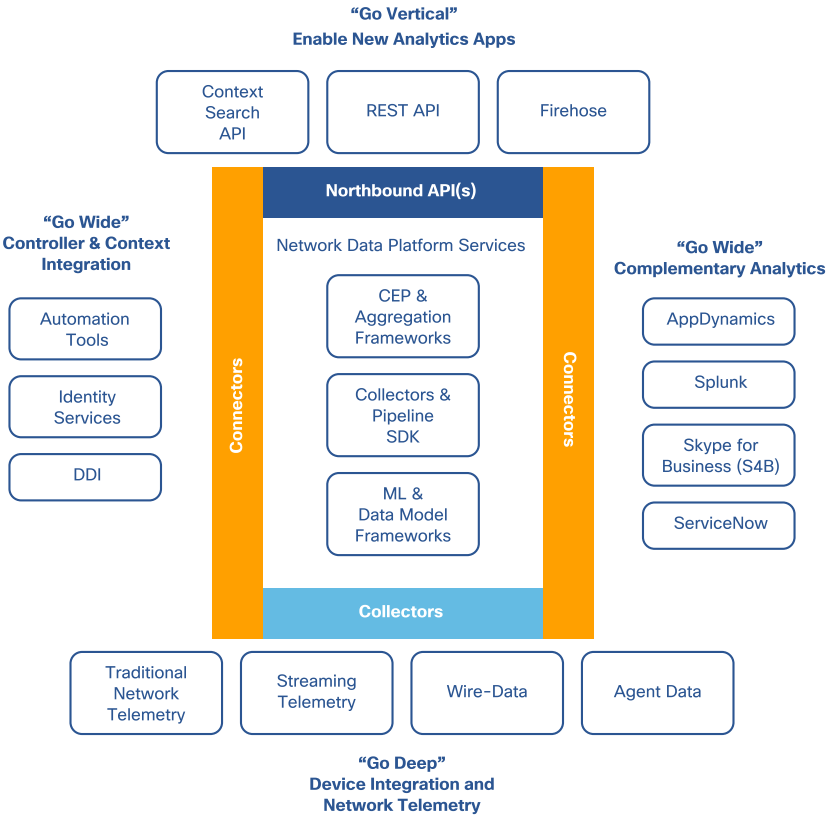
The above underlines the strong link between Automation and Assurance as one system. It is important for a network manager to know if a change - for example, an automation event - has worked as expected or not. Either way, the network manager wants to know the outcome - especially for changes for which they need to document the result and/or initiate a rollback. Conversely, an automation event may be triggered

by Assurance. As an example, a trending event detects over-utilized links and the admin needs to react. For example, this may be by changing the link speed or adding a link.

Open Integrations via Platform APIs

Open interfaces provide the flexibility, accessibility and extensibility for building custom applications and integrations with complementary industry standard platforms such as ServiceNow, Skype for Business, LiveAction and Tableau, amongst others.

DIAGRAM Cisco DNA Center - Open Platform Integration

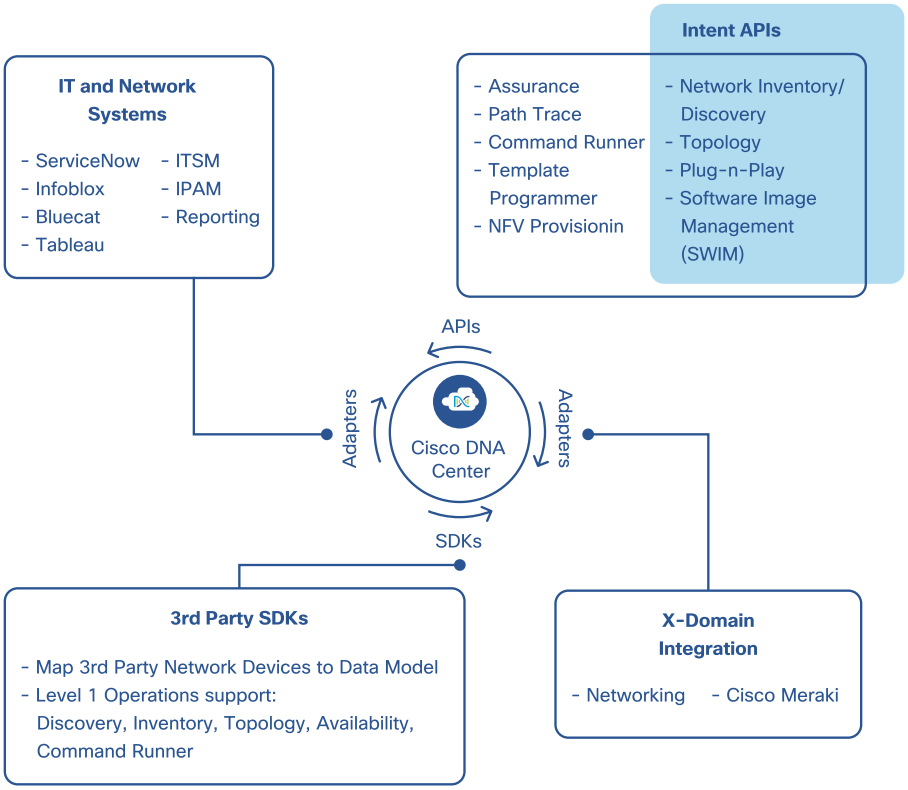


Cisco DNA Center Platform

Cisco DNA Center is the heart of Cisco Intent-Based Networking, supporting the expression of business intent for an array of proactive monitoring and troubleshooting use cases within the Enterprise network. As cloud applications proliferate in mainstream Enterprises, APIs are rapidly becoming the standard for modern IT organizations to ensure integration with best-of-breed solutions to increase productivity and enable innovation. While legacy integration practices such as the Enterprise Service Bus (ESB) are still prevalent for on-premise applications, they are being quickly deprecated in favor of API connectivity. Furthermore, to meet the need to scale and accelerate operations in modern Enterprise networks, IT operators require intelligent and end-to-end cross functional workflows built around open APIs. Today, it is not a question about whether or not we need APIs, but more about which APIs are being exposed and how they will be published for consumption.

The Cisco DNA Center Platform brings in 360-degree extensibility and openness that allows Enterprises to leverage the network as a platform. By enabling IT applications in cross-functional domains to take advantage of the network intelligence inherent to Cisco DNA Assurance, IT can now automate network operations and deployments by building new applications or integrating existing ones.

DIAGRAM Cisco DNA Center Platform Capabilities - APIs, Adapters & SDKs



The Cisco DNA Center Platform exposes native capabilities via APIs, integration workflows, events, and notifications. Furthermore, it can also support multi-vendor devices or applications by leveraging Software Development Kits (SDKs). Some of the key capabilities of the Cisco DNA Center Platform are:

- **Intent APIs**
  - Intent APIs are northbound REST APIs that expose specific capabilities.
  - Intent APIs provide a policy-based abstraction of business intent focused on the outcome instead of the mechanisms to implement that outcome.
  - The APIs conform to the REST API architecture and are simple, extensible, secure to use and support the standard REST methods namely, GET, POST, PUT and DELETE operations over HTTPS.
- **Integration Flows**
  - Integration capabilities are part of east/west interfaces exposed by the platform.
  - Cisco DNA Center Platform is an instrument for integrating Cisco DNA Assurance workflows and data with IT and Network Systems and X-domain integrations.
- **Multivendor Support (Third-Party SDKs)**
  - The Platform can manage third-party network devices and multi-vendor applications.
  - A purpose built device package using SDKs can be used to communicate with third-party devices.
- **Events and Notification Services**
  - Events within Cisco DNA Center can be forwarded to third-party applications via WebHooks.
  - Event type, publication frequency, host, and URL path to send events data can be configured by the network administrator via the Platform user interface.

Platform Capabilities

Application Programming Interfaces are critical components provided by the Cisco DNA Center Platform for enabling the management of multi-vendor devices and enabling the rich ecosystem of applications and solutions. APIs allow for a standardized method for interfacing Cisco DNA Center with external devices and services. Cisco DNA Center offers robust API integration, event notifications, and reporting, as described below.

Platform APIs

The Intent API is a northbound API which exposes the capabilities of Cisco DNA Center to external services that may wish to leverage it. This API is based on abstraction. The policy that can be triggered through the API is translated into the network device capabilities and configured by Cisco DNA Center. The focus is on the outcome - the "what" and not the "how". This simplifies the way an engineer "talks" to the network, as they no longer need to struggle with the feature details of configuration. The APIs used in this case leverage a RESTful approach and use HTTPS in JSON format.

Some of the Cisco DNA Assurance capabilities available via these APIs include:

Overall Client and Network Device Health Monitoring: These APIs provide the overall health of the clients and network devices for any given point in time.

- GET /dna/intent/api/v1/client-health
- GET /dna/intent/api/v1/network-health

Client and Network Device Details: These APIs provide detailed information on the client and network devices for any given point in time. This allows the external application to retrieve the client and device details at a specific point in time in the past. This is specifically useful for debugging network and client issues.

- GET /dna/intent/api/v1/client-detail
- GET /dna/intent/api/v1/device-detail

Global and Site Health: Returns overall health information for all sites.

- GET /dna/intent/api/v1/site-health

Path Trace: The Path Trace APIs allow the user to analyze the data path for any application flows between any two network endpoints.

- POST /dna/intent/api/v1/flow-analysis
- GET /dna/intent/api/v1/flow-analysis/${flowAnalysisId}

An example of the Network Device Details API and the information it provides follows. This can be used by external applications to monitor the health of the clients connected to the Enterprise network.


```
{

    "response": {
        "managementIpAddr": "x.x.x.x",
        "nwDeviceName": "LA1-9300-ACC-2.corp.local",
        "communicationState": "REACHABLE",
        "platformId": "C9300-24UX",
        "nwDeviceId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx",
        "sysUptime": "24 days, 16:58:47.74",
        "nwDeviceRole": "DISTRIBUTION",
        "nwDeviceFamily": "Switches and Hubs",
        "macAddress": "xx:xx:xx:xx:xx:xx",
        "collectionStatus": "SUCCESS",
        "deviceSeries": "Cisco Catalyst 9300 Series Switches",
        "osType": "IOS-XE",
        "softwareVersion": "16.6.2",
        "nwDeviceType": "Cisco Catalyst 9300 Switch"
    }
}
```

All the Cisco DNA Center APIs are documented in the API Catalog hosted within the Cisco DNA Center user interface. They are also available on the Cisco DevNet portal at *https://developer.cisco.com*. The API catalog provides detailed information related to each API, including the query, header parameters, response codes, request and response schema, as well as the capability to generate sample code previews and try out the APIs from the UI.

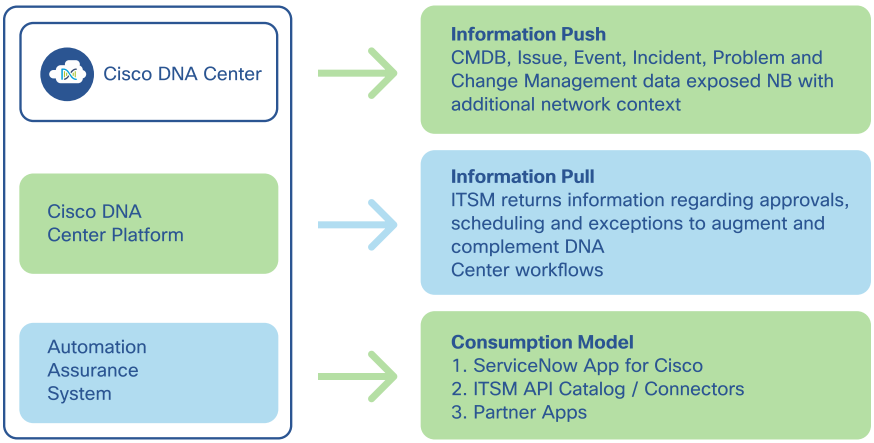
IT Service Management Integration. One of the primary goals of the Cisco DNA Center Platform is to streamline the end-to-end IT processes across the IT value chain. The Cisco DNA Center Platform achieves this by integrating with various ecosystem domains such as IT Service Management (ITSM), IP Address Management (IPAM), and Business Intelligence (BI) Reporting. By leveraging the REST-based Integration Adapter APIs, bi-directional interfaces can be built to allow the exchange of contextual information between Cisco DNA Center and external third-party IT systems.

Specifically, the Cisco DNA Center Platform provides the capability to integrate with ITSM tools and systems. This minimizes the duplication of issues and the need for handoffs, and optimizes processes for proactive insights and faster remediation. This is achieved by integrating Cisco DNA Center with various ITSM workflows:

- Sync the CMDB between Cisco DNA Center and ITSM tool.
- Event, incident, change and problem management workflow.
- ITSM approval and pre-approval chains.
- Formal change and maintenance window scheduling processes.

This is a two-way integration between Cisco DNA Center and the ITSM tool, which provides the capability to publish network data, events, and notifications to external systems and at the same time consume information in Cisco DNA Center from connected ITSM systems. Examples of ITSM systems include ServiceNow, BMC Remedy, RT Request-Tracker, and other in-house ticketing systems.

DIAGRAM IT Service Management (ITSM) Integration



The Cisco DNA Center Platform exposes integration APIs and events via WebHooks to integrate with any ITSM tool. The integration between Cisco DNA Center and ServiceNow is available out-of-the-box as an example reference application.

Event Notifications via WebHooks

Cisco DNA Center Platform provides the ability to publish Event notifications that enable third-party applications to receive any issues detected by Cisco DNA Assurance, as well as Cisco DNA Center System level and task-based operational notifications. It also provides an ability to receive custom notifications when Events are triggered. This is valuable for third-party systems that would like to take business actions based on the type of Event triggered; for instance, if any of the devices in the network are out of compliance, a custom application may want to receive notifications and execute a software upgrade action.

Also, consider the case of performing automation workflows in Cisco DNA Center which require a stipulated time. With legacy solutions, for example, an application needed to poll Cisco DNA Center frequently to get the status update for the task. By subscribing to the task completion event and receiving notifications, polling could be avoided completely. This allows for optimization of network and compute bandwidth, as well as the costs involved in polling resources.

In order to receive Cisco DNA Center events, a user must provide a receiving or "callback" URL. Cisco DNA Center Platform can then publish events to the callback URL with an HTTPS POST.

DIAGRAM

The Cisco DNA Center Platform notification leverages WebHooks to push Event messages northbound using the standardized IT4IT schema. The information provided via these Event notifications can be used to build integrations with various ITSM systems. The various attributes (Category, Severity, Type, or Workflow) for each Event are predefined based on industry standards, and the user has the option to customize this based on their Enterprise processes. The Event framework allows the user to filter Event notifications based on Event types, sites, domains, and categories.

Email Notifications

Effective email notifications based on the “less is more” paradigm can be a powerful engagement tool from a Cisco DNA Center Platform standpoint, especially since network operators are not expected to be sitting in front of their screens waiting for a network problem to occur. Furthermore, given the global nature of the business and IT operations, operators expect to be informed whenever an event of interest is likely to impact the user experience.

The email notification workflow within Cisco DNA Center permits the customer to configure rules (issue priority, issue occurrences, impacted client count, time of the day, and email aliases) to dictate the exact conditions for which they would like to receive email notifications. If an alert matches the criteria, then an email will be automatically generated with the right amount of information (priority, severity, site, issue description, and potential remediation) related to the issue, to ensure easier resolution. To avoid being overwhelmed, customers can also define the number of times the same issue needs to recur before Cisco DNA Center sends out an email notification.

Reporting

The Cisco DNA Center Platform supports on-demand reports for Cisco DNA Center Assurance clients and inventory information. High fidelity and roll up (aggregated) data is available for piecing together tactical or business intelligence reports.

Report generation can be uniquely curated based on the following configurable settings:

- Data Filters: including location, SSID, or wireless band for client reports
- Schedule: now, later or recurring
- Time Range: from 3 hours to the last 7 days, or a custom time period
- Output file type: spreadsheet .csv, PDF, or Tableau data extract
- Report type: summarized or detailed

Data Retention

Cisco DNA Center is designed to retain data with consideration for multiple factors e.g. criticality of data, severity of the incidence, summarized or raw data depending on the volume of data and application requirements.

The Value of Assurance Data

1 **High Fidelity data up to 14 days for problem replication**

- Network operators are frequently challenged by the inability to go back into the past and effectively reproduce network issues that are ephemeral in nature. This is especially true of wireless networking or other highly dynamic environments where diagnosing persistent, but transient problems, which are the cause of dramatic performance degradation from an end user standpoint, is difficult.
- High fidelity data powers the Health and Sensor Dashboards, 360-degree views, and Issue insights.

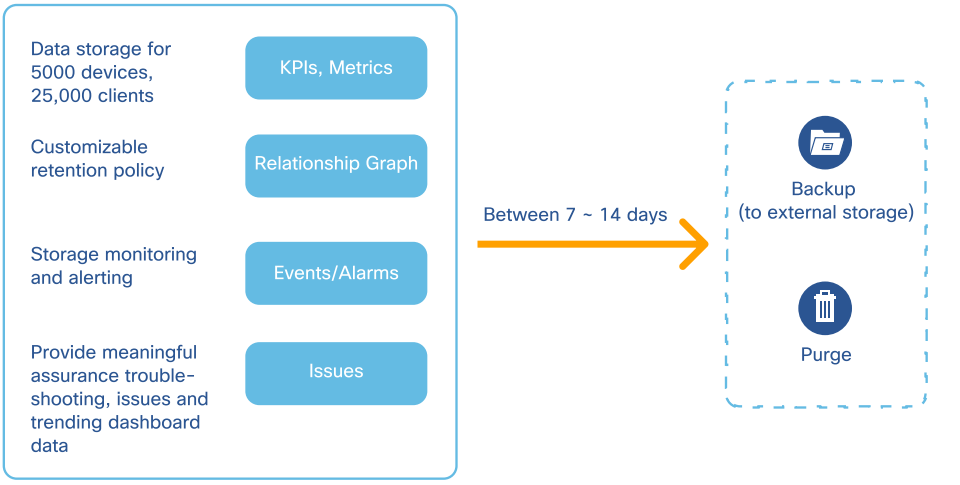
2 **Aggregated data for Trend Analysis and Reporting**

- Network architects rely on periodic trend analysis and reporting for meeting new business needs and optimizing network operations. Trend analysis is typically done on data across a few weeks or months for deriving insights.
- Cisco DNA Center offers out-of-the-box reports for analyzing data within 14 days.
- Beyond 14 days, Cisco DNA Assurance data can be offloaded to an external source such as Tableau or data lakes for trend analysis.

Configurable Data Retention and Purging

Cisco DNA Assurance provides configurable data retention and purge settings and schedules. By default, the data is stored for 14 days and can be retrieved via the time travel capability that is inherent within any Health or 360-degree view pages in Assurance. Flexible purge policies can be configured on certain SSIDs, such as Guest SSID, to optimize the system performance and to adhere to organizational policies around privacy.

DIAGRAM Retention and Export



Cisco DNA Infrastructure

Digital Ready Network Infrastructure

Digital transformation requires connecting millions of previously unconnected endpoints with data from disparate sources and infrastructure for businesses which are becoming more dynamic and distributed. Trends such as cloud, mobile, and social networking have become pervasive. This fuels the need for a digital-ready infrastructure that is capable of the following:

- Simple to operate.
- Intelligent and responsive to changing conditions.
- Automated to manage scale and complexity.
- Inherently secure.

Cisco's Digital Ready Infrastructure is the foundation for digital transformation and is comprised of robust physical and virtual routing, switching and wireless - products that are built with software capabilities to enable rapid digital transformation with built-in security features.

Cisco's unified DNA architecture provides an ideal platform for the development and delivery of innovative, market-leading solutions. Using Cisco DNA Center, policies can be created and applied across the entire network with a few clicks. Diagnosis of real-time and historical issues becomes greatly simplified with Cisco DNA Assurance.

Cisco DNA Center is built to deliver rapid, accurate, and powerful data and insights. Cisco DNA Assurance leverages the digital-ready network infrastructure to enhance data ingestion, providing more rapid processing and faster correlation of disparate data sources by adopting the next generation of telemetry, message formats and protocols, while also retaining backwards compatibility with brownfield deployments.

Supported Hardware and Software

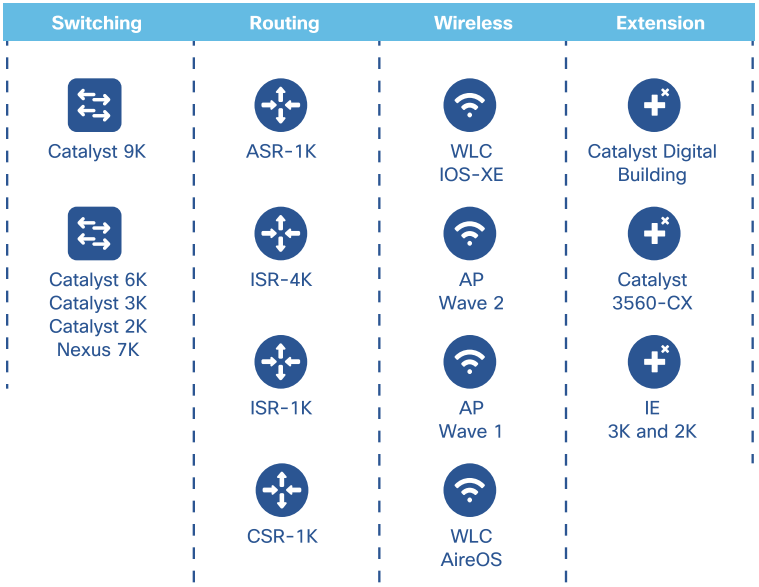
From an infrastructure standpoint, the Cisco Digital Network Architecture supports both brownfield and greenfield deployments. Most Cisco routers, switches, and wireless devices shipping today are supported by Cisco DNA Center "as is" or at most with a software update. The support of brownfield deployments makes Cisco DNA Assurance compelling and future-proof, and is unique in the market.

Hardware

To protect and get the full value of such investments well into the future with access to ongoing software innovations, Cisco recommends the transition to Cisco DNA capability-enhanced products, such as the Catalyst 9000 series of switches and WLAN controllers, Access Point 4800, and 1800s wireless sensors.

For full details on the hardware supported by Cisco DNA Assurance, please refer to the following URL:
http://cs.co/dna-center-1x-supported-devices

DIAGRAM Cisco DNA Ready Infrastructure Portfolio



Software

The power of software is enabled on the digital-ready hardware noted above. For brownfield environments, a software update can make the network device digital ready. Below is a matrix of the recommended software version for each device family at the time of writing.

Hardware	Recommended Software
Cisco DNA Center	1.2.5 and above
Catalyst 9K, 3K **ISR 4K** **ASR 1K, CSR1K**	IOS XE 16.9.2 IOS XE 16.8.1 IOS XE 16.6.4
Catalyst 4K	IOS XE 3.10
Catalyst 6K	IOS 15.5(1)SY1 IOS 15.5(1)SY2
WLC 3504, 5520, 8540, and 9800 **APs Wave 1 and Wave 2**	IOS XE 16.10.1 AireOS 8.5.135.0 (minimum supported) AireOS 8.8.100.0 (latest) Wireless Sensor 1800s (8.8.258.0)
Cisco IE 4K, 5K **Cisco CDB Switch** **Cisco Catalyst 3560-CX**	15.2.6E1

Cisco DNA Licensing and Feature Matrix

Cisco DNA licensing contains two levels of available subscriptions: Cisco DNA Essentials and Cisco DNA Advantage license levels. The subscription periods are available for three, five, or seven-year terms, and are associated with network devices. With these software subscription offers, customers can quickly capitalize on their investment with new software-based innovations.

The Cisco DNA Essentials license permits customers to deploy and use basic Assurance capabilities. This includes a basic Health dashboard for network, clients, and applications.

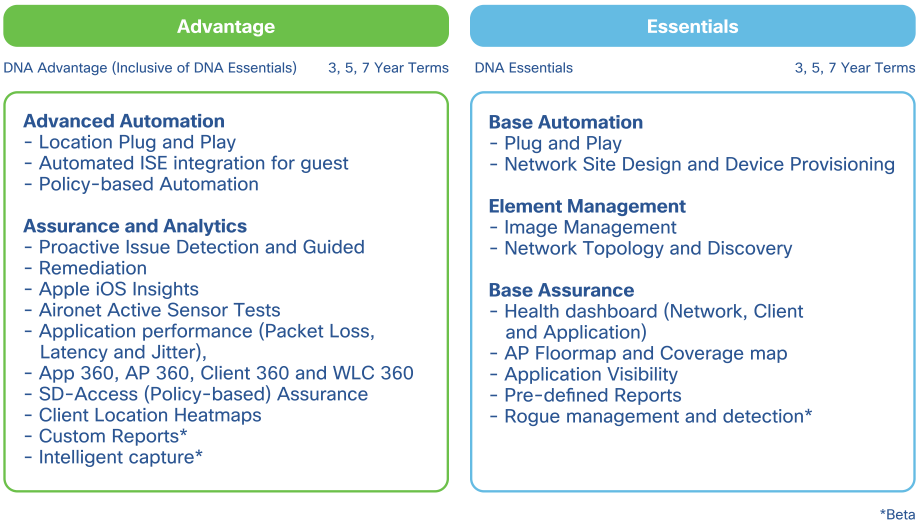
The Advantage license enables the full capability of Cisco DNA Center. This license level provides for the deployment and use of full Cisco DNA Assurance and Analytics functionality. This includes Global Insights and Trends reports, as well as 360 Degree views for Network, Client, User and Application, including performance data such as loss and jitter. In addition, several upcoming innovations are planned for coverage by the Cisco DNA Advantage license, including Intelligent Capture and support for wireless sensors.

The Cisco DNA subscription licenses also enable more features inside a given network device. For example with Cisco DNA Advantage license on the Catalyst 9000 series of switches, full flexible NetFlow is enabled.

A major advantage is that the Cisco DNA Advantage license always includes Automation as well as the Assurance and Analytics capabilities. This provides a great deal of flexibility for customers starting their Cisco DNA journey. In the case of Cisco DNA Assurance, getting started is quite straightforward, and can be accomplished with both brownfield and greenfield deployments. If Automation will be the next phase, the Cisco DNA Advantage license already provides the necessary coverage, without any additional purchase.

To use Cisco DNA Assurance and Automation, customers need to obtain and use a Cisco DNA Center appliance. There is no specific license for the appliance itself, since licensing is based on the per-network device license on the deployed switches, routers and WLCs in use.

DIAGRAM Cisco DNA Licensing Tiers



Cisco DNA Assurance Feature Matrix

There is a wide variety of advanced Assurance features available, both on the network infrastructure devices themselves as well as via Cisco DNA Assurance use cases. The following Cisco DNA Assurance features are supported by the Cisco DNA Ready Infrastructure portfolio at the time of writing this book, and with Cisco DNA Center version 1.2.5 and above:

Cisco DNA Assurance Feature	Cisco DNA-Ready Infrastructure Portfolio			
	Wireless	Switching	Routing	Extension (IoT)
Client Experience (Health, 360 Degree views, Time Travel, Issues and Trends, Onboarding and Path Trace)	Yes	Yes	N/A	Yes
Network Experience (Health, 360 Degree views, Time Travel, Issues, Physical Neighbor Topology and Path Trace)	Yes	Yes	Yes	Yes
Application Experience (Health, 360 Degree views, Time Travel, Issues and Application Metrics)	No*	No*	Yes	No
Issues and Guided Remediation	Yes	Yes	Yes	Yes
1800s Wireless Sensor Tests	Yes	No	No	No
Intelligent Capture	Yes	n/a	n/a	No
Software Defined Access (SD-Access Fabric) Support	Yes	Yes	Yes	Yes**

* NetFlow for Application Experience is supported by the device, but not applicable for current Cisco DNA Assurance use cases

** Participates as an extended node from the Fabric edge

Digital Ready Infrastructure as an Enabler for Cisco DNA Assurance

The use of Cisco's Digital Ready Infrastructure results in accelerated incremental innovation and associated benefits on the journey to an Intent-Based Network. It is also a key enabler for Cisco DNA Assurance, providing increased visibility and allowing for proactive troubleshooting and guided remediation, wherever customers may be in their digital transformation lifecycle.

Digital Ready Telemetry

Why is Telemetry Required?

Telemetry is vitally important to Cisco DNA Assurance and the capabilities that are provided since this data is the basis for the issues, insights, and problem remediation. Being able to gather appropriate, timely, and thorough telemetry from the underlying network is critical to the in-depth functionality that Cisco DNA Assurance provides. Sources for telemetry can include not only switches, routers, WLCs, and APs, but can also be sourced from AAA and DHCP infrastructure for additional contextual views.

Streaming telemetry can provide much more data in formats that enable faster processing and more efficient data manipulation and validation, with exponentially greater speed and efficiency. When considering network upgrades it is important to explore the telemetry capabilities of the devices involved in order to maximize the visibility and insights available through Cisco DNA Assurance.

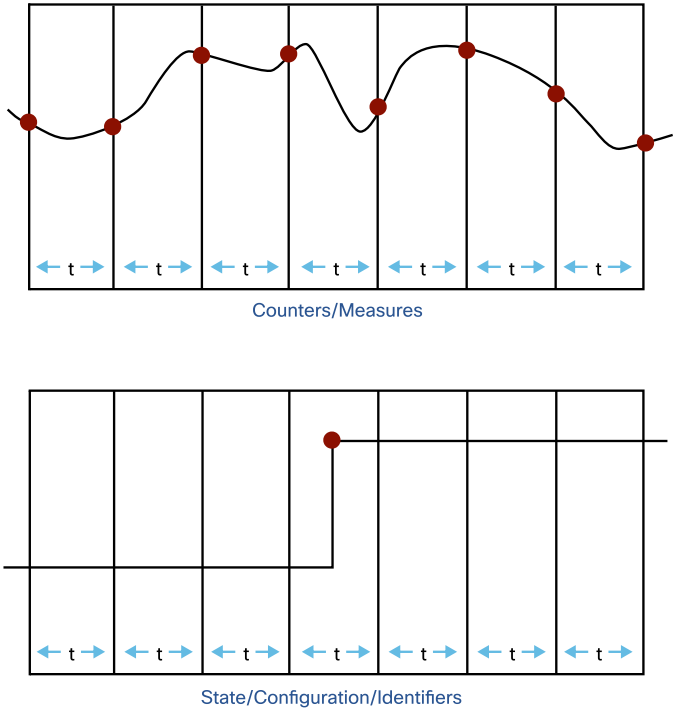
How is Telemetry Gathered?

Telemetry data has traditionally been gathered using protocols such as SNMP, Syslog, and even some CLI commands. Cisco DNA Assurance uses these protocols for gathering network telemetry data if supported, which may be the case for older devices, or devices running older software versions. However, an exciting new alternative for network telemetry has appeared in the last few years: Streaming Telemetry.

- Streaming telemetry is based on standardized machine-readable YANG data models and is transmitted using highly-efficient protocols including NETCONF and RESTCONF over TCP. This makes it far simpler to implement machine-to-machine communication in a standardized fashion. It does this in a way that is more reliable and less impactful to the network devices involved by reducing CPU, memory, and bandwidth requirements.

- Streaming telemetry provides two options for data publishing from network devices: Time-based or Event-based. The export of counters every thirty seconds is an example of time-based publication. Every thirty seconds the data will be published to Cisco DNA Assurance. The export of data when conditions change is an example of event-based publication. When the utilization of a link goes over a pre-defined value, or when a configuration change is made, the relevant data will be exported to the subscriber.

DIAGRAM Time and Event Based Publication



Enabling Telemetry to Cisco DNA Center

It is recommended to enable telemetry in the network. Cisco DNA Center assists with the configuration by discovering the telemetry capabilities of network devices, and presenting the network operator with the opportunity to enable telemetry automatically per device family or by using telemetry profiles.

Wired Infrastructure Telemetry

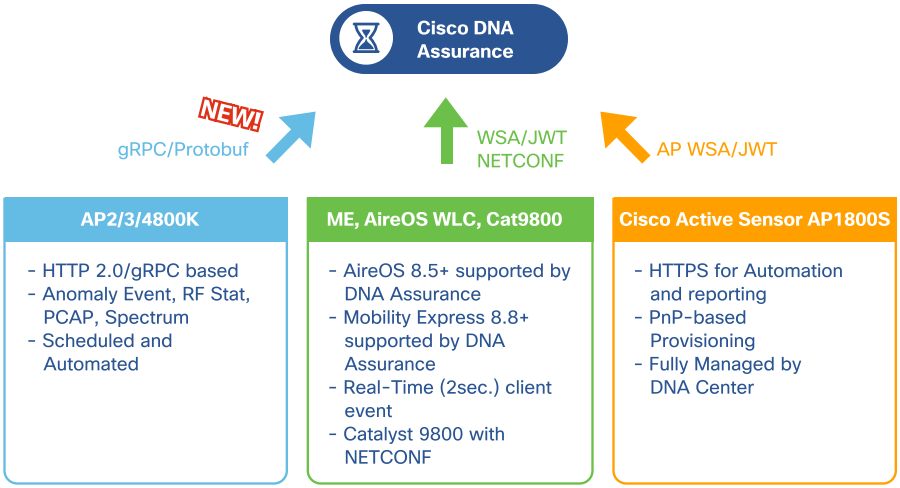
The Catalyst 9000 series switches supports programmability and streaming telemetry that exports rich and consistent datasets. The superior CPU, ASIC, and TCAM capacity on the Catalyst 9000 platforms ensure that model-based streaming telemetry data is exported at rapid rates and with minimal impact to the device. Catalyst 9000 series switches also utilize the gRPC protocol for streaming telemetry.

Cisco DNA Assurance also consumes NetFlow from routers. NetFlow is derived from the NBAR2 engine. The latest version of NBAR2 / NetFlow supports not only quantitative metrics but also supports qualitative metrics using ART - Application Response Time. ART includes packet loss, network-side delay and server-side delay information for TCP-based traffic flows. This data is exported alongside NetFlow and it gives network operators greater visibility into the end user applications that are in use.

Wireless Infrastructure Telemetry

Wireless LAN Controllers publish model-based streaming telemetry and provide contextual data to Cisco DNA Assurance, giving network administrators insight into the users and client devices that are connected to the wireless network. The Wireless Service Assurance, or WSA, is a feature on the AireOS wireless controllers that use RFC7529-compliant JSON Web Tokens (JWT) to secure the telemetry data. The JWT exchange provides an additional layer of security to the HTTPS data transfer from the WLC to Cisco DNA Assurance. Mobility Express wireless controllers also support the same WSA capabilities as the traditional AireOS WLC appliances. The Catalyst 9800 IOS XE Wireless LAN Controllers support YANG model-based streaming telemetry over the NETCONF interface into Cisco DNA Assurance and provide similar capabilities to AireOS.

DIAGRAM Streaming Telemetry Options from Wireless Infrastructure



Access Points 2800, 3800 and 4800 series provide direct streaming telemetry from the Access Point to Cisco DNA Assurance. These APs use gRPC as the telemetry protocol and provide the following advantages:

- Binary transport protocol for data types, including PCAP and RF spectrum data.
- Supports for Local, Flex, and Fabric modes of deployment.

This powerful telemetry is foundational for features such as Intelligent Capture as it enables enhanced and faster issue detection capabilities through anomaly-driven PCAP and real-time RF statistics. This capability is significantly enhanced with the AP4800 which utilizes a dedicated third radio to capture full data packets while still serving clients on the other two radios and bands.

Wireless 1800s sensors also utilize WSA streaming telemetry to publish sensor test results into Cisco DNA Assurance.

Best Practices

Overview

This chapter details some high-level best practices, references, and guidance when deploying Cisco DNA Assurance.

It is not meant to replace the Installation, Deployment, Assurance, or other User Guides for Cisco DNA Center, but instead addresses several common questions and issues.

Prerequisites

Cloud Upgrades

Software upgrades for Cisco DNA Center are initiated from within the Cisco DNA Center User Interface. The Cisco DNA Center requires access to several URLs to access the update servers, so it is recommended to whitelist "*https://*.ciscoconnectdna.com:443*" through any security appliances that are protecting Cisco DNA Center's management network. If URL filtering is not able to use wildcards, the following individual URLs can be added:

- *https://www.ciscoconnectdna.com*
- *https://cdn.ciscoconnectdna.com*
- *https://registry.ciscoconnectdna.com*
- *https://registry-cdn.ciscoconnectdna.com*

Port Requirements

If there is a firewall between Cisco DNA Center and the Enterprise network, then the firewall must be configured to allow traffic to and from Cisco DNA Center. Inbound rules for access into the Cisco DNA Center Appliance use the following protocols and ports:

- HTTPS - TCP port 443, to receive streaming telemetry and UI access.
- NTP - UDP port 123, for time synchronization of network devices.
- SCEP - UDP port 16026, for the Simple Certificate Enrolment Protocol.
- SSH - TCP port 2222, for accessing the Cisco DNA Center console.

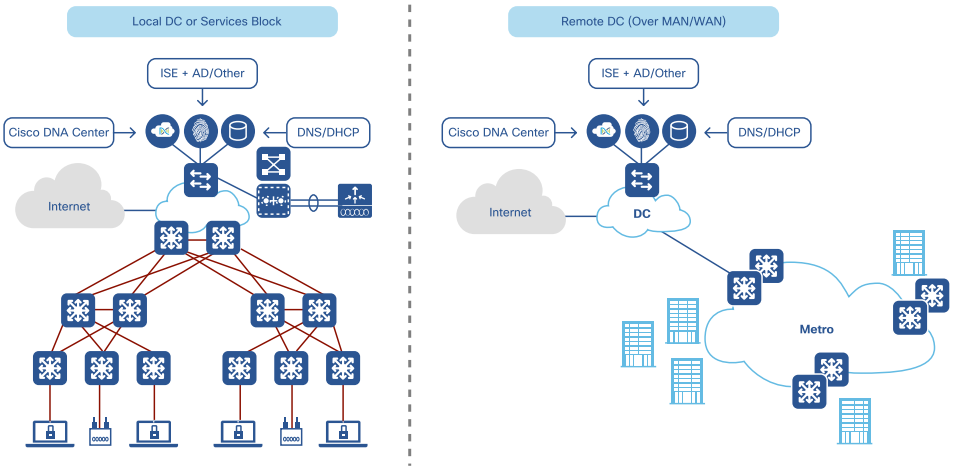
Outbound rules that allow the Cisco DNA Center access to network devices and resources use the following protocols and ports:

- SSH - TCP port 22, to access network devices.
- Telnet - TCP port 23, to access network devices.
- DNS - UDP port 53, to resolve DNS names.
- HTTP - TCP port 80, if used.
- NTP - UDP port 123, for upstream time synchronization.
- SNMP - UDP port 161, for telemetry.
- HTTPS - TCP port 443 for cloud-tethered upgrades.

Cisco DNA Center Placement

The Cisco DNA Center appliance must be installed and physically located in a local or remote data center within the Enterprise network. These appliances typically connect into the same core services block where existing services reside, including DNS, DHCP, AD, ISE or AAA, and NTP services.

DIAGRAM Cisco DNA Center Placement



The Cisco DNA Center Appliance is a one rack-unit UCS chassis and ships pre-installed with the Cisco DNA Center software. The appliance contains two physical CPUs with 44 CPU cores at 2.2GHz, 256GB of RAM, 12TB SSD in a RAID configuration, and redundant power supplies.

The Cisco DNA Center appliance has several Ethernet interfaces for the various networks to which it attaches, including:

- **Cluster Port:** Used to communicate between the master and add-on nodes in a Cisco DNA Center cluster (must be a 10Gbps port).
- **Enterprise Port:** Used for connections to the Enterprise network for communications and management of network devices.
- **CIMC Port:** Used to access the out-of-band appliance management GUI.
- **Cisco DNA Center GUI Port:** Used to provide access to the Cisco DNA Center GUI.
- **Cloud Port:** Used for connecting to the Cisco DNA Center Cloud for downloading software updates.

For more details of Cisco DNA Center Appliance, refer to the Installation Guide at ***http://cs.co/dnacenter-install-guide***

Considerations When Deploying Assurance

Cisco DNA Assurance is supported for both brownfield (existing) and greenfield (net-new) network deployments. The following considerations are important to note when planning both deployment types.

Import Floor Maps during Site Creation

- Floor Maps and AP placement previously compiled with Cisco Prime Infrastructure can be imported to Cisco DNA Center.
- The existing site hierarchies on the Cisco DNA Center if any will be replaced by the data imported.
- More details about managing the map export and import process can be found in the Cisco DNA Center User Guide at *http://cs.co/dnacenter-user-guide*.

Discovering Network Devices

- Network devices must be discovered by the Cisco DNA Center.
- In the Discovery phase, the Cisco DNA Center pushes certificates and configuration to network devices.
- SNMP credentials entered on the Cisco DNA Center will be pushed to the network devices if they are not already configured.
- If unique, the Username used for discovery can be used to track configuration changes made by the Cisco DNA Center via AAA accounting.
- If the CDP / LLDP protocol is used for discovery of network devices from the seed device, ensure the discovery level is set correctly to limit the number of network devices discovered by the Cisco DNA Center.
- Cisco DNA Center enables IP Device Tracking (IPDT) on the discovered switches (can be disabled via "Device Controllability" in Settings).

For more information on the discovery prerequisites, please refer to the Assurance User Guide at *http://cs.co/dnaassurance-user-guide*.

For more information, refer to the Device Controllability section within the Cisco DNA Center Administrator Guide at *http://cs.co/dnacenter-device-controllability*.

Assign Network Devices to Sites, Building, and Floors

- Assigning WLCs to sites enables WSA (Streaming telemetry).
- Create a Telemetry profile in the telemetry application, and assign it to a site before the wired devices are assigned to the site, to ensure Cisco DNA Center enables telemetry on the devices automatically.
- More information can be found in the "Configure Telemetry Profile" chapter of the Cisco DNA Center User Guide at *http://cs.co/dnacenter-telemetry-profile*.

Integration with Cisco ISE

- Cisco Identity Services Engine (ISE) integration with Cisco DNA Center is optional if only Cisco DNA Assurance is being enabled on the network.
- With ISE integration, Cisco DNA Assurance shows usernames for wired end clients.
- More information about this integration is available in the ISE integration chapter in the Cisco DNA Center User Guide at *http://cs.co/dnacenter-ise-integration*.

SNMP Collector

- Additional KPIs have to be added to the SNMP collector for SD-Access Fabric Assurance.
- More information can be found in the "Monitor and Troubleshoot Network Health" chapter of the Cisco DNA Assurance User Guide at *http://cs.co/dnacenter-snmp-collector*.

Data Anonymization

- If it is required by company policy to hide end client identity, Data Anonymization on Cisco DNA Center can optionally be enabled, and will then ensure that usernames of wired and wireless end clients are hidden from the Cisco DNA Assurance dashboard.
- More information on how to enable Data Anonymization can be found in the Collector Configuration section of the Cisco DNA Center User Guide at *http://cs.co/dnacenter-anonymize*.

Summary, Next Steps, and References

Summary

The Digital Network Infrastructure hardware and software that is supported and managed by Cisco DNA Center enables unparalleled capabilities that have not been available until now.

As the network takes on more and more services and becomes even more important to the role of business operations, the capabilities discussed in this book help in delivering top notch network operations.

The introduction of highly efficient streaming telemetry protocols across both wired and wireless infrastructures, Intelligent Capture for real time wireless client troubleshooting, and the proactive monitoring capabilities with sensors and Assurance, have changed the way networks have been managed historically.

Cisco's DNA Assurance solution has developed a full technology stack from the ground up to address customer needs to proactively identify issues and trends through correlation and machine learning algorithms, provide guided remediation for issues, and is designed to scale across the Enterprise.

Cisco DNA Assurance provides amazing new Intent-Based Networking capabilities that modern networks just cannot live without.

The Network. Intuitive.

Customer References and Testimonials

"Cisco DNA Assurance helps me find problems proactively, before users contact me."
Manuel Ortiz II Senior Wireless Engineer, Houston Methodist Hospital

"It's not just about pervasive wireless access, but what we can do with all that data. Cisco not only provides wireless access, but also intelligence."
Travis McIntosh, Network Communications Officer, Victoria University

"Cisco DNA Assurance gives me issues with context so that I can make decisions quickly"
Shai Silberman, Director, Network Services, San Jose State University

"Since introducing our next-generation Wi-Fi, we've increased revenues up to 20 percent per month"
Dania Duke, General Manager, Hyatt Regency Santa Clara

"The new Cisco Catalyst 9300 provides us the performance we need and the security features that are critical for our healthcare records. The new network, powered by Cisco Digital Network Architecture (DNA), gives us granular insight into who the users are, the devices they use, and the applications they access."
Michel Fontaine, Network Architect, Centre Hospitalier Chrétien (CHC), Belgium

"IT doesn't have to factor in things like outages and latency for business applications. Cisco Services and Cisco DNA helped make it possible."
Patrick Drew, Assistant VP Network Infrastructure, Huntington National Bank

Cisco Case Study: University of Wollongong
Providing a world class experience with Cisco DNA Assurance
http://cs.co/dnaassurance-university-successstory

References

Additional sites which offer more detailed information on Cisco DNA Assurance include:

Cisco.com:
https://www.cisco.com/go/assurance - provides a solution overview and additional information on all components and aspects of Cisco DNA Assurance, supported platforms, customer references and testimonials, and a wealth of the most up-to-date information on Cisco DNA Assurance capabilities.

http://cs.co/dnaassurance-white-paper - Cisco DNA Assurance Whitepaper. Requirements for Cisco DNA Assurance.

http://cs.co/dnaassurance-user-guide - References the Cisco DNA Assurance User Guide.

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

- Cisco DNA Analytics and Assurance - The Shortest Path to Network Innocence! - BRKRST-2777
- Cisco DNA Wireless Assurance - Isolate problems for faster troubleshooting - BRKEWN-2034
- Cisco DNA Cloud-Based Machine Learning / Analytics architecture - BRKEWN-2033
- Exploring Cisco DNA-C as a Platform - DEVNET-2877
- Cisco Silicon - The Importance of Hardware in a Software-Defined World - BRKCRS-2901
- Cisco SD-Access - Assurance and Analytics - BRKCRS-2814

Cisco DNA Assurance YouTube channel:
www.youtube.com/user/cisco(search for "Cisco DNA Assurance")

Acronyms

9K - Catalyst 9000 series switches

AAA - Authentication, Authorization, and Accounting

ACL - Access Control List

AD - Active Directory

AireOS - Aironet Operating System

AP - Access Point

API - Application Programming Interface

ART - Application Response Time

ASIC - Application Specific Integrated Circuit

ASR - Aggregation Services Router

BI - Business Intelligence

CDP - Cisco Discovery Protocol

CDR - Call Detail Record

CEO - Chief Executive Officer

CEP - Complex Event Processing

CIO - Chief Information Officer

CLI - Command Line Interface

CMDB - Configuration Management Database

CMX - Connected Mobile Experience

CPU - Central Processing Unit

CRC - Cyclic Redundancy Check

CSR - Cloud Services Router

CSV - Comma-Separated Values

DDI - DNS and DHCP Infrastructure

DHCP - Dynamic Host Configuration Protocol

DNA - Cisco Digital Network Architecture

DNS - Domain Name System

EAP - Extensible Authentication Protocol

EAP-TLS - EAP Transport Layer Security

ERSPAN - Encapsulated Remote Switched Port Analyzer

ESB - Enterprise Service Bus

FTP - File Transfer Protocol

gRPC - Google Remote Procedure Call

GUI - Graphical User Interface

GHz - Gigahertz

HTTP - Hyper Text Transfer Protocol

HTTPS - Hyper Text Transfer Protocol Secure

HVAC - Heating, Ventilation, and Air Conditioning

IBN - Intent-Based Networking

IMAP - Internet Message Access Protocol

iOS - iPhone Operating System

IOS - Internetwork Operating System

IP - Internet Protocol

IPAM - IP Address Management

IPDT - IP Device Tracking

IP SLA - Internet Protocol Service Level Agreement

ISE - Identity Services Engine

ISR - Integrated Services Router

IT - Information Technology

ITOA - IT Operations Analytics

ITSM - IT Service Management

JSON - JavaScript Object Notation

JWT - JSON Web Token

KPI - Key Performance Indicator

LAN - Local Area Network

LLDP - Link Layer Discovery Protocol

MAC - Media Control Access

ME - Mobility Express

MIB - Management Information Base

ML - Machine Learning

MOS - Mean Opinion Score

MPLS - Multi Protocol Label Switching

NB - Northbound

NBAR - Network Based Application Recognition

NDT - Network Diagnostic Tool

NETCONF - Network Configuration Protocol

NFV - Network Function Virtualization

NMS - Network Management System

NOC - Network Operations Center

NTP - Network Time Protocol

OSPF - Open Shortest Path First

PCAP - Packet Capture

PDF - Portable Document Format

PEAP - Protected Extensible Authentication Protocol

PoE - Power over Ethernet

POP3 - Post Office Protocol 3

POS - Point of Sale

QoS - Quality of Service

RADIUS - Remote Authentication Dial-In User Service

RAID - Redundant Array of Independent Disks

RAM - Random Access Memory

REST - REpresentational State Transfer

RESTCONF - Rest Configuration Protocol

RF - Radio Frequency

RFC - Request For Comments

RSSI - Received Signal Strength Indicator

S4B - Skype for Business

SCEP - Simple Certificate Enrolment Protocol

SD - Software Defined

SD-WAN - Software-Defined Wide Area Network

SDA - Software-Defined Access

SDK - Software Development Kit

SGACL - Security Group Access Control List

SLA - Service Level Agreement

SN - ServiceNow

SNMP - Simple Network Management Protocol

SNR - Signal-to-Noise Ratio

SSD - Solid-State Drive

SSH - Secure Shell

SSID - Service Set Identifier

SWIM - Software and Image Management

TAC - Technical Assistance Center

TCAM - Ternary Content Addressable Memory

TCP - Transmission Control Protocol

UADP - Unified Access Data Plane

URL - Uniform Resource Locator

UI - User Interface

UX - User Experience

VLAN - Virtual Local Area Network

VoWiFi - Voice over WiFi

VPN - Virtual Private Network

VRF - Virtual Routing and Forwarding

WAN - Wide Area Network

WLC - Wireless LAN Controller

WPA2 - Wi-Fi Protected Access 2

WQE - Work Queue Element

WSA - Wireless Service Assurance

YANG - Yet Another Next Generation