Artificial Intelligence/Machine Learning for Intent-Based Networking – Primer

Contents

Introduction – The Cisco advantage: Best data, best knowledge base

With over 35 years of networking expertise, Cisco has deployed more than 50 million networks in the past 20 years. This experience has allowed us to create the world's largest data platform. The quality, diversity, and volume of this data platform is the foundation for feeding and training Cisco's advanced machine learning platform: Cisco AI Network Analytics. This platform, nurtured over the past decade by Cisco engineers, uses a collection of highly advance machine learning algorithms to keep customers better informed so that more-relevant anomalies can be detected and communicated with insight. Along with these communications, Cisco also provides logical resolution recommendations to help IT fix the anomalies. This empowers network administrators to react in real-time to the dynamic nature of today's networks while constantly improving the user experience. This incredible technology is now included within the Cisco DNA Assurance capabilities of Cisco DNA Center. All Cisco DNA Advantage customers will have access to Cisco AI Network Analytics at no additional charge. This short technology primer will take a non-technical look at the use of AI/ML in enterprise networking and the specific use cases where Cisco customers will see the most benefit.

Why AI/ML?

Intent-based networking is providing easier operations for today's complex, software-defined networks. But, as these networks grow increasingly larger, the vast programmability of devices and flexibility in their configuration leads to unimaginable levels of complexity. A network analytics engine, driven by Artificial Intelligence and Machine Learning (AI/ML), is simply the only way for humans to navigate this complexity. This short primer will explain why we need AI/ML, the basic concepts of AI/ML related to network analytics, and the role they play in intent-based networking.

First let's look at the challenges facing IT teams today.

1. There is a proliferation of client devices connecting to the network such as laptops, smartphones, cameras, sensors, machines, robots, thermostats, lighting, etc. Each one of these client devices requires a distinct set of parameters to be configured in the network in order to guarantee user experience and security. The Cisco® Visual Networking Index (Cisco VNI™) forecast for 2019 projects that there will be, globally, 28.5 billion networked devices and connections by 2022 (that is, three times the human population).

2. Users are moving to wireless as the primary medium of network connectivity in the campus. Wireless communications are much more complex in the number of parameters that need to be configured in order to assure an optimal user experience. Additionally, the wireless medium is very dynamic, and performance can vary depending on the number of users, services, and applications and levels of interference. The Cisco VNI for 2019 projects 5-7X growth in mobile traffic by 2022.

3. Applications are moving to the cloud. The network architecture needs constant updating to support the many different entrance points for data into the campus and the diverse paths that the data will travel. IDC estimates that 93 percent of organizations will use multiple clouds by 2019.

The goal of intent-based networking is to automate the network to dynamically meet business priorities and intent; the network is constantly learning and adapting to securely maintain business intent. First, business intent is translated into policy based on user or device identity and application requirements for that job role or device function. For example, a salesperson's job requires reliable and quality video conferencing, finance may require low-latency connectivity to an off-shore banking database, and a factory emergency shut-off valve would need instant transmission of very low amounts of data. Then, these policies are translated into network infrastructure configurations and deployed via controller-based automation throughout the network. Finally, the network constantly monitors, collects data, and analyzes to make sure business intent is being realized.

Supporting these new challenges means collecting information in the form of real-time telemetry throughout the network, in order to track Key Performance Indicators (KPIs) and identify anomalies – things underperforming in the network. But the number of anomalies and alerts being generated is simply too much to be useful. Today's networks are generating massive amounts of data, and this means too much noise for humans to deal with in a timely manner. AI/ML can learn to differentiate between important alerts and trivial anomalies, thereby reducing this noise.

Analytics: The foundation of AI/ML

In intent-based networking, analytic engines are critical in helping IT teams improve network performance. Analytics has been used for years in process control networks for manufacturing, utilities, mining, and oil and gas. Its success is undisputed in being able to make these industrial networks safer, more productive, and less expensive to operate. Analytics in process control began life many years ago as simple sensors connecting to a controller using if-then commands such as: "if the pressure goes above X, shut the oil pump down"; or: "if the motor rises above a certain temperature, slow to half speed." With time, these commands became more complex: "if the temperature is above N, AND humidity is above X, AND vibration sensor reaches level Y, do Z." A typical analytics model will have a long string of these "if-then" variables, called a decision tree, which allows decisions on the network to be automated based on this preprogrammed model. The model is usually updated from time to time as the network conditions change. A good example of an analytics model in campus networking is Cisco CleanAir® technology. This is the silicone-level intelligence in Cisco Wi-Fi solutions that keep access points away from wireless channels with high interference by automatically moving the active channel. This technology uses a sophisticated analytics model that considers many variables before making the decision to change channels. Today, Cisco DNA Assurance uses a powerful analytics engine to troubleshoot issues such as slow Wi-Fi device onboarding, or poor application performance on a media screen, such the Cisco Webex® Board. Analytics models are very powerful, but they have one drawback: they are fixed models. Even the best analytics model, using a very complex decision tree, cannot be modified on site for differences that exist from campus to campus. This is important because no two networks are the same. The perfect analytics model would be able to adapt its decision tree parameters based on user trends, services, and application metrics that are specific to the local network. AI/ML can give this type of flexibility to a static analytics model. AI/ML is used to learn the optimal performance configurations for a local network and then create customized decision trees for alerts, troubleshooting, and remediation based on optimized models and baselines. This creates highly personalized network baselines with multiple levels of granularity that define the personalized "normal" for the local network.

Artificial Intelligence (AI)

Artificial Intelligence (AI) is where sophisticated computer models are used to simulate the cognitive processes of human thought. We create a software program that uses mathematical models to perform the same logical steps that a human would take to solve a certain query.

AI is being applied to more things in your life than you can imagine. From your Apple Watch health settings, to your Netflix selections, and even the types of milk that are available in your local supermarket. An example would be having a computer identify which of five given pictures contain cats, when ride-sharing apps determine wait time, real-time ride pricing, or when your email program automatically filters junk mail for you.

AI is everywhere and is being applied in many different categories to solve a myriad of queries.

Machine Learning (ML)

One of the subcategories of AI is Machine Learning (ML), which is used to find the probability of a certain outcome using analytical experimentation. ML is learning through reasoning based on probability mathematics. If you studied statistics in school, you will remember that mathematical formulas (regressions) can be quite accurate in calculating the probability of a given outcome. For example, we know that when interest rates on mortgages go up, house values tend to come down, but it's not easy to say by how much. This requires that loads of historical data be fed into a statistical model before we can get close to an accurate number. The more data we have, the more accurate our estimate will be. ML is powerful because it can handle more data from more sources than a human could ever imagine. By feeding large quantities of data and diverse categories of data, we can use ML to calculate very accurately these statistical outcomes. Over the past few years we have seen the accuracy of these ML models on Wall Street as ML-equipped firms have been able to calculate outcomes to almost any scenario and react in a near instant to real-market fluctuations. These same ML predictions can be applied to almost any industry. If we have enough data, we can calculate the best outcome for any set of variables. Cisco's ground-breaking Worldwide Data Platform provides a plethora of data required to bring this exciting technology to enterprise networking.

Cisco AI network analytics
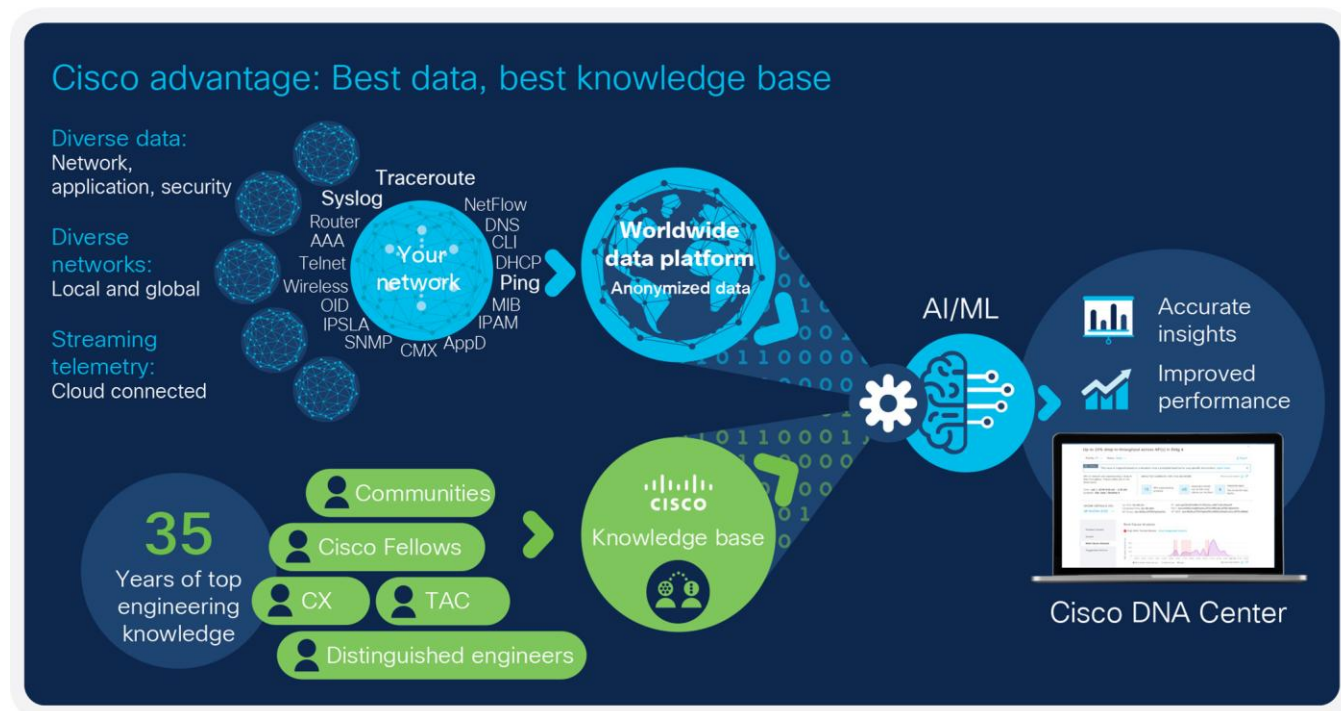
Cisco is using AI/ML and data to make Cisco DNA Center smarter! The new Cisco AI Network Analytics solution, within Cisco DNA Center, provides highly personalized information to our customers' environments that allows them to see problems sooner, solve problems faster and cut out the noise in their network. The computing power for Cisco AI Network Analytics resides both in the Cisco AI Network Analytics cloud (on secure and powerful compute servers) and on premises (within the Cisco DNA Center appliance). Streaming telemetry and other data from network events on the customer's network are anonymized on site, and then sent to the Cisco cloud, where it is merged with anonymous data from networks around the world. The more networks that are using Cisco AI Network Analytics the more intelligent the system will become. Along with this global data set, we are encapsulating human knowledge; decision-making from Cisco's best engineers are in this software. All of our best practices and 35 years of networking experience are injected into the decision-making algorithms in the system. Against all this information, we are applying the industry's most advanced AI/ML algorithms to drive better outcomes. The models are being personalized to local network conditions and prioritized for more relevance, based on your Cisco DNA Center settings. The results are accurate insights leading to improved performance.

How Cisco AI network analytics works

Visibility - Personalized baselining: No two networks are the same. AI-driven technologies can learn the user trends, services, and application metrics that are specific to your network. Cisco DNA Assurance can then create a customized performance curve for analytical decisions. The AI-driven baseline for the performance parameters that are unique to your network is constantly adapted as your network grows and changes. From there, the AI-driven analytics engine (both on premises and in the Cisco cloud) can make accurate decisions for what is normal and what is not, based on this personalized baseline. There are a number of features that put this into action, such as:

Insight – Intelligent analysis: AI-driven anomaly detection will surface any deviation from our AI-created personalized baseline for this network. This allows Cisco DNA Center to make sense of all the network data. The system can accurately detect performance issues and ignore unusual, but harmless, network anomalies. This reduces noise while accurately identifying anomalies that have the greatest impact on your network. AI-driven predictive analytics and proactive insights allow users to anticipate and prevent failures. Here, the machine learning engine can predict increases in Wi-Fi interference, onboarding delays, office traffic load, etc. This is because, in IP networks, a problematic event is often proceeded by a benign event or series of events. By learning how series of events are correlated to one another, predictive analytics can help network administrators anticipate the unexpected.

There are two categories of proactive insights:

1. **System-generated insights** appear on the Network Insights menu in Cisco DNA Center. These insights are the most important trends and deviations from the regular performance trends in your network. These insights can help you plan the next steps in growing or planning for network expansion, in order to keep one step ahead of today's constantly growing network demand.

2. **Proactive exploration** where customers can investigate any part of the network, or service, or application that they want to understand better. An example of proactive exploration is the network heatmap, where a user can compare performance of multiple wireless access points to find opportunities for improvement. Additionally, there are features for site comparison, allowing network administrators to compare different floors in a building or different branch sites. Using the power of anonymized and encrypted data, the user can even compare their network performance with other similar, and anonymous, networks.

Action – Accelerated remediation: Cisco AI Network Analytics provides accelerated remediation through machine learning, which identifies the most critical variables related to the root cause of a given problem. This helps users detect issues and vulnerabilities, perform complex root cause analysis, and execute corrective actions faster than ever. In coming releases, we will enable machine reasoning to execute the logical troubleshooting steps that an engineer would perform in order to resolve a problem. Both of these capabilities accelerate remediation making your team more precise in problem solving and more productive overall.

Product usage telemetry: Customers that turn on the Cisco DNA Center product usage telemetry option can receive additional benefits through the use of a Machine Reasoning Engine (MRE). The MRE can proactively identify potential security issues, improve services and support, verify usage of new features that IT may not be aware of, and assist IT teams with inventory in general. Cisco DNA Center's MRE can parse through thousands of network devices to verify that all devices have the latest software image and look for potential vulnerabilities in device configuration. If your teams are not taking advantage of the latest upgrade features, it can flag suggestions. Product usage telemetry makes sure your network devices are up to date and your team is getting the most from Cisco DNA Center.

AI/ML is arriving at the perfect time for intent-based networking. More devices are communicating anomalies and sharing data, telemetry is now available from every part of the network, and cross-domain functionality is bringing intelligence in from outside the campus. The noise is deafening to IT teams, and a solution is needed. By customizing the local network's baseline for decisions and developing a flexible analytics engine, both on premises and in the cloud, Cisco is reducing the noise and clarifying the issues that are impairing performance in the network. This is how AI/ML is making Cisco DNA Center smarter.

Cisco AI Network Analytics is now a standard part of Cisco DNA Center and is included in the Cisco DNA Advantage licensing tier.

Glossary of terms

Intent-based networking

The intent-based network captures business intent and uses analytics, machine learning, and automation to align the network continuously and dynamically to changing business needs.

Cisco DNA

Cisco's Digital Network Architecture is the software-defined platform delivering on intent-based networking across campus, branch, WAN, data center, and cloud.

Cisco DNA Center

This appliance-based software platform is the all-in-one command-and-control center that acts as the core for Cisco DNA through automation, analytics, security, and an open platform.

Cisco DNA Assurance

A function of Cisco DNA Center, Cisco DNA Assurance offers visibility and insight into the network, automatically detecting and prioritizing network issues. By implementing artificial intelligence, machine learning, and machine reasoning, Cisco DNA Assurance can keep your network performing at its optimal level and reduce the amount of time your team spends managing the network.

Cisco AI Network Analytics

- Artificial Intelligence (AI) is field of study to make computers have human-like intelligence when performing a task.

- Machine Learning (ML) is field of study that gives computers the ability to learn without being explicitly programmed.

- Machine Reasoning Engine (MRE) involves algebraically manipulating previously acquired knowledge in order to answer a new question.

Resources to learn more

- Artificial Intelligence and Machine Learning

- Cisco DNA Assurance Solution Overview

- What is Network Analytics

Printed in USAs

C22-742605-00 09/19