Master of Science in Internetworking

Department of Electrical and Computer Engineering

Project Title:

AI in Enterprise Networking

Supervisor:

Juned Noonari

Provided By:

Jianhui Lyu

Fall 2021- Winter 2022

Table of Contents

List of Figures

List of Tables

Abstract

Traditional enterprise networking requires lots of manual operation, such as manual troubleshooting, configuration, monitoring and analysis. Especially for large enterprises, which might have hundreds or even thousands of sites, the labor cost of manual operation is exceptionally high, and the efficiency is low. As the scale of enterprise networks continues to expand, network automation is an inevitable trend, and AI (Artificial Intelligence) is the critical technology needed to automate networking operations. The application of AI technology can save a lot of trivial manual processes, which would generally improve the work efficiency of network administrators and the timeliness of network management. Specifically, artificial intelligence, which requires machine learning or the evolved, more complex structured models like deep learning, can carry out real-time monitoring, analysis, prediction and evaluation for more complex computer network structures, effectively solving the difficulties that the traditional method of operation cannot solve, and ensuring the smooth operation of enterprise networks. Nowadays, since more and more enterprises are moving into AI-based networking, it is necessary to deeply understand and research the application of AI technology in enterprise networking.

Acknowledgment

I would like to express my sincere gratitude to Dr. Mike MacGregor and Juned Noonari for giving me the chance to work on this practical project and for their advice and supervision.

I would also like to express my gratitude to Shahnawaz Mir and Sharon Gannon for their support during the program.

Finally, I would like to express my gratitude to my parents and wife for their unwavering support and encouragement during my challenging times.

Chapter 1: Enterprise Networks

1.1 What is “Enterprise Network”?

The term "enterprise network" refers to the IT infrastructure used by midsize and large businesses to link users, devices, and applications. The goal is to help companies achieve their goals by reliably and securely offering linked digital services to workers, partners, customers, and, increasingly Things. [1]

To adapt to the development of enterprise information technology to meet the growing communication needs and the stable operation of the network, today's enterprise network construction puts forward higher requirements than the traditional enterprise network construction.

First, modern enterprise networks need high bandwidth and high performance to meet the growing communication needs of enterprise workers. Second, modern enterprise networks need higher reliability and real-time performance to ensure the normal operation of enterprise production. Again, modern enterprise network needs to provide perfect end-to-end QOS guarantee to meet the demand of enterprise network multi-service bearing. Finally, modern enterprise networks should provide better network security solutions to block virus and hacker attacks and reduce the economic losses of enterprises.

1.2 Requirements for enterprise network design

1.2.1 Scalability

Scalability refers to the growth of the network size that the network can support. For enterprise networks, network scalability is the primary requirement. In the process of development, enterprises will increase network users, applications, new access points and connections to external networks at a very rapid rate, so the enterprise network design must be able to meet the network use and a certain range of growth.

1.2.2 Availability

Availability refers to the length of time that a network can be used by customers and is often an important metric to consider in network design solutions. Availability is positively correlated with redundancy. Redundancy is not a goal of network design but rather a solution that ensures high network availability. Redundancy is the addition of multiple identical network connections

to the network to prevent abrupt network downtime due to equipment failure, etc. Network availability is also related to network resilience. Recoverability refers to the ability of a computer network to recover quickly from a series of problems caused by natural or unnatural disasters, human errors, and serious hardware and software errors in the shortest possible time. An enterprise network with availability usually has good recoverability.

1.2.3 Network performance

When designing the technical parameters of the network, the technical indicators required by the enterprise should be properly distinguished. These technical indicators should include throughput, accuracy, efficiency, latency and response time, etc. Throughput is the total amount of error-free data transmitted per unit of time. Ideally, throughput should equal capacity, but this is usually not achieved due to a variety of factors. The size of the capacity is usually determined by the physical layer technology used. The network capacity should match the load provided by the network, even at times of peak network traffic. From a purely theoretical point of view, the throughput should increase as the available load increases, up to the full capacity of the network. The network medium, access method, network load and error rate also affect the network throughput.

The goal to be achieved by the accuracy is that the data sent by the source node must be the same as the data received by the destination node. The accuracy goal can be illustrated by the BER readout value. When the BER is higher than the specified read value, this accuracy is considered unacceptable.

Network efficiency responds to the system resources to be occupied by sending communications, regardless of whether these resource occupations are caused by collisions, token passing, error reporting, rerouting, answering, and larger frames.

Latency is the sum of propagation delay, transmission delay and queuing delay, and the magnitude of the delay is related not only to the data transmission technology but also to the physical distance. Response time is one of the most important network performance objectives for enterprises, and network users usually do not understand either propagation delay and jitter or throughput. They would become impatient when response times exceed 100 milliseconds.

1.2.4 Security

As computer technology continues to evolve, the security risks faced by network systems are all

increasing, and network security is receiving increasing attention. The design of the network usually needs to take into account the security of the network, able to prevent the loss of business data and other resources, damage or unauthorized access. Security threats usually include both external and internal factors, with internal factors usually including various computer viruses, operational errors, malicious behavior, etc. Also, when designing the network, the most basic security needs of the business should be considered, i.e., to ensure that hardware resources such as network hosts, servers, user systems, interconnected network devices, system and application data are not easily stolen reworked or damaged, etc.

1.2.5 Manageability

The network design must take into account the future maintenance and management of network facilities. The network is faced with maintenance and upgrading of equipment in the process of use, so a network that can be effectively managed and maintained is very important to the enterprise.

1.2.6 Usability

In order to maximize the ease of use of the network can be used, such as user-friendly host naming rules, dynamic configuration protocols and other methods to achieve.

1.2.7 Adaptability

When designing a network, the compatibility of the network should be considered from many aspects and angles to prevent unnecessary problems during the network construction process. An excellent network design plan should take into account the compatibility of existing and future technologies and be able to adapt to new technologies and changes during the use of the network.

1.2.8 Affordability

Affordability means maximizing the benefits of network design and operation within a given financial budget. In the network construction process, it is important to consider not only the current cost of the network construction but also the subsequent operating costs.

1.3 Network Interconnection Devices

Common network devices include hubs, repeaters, switches, routers and gateways. The role of both hubs and repeaters is to extend the network transmission medium. Switches work at the data link layer to exchange data based on addresses at the data link layer. Routers work at the network layer and provide network transmission path selection based on network layer addresses. Gateways work at the transport layer to interconnect networks between different high-level protocols, acting as a converter between networks with different communication protocols, different data formats or different architectures.

The following focuses on switches and routers:

1.3.1 Switches

A switch is an important network interconnection device. Each different network segment that is connected using a switch is a separate conflict domain. This means that nodes connected to the same switch will not interfere with each other as long as their IP addresses are not in the same network segment.

A traditional switch is a link-layer network device, so it addresses and forwards data through the MAC (Media Access Control) address of the data frame.

The switch has three main functions:

Address Learning

In the switch, a MAC address table is maintained that records the MAC addresses of the devices connected to the switch interface. When the switch performs data forwarding, it first looks up the MAC table based on the destination address of the data frame and forwards it based on the result found. If no match is found, the data frame is broadcast, and the device matching the destination MAC address will respond. When the returned response data frame comes back to the switch, the switch will record the new entry.

Each entry in the MAC address table is not fixed and has a life cycle. If an entry is not used for a period of time, it will be deleted. If the contents of an entry change, the entry will also be updated.

Data forwarding

When the switch receives a data frame, it forwards the data according to the MAC address table. Data forwarding is the main function of the switch, and there are three data forwarding modes.

(1) Fast forwarding

When the switch receives a data frame, as long as its length is greater than 14 bytes, it gets the destination address from it and forwards it immediately.

(2) Store-and-forward

When the switch receives a smaller frame, if it is part of a complete frame, it stores it first and waits for the complete frame to be received and then forwards it after ensuring that the checksum is correct.

(3) Non-fragmented straight-through forwarding

Fast-forwarding does not guarantee data integrity, and store-and-forward has high latency, so a compromise solution is proposed. After the received data frame reaches 64 bytes in length, the destination address is read, and forwarding is performed

Eliminate loops

Frequent changes to the network nodes attached to the switch can cause loop problems in the switch. The switch can eliminate loops by using the spanning tree algorithm.

1.3.2 Routers

A router is another important network interconnection device which works at the network layer of OSI. The main function of a router is to select the appropriate forwarding path for data packets based on the destination IP address. Routers are usually used to connect LANs or WANs of different network segments.

The core function of a router is routing, which is generated by the associated routing protocols. Common routing protocols include:

1. Static routing protocols

Static routing protocols are configured manually by the administrator through relevant commands. After the static route is configured, it is fixed and does not change automatically according to the changes in the network and requires manual maintenance. However, its advantage is that it is simple to configure, does not require computational overhead, and is suitable for simple and fixed networks.

2. Dynamic routing protocols

Dynamic routing protocols routing information is done by route generation algorithms. They use some messages, generation rules and routing algorithms to calculate the best path between source and destination addresses. When the network topology changes, they can sense these changes, automatically adjust the routing information in the routing table, and converge in a shorter time.

According to the scope of work, dynamic routing protocols can be divided into two categories:

(1) Interior gateway protocols

Interior gateway protocols work within an autonomous domain, generating and exchanging routing information within the autonomous domain; representative protocols are IS-IS and OSPF.

(2) External gateway protocols

External gateway protocols are used to connect different autonomous domains. That is, they work between autonomous domains. The routing information within the autonomous domain is exchanged to other autonomous domains through the external gateway protocol to complete the generation of routing information between autonomous domains. The representative protocols are BGP.

In addition, dynamic routing protocols can be classified according to the routing algorithm:

(1) Distance vector routing protocols

Distance vector routing protocols use direction and distance proximity (vectors) to identify the relationship between source and destination addresses and select the best path among them by calculating the distance values of all possible routing.

The advantages of distance vector routing protocols are simple configuration and low consumption of computing resources.

The disadvantages of distance vector routing protocols are slow convergence and poor scalability.

(2) Link State Routing Protocol

The link-state routing protocol is implemented based on Dijkstra's optimized path algorithm. The section between any two nodes in the path is marked with a weight value, and the optimal path is calculated based on the weight value.

The link-state routing protocol is concerned with the link state of the whole network, and only when the link state of the whole network is known can the computation be performed in the corresponding directed graph. Each router in the network informs other routers of its saved link

state in the form of LSA (Link State Advertisement), which eventually makes each router have a topological state graph of the whole network.

The advantage of link-state routing protocols is that when the network topology changes, only some routers are affected by the routing information.

The disadvantage of link-state routing protocols is that they consume a lot of computing resources.

1.4 The different types of enterprise network

1.4.1 Campus, branch, and Internet of Things (IoT)

Users and things can connect to these networks via wired and wireless connections. They can be found in all parts of a company, including offices and operating locations like manufacturing sites and warehouses. These networks are designed with transparent, secure access and high density.

1.4.2 Datacenter and hybrid clouds

Within on-premises data centers and private and public cloud services, these networks link to and among applications, workloads, and data. They are designed with low latency, security, and mission-critical dependability in mind.

1.4.3 Wide-area networks (WANs)

These networks connect facilities, buildings, or campuses to other branches, to data centers, or to cloud resources. They've been designed with the user's experience and bandwidth efficiency in mind. [1]

1.5 Some classic enterprise network architecture

1.5.1 Three-layer networking model

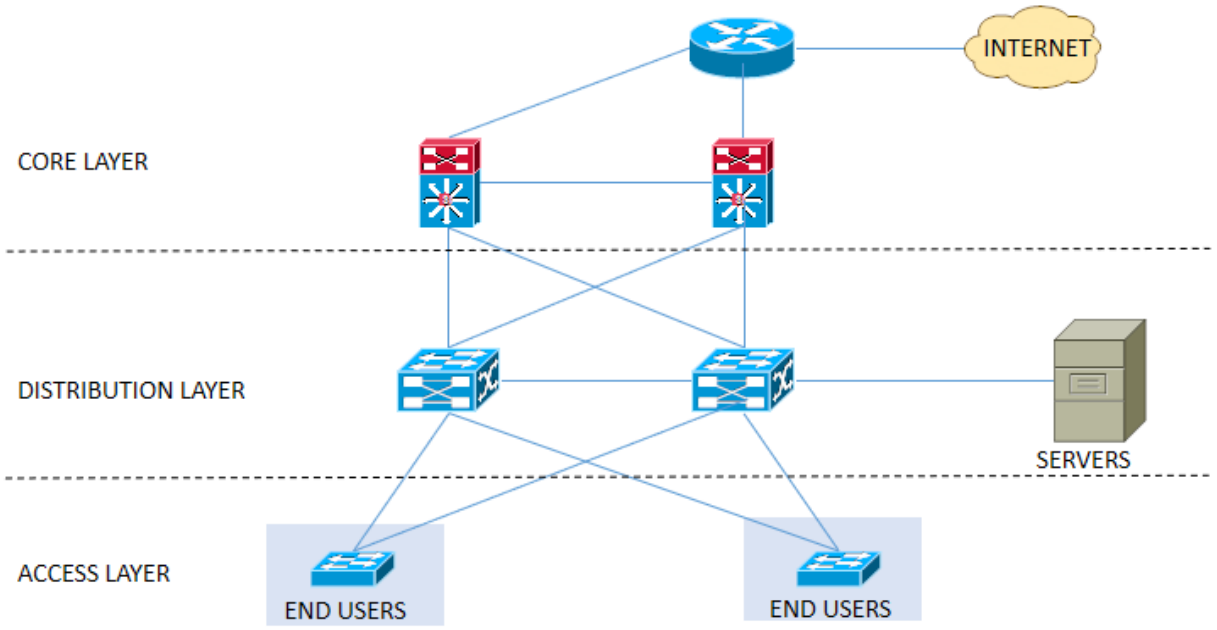

Figure 1. Three-layer networking model

Core layer:

The function of the core layer is mainly to achieve optimized transmission between backbone networks. Generally, it is considered that the ultimate carrier and aggregator of all traffic is the core layer, so the requirements of the core layer network equipment and its design are very strict. The core equipment will account for the main part of the network investment. The core layer can make the network more scalable, so it needs to consider a redundant design.

Distribution layer:

The primary function of the distribution layer is to connect the access layer nodes and the core layer center. The distribution layer (or convergence layer) is designed to connect to the local logic center, requiring high performance and rich functions.

Access layer:

It usually refers to the part of the network that users directly connect to or visit. The access layer uses optical fiber, twisted pair, coaxial cable, wireless access technology and other transmission media to connect to users and allocate services and bandwidth. Allowing end-users to connect to the network is the purpose of the access layer, so access layer switches are generally low-cost

and high-port-density.

1.5.2 SMB (Small and medium-sized business) network

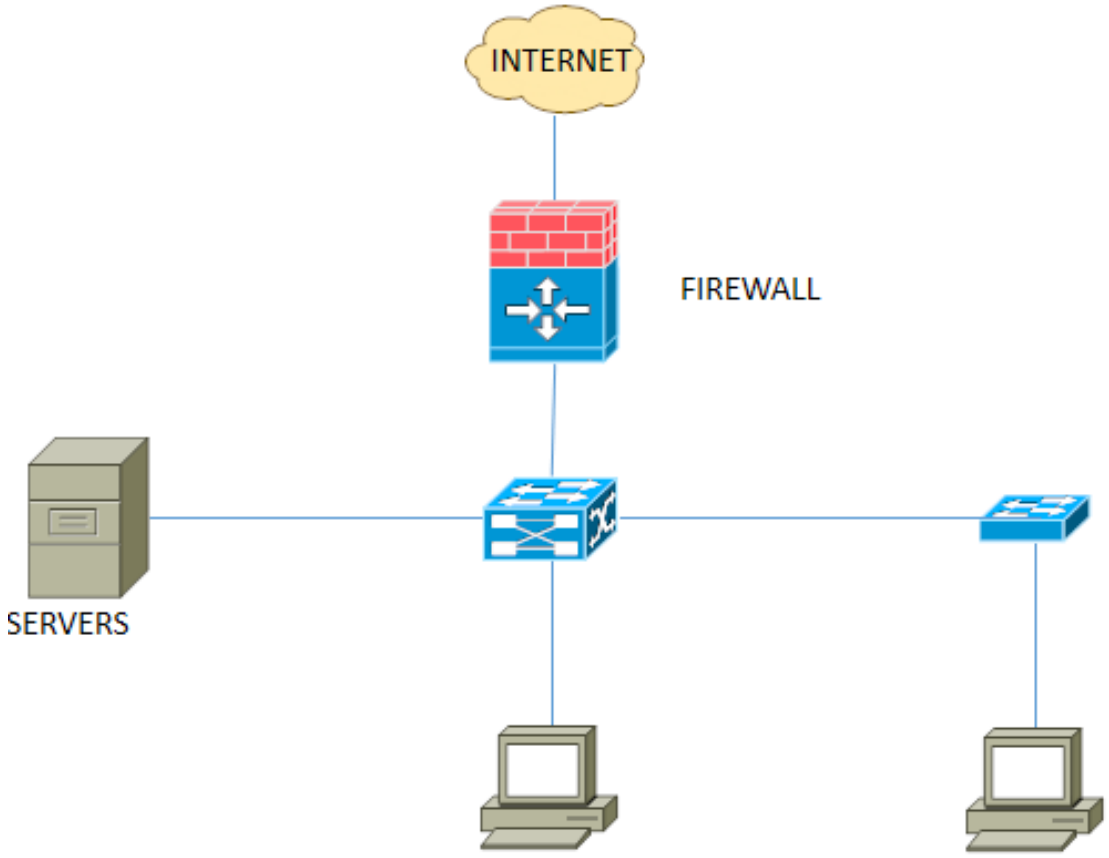

Figure 2. SMB (Small and medium-sized business) network

The disadvantage of the SMB network is that once the core three-layer switch fails, the entire network will be paralyzed, quickly causing a single point of failure.

1.5.3 Wireless campus network

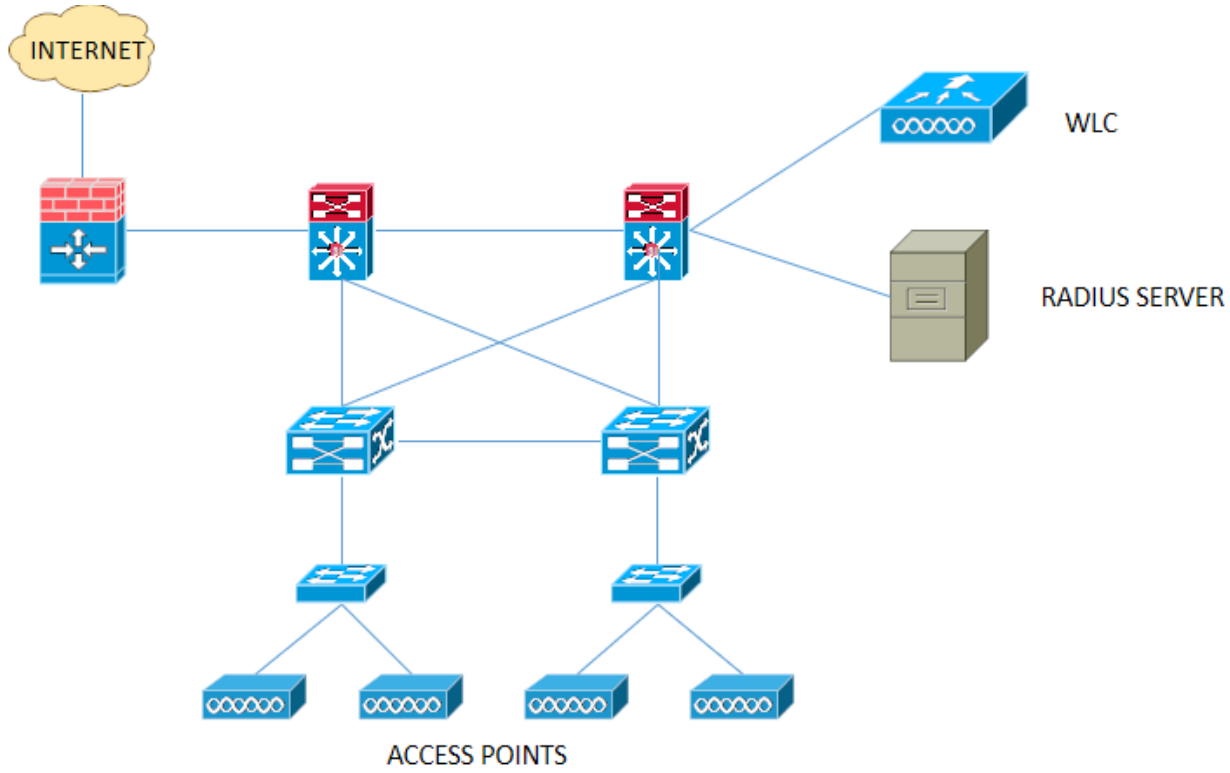

Figure 3. Wireless campus network

Characteristics of Enterprise Wireless Networks

Currently, enterprise wireless networks are more likely to use the 802.11ac standard. 802.11ac is compatible with all existing and upcoming standards and specifications of the full 802.11 series and also features high throughput, wider channel bandwidth, higher-order modulation, more null split streams, support for MIMO (multiple-in, multiple-out), enhanced carrier listening, and enhanced message aggregation technologies. In terms of security, it enables wireless connections to meet the needs of enterprise-class users in terms of security. 802.11ac transmits through the 5GHZ band with a speed of up to 1.3Gbps, and its high bandwidth undoubtedly brings great benefits to enterprises.

Enterprise wireless networks generally have the following features and performance:

(1) non-disruptive scalability and support for transparent access conversion to standard access.

(2) Access points are generally dual-radio wireless access with dual Gigabit Ethernet ports.

(3) Support for dense deployments, with growing capacity requirements requiring more access points.

(4) Enhanced management capabilities that improve throughput and reliability while also improving management efficiency and total cost of ownership, enabling each WLC to handle more users and manage more devices.

Enterprise wireless network deployment often uses WLC + AP deployment method, through the WLC to all wireless AP unified management control, unified set security policies and authentication. Different enterprises can flexibly develop different network architectures and solutions according to their own needs.

Introduction of WLC

The Wireless Controller (WLC) is a device that plays a major role in Wireless Network solutions. The traditional role of the access point AP, such as association or authentication of wireless clients, is performed by the WLC. The Lightweight Access Point LAP registers itself with the WLC and tunnels all management and data packets to the WLC, which then exchanges them between the wireless clients and the wired portion of the network. All configuration is done on the WLC. The LAP downloads the entire configuration from the WLC and acts as the wireless interface for the client.

The WLC has both physical ports for Layer 2 switches and virtual interfaces, which are very similar to VLAN (Virtual Local Area Network) interfaces. Each physical port can support many APs and WLANs. Ports on the WLC are essentially trunk ports that can transmit multiple VLANs to the switch for distribution to multiple APs, and each AP can support multiple WLANs.

There are three options available to access the WLC: first, via HTTP or HTTPS with a GUI; second, via Telnet, SSH with a CLI or with a console; and third, via a service port.

1.5.4 Government Network

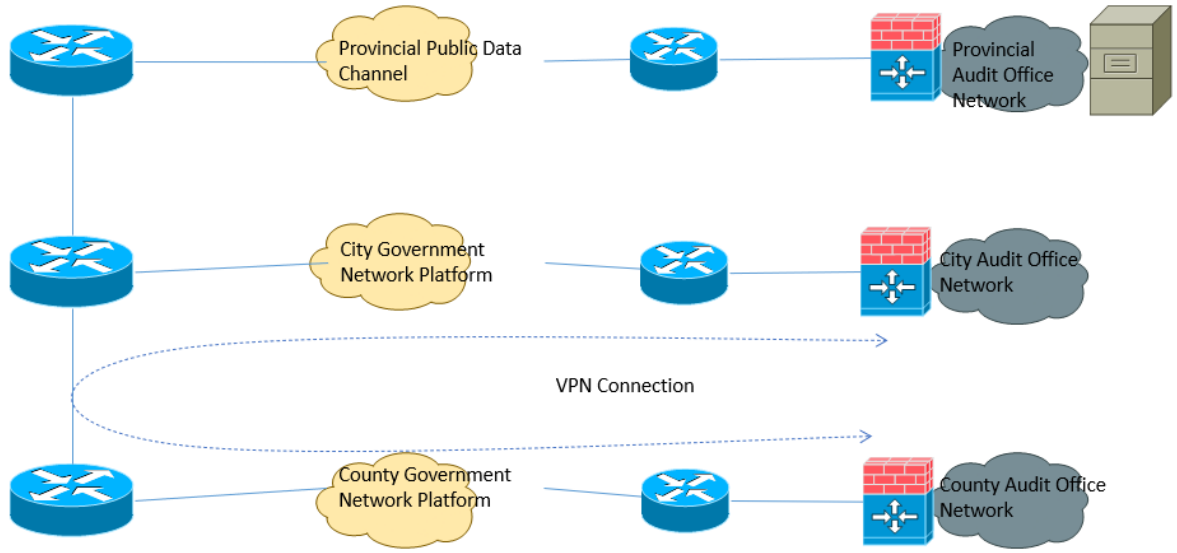

Figure 4. Government Network

Designing government networks is most concerned with security issues, which are mainly hacker invasion, the spread of network viruses, irregular operations by legitimate users of the system, and security problems in the network system itself. In order to prevent these security problems from occurring, corresponding security measures need to be taken to improve the security performance of the network.

1.5.4.1 Common Network Security Technologies

(1) Intrusion detection technology

Intrusion detection is the detection of the emergence of network intrusion damage behavior. Intrusion detection technology collects and analyzes network security logs, network behavior, audit data, and important information within the computer system, detects network behavior based on this information, and determines whether an intrusion exists. Intrusion detection technology can detect internal and external network attacks and operational errors in real-time, and can stop illegal intrusions before they cause damage to the network or system, so intrusion detection technology is a proactive network security protection technology.

In network security, intrusion detection technology and firewall technology complement each other, and the two work together to deal with network attacks, effectively improving the security performance of the network but also facilitating the management of managers.

Intrusion detection technology mainly includes rule-based detection and statistical anomaly detection, etc.

(2) Anti-virus technology

Computer viruses are computer instructions or codes written or inserted into programs that can maliciously damage computer systems and have the ability to self-replicate and spread. According to the process of virus processing, anti-virus technology can be divided into computer virus prevention technology, detection technology and removal technology.

Computer virus prevention technology is dynamic, based on the rules of behavior to determine the use of relevant technology to prevent the computer from virus infection and damage; computer virus detection technology is through a certain technical method to detect and judge the type of virus characteristics infecting the computer. In the current environment, there are two specific methods to determine the type of virus characteristics: one is based on virus keywords, virus characteristics and infection mode, etc., and the other is the specific virus program's own verification technology; the ultimate goal of computer virus detection is to remove the virus, remove the computer virus is the reverse process of computer infection virus.

(3) Vulnerability scanning technology

Vulnerability scanning technology is a key technology in network security technology. It is used in conjunction with firewall technology and intrusion detection technology, which can bring security to the network. By scanning the network, the security loopholes in the network can be found in time, and the network security parameters can be set in time according to the scanning results so that they can take the initiative before hackers attack the network and improve network security. In network security technology, firewall technology and network monitoring system are called passive protection strategies, while vulnerability scanning technology and intrusion detection technology are called active protection strategies, which can effectively prevent the network from being attacked.

(4) Firewall technology

Firewall technology was originally designed to protect information against various insecurities in the Internet network environment. As the name implies, the firewall is a barrier set up between the internal network and the external network so that the information inside the network is not affected by illegal operations outside the network. Firewall technology is the first barrier to

protect network security, which is a combination of computer hardware and software to set a lock between the internal and external networks so as to prevent the information inside the network from being invaded by illegal operations from outside. Firewall mainly includes four parts: service access policy, authentication tool, packet filtering and application gateway, which are generally deployed at the exit of the computer network in order to filter the communication data flowing into and out of the intranet.

(5) Data encryption technology

Data encryption technology uses a key to process the plaintext information that needs to be transmitted, turning it into ciphertext information that cannot be read directly, and the receiver of the information must decrypt the information using the decryption key to restore the ciphertext information in order to read the data information. Data encryption technology is to transmit data in a covert way to ensure the security of data.

(6) Access Control Technology

Access control is a measure to prevent computer data and information from being accessed by illegal users and to prevent legitimate users from accessing unauthorized data and information. In the computer application system, there are users with different rights, and users can only operate the data information within their access rights. If beyond the corresponding access rights, the access will be blocked, the system to protect the security of computer data information.

(7) Authentication technology

Authentication technology is an information security technology that confirms the identity of the user in the network environment through a certain technology. When using a computer for data storage, the information is all represented by data consisting of 0s and 1s, and so is the user identity information. In the complex network environment, how to ensure the consistency of the user's physical identity information and digital identity information is the problem facing authentication technology.

1.5.4.2 Internal and external network isolation technology

In network security technology, network isolation can also effectively improve the security of the network, which is implemented at different levels of the network architecture according to different network protocols. At present, network isolation methods can be divided into logical isolation, physical isolation and protocol isolation, etc.

(1) Logical isolation

As the name implies, logical isolation refers to the process of information transfer in the network being disconnected, while the actual internal and external networks are connected in the physical connection. The methods of logical isolation include setting up firewalls, building virtual private networks and virtual local area networks, etc.

A firewall is a barrier set up between different ranges of networks, which separates the internal and external networks according to a series of security control policies, thus achieving the purpose of protecting the internal network from external illegal intrusion. At present, there are many types of firewalls, and in practical application, different types of firewalls can be used according to different needs to isolate the internal and external networks and control the incoming and outgoing data flow, so that the firewall can better play the role of protecting network security.

Virtual Private Network (VPN) is a secure and reliable private logical network based on the public network, using password and tunnel technology. VPNs are not isolated from the public network. The most distinctive feature of VPN is the use of cryptography and tunneling technology to ensure network reliability while reducing network construction costs based on the public network.

The users in a VLAN are not affected by geographical location, and the network users are logically segmented according to their needs. VLANs are flexible, easy to expand, convenient for network maintenance, and the reasonable use of virtual LAN technology can improve network operation efficiency.

(2) Physical isolation

Physical isolation belongs to passive isolation. The key is to build the network when the internal and external networks are truly separated. Once the isolation is successful, it will be static. Unlike logical isolation, physical isolation uses physical methods to separate the internal network from the complex and extensive network so that the internal network data will not be leaked and stolen from illegal external invasion and malicious damage, creating a safe and reliable protection barrier for the internal network. In practical application, to realize the physical isolation of internal and external networks, it is necessary to realize the isolation of internal and external networks both in terms of physical connection and physical radiation, and also to isolate the network environment of internal and external networks in terms of physical storage.

(3) Protocol isolation

In general, protocol isolation plays a role in the connection of the internal and external networks, and the two networks are isolated by configuring the corresponding network protocols to protect network security. In the actual configuration application, protocol isolation should be used in combination with cryptography.

1.5.5 School Campus Network

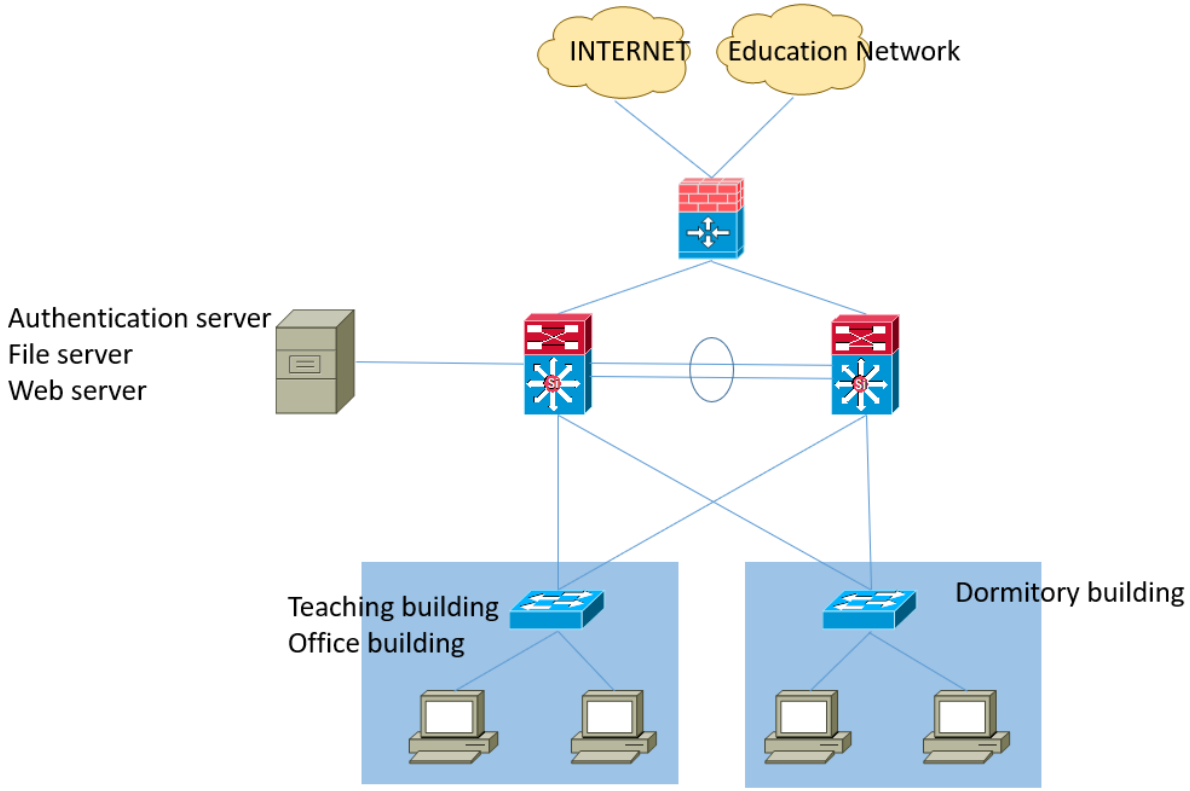

Figure 5. School Campus Network (small and medium network)

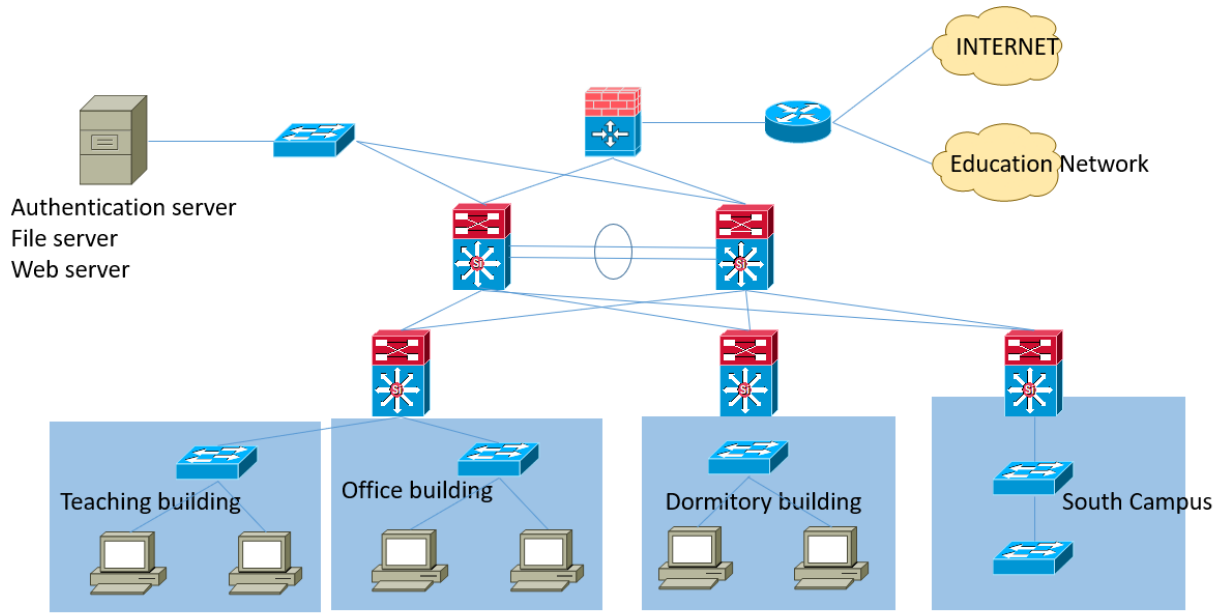

Figure 6. School Campus Network (large network)

At present, the campus network can basically meet the design requirements of 10-gigabit main line, gigabit convergence, 100-gigabit entry, and access to external networks such as the Internet and education network, which is a large intranet environment isolated from the Internet.

In terms of network topology design, the overall planning of the campus network can be divided into several parts, such as core switching area, data switching area, security egress area, terminal access area, operation and maintenance management area and outreach area according to independent functional modules. Among them, the backbone network adopts 10 Gigabit links and connects other areas by the core switching area. At least two high-performance Ethernet switches are deployed in the core switching area, and a dual redundant power supply system is used to ensure the operational reliability of the core equipment.

A high-speed data exchange channel is established between the core switching area and other areas, where the security egress area is the boundary of the campus network and needs to realize functions such as data forwarding, security audit and traffic control. In the data center area, firewall and intrusion detection technology, etc., need to be adopted to meet the security requirements of the campus network. Meanwhile, the operation and maintenance access protocol access support are provided by the operation and maintenance management zone to realize functions such as identity identification and risk identification.

1.5.6 Financial Network

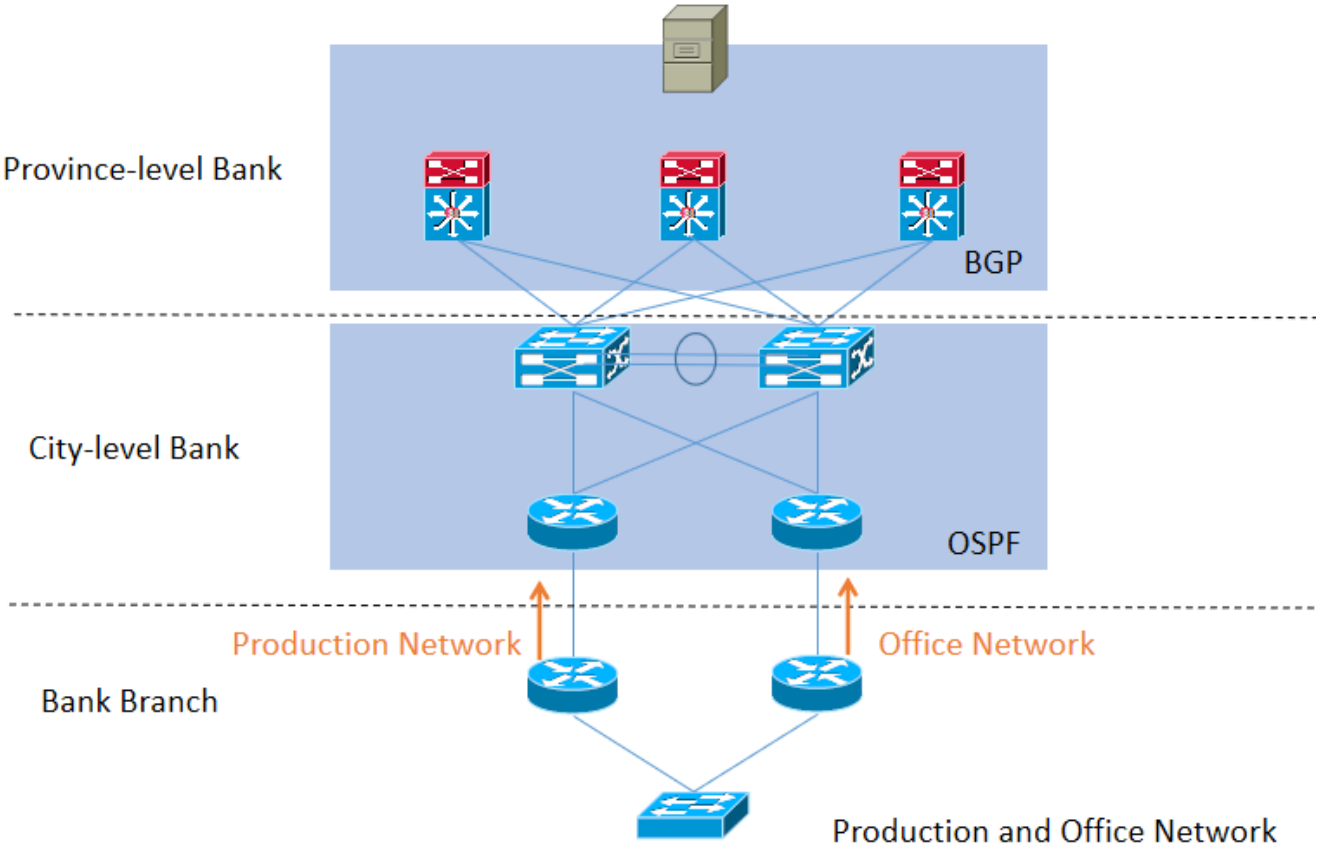

Figure 7. Financial Network

The bank's network construction project not only provides a platform for the bank to produce and inform its office but also lays a solid foundation for the wide application of various data-based, voice and video services of the bank in the future. In order to achieve the target requirements of high quality and high interconnection, the following network principles have been adhered to in the network construction.

High reliability: The network system must have a high degree of security and reliability, especially for the business data transmission of commercial banks must be foolproof, communication lines, key equipment must have backup measures. The key equipment of the network is made of highly reliable network products and equipment with full consideration of redundancy capability, fault tolerance, self-healing capability of the network, reliable backup strategy, etc.;

Advanced technology and practicality: to provide the best performance/price ratio for the system.

High performance: to ensure the good operation of the network, to ensure a variety of data (data,

voice, video, image) of high-quality transmission.

Also, consider the manageability of the network, scalability, security and so on.

1.6 Network Provisioning

Network provisioning refers to the process of configuring a network so that authorized users, devices, and servers have access to it. In practice, network provisioning primarily focuses on connectivity and security, which means heavy concerns on device and identity management.

The Definition of provisioning

When something is provisioned in IT, it is ready for use. For example, when a user successfully connects to Wi-Fi, Wi-Fi is provisioned to that user.

The benefit of network provisioning on businesses

When done correctly, network provisioning can increase enterprise efficiency and security. Network administrators can spend less time setting up and configuring networks, and business operations are more secured and streamlined.

The challenges of network provisioning

Without automation, the key challenges are the increased number and variety of equipment and devices, the complication of remote work settings, and the high activity facing modern business networks.

Network provisioning can be very time-consuming for organizations with many WANs users, a lot of temporary users, or a requirement to scale up or down quickly.

Network provisioning improve automation

Network administrators save time on establishing and implementing policies, assigning IP addresses, and configuring IP-based devices thanks to automated provisioning. Errors that slow network speed can be reduced by automating the process.

In many circumstances, instead of a team, one individual may handle the automated provisioning procedure. As the network expands and evolves, automation technologies assist in monitoring and improving network optimization. The tools keep track of actions so that system audits can be performed later. [2]

1.7 Network Management

The process of managing, administering, and operating a data network via a network management system is network administration. Modern network management systems collect and analyze data in real-time and push out configuration changes to improve performance, reliability, and security.

The function of the network management system

Network devices such as wireless controllers, routers, access points and switches are all controlled by the network management system. To collect data from network elements usually requires a centralized server. On-premises, in a private data center, or in the cloud are all viable options for the server.

On the network, devices, clients, and programs can transmit status updates to the server. Logging in to the server, commonly using a web browser or a smartphone app, allows network administrators to monitor network operations.

The way network elements send data to the system

Network endpoints like cellphones, Computers, cameras, machines, and sensors, as well as networking devices like routers and switches, deliver data to the system in one of two ways:

Since the early 1990s, The Simple Network Management Protocol (SNMP), an open standard, has become the de facto network administration protocol. The vast majority of network component vendors support it. To "poll" each network element, the network management system uses SNMP. Then the system receives each element's response.

Telemetry refers to a software agent installed in a network node that allows the automatic communication of critical performance information in real-time. Because telemetry is more efficient, can create more data points, and is more scalable, it is gradually replacing SNMP. And telemetry standards like NETCONF/YANG are gaining interest as a way to provide multivendor support similar to SNMP. [3]

Network Management Functions

Network management consists of five major elements: fault management, configuration management, account management, performance management, and security management (FCAPS). Network management expert Amy Larsen DeCarlo details these elements, explaining

their importance in managing enterprise operations.

For these elements to serve their purpose, network professionals monitor the network end-to-end using monitoring tools that provide an implementation view of performance, traffic, usage, failures and availability. As expert Ed Tittel and IT writer Kim Landros explain, "Careful network monitoring can facilitate proactive strategies, such as justifying the cost of hardware or infrastructure upgrades needed to eliminate long-term network bottlenecks."

While network monitoring can be used as network device logging, open-source tools, or proprietary monitoring capabilities built into network products, it is often more powerful as a fully dedicated platform with a rich feature set and vendor support.

In addition to network monitoring, organizations should consider implementing network analytics tools to compile the data collected through monitoring and generate insightful and actionable reports. Network analytics and network monitoring solution should be able to span on-premise, cloud or hybrid deployment environments and unify the configuration of wired and wireless infrastructure.

Conducting a network assessment to account for the various network components that can collect and analyze telemetry data is critical to selecting the most appropriate enterprise tool. For example, specific platforms place a strong emphasis on monitoring and reporting, providing some off-the-shelf analytics. In contrast, others focus on in-depth root cause analysis and artificial intelligence customization. In addition, one needs to ensure that the IoT environment is included in the assessment, if any.

Good practices for managing enterprise network

Inventory network assets. Enterprises need to accurately inventory all devices and applications on the network. Use tools that can automatically discover devices to make this task less complicated and cumbersome for IT staff.

Reduce manual management. Automated network management is considered a good practice, but the concept is too general to automate at scale. Automation should be kept simple, low-risk and quick to start. For example, the network team can automate the device locator to find out where devices are connected to the network, perform application connectivity checks to verify that devices are correctly connected for each network infrastructure, and look for discrepancies between parts of the network configuration the enterprise configuration template. As teams succeed with this configuration, they can move toward automation of intermediate and advanced

tasks that include verifying border gateway protocol connectivity and automating access control list updates.

Assess the scope and risk of changes. The network change management process is also driven by good practices that can reduce the risk of change failure. Applying some basic operating principles, such as assessing the scope of proposed changes, can prevent potential errors.

A risk analysis should accompany the assessment of scope. The network team should make changes through peer review, pre-deployment testing and validation, implementation and testing, and documentation and network management updates.

Make processes (including troubleshooting) repeatable through documentation.

Documentation is helpful in most areas of network management, especially when trying to resolve wired network and wireless connectivity issues. For example, IT identifies and resolves wireless network connectivity issues that should be documented and reused to save time and avoid configuration errors.

Why is network management so important?

To better illustrate the need for a well-designed network management strategy, IT teams should understand the cost of network downtime. Network downtime will impact business revenue, lost productivity, reputational damage, failed investments, and increased operating costs.

A survey by network monitoring software provider Netrounds shows that network outages can lead to unexpected and unplanned network degradation, costing each organization an average of about $600,000. Downtime can be costly, expected and unanticipated, but businesses can avoid or reduce them through network management.

Achieving comprehensive visibility and monitoring requires a large number of skilled staff, so enterprises are looking for a more manageable approach to network management. Network automation eases this burden by eliminating everyday labour-intensive manual network tasks such as provisioning, scripting, fulfilling change requests, and determining the cause of delays and outages.

Network Management Tools

Network management vendors want to reduce the complexity of their products and increase their interoperability and feature set. Most enterprises use multiple network management tools for various products and devices, which only adds to the complexity. The following examples show

the advancement achieved in network management interoperability.

Integrated network monitoring and security

Integrating network management and monitoring with security tools to provide more comprehensive security insights brings more value to the enterprise. With this capability, network administrators can play a more significant role in addressing security risks and can share critical information with security teams.

Integrated network management security is beneficial for the labour-intensive task of performing security audits. IT teams can automatically validate configurations and standards across devices and deliver results more efficiently.

Ready-to-Serve Network Monitoring

Vendors are also working on how to help network teams monitor the performance of cloud computing environments, particularly IaaS, SaaS and PaaS. For SaaS monitoring, network teams have to find a tool that allows them to monitor the end user's path from the ISP to the public cloud to measure service latency, DNS speed, accessibility, and content delivery network responsiveness from the end user's perspective.

Hybrid Cloud Monitoring

Cloud providers typically only help enterprises monitor their environments. Still, emerging network monitoring tools are springing up to meet multi-cloud monitoring, and hybrid cloud monitoring platforms use passive network devices to capture traffic data across hybrid cloud environments. Through analysis, they can identify potential failures before they cause serious problems.

Open Source Network Monitoring

Open source network monitoring is an attractive option for enterprises with tight budgets but under pressure to meet service level agreement requirements. Skilled developers in the industry are already collaborating on these areas, and these products have been rigorously vetted by peers and users alike.

Open source tools can also help enterprises avoid the added cost of adding more components. Using open source technologies, enterprises can scale the environments they need to manage, including servers and switches, without going over budget.

Configuration Management

Configuration management improves network maintenance and helps keep track of connected devices, device configurations and device connections. Network teams can achieve three goals with configuration management: maintain accurate configuration records, enable effective network scanning, and enable network automation capabilities.

Automated Network Testing

Automated network testing can complement network management tools, validate physical connectivity, routing protocol functionality, path performance, and more. However, network management issues around abstraction, virtualization, and overlays are also applicable to automated network testing.

Network automation tools fall into three categories.

1. Tools built primarily for server and application automation but extended to include networking

2. Tools designed specifically for networking

3. Software-defined platforms that create software overlays across LAN hardware.

These tools offer features and functionality that eliminate error-prone manual tasks such as configuration backup, tool access control, regulatory compliance monitoring and verification, vulnerability assessment, and network orchestration. Enterprises can explore leading network automation tools.

Network professionals can incorporate network automation tools to create end-to-end services to help with design, implementation, and testing.[4]

1.8 Network Automation

Within a network, network automation automates the configuration, management, testing, deployment, and operation of physical and virtual devices. Network service availability improves as daily network work and operations are automated, and repetitive processes are controlled and handled automatically.

Network automation can be used on any sort of network. Data centres, service providers, and businesses can use hardware and software-based solutions to automate their networks, increasing productivity, reducing human error, and lowering operational costs.

The need to automate the network

The rise in IT costs for network operations is one of the most pressing concerns for network administrators. Data and device development are beginning to exceed IT capabilities, making manual procedures practically unfeasible. Despite this, up to 95% of network changes are done manually, resulting in operational costs, which can be up to 3 times greater than the network's cost. Businesses must increase their IT automation, which must be handled centrally and remotely in order to keep up with the digital world. [5]

Automation also brings the following benefits:

1. Reduce human error;

2. Quickly provide new services;

3. Be able to locate and identify the root cause of network security issues;

4. Reduced security risks, as fewer manual processes mean fewer configuration or policy errors that could create vulnerabilities.[4]

1.9 Network Orchestration

Network orchestration is the action taken when network controllers set devices, applications, and services in the network to meet. It's similar to how an orchestra conductor directs individual players as they execute a piece of music as a group.

The benefits of network orchestration

The following are some of the advantages of network orchestration:

The network controller has a brain. The controller translates business requirements into network requirements, configures the network to meet those requirements, and monitors it to ensure that those requirements are satisfied.

It considers the network as a whole rather than individual components. Also, it synchronizes all network components to achieve the joint objectives.

The reason the IT team need network orchestration

Most businesses rely on their networks to help them conduct their operations. Aside from connecting various user and IoT (Internet of Things) devices, networks also transport data around

the company, manage resources and applications in data centers and clouds, and assist in the security of all elements. And, because business needs quick change, networks should be able to adjust swiftly and affordably.

Networks that are supposed to perform so much are becoming more difficult to manage.

Any significant change must be reflected in several areas. For example, setting up a new user may necessitate changes to numerous switches, routers, firewalls, AAA servers, and other devices. These modifications allow the user to be properly verified and approved, as well as set up with the necessary application-access levels.

Many tasks may be required while deploying a new application in the public cloud. The tasks could include dynamically obtaining cloud compute, storage, and network resources, provisioning software-defined WAN (SD-WAN) to offer the quality of service (QoS) that meets the traffic of the application, and configuring switches and access points to enforce access rights.

With adequate orchestration, the network can complete such complicated steps without skipping a beat.

The needs of network orchestration

Network orchestration is typically beneficial to enterprises with 20 or more network devices or 250 or more users.

Growing businesses that are adding users and IoT devices, hosting a broad group of users with different needs, or requiring stringent data security standards should look at how network orchestration might help them reach their goals.

Organizations that have frequent traveler personnel, host applications in their data centers, use public cloud services or have regular network modifications should look into how network orchestration might benefit them.

The mechanism of network orchestration

All network setup was done manually before the invention of software-defined networking (SDN) and network automation. Of course, manual configuration is no longer a good idea. Organizations instead rely on network controllers and programmable network devices to carry out their tasks in a systematic manner.

This execution is orchestrated by network controllers. They understand the network's

architecture, infrastructure parts, configuration, users' devices, and traffic patterns inside and out.

Controllers that use the intent-based networking model enable the input of business goals, which they then translate into network activities.

The difference between network orchestration and network automation

The term "network automation" refers to the automated completion of discrete, generally simple tasks. Uploading a newly configurated file to a switch and upgrading the switch's software image are two examples of automation—jobs that each accomplish a single goal.

Orchestration is the process of completing related tasks in order to reach a more complex goal. A network controller performs automatic tasks in a predetermined order and validates the completion of each operation before moving on to the next.

Identifying and reconfiguring the right access points and wireless LAN controllers, as well as setting up proper credentials, security methods, authorized bandwidth, and so on, are required to orchestrate new wireless, for example.

The difference between network orchestration and network management

Functions for administering and operating networks are referred to as network management. These functions are performed by a central network management system, usually the network controller, using its automation and orchestration capabilities. Network orchestration, in other words, is a subset of network management. [6]

1.10 Network Monitoring

Network administrators are provided by network monitoring with the data they need to assess whether a network is performing optimally in real-time. Administrators can use tools like networking monitoring software to detect flaws early on, improve productivity, and more.

The definition of network monitoring systems

Network monitoring systems are software and hardware solutions that track many elements of a network's operation, including traffic, bandwidth usage, and uptime. These systems can monitor and update the status of devices and other items that make up or touch the network.

Network administrators rely on network monitoring tools to swiftly detect device or connection failures, as well as issues like data traffic bottlenecks. The capacity to detect problems now

extends beyond the usual demarcation lines of the network. These systems can network analytics to send email or text alerts to inform administrators and generate reports.

The protocols for network monitoring

Protocols are rules and instructions that manage how devices on a network communicate with one another. To transport data, IT teams must employ protocols on network hardware. Protocols are used by network monitoring systems to find and report on network performance issues. [7]

1.11 Network Analytics

Any process that collects and analyses network data in order to improve the network's performance, reliability, visibility, or security is known as network analytics.

Processes for network analytics are becoming increasingly automated today. As a result, IT employees can better monitor performance, troubleshoot problems, and complete other increasingly sophisticated jobs.

The mechanism of network analytics

In terms of network analytics, a software engine analyses and extracts insights from data acquired from numerous sources, which includes network devices (switches, routers, and wireless), servers (Syslog, DHCP, AAA, configuration databases, and so on), and traffic-flow details (wireless congestion, data speeds, latency, etc.).

Network analytics operations are automated, allowing for more comprehensive analysis than was previously feasible. Network analytics can grow to accommodate a large number of devices, clients, users, and applications without significantly raising running costs.

Machine learning (ML) and artificial intelligence (AI) and technologies are being used by more advanced network analytics systems to improve the insights they provide.

The benefit of network analytics

Network analytics can be used for many purposes, including finding bottlenecks, analyzing device health, root-cause analysis, issue repair, identifying connected endpoints, and probing for potential security gaps.

To optimize operations and discover abnormalities, IT teams compare incoming data with preprogrammed models in network analytics. The real-time telemetry data is incorporated into a

network performance model that is optimum. The analytics engine may offer adjustments and measures to improve performance when a data source detects less-than-ideal performance or deviates from operational benchmarks.

For discovered network faults, network analytics may offer corrective steps, which can include guided remediation, in which the engine recommends steps for a network administrator to follow. In more complex systems, it can do closed-loop remediation, in which it sends instructions to the network controller's automation section to make modifications automatically.

Network analytics looks into traffic to and from the endpoint to detect protocols, then uses AI to correlate that data with data from other sources to create a profile for the endpoint.

Network analytics checks endpoint behavior and traffic (including encrypted) for anomalies that could signal that the endpoint has been hacked, such as by malware. [8]

1.12 Network Troubleshooting

The act of detecting and correcting problems with connectivity, performance, security, and other elements of networks is known as network troubleshooting.

The value of network troubleshooting

A cornerstone of company resilience is quick and effective network troubleshooting. More mission-critical business processes are being performed on today's networks than ever before. Networks might suffer from significant downtime if they don't have comprehensive troubleshooting and quick resolution of issues.

Reduced productivity and the economic effects of disrupted or failing services, data breaches, and malware are all examples of downtime costs. These ramifications can cost a lot of money and harm brands for a long time.

The way organizations handle troubleshooting

Of course, troubleshooting entails more than simply changing user passwords or restarting equipment. It's about a set of procedures, methods, and technologies used to process multiple requests by a complicated mix of users and scattered network assets and infrastructure, especially in large enterprises.

A large company usually has an entire team dedicated to network troubleshooting. The engineers on the team deal with difficulties on three levels: Tier 1 for basic issues like password resets, Tier

2 for situations that can't be fixed by Tier 1, and Tier 3 for mission-critical issues.

Tier 1 troubleshooting is frequently outsourced. An escalation structure is utilized to efficiently route requests and guarantee that upper-level engineers are suitably tasked.

In recent years, machine learning (ML), artificial intelligence (AI) and automation have been utilized to fill skill gaps. These technologies provide Tier 1 engineers with guided remediation tools that allow them to quickly resolve complicated network issues.

Many firms have different network troubleshooting tools, which require training and management from their IT department. Network troubleshooting is frequently integrated into a network management system (NMS).

The relationship between NMSs and troubleshooting

Network troubleshooting teams in large enterprises don't just sit around waiting for users to report problems.

A network management system (NMS) continuously monitors networks. It provides status updates—and alerts—on network key performance indicators (KPIs) like connection speed, bandwidth, latency, users, and access when they're needed.

The NMS performs monitoring by querying the many portions and nodes of the network to update status at an interval defined by the IT team. Newer network nodes, on the other hand, use telemetry to automatically send their KPIs.

Tracking and collecting data on network events is an important element of network troubleshooting. This procedure is carried out using an IT service management (ITSM) ticketing system. The information gathered from the tickets can be used to pinpoint issue locations and direct network optimization and enhancements. [9]

Network events

An event is an occurrence that initiates a network troubleshooting procedure. The following are some commonplace occurrences.

Connection failures	Cables and plugs that aren't connected properly could cause such incidents.
Security lapses	These activities could range from a full-fledged

	malware attack to the attempt of an unauthorized user to connect to Wi-Fi.
KPIs missed	KPIs can provide early warnings of network faults before they affect users if they're well-calibrated.
Application failures	A failure in locally hosted programs could indicate an uninstalled update or the presence of old hardware.
Policy failures	When network regulations such as security, traffic management, and access control inadvertently contradict each other, network performance suffers.
Endpoint issues	Endpoint connectivity problems, for example, might be caused by endpoints being too far away from network routers, network interference, or problems with a remote worker's local network.

Table 1. Network events

Troubleshooting processes

After receiving alerts or requests and ruling out fundamental issues like hardware connections and user connectivity, network troubleshooting often entails some of the following steps.

IP-configuration checks	IP address issues can cause many network problems. If a prior IP address was incorrect, assigning a new one can typically resolve the problem.
Ping and tracert testing	If the IP address is accurate, the network problem could be occurring upstream of the modem. IT teams can use the ping utility or the tracert command to test connections with remote servers and return information about

	the signal path to help diagnose the problem.
DNS checks	A DNS check will detect whether a server to which networks are attempting to connect has an issue. When an IT team does a DNS check and gets findings like "Request timed out" or "No response from the server," the issue could be with the destination's DNS server.
Service provider checks	Even major cloud providers and cloud-based services experience outages. Outages that may be hurting network performance are reported on provider status pages.
Virus and malware checks	Viruses and other malware may wreak havoc on a network's performance, and they're typically difficult to spot. Security tools should be used by IT teams to see if new attacks have been detected.
Database logs	Databases that are overburdened or full might cause network performance to suffer. If this is the case, a new inspection of database logs will reveal it.
Command-line tools	Ipconfig and nslookup are two of the most commonly used command-line utilities. Others, such as iptables, netstat, tcpdump, route, arp, and dig, can also aid in the detection of network problems.
Test environments	IT teams may need to develop test environments to re-create problems and test solutions in scenarios that are particularly difficult or contain sensitive or restricted data.

Table 2. Troubleshooting processes

1.13 The challenges and demands of enterprise networking operations in practical work

Network Management Challenges

Even with excellent practices, network management can pose challenges for organizations.

Traditional network tools. Managing decentralized environments, including virtual and cloud-based networks, can become complicated if organizations rely on primitive and cumbersome monitoring tools.

Complexity and abstraction. The adoption of modern technologies also faces some challenges because they increase the complexity of the network environment. For example, traditional network monitoring tools are forced to interact with virtual machine hypervisors in virtualized environments. VM hypervisors cause a split between device-based network components, virtual routers, switches, and firewalls and can complicate end-to-end visibility. Overlay networks have similar problems, as they can hide underlying hardware and software from monitoring tools.

Interconnectivity. Despite the interest generated by multi-cloud environments, bridge connecting environments create configuration challenges, inconsistent performance, and security concerns that network professionals must address. [4]

Take the perspective of city-level bank branches as an example:

The main challenge is optimizing the repetitive work in daily work:

1) Since the main line and backup line are used on aggregation devices, when a line failure occurs, the main line will generate an alarm as configured, but the backup line will not be alarmed if there is a failure because it is not in use. We can only manually check the port status of the backup line every day.

2) It is expected that the configuration files of all devices can be automatically backed up in full regularly and stored on one computer or server as a disaster recovery measure.

3) When the provincial branch distributes the unified configuration script, it will dramatically improve efficiency if it can automatically compare with the existing configuration and only configure the places to be added.

Take the perspective of province-level bank branches as an example:

1) In terms of automated operation and maintenance, it is hoped that automated monitoring of all network devices under the jurisdiction can be achieved. Information about all devices is automatically collected on a unified operation and maintenance management platform to avoid sending emails and inefficient manual statistical methods. Meanwhile, it can also issue change commands and assign tasks to all network equipment under the jurisdiction of city-level branches and other branches.

2) In the firewall configuration, it is necessary to isolate the boundary hardware according to the principle of minimum authorization and configure and change the on-demand communication strategy. In the past, it was required to do it manually. Therefore, it is hoped that there is a module that can only submit the necessary change information and automatically generate commands and that it can be executed automatically. At the same time, the equipment that needs to take effect can be selected to reduce the scope of risk.

3) In the local area network operation and maintenance, it is hoped that there is a platform that can automatically obtain information and quickly locate a specific user's IP and MAC address. At the same time, it can also bring convenience when new users are assigned with IP.

4) In terms of hardware operation and maintenance, it is hoped that SDN-based automated operation and maintenance and python scripts can be used to achieve automation; The data dedicated line connected to the secondary branch is expensive, so it needs to control the traffic. Traditionally, the QOS is used but not effectively. The use of SDN can achieve automatic tuning and avoid congestion.

At the same time, SDN can also be used to deliver configurations in batches, and manage, monitor, operate and maintain through the controller.

1.14 Next-Generation Network Monitoring Technology

Intent-based networking is one of the most promising technologies for network management, which uses automation and orchestration to change the way network configurations are deployed. The goal is to create self-managing, self-healing networks that use artificial intelligence and machine learning to perform network tasks.

Admittedly, IT teams are wary of this level of automation, fearing that it will take them away from day-to-day operations. When enterprises hire network professionals, they should ensure that

candidates are willing to control emerging automation and intelligence tools to better automate across the enterprise.

On the security side, artificial intelligence and machine learning will help network teams identify dangerous activity by identifying disruptive traffic patterns that differ from regular exercise. This is becoming particularly important in the IoT environment.

AI and machine learning will also improve network operations by enabling analytics applications to discover the root cause of problems and automate the correct remediation process.

One of the benefits of artificial intelligence and machine learning is significantly reducing the number of events that staff must handle each day, potentially from millions to a handful of critical events.

Network management technologies are also evolving rapidly with the introduction of new and emerging technologies, making IT teams more strategic in managing next-generation networks.[4]

1.15 Software-Defined Networking (SDN)

With the increasing scale of the network, the growth rate of Internet traffic, and the change of users' demand for traffic, programmable networks have emerged as an idea to solve the complex problems of the network. Based on this programmable idea, researchers have proposed the concepts of forwarding abstraction, distribution state abstraction and configuration abstraction, decoupling the control function of switches from the traditional network and leaving it to the control plane, adding a standard interface connecting the data plane and the control plane, and retaining only the function of switches to identify the exchanged data. The control plane abstracts the global view of the distributed devices of the whole network and integrates the information of the whole network so that the applications of the application plane are based on the information of the whole network for the unified configuration of the network. At the same time, the user can automatically complete the unified deployment of forwarding devices along the path by simply configuring the application interface provided by the control plane. As a result, the data forwarding path in the network no longer depends on the data plane but produces a software-defined network architecture with decoupled data plane and control plane and uniform interface standards. [10]

The advantages of software-defined networking are the separation of forwarding and control, support for software programmability, and centralized control of network state, which have been

widely used in the fields of network virtualization, data center networks, wireless LANs, and cloud computing. The structure is flexible and easy to manage. Figure 8 shows the architecture of SDN.

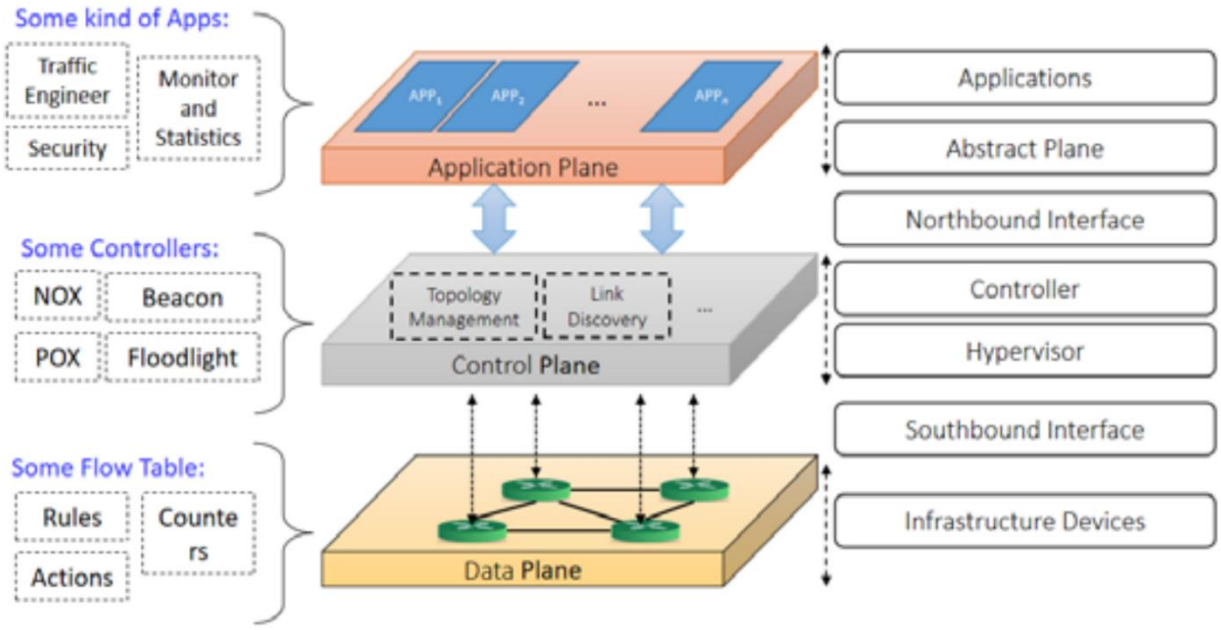

Figure 8. SDN architecture [10]

As shown in Figure 8, the SDN architecture consists of an application plane, a control plane, and a data plane from top to bottom. The application plane reflects user intent, and users can develop applications based on their intent and actual needs. In the application plane, developers develop network visualization applications and network automation-related applications by collecting network data, such as topology state, network statistics, and so on. These applications can provide end-to-end solutions based on actual requirements. The application plane is connected to the control plane through a northbound interface, which allows users to customize the development according to their actual needs. Currently, most traditional northbound interface development is based on providing programming interfaces to existing devices for business applications to invoke. The control plane is responsible for managing the underlying physical network and can flexibly control the controller according to demand, ensuring the stability of the network by obtaining and maintaining different types of network information, topology information, etc. It is the control center of the network system. [10]

SDN controller-based solutions in the market can be divided into commercial and open source solutions: commercial solutions provided by large network equipment vendors, such as Cisco Open SDN controller provided by Cisco, NEC Corporation developed PFC SDN controller and

Brocade SDN controller, etc.; open-source solutions Generally provided by community organizations, due to the system open source widely used by individual users, the current better open-source solutions include Ryu, OpenDaylight, Floodlight, etc., the typical controller comparison is shown in Table 3.

The control plane is responsible for the implementation of the physical layer of the switch. The switch is initially in the form of hardware, with the continuous development of virtualization technology, open vswitch (OVS) to overcome the bottleneck of the development of hardware switches, while virtualization integration and switch functionality, support for multiple physical machine distribution environments, based on open source technology to achieve virtualized networking. Currently, OVS supports traditional standard management interfaces such as NetFlow and sFlow. The southbound interface connects the control plane and the data plane, and many organizations have started to standardize the southbound standard interface. For example, the OpenFlow protocol was proposed by the Open Networking Foundation (ONF), in addition to other protocols such as the extensible messaging and presence protocol (XMPP) defined by the Internet Engineering Task Force (IETF).[10]

The creation of OpenFlow breaks the barriers of the SDN hardware market and allows applications to communicate with SDN controllers to transmit data in the form of software. The data plane consists of various software/hardware-based infrastructure devices that receive commands from the upper layer through the southbound interface, process network data according to the instructions from the upper layer, and send back information to the upper layer through the southbound interface, such as instructions for processing data results and running time.

Controller	Language	Creator	Openflow Version
NOX/POX	Python, C++	Nicira	1.0, 1.3
ONIX	-	Google, Nicira	-
Beacon	Java	Stanford university	1.0.1
Maestro	Java	Rich university	1.0
Floodlight	Java	Big switch networks	1.0
Floodlight-plus	Java	Big switch networks	1.3
Ryu	Python	NTT labs	1.0-1.4

(ODL)Open daylight	Java	Linux foundation	1.0, 1.3

Table 3. Comparison of controllers

The simulator can simulate the creation of an SDN-enabled network, and the packets passing through the Ethernet port are received and processed by switches and routers to realize the network simulation process. Currently, many network simulation experiments are based on this. The simulated network can add new functions to the network and perform related tests, and then deploy the corresponding functions to the real hardware environment based on the experimental results. Table 4 gives a description of the simulators that exist today and are widely used.

Simulator	Opensource	Language	Platform	Openflow Version
Mininet (simulator)	Yes	Python	BSD open source	OF 1.3 of the reference user switch and NOX from CPqD and Ericsson
NS-3 (simulator)	Yes	Python, C++	GNUGPLv2	Pre OF 1.0 and version of OF-SID that support MPLS
EstiNet (emulator/simulator)	Yes	-	-	OF 1.3 and 1.0

Table 4. Comparison of SDN simulators and emulators

Chapter 2: Artificial Intelligence

2.1 The meaning and characteristics of Artificial Intelligence

2.1.1 The meaning of Artificial Intelligence

The concept of artificial intelligence was first proposed by scientists in 1956, and after continuous development, artificial intelligence has gradually become a comprehensive discipline covering various subjects. Specifically, artificial intelligence is the process of imitating intelligent human behavior and thinking through the application of computers. Artificial intelligence belongs to one of the sub-disciplines of computer science. Its research focuses on using machines to replace humans to deal with some complex work to reduce personnel and cost losses to optimize resource allocation and improve human labor quality and efficiency. The research areas involved are diverse, including language recognition, natural language processing, image recognition, professional systems, robotics, etc. With the continuous development of intelligent technology, its application areas will certainly broaden.

2.1.2 Characteristics of Artificial Intelligence

Super computing power

Influenced by the revolution of computer processing technology, artificial intelligence has a strong computing ability, which can perform high-speed and stable computing on a large amount of data information and complete very complex operations in a very short time; at the same time, it can also quickly extract and use effective content in a large amount of information; at the same time, influenced by various characteristics such as inanimate, emotionless and fatigue-free computers, which makes artificial intelligence more accurate for data processing It can reduce people's working time and work difficulty, and can reduce the probability of error, which has a very positive significance for the improvement of work efficiency.

Effective cost reduction

Artificial intelligence can accurately and quickly process and calculate data and information and reduce costs to a large extent. Mature artificial intelligence products have a wide range of applications, large user groups and other characteristics; at the same time, artificial intelligence also has the features of processing uncertain information, can be changed with the help of network fuzzy analysis of the inherent program hindrance, and thus achieve the effect of all-round mastery of system resources and access to more valuable information. In addition, after the algorithm design is completed, artificial intelligence only requires regular maintenance in the use

process, which is a product that can be reused and used efficiently and can significantly reduce the operating costs of enterprises or individuals.

Ability to process data accurately

Humans are organic life forms, both physiologically and psychologically exhausted, while under the pressure of heavy work, humans also have apparent mood swings, such as depression, irritability, etc. In physiology, injuries and other phenomena may appear. These problems may arise objectively and are difficult to avoid. This characteristic also determines that in the production work, if only rely on humans to deal with, so long cannot completely guarantee that the work in the link can be 100% correct and can avoid the development of errors altogether. However, errors in some parts of the production process are likely to cause serious consequences, such as errors in the input of enterprise reports may bring significant economic damage to the enterprise, and errors in the factory safety system may pose a threat to the safety of workers. The application of artificial intelligence is an excellent solution to the above problems, and human labor, artificial intelligence is the carrier to carry out the work of the computer, only need to set the program, even if the very complex operation, for the computer is the only mechanical repetition of the calculation and process. Compared to humans, computers are inanimate and emotionless. They do not suffer from fatigue or mood swings, so they can perform data calculations more accurately and ensure the accuracy and precision of mathematics. In general, the application of artificial intelligence can quickly improve productivity and improve the accuracy and reliability of work. Compared with the work mode based on human labor, artificial intelligence can significantly reduce the risk of errors and improve work efficiency, which in turn can achieve cost savings and improve the effectiveness of the effect.[11]

2.2 Key AI Technologies

Machine learning (ML), which employs algorithms to read data, learn from it, and determine or forecast without explicit instructions, is required for AI to succeed. ML has lately evolved into more complicated structured models, such as deep learning (DL), which uses neural networks for even better insight and automation, thanks to increases in compute and storage capacity. Another area driving recent AI growth is natural language processing (NLP), which is notably prevalent in virtual homes and IT assistants. Natural language processing (NLP) employs vocal and word recognition to make interacting with machines via natural language cues and inquiries easier. [12]

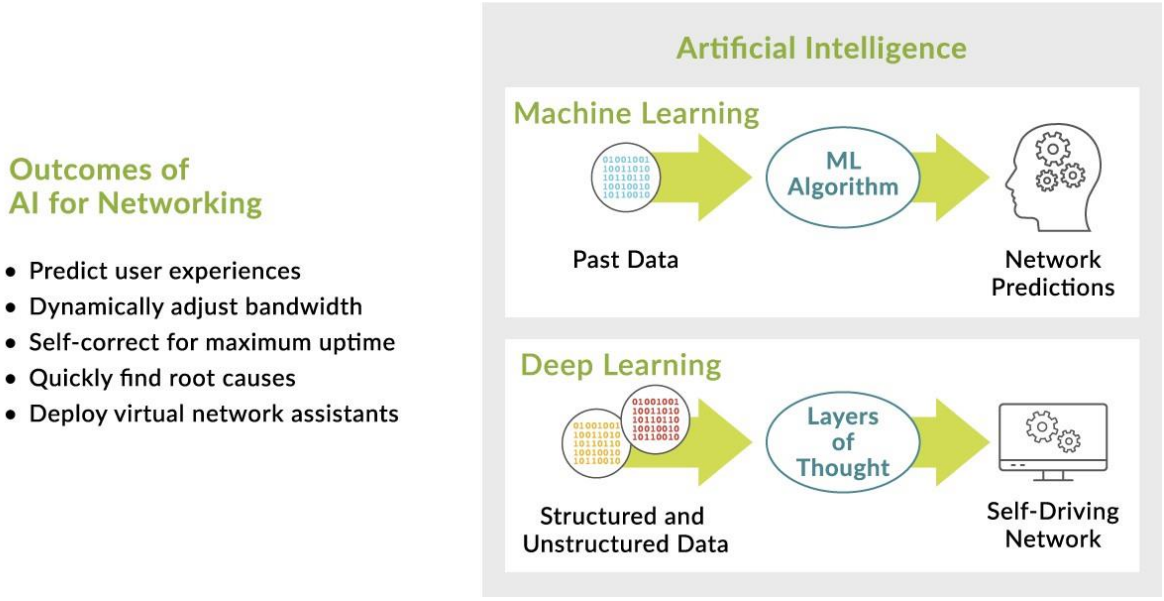

Figure 9. The role of AI in network environments [12]

2.3 How to build an AI system

IT just cannot keep up with today's heavy network requirements without the correct AI strategy. An AI plan should include the following technology pieces.

Data

Any useful AI solution must start with a large volume of high-quality data. Through data collection and analysis, AI develops its intelligence over time. The AI solution grows bright as the data collected becomes more diverse. It's critical to collect data from every edge device in real-time for real-time applications employing highly distributed "edge" devices, such as mobile devices and IoT. Using AI techniques, quickly process it locally or nearby in an edge computer or the cloud.

Domain-specific expertise

AI solutions require labeled data based on domain-specific knowledge, whether they are assisting a doctor in diagnosing cancer or enabling an IT administrator to discover WiFi faults. These information chunks aid AI in breaking down the problem into manageable parts that may be utilized to train AI models. Design intent metrics structured data categories can be used to identify and monitor the wireless user experience.

Data science toolbox:

Once the problem has been broken down into domain-specific metadata bits, the data is ready to be fed into the mighty world of machine learning and big data. To evaluate data and deliver actionable information, IT teams should use various techniques such as supervised or unsupervised machine learning and neural networks.

Virtual network assistant

Collaborative filtering is a machine learning technique that many people encounter while they are watching a movie on Netflix or purchasing something on Amazon and receive recommendations for comparable movies or things. Collaborative filtering can be used to search through massive data sets and find and correlate those that create an AI solution to a specific problem, in addition to providing suggestions.

In AI for networking, the virtual network assistant could act as a virtual wireless expert in a wireless environment, assisting with complex challenges. Consider a virtual network assistant that combines domain expertise, quality data, and syntax (classifiers, metrics, correlations, root causes and ranking) to deliver predictive advice for avoiding problems and actionable insights for resolving current problems. It can pick up on the subtleties of wireless networks and react to inquiries like "What went wrong?" and "Why did that happen?" AI is allowing for these kinds of automated advancements. [12]

2.4 Advantages of Artificial Intelligence in Computer Network Technology

Providing comprehensive information

Compared with the human brain, computer development is relatively unlimited, and computer technology also shows a very high level of ability in processing the acquired information. Even in

the face of unfamiliar areas, computer technology can easily break the obstacles to learning or work. The application of artificial intelligence in computer network technology can make the information processing process intelligent and comprehensive while maintaining a high standard of information processing capability. To find more valuable information, computer users can also search through a series of big data-related information provided by AI to learn to develop various knowledge and skills with the support of comprehensive information provided by AI technology.

Optimization of hierarchical management

Computer technology has been popularly used in various industries and even across multiple work areas throughout society. Computer network technology has become an indispensable part of people's daily lives in the current computer era. The management of computer use has undoubtedly been put forward to higher requirements. Network technology in the process itself has a certain degree of complexity; if the IT team wants to achieve an excellent network management effect, it is necessary to apply a more powerful technical system to solve the complex management problems. However, in the traditional computer network hierarchical management, the management effect is not very satisfactory because its management mode does not have good communication ability. It is difficult to give full play to the effectiveness of the hierarchical management application. But when artificial intelligence technology emerges, this weakness is well compensated for, for the high complexity of the computer system, artificial technology can well solve the network security problems to achieve scientific and efficient management. From the application of artificial intelligence technology advantages, its value is mainly reflected in the artificial intelligence technology directly broke the traditional computer management form of hierarchical management between the wall, management communication ability has been improved, each hierarchical, each department and each link between the smooth path of information exchange, computer security issues have also been well resolved.

Organize fuzzy data

Computer users in the use of computer networks are not difficult to find, with the help of time, the computer will generate a lot of complicated, disorderly, irregular information data, these fuzzy computer information data if only rely on the user's own regular extraction, not only need to spend more time and energy, for the user's own computer ability literacy also has specific requirements. However, with the application of artificial intelligence technology for fuzzy data sorting, the difficulty of the work will be significantly reduced, artificial intelligence in a brief period will be able to accurately extract the main line of information, followed by practical,

logical reasoning, can save a lot of time for the computer users. From another point of view, computer technology is changing rapidly. The computer network is always in the process of updating the development of the times. The traditional computer management tools are far from meeting the actual needs of computer technology work. Therefore, through artificial intelligence technology to update the corresponding computer management tools is to assist in upgrading computer technology, the key to innovative computer management tools.[13]

Improving Collaboration Capabilities

In recent years, science and technology have been improving, and the application of computer networks has been realized in many industries and fields. To further expand its development scale on the existing basis, it should be effectively combined with various current advanced science and technology. From the current point of view, today's computer network technology is not the traditional single network technology management. Still, it should be carried out for the improvement of the network level, the implementation of supervision in each network system of each level of cooperation, to guarantee the effectiveness of collaboration fundamentally, it can effectively ensure the orderliness of the entire computer network management, and promote its more sustainable and smooth operation. [14]

Low operating costs

Unlike other emerging technologies, artificial intelligence technology can control the amount of energy consumed when used to calculate and analyze data and information in network systems, which means that its application advantages are significantly better than traditional computer technology. At the same time, the application of artificial intelligence technology in the field of computer network system-related algorithm control can change the original calculation speed and even use the optimal solution to complete a one-time calculation task to meet the requirements of saving computing resources, significantly improving the application of network technology. For example, traditional market research methods are mostly questionnaire surveys. Such surveys are more one-sided, often requiring a lot of time and capital investment, and the analysis of the link results can not be separated from human support. The use of artificial intelligence technology can fill the shortcomings of traditional survey mode and defects to achieve the goal of intelligent analysis and processing of user information.

Strong learning ability

Artificial intelligence technology has a strong learning ability. The Internet system contains many

information and theoretical concepts, with distinctive features such as straightforward content and low structure level. After systematic processing, it can excavate precious details from the above content. Take enterprise product development as an example. We can use big data technology to derive the data analysis results of users, formulate the general direction of product development, and further improve product development and advertising accuracy and effectiveness. For example, the higher-ranked questions, keywords or content with more hits in search engines can be regarded as a channel for enterprises to understand the current hot topics of public concern so that they can provide a comprehensive reference for decision making, judge and evaluate whether there are other problems in their own decisions, and try to make decisions based on what users are concerned about.[15]

2.5 Principles of Artificial Intelligence in Computer Network Technology

The principle of freedom

The application of artificial intelligence in computer network technology needs to strictly follow the principle of freedom, the relevant technical personnel in the actual development and application of artificial intelligence in the process of fully safeguarding human rights and freedom, the future development of artificial intelligence should also be based on the protection of privacy, strengthen the development of personal data control work, to minimize the misuse of data phenomenon.

The principle of justice

In addition to the principle of freedom, in the process of applying artificial intelligence, the principle of justice should be strictly followed to ensure the transparency of the algorithm decision itself, which should be reasonable, fair and non-discriminatory when setting the algorithm. For the artificial intelligence decision, it will have a certain degree of impact on the rights of individuals, so it should ensure the fair distribution of the advantages of artificial intelligence as far as possible to reduce the digital divide.

The principle of security

In the actual development, design and application of artificial intelligence, the network information, assets and personal security should be fully guaranteed. The collection and application of personal data should be adapted to the requirements of relevant laws and

regulations to fundamentally improve data security. The appropriate staff should combine the risk objectives of artificial intelligence, scientific and reasonable development of suitable plans and measures, and at the same time to strengthen the development of artificial intelligence education work for relevant personnel, to promote its continuous improvement of the importance of its security.[14]

2.6 Analysis of Artificial Intelligence application problems

Security Issues

The precondition for developing and applying any technology is safety, which is the priority. Artificial intelligence, as highly sophisticated technology, will cause serious security problems if it is out of the control of human beings. One of them is the security crisis caused by the misuse of technology. Criminal elements like hackers may use artificial intelligence to attack the country's website and steal confidential information through intelligent technology. In addition, hackers can also use computer technology to break through the company's firewall, illegally obtain the company's financial information, and even transfer the funds of the company's finances to their own names; second, the security risks induced by technical defects or improper management. So far, the artificial intelligence system is not mature enough, and there are loopholes in some technologies that may make the artificial intelligence system abnormal or malfunction. For example, deep learning technology is imperfect, and robots' offensive production and installation can lead to severe consequences.

Ethical Issues

The creation of artificial intelligence brings new ethical issues. Can the rules of behavior of intelligent machines be compatible with social norms? Robots also have to abide by social ethics and act by human ethics. If not, it raises particular ethical issues. The driver-less cars developed by Google and other companies remove the steering wheel, gas pedal, and brakes and rely only on intelligent systems to sense the surrounding situation and determine the direction of travel based on big data analysis. If the car is usually driving and no accidents happen, the smart car can drive safely. However, when five people are running red lights in front of the IT team and two people waiting on the side of the road, if the IT team cannot brake in time, will the driver-less car choose to go straight or turn to the side of the road? And who will be responsible for such traffic accidents? This is a difficult choice for human beings.[16]

2.7 The current state of development of Artificial Intelligence technology

Expert System

The expert system refers to an intelligent computer program system, one of the most widely used and essential fields of artificial intelligence technology. The system covers much expert-level knowledge and experience in a particular field. It solves the problems encountered in the area for users by applying human expert-level knowledge in the field. The expert system effectively extends human intelligence into the professional field, realizing the goal of transitioning from theoretical research to practical application, significantly improving the efficiency of human processing of professional problems. The expert system relies on complex algorithms to make more comprehensive calculations on the possibility of future development of professional issues. The work efficiency will even be more efficient and accurate than human experts. With the continuous research on expert systems, many expert systems can make intelligent responses and judgments in different application scenarios based on the simulation of human behavior and can use the knowledge base to dig deeper into the intrinsic connections of complex problems. Expert systems have been widely used in many fields, helping enterprises to figure out the market laws more objectively to make correct production decisions, scheduling planning, resource allocation plans, etc., significantly improving the scientific nature of business operations and enabling enterprises to obtain better economic benefits while saving production costs. The architecture of the expert system is shown in Figure 10.

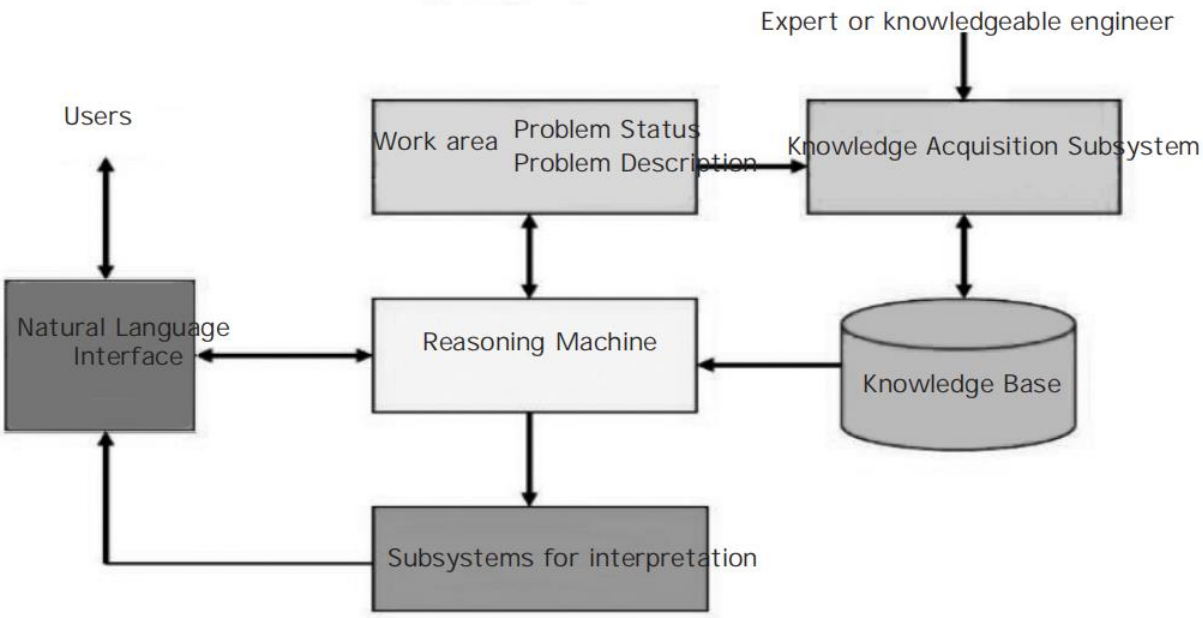

Figure 10. Expert System Architecture

Pattern recognition

Pattern recognition uses computer technology to classify objects into different categories according to specific characteristics. The main research directions of artificial intelligence technology in pattern recognition currently include speech-language information processing, computer vision, brain network groups, etc. It is hoped that artificial intelligence technology can recognize and process complex information. This application can promote the development of several industries in the direction of intelligence, such as the military field, medical field, etc.

Robotics

The main research direction of robotics is the design, manufacture and application of robots. With the maturity and application of artificial intelligence technology, the intelligence level of robots has been increasing, and their application in different industries has become more common. Common robots in everyday life include floor sweepers, welcome robots, delivery robots, early education robots, drones and more. They can be operated by mobile devices, which significantly enhances the intelligence and convenience of people's lives.

Machine learning

Machine equipment cannot think independently. Its response in different application scenarios is based mainly on computing network technology and algorithms to simulate human thought patterns and fully digest human behavior to optimize performance.

They simulate human patterns of thought and digest human behavior to optimize their own performance and be able to deal with different problems. Machine learning is a multi-disciplinary and highly complex science that encompasses statistics, probability, algorithmic complexity theory, etc. It is the core technology of artificial intelligence and the critical technology that drives the development of computers in the direction of intelligence.

Artificial Neural Networks

Artificial neural networks have been the focus of extensive research in artificial intelligence technology since it entered a period of rapid development. Computer algorithms are used to simplify, abstract, and pattern the human brain's neurons and build a network structure similar to the neuronal network of the human brain. The maturity and development of artificial neural network technology have provided technical support for developing expert systems, pattern recognition, robotics, biology, economics and many other disciplines and has solved many practical problems in developing artificial intelligence technology.[17]

2.8 The path of integration of Artificial Intelligence in computer network technology

The application of artificial intelligence to computer networking technology enables significant improvements in intelligent control, machine perception, language processing, neural networks, data mining, logical reasoning and other capabilities. The ability to process large amounts of data proactively and efficiently and draw rigorous conclusions based on scientific data analysis facilitates the practical application of computer network technology.

Build a sound network security management system.

As the scope of network applications becomes more and more extensive, data information security issues are emerging, and network information security has become one of the current issues of general concern to society. However, because of the intricacies of the network space, the analysis and computing ability of computers is limited. It cannot pinpoint and discover potential flaws and loopholes in a timely manner. With the application of artificial intelligence in computer network technology, the network management work begins to show forward-looking, advanced and comprehensive characteristics. It gradually builds up a perfect system consisting of software and hardware, fuzzy identification and biometric identification, expert system and geographic system, genetic algorithm and evolutionary algorithm. Among them, the use of artificial

intelligence to establish an information tracking system, combined with automatic tracking and retrieval of a large amount of data, timely detection of network vulnerabilities, and processing solutions, without spending a lot of time searching and modifying the program, reducing the difficulty of investigation. Artificial intelligence can quickly identify insecure information and quickly block abnormal information, preventing information stored on computers from leaking through illegal channels and improving the quality of network information security management. For example, an intelligent firewall can be installed in a computer to form a network barrier that intelligently identifies all kinds of operational information and completes the blocking work itself, protecting the information in the computer from being stolen.

Drive hardware and software updates.

Artificial intelligence technology has a strong learning ability and can simulate human thinking and behavior patterns, accelerating the iteration of updates through learning and research in the use process. The premise of computer network technology development is to obtain the support of computer software and hardware. It is inevitable to promote the development of computer network technology through hardware updates and software upgrades. By applying artificial intelligence to the process of updating hardware and upgrading software in computer network technology, it can bring into play its powerful learning and research capabilities, automatically retrieve the actual needs of users for software, and constantly break through the configuration standards of hardware facilities. Artificial intelligence can retrieve the hardware and software that needs to be updated at any time and then use the system to issue reminders to users and follow up with them according to their choice, ensuring that hardware is updated and software upgraded in a timely manner. For example, in terms of hardware, according to the needs of different users and the nature of data flow, gateway devices suitable for various data formats, computing languages and communication protocols can be selected and upgraded, enabling the connection, conversion or blocking of intranets, extranets, public networks and private networks. In terms of software, artificial intelligence agent software can be applied to enrich the software knowledge base and realize intelligent control of daily study, life and work, such as meeting time, product recommendation, weather inquiry, itinerary arrangement and email sending and receiving.

Promote the sharing of quality resources.

The sharing of resources in cyberspace has become a hot phenomenon, and more users are sharing resources through online channels, increasing the possibility of accessing quality resources. In the face of the vast amount of resources available on the web, artificial intelligence

technology can be used to guide users to filter and access useful and practical quality resources efficiently. By using AI to search for fuzzy information, users can quickly narrow down the scope of resources they are looking for and use the association function to pinpoint similar resources, helping users to accurately search for and quickly locate the resources they need and complete the download process, ensuring that resources are available on time. For example, the use of artificial intelligence technology to establish an expert system, the pooling of experience and knowledge in medicine, economics, education, business, information technology and other aspects of the integration of logical reasoning technology for the operation of computer networks and the individual needs of users, to take personalized solutions, saving a lot of human, material and financial resources, reflecting the efficiency and convenience of computer network technology.

Promote the proper cleaning of spam information.

Entering the era of big data, the explosion of network information is both for the convenience of users' life and learning and bringing users to dispose of spam and prevent harmful information worries. The application of artificial intelligence technology in computer networks can realize personalized customization on the one hand and set the program according to the actual needs of users to screen various kinds of disturbing information such as messages, emails, website pop-ups and commodity push links in practical applications, and clean up spam information by blocking or deleting channels to purify cyberspace continuously. On the other hand, it can realize active identification, change the traditional passive and rough filtering, make a scientific judgment and source audit of data and information, make processing from data technology and feedback means, screen out the useless, abnormal and even harmful information, send a warning to users in time for details with dangerous factors, which can effectively prevent users from losses caused by improper operation and carelessness. For example, applying artificial intelligence technology in the mail system can implement categorization management and increase the automatic defense function to effectively intercept spam, fraudulent, phishing and illegal mails and reduce or avoid the risk of privacy leakage and property loss of users.

Optimize the intelligent processing of network data.

With the support of artificial intelligence technology, network management has powerful data computing ability, which can filter information in all aspects and then complete the analysis, screening, blocking, and access to improve network management efficiency. Artificial intelligence can also accurately identify the face and fingerprints, representing biometric technology. The application of artificial intelligence can realize the correlation of fuzzy

information, effectively reduce the blind spot of information recognition, reduce the false alarm rate and false alarm rate of the system, and improve the comfort of users and the accuracy of data detection. In addition, artificial intelligence can achieve rapid analysis and classification of network data, effectively solving the shortcomings of the traditional data processing process, and efficiently carry out data collection, analysis, screening and other work to provide a reference for the final research and use. The application of artificial intelligence technology in the control process can optimize the control process, automatically identify risks and improve the quality of data security monitoring. For example, biometric technology can be used to accurately identify the face and fingerprints of different users and collect virtual and actual identity information, which can be used for payment, transferring money, unlocking cell phones, and accessing privileges. The dual system of biometrics and fuzzy recognition provides unlimited convenience for social production and home life, reduces redundant steps in network management, and significantly enhances the effectiveness of big data and intelligent control.[18]

2.9 Analysis of the current state of research on the integration of different planes of SDN with artificial intelligence

When artificial intelligence was first applied to SDN, it could only handle small-scale, low-complexity scenarios in routing, security, and architecture. The traditional SDN separates the control plane from the forwarding plane, and the switch receives the uniform standard rules from the controller through the standard interface and performs the corresponding actions. However, the traditional SDN mode of operation can no longer meet the large-scale and complex traffic structure in today's big data era, and it is impossible to make corresponding rules according to the traffic data itself to achieve intelligent network provisioning. Therefore, many researchers are working on adding larger and more intelligent work in SDN routing, security, and architecture [19].

2.9.1 Data plane

Data plane-related technology research includes two aspects: switch design research and forwarding rules research. Switch design research includes the design of scalable and fast-forwarding devices, which can quickly forward data streams on the basis of flexible matching rules; secondly, research related to forwarding rules, including forwarding rules that consider

solving unexpected situations, such as the problem of consistency update after rule failure, etc.

Switches are divided into hardware switches and software switches. Regulation of hardware switches can store and increase the rate of data forwarding, but, if over-reliance on hardware switches will make the network upgrade rate is too slow, high cost; and these technologies are monopolized by large companies, will produce a relatively closed market, it is difficult for new forces to survive, the market lacks innovation and competitiveness, hindering the development of the network equipment industry. Therefore, the focus on the development of software switches, some of the services implemented in the software from the hardware switch to the software, not only to reduce costs but also to make the network configuration more flexible, thus opening up the hardware vendors to monopolize the market barriers. The International Software Switching Forum gives the following definition: software switches are based on packet networks using programmable software to provide call control functions of equipment and systems that can provide more packet processing. However, when adding new features, there are drawbacks such as a large amount of code, the need to modify the kernel and the extreme reliance on the expertise of the modifier. Rahimi et al. developed a new packet I/O framework called Netmap and compared the performance of OVS, IP forwarding, Linux bridges, and DPDK vSwitch by running OVS on Netmap.[20]

The research direction based on data plane forwarding rules mainly includes two aspects: developing new southbound interface protocols or proposing intelligent protocols. However, the above separation of control plane and data plane requires frequent interaction of various controller southbound interface messages between OpenFlow switches and controllers, which puts high demands on the controller's processing power, datapath processing delay, and a channel bandwidth of the southbound interface, etc. Zheng et al. propose a southbound interface technique based on traffic characteristics. They propose a network-wide power manager and several related heuristics to dynamically turn on/off the network elements to meet the performance requirements of network traffic. They propose a network-wide power manager and several associated heuristics to dynamically turn on/off network elements to meet different traffic loads. However, the above research on protocols is limited to heuristic algorithms, which can play a role in intelligent control of routing or traffic to some extent but increase the computational burden of the data plane. Therefore, various algorithms based on the data plane must still take into account the growing scale of data and save energy by reducing the computational complexity.[21][22][23]

2.9.2 Control plane

The control plane is the brain of the entire network, and its core component is the controller. The controller logically controls the switches centrally, forwards network data quickly, and manages the network securely with a global view, thus improving the overall performance of the network. Currently, the research on controllers is divided into the following areas:

Distributed controllers. Single centralized control has a single point of failure, limiting the scalability of the network; on the other hand, in large-scale networks, single centralized control is slightly weak in dealing with delays between other domains and switches. Therefore, most of the distributed controllers are used to solve the above problems.

Controller security. The controller is the core of the SDN network, and from the security point of view, the centralized and open nature of SDN network architecture brings huge hidden danger to SDN network security while increasing the flexibility of the whole network. Most of the traditional SDN controller security protection methods use OpenFlow flow-based traffic monitoring and intrusion detection, using the advantages of SDN to achieve algorithm improvement and performance optimization. However, these methods ignore the security information contained in historical data and cannot prevent future security attacks. By introducing artificial intelligence algorithms, SDN network security models can be built to achieve intelligent optimization of the control plane.

Since the network state is closely related to the human behavior pattern, it is possible to predict the traffic load, improve the bandwidth utilization, and reduce the network loss through a comprehensive analysis of human behavior characteristics such as network coverage, user distribution, and services by artificial intelligence techniques, so as to achieve network-wide load balancing. For example, Tang et al. proposed a new deep learning-based traffic load prediction algorithm for predicting the future traffic load and blockage in the network, and on this basis, combined with a deep learning-based partially channel assignment algorithm (DLPOCA) into solving the problem of intelligent channel assignment to individual links in SDN-IoT networks, to intelligently avoid potential congestion, and to rapidly assign appropriate channels in SDN-IoT. Leguay et al. explored the potential of SDN to run computationally intensive machine learning tools and solve complex optimization problems in a centralized manner by exploring some algorithms of SDN and machine learning. [24][25]

On the other hand, by introducing artificial intelligence techniques in the control plane, it is

possible to classify attackers and legitimate users based on historical data and effectively identify attackers based on their characteristics, effectively securing the SDN control plane. The subnet is blocked to restrict the access of potential attackers. However, at present, artificial intelligence-based network security methods applied to the control plane still lack real-time feedback for attack evaluation, and only historical data cannot be accurately identified for new attacks. [26]

2.9.3 Application plane

The SDN application plane consists of several applications that can be programmed to submit the requested network behavior to the controller through the northbound interface. Research based on the application plane is broadly divided between the development of northbound interfaces and the development of SDN applications. Traditional networks began to think about dynamic and flexible traffic problems as early as the description of Google's B4 architecture, which provided network connectivity between data centers, specifically for synchronizing data replication, pushing indexes for interactive service systems, and computing availability copies of user data, but the architecture was still unable to effectively handle dynamic traffic problems.[27]

Artificial intelligence-related technologies combined with SDN can be a good solution to these problems. For example, Shi et al. propose a new feature optimization method and feature selection algorithm for robust optimal traffic based on deep learning, which uses the feature of removing the irrelevance of network traffic datasets to ensure symmetry, and then generates a corresponding model based on deep learning to apply the feature. However, Internet traffic has complex nonlinear characteristics, and the existing feature selection (FS) techniques are not very robust for traffic classification and cannot reliably provide optimal and stable features for machine learning (ML) algorithms. To solve the above problems, Shi et al. proposed a new feature extraction and selection method based on the existing algorithms: first, using the wavelet prior multifractal formalism, multifractal features are extracted from the flow stream to describe the flow stream; then, the FS method based on principal component analysis is applied to these multifractal features, and the irrelevant and redundant features are removed to obtain the desired features. [28][29]

Other studies include stream-based classification by comparing different types of Internet traffic and content delivery traffic by Bayesian networks, decision trees, and multilayer perceptrons, investigating the amount of training data on which different traffic classification performances depend, and deriving the results of Bayesian networks and decision trees that are suitable for high-speed Internet traffic classification.[30][31]

Chapter 3: AI in Enterprise Networking

3.1 Evolution of enterprise networks

Pere Monclus, VMware's vice president and chief technical officer of networking and security, says, once commented that networking nowadays is no longer about connecting machines with cables. Instead, networking is about connecting any device and any application across any cloud. As a result, networking nowadays is all about this matrix of connectedness between users, programs, and data, according to Monclus.

The term engagement is altered when networking technology is defined in this way. Monclus explains that networking now refers to how networks perform rather than how their physical components are configured.

That's a significant distinction. It introduces the concept of intent-based networking, in which a network is structured to support, detect, and protect the applications running on it, based on how an organization wants it to behave.

The network's relationship to applications is also flipped with this expanded definition. It's now all about the app, as Rajiv Ramaswami, VMware's Chief Operating Officer for products and cloud computing, pointed out that networking is changing toward offering a set of capabilities and services to the application. That's where AI comes into play in terms of networking's potential future.

Automation and machine learning, two AI capabilities now built-in networking, improve the speed and quality of every part of the application lifecycle, from autonomous provisioning and deployment to security and connectivity across private and public clouds.

As artificial intelligence (AI) becomes more prevalent in networking processes, the networking industry as a whole will shift from components to capabilities. [32]

With the rapid use of Intent-Based Networking (IBN), Network Orchestration, AI, ML, IoT, SD-WAN, and other advanced technologies, network automation is taking on a new look. AI is assisting networks in becoming more experience-centric, facilitating intelligent decisions by offering a seamless experience to the user. IBN reduces human interaction, downtimes, and delivery time by combining AI, machine learning, and network orchestration to provide safe optimization and automation of network processes.

IBN's market value is predicted to exceed $4 billion by 2026, according to a recent analysis by Global Market Insights. The market is predicted to significantly increase as demand for network

infrastructure management that is aligned with corporate processes and goals grows.

Mapping the business goal with the network and offering The four capabilities needed for a comprehensive IBN using AI (according to Gartner) are:

Validation and translation

The implementation that is fully automated

Knowledge of the current state of the network

Assurance and optimization in real-time

The entire process, as well as the feedback generated, is essentially AI-driven. By knowing about the role of AI in IBN more, we can better comprehend the role of AI in this entire "mapping the intent" process.

The business goal is defined by the network operator and presented in human language. Natural language processing (NLP) and Deep Neural networks are then used to convert the intent into regulations, bridging the intent with the networking-specific framework and allowing for easy and automated execution. To make this procedure more efficient and secure, various validation and authentication modules have been introduced.

Any incident, such as a bandwidth constraint, is identified after it has occurred in traditional networks. For scanning the network and recognizing the difficulties that are likely to develop in the event of a breakdown, AI-driven networks combine real-time predictive analytics with the capability of visualization. Such networks are also capable of dynamically optimizing operations via a feedback loop.

It is critical that the network runs smoothly and safely. Advanced simulations can be done to detect and fix loopholes, as advanced neural nets understand the domain and latent space of the data. [33]

3.2 AI technologies in enterprise networks

Network automation and AI/ML

Through analytics and AI/ML, IT can gather insights that lead to more trusted automation processes, lowering network operations costs and providing users with the best possible connected experience. These technologies aid IT automation in the following areas:

- deploying and managing network policies
- integrating zero-trust security solutions to ensure network consistency
- identifying and classifying network devices

AI will enable networks to learn, self-optimize continuously, and even forecast and correct service degradation before it occurs as time goes on.

AI and ML models

Users can observe network-health benchmarks based on network data collected over time using powerful AI/ML algorithms. The following are some suggestions for network optimization:

- Long-term variations in performance patterns
- Comparison of network health inside an organization or with industry peers

AI/ML and telemetry

AI/ML engines can ingest and process Telemetry data from the network via a network controller and management dashboard to:

- Identify abnormalities
- Eliminate false positives
- Make recommendations for improvement

AI and machine reasoning (MR)

Another major category of AI is machine reasoning (MR). Machine reasoning navigates a series of alternative outcomes toward an ideal end using the acquired information. MR is highly suited to tackling challenges that necessitate extensive domain knowledge. For a machine reasoner to operate on fresh data, humans must explicitly capture all knowledge a priori. Because it may build on the conclusions offered by ML and investigate probable causes and improvement

choices, MR is an excellent complement to ML.

AI/ML and predictive analytics

Simply described, predictive analytics is the application of machine learning to predict events of interest, such as failures or performance difficulties, using a model trained on past data. The system can model the network and decide where and when measures should be made to prevent network degradation or failures using mid- and long-term prediction methodologies. [34]

3.3 Use cases of AI in enterprise networking

AI/ML for improving Wi-Fi performance

NetOps staff can be forewarned of spikes in Wi-Fi interference, network congestion, and office traffic loads using machine learning. System-generated insights can assist in predicting future incidents and inform IT professionals with suggestions for corrective measures by learning how a sequence of events is correlated.

AI/ML for tracking IoT endpoints

Internet of Things (IoT) deployments benefit from AI/ML. IoT devices have a wide range of applications and might be difficult to identify and categorize. Using network probes or application layer discovery techniques, IT teams can utilize machine learning algorithms to find IoT endpoints.

Machine learning for policy automation

Machine learning can look at traffic flows from endpoint groups and provide specific information like source and destination, service, protocol, and port numbers. These data can be used to create policies that allow or disallow interactions between various groupings of devices, users, and apps.

Machine reasoning for improved lifecycle management

Machine reasoning can go through tens of thousands of network devices to ensure that all devices have the most recent software image and to hunt for any configuration flaws. If an operations team isn't using the most recent update features, it can raise a red alert. [34]

Detecting time series anomalies

Many of the devices on today's networks were created more than two decades ago and can not handle modern management messages. AI can discover time series anomalies with a correlation, allowing network engineers to swiftly identify links between occurrences that would otherwise be

missed by even the most experienced network professional.

Event correlation and root cause analysis

In a range of minutes, AI can analyze terabytes of data using various data-mining techniques. This capability allows IT departments to quickly determine which network feature (for example, OS, device type, access point, or switch) is most related to a network problem, allowing them to resolve the issue faster.

Predicting user experiences

Currently, application bandwidth apportionment is generally accomplished through capacity planning and manual modifications. AI will soon be able to forecast a user's Internet performance, allowing a system to dynamically alter bandwidth capacity based on which applications are being used at any given time. Predictive analysis based on previous trends and current calendar information will replace manual planning.

Self-driving

AI allows IT systems to self-correct for optimal uptime and propose prescriptive methods for resolving issues. Furthermore, AI-driven networks can capture and save data prior to a network event or outage, which helps to debug faster. [12]

3.4 AI Solves Specific Problems in SDN

Artificial intelligence can perform data analysis and network optimization based on the centralized control and management of SDN to make the management more intelligent.

3.4.1 Intelligent routing optimization methods

Routing is a fundamental function of the network. In SDN networks, the controller controls the routing of traffic by modifying the switch's flow table, directing the switch to drop a flow or route it to a specified path. Inefficient routing policies can lead to data loss, load imbalance and resource waste. Therefore, a good routing policy is important for network data transmission. Currently, most of the routing policies are optimized or improved based on the shortest path first policy or heuristic algorithms. The research on routing under the integration of software-defined networks with AI includes both routing policy optimization and research on software-defined routing.

3.4.1.1 Policy Optimization

SDN is proposed to solve the problem of increasing network complexity due to centralized management difficulties, vendor dependencies and process changes. In current SDN networks, the routing algorithm is mostly based on Dijkstra's algorithm, which selects the shortest flow path to deliver packets. However, considering only the length of the path without considering other parameters such as bandwidth overhead can lead to network congestion when a large amount of traffic enters the network.

To solve the above problem, researchers consider combining artificial intelligence approaches to plan routing algorithms. Mhdawi et al. develop an intelligent power reduction decision routing protocol (IPRDR) in a medium-sized hybrid software-defined network data center environment. This algorithm routes large traffic to highly indexed devices with optimal power paths based on calculated metric values and aggregates and isolates them. Kim et al. propose a Q-learning-based mechanism for efficient SDN routing to prevent network congestion, which can greatly improve network congestion by re-routing paths and changing flow tables using predefined thresholds and Q-learning routing algorithms.[35][36]

However, these methods are only applicable to fixed traffic generation patterns and bandwidth sizes. In order to meet more complex network conditions, more complex and scalable factors need to be considered. Pasca et al. optimize routing policies from the perspective of traffic

prioritization, arguing that traffic should be prioritized and that scheduling traffic with high priority can be done first to effectively avoid multiple flows competing for limited resources. Based on this, an application-aware multipath packet forwarding framework is proposed, which integrates machine learning and SDN to prioritize each flow using a machine learning algorithm, and routes the flows according to their priority and network state using SDN. However, the above algorithm does not take into account user experience and some QoS requirements in the classification step of the application when performing the multipath assignment.[37]

With the development of wireless networks, efficient network traffic control such as routing methods in wireless backbone networks has become a key challenge due to the fact that traditional routing protocols do not learn network anomalies, such as congestion, from historical experience, so intelligent network traffic control methods are the key to solve such problems. To address this problem, Mao et al. propose a new real-time deep learning-based intelligent network traffic control method that uses deep convolutional neural networks (DCNNs) with unique input and output characteristics to represent the considered wireless mesh network (WMN) backbone to reduce the average delay and packet loss rate.[38][39]

3.4.1.2 Software-Defined Routing

The way the Internet core and wired/wireless heterogeneous backbone networks are built has remained largely unchanged over the years, so in essence, the main algorithms behind routers are very similar in principle. To accommodate the growing size of the network, IT teams continue to expand the Internet core data by adding more and larger routers and more links. Advances in software-driven routing policies have always seemed to lag behind popular routing policies, but software-defined routing (SDR), also known as programmable routers, provides a cost-effective packet processing platform with easy scalability and programmability. Academic and industry researchers have shown great interest in using CPUs or GPUs to provide multi-core or threaded parallel operation of routing tasks to increase processor processing throughput, and multi-core platforms have significantly increased the parallel computing power of SDRs, enabling them to employ artificial intelligence techniques, namely deep learning, to manage routing paths.[40][41]

There are many scholars working on SDR. For example, Mao et al. used supervised DBA to calculate the traffic patterns of subsequent nodes and edge routers as input and a deep learning-based routing table construction method. Simulation results show that the routing method based on a deep learning approach can indeed greatly improve the control of backbone routing. However, this method does not consider the security issues at the network layer. Geyer et al.

proposed a graph-based deep learning method for generating distributed routing protocols, which is independent of the underlying structure of the topology and therefore applied to a wider range of network topologies than the method of Mao et al. SDR provides flexibility for programming network devices to achieve different goals and eliminates the need for third-party vendor-specific hardware.[42][43]

3.4.2 Intelligent Approach to Network Security

SDN manages the entire network with a central controller to simplify network management. While this management mechanism provides users with good network programmability, it also exposes the core of the entire network to attackers, who can access the center of the network only by coding, exposing the SDN network to the risk of attack and reducing the security of the entire network.

Wang et al. reviewed the SDN network security mechanism and analyzed and summarized the typical security threats in SDN. They discussed SDN security in detail in terms of the development of SDN security controller, the development and deployment of controller combinable security module library, controller DoS/DDoS attack defense methods, flow rule legitimacy and consistency detection northbound interface and application security, etc. The global network view of the SDN controller simplifies the collection and analysis of network traffic. In addition, the programmability of SDN provides the network with the ability to react immediately when an attack is detected. In SDN networks, there has been a lot of research on artificial intelligence-based intrusion detection, such as **intrusion detection** and **DDoS attack detection**. [44]

The purpose of **intrusion detection** is to identify whether access is normal or not and to secure the network by classifying traffic into normal and attack flows and blocking abnormal access. Artificial intelligence methods use a set of attributes and associated labels to describe each flow, based on the type of attributes, to determine the relevant techniques used for anomaly detection. For example, Sanda et al. use the predicted output of machine learning algorithms to define security rules for SDN controllers to prevent malicious users from accessing the network. They used four machine learning methods, C4.5, decision tables, Bayesian networks, and plain Bayesian algorithms, to predict the host of an attack based on historical data. However, in the method of classifying access flows using artificial intelligence methods, only specific attacks can be addressed, or specific defense methods proposed and do not address the basic needs of detecting and controlling malicious or suspicious traffic.[45]

In addition, there are still many undiscovered vulnerabilities in the SDN controller that attackers can exploit to continue to threaten the SDN. Therefore, it is important to create a comprehensive security design that can defend against a variety of vulnerabilities in the SDN to defend against various potential attacks. To address the above issues, Song et al. propose a network intrusion detection system based on SDN and machine learning techniques for sensing real-time threats, introduce an intrusion response system that uses reactive routing for impact analysis in SDN, implement the prototype in an open-source project in SDN, and evaluate the proposed system using publicly archived data from the network and real-time data. Anderson et al. proposed ATLANTIC, an anomaly detection, classification and mitigation framework for SDN-based networks, which consists of a lightweight phase responsible for monitoring traffic and a heavyweight phase responsible for anomaly classification and mitigation: the lightweight phase uses information theory to compute deviations from flow table entropy, and the heavyweight phase uses SVM algorithms to classify anomalous traffic. Depending on the magnitude, different methods are used to classify traffic anomalies and to block malicious traffic by using the information collected to process each traffic profile in a specific way.[46][47]

DDoS attacks are a major threat to the security of SDN networks. The goal of DDoS attacks is to exhaust system resources by using many puppet machines to send a large number of fake requests at the same time, thus making it impossible to satisfy the requests of legitimate users. In SDN networks, DDoS attacks can deplete network, storage, and computational resources in the data plane and control plane, making the SDN network unavailable. Therefore, DDoS attack detection is essential for the normal operation of SDN networks.

Artificial intelligence techniques can be applied to distinguish network traffic based on certain features associated with traffic characteristics and classify them as malicious or benign to mitigate intrusions and DDoS attacks on SDN controllers or switches. Niyaz et al. built the system as a network application on SDN controllers and used deep learning algorithms to reduce the large number of features derived from network packet headers. They proposed a deep-learning-based multi-vector DDoS detection system in an SDN environment. However, none of the above algorithms has the ability to extract features directly from the original bytes but reduce the feature dimension from the derived features. Chen et al. start from the SDN controller perspective and improve the decision tree method by combining the classifier XGBoost to perform DDoS detection using the collected stream packet dataset. However, up to now, SDN-based DDoS traffic detection still cannot meet the application-specific requirements of DDoS attack detection. Among them, the traffic threshold for DDoS attack detection may vary from

application to application, yet the existing solutions do not implement any mechanism to meet this important requirement and set the corresponding constraints.[48][49][50][51]

In addition, DDoS traffic inspection with SDN is often performed using a single controller as the solution, which not only causes bottlenecks in network traffic but also leads to a single point of failure in the SDN network. Although SDN can integrate distributed platforms and centralize control of the entire network, existing solutions have not yet realized their full potential.

3.4.3 Artificial intelligence-based traffic engineering

Traffic engineering (TE) is an important mechanism for optimizing the performance of data networks by dynamically analyzing, predicting, and regulating the behavior of transmitted data. To date, most of the work done in conjunction with SDN research has been focused on developing SDN architectures rather than developing TE tools for SDN. SDN dramatically simplifies network management, reduces operational costs, and facilitates innovation and growth in current and future networks. These unique features of SDN provide tremendous momentum for new TE technologies that can be leveraged to better control traffic and manage global network views, state, and flow pattern characteristics.

The advantage of SDN-based traffic engineering is that Internet applications require an underlying network architecture that can react in real-time and scale for large volumes of traffic. The architecture should be able to classify various traffic types from different applications and provide appropriate specific services for each traffic type in a very short period of time; secondly, in the face of the rapid growth of cloud computing and the needs of large-scale data centers, appropriate network management should be able to improve resource utilization to obtain better system performance. Therefore, an urgent need for new network architecture and more intelligent and efficient TE tools.

By combining artificial intelligence technologies to identify different traffic types and provide a fine-grained network management approach for SDN networks, network operators can more effectively handle different services and allocate network resources and achieve efficient and accurate network optimization by predicting the dynamic changes of traffic and designing corresponding response strategies. Artificial intelligence-based traffic engineering is broadly divided into traffic classification identification and dynamic traffic scheduling optimization. The following is a brief overview of the research related to AI-based traffic engineering methods.

3.4.3.1 Traffic Classification

SDN-based data traffic has different characteristics in different contexts, and there are two ways to classify traffic: one is to **classify traffic into elephant and mouse flows**, where elephant flows are large and continuous flows, and mouse flows are small and short flows; the other is to **classify traffic according to QoS**.[52][53][54]

In the data center, 80% of the traffic is mice flow, but 20% of the elephant flow occupies 80% of the bandwidth, so it is important to identify elephant traffic and mice traffic to accurately identify data center traffic and achieve appropriate network traffic scheduling. SDN provides flexible management for data center networks through traffic control. However, this fine-grained management consumes a lot of bandwidth between the data and control planes, resulting in bottlenecks in the scalability of SDN-based data centers. The "elephant and mice phenomenon" shows that only a very small amount of elephant traffic carries the majority of bytes in the data center, so it can be improved by detecting and rerouting elephant traffic to improve management. However, existing mechanisms for elephant traffic detection face the challenges of high bandwidth consumption and long detection times.

To solve the above problem, Tang et al. proposed an efficient sampling and classification approach (ESCA) for elephant traffic detection. In the first stage, ESCA improves the sampling efficiency by estimating the arrival time interval of elephant traffic and filtering out redundant samples using a filter traffic table; in the second stage, ESCA uses a new supervised classification algorithm to classify samples based on the correlation between data streams. The elephant traffic detection is achieved by these two stages. Since the redundant part of the data is filtered, the bandwidth consumption and computation time of the whole system are reduced. However, the drawbacks based on this approach are: on the one hand, it cannot meet the granularity requirements of SDN data centers and campus networks; on the other hand, the huge computational overhead reduces the scalability of the measurement framework.[55]

QoS-aware traffic classification aims to identify the QoS classes of traffic. With the exponential growth of applications on the Internet, it is difficult and impractical to identify all applications. However, applications can be classified into different QoS classes based on their QoS requirements (e.g., latency, jitter, and loss rate). Many different applications may belong to one QoS class, so classifying traffic according to its QoS requirements is a more efficient approach. The application of artificial intelligence algorithms enables: (a) multidimensional key performance indicators (KPI) analysis and discovery of new correlations, performing root cause

analysis and predicting QoS violations; (b) implementation of data cleaning techniques to deal with incomplete, missing or corrupted data; and (c) support for robust and scalable architectures, that can collect data from both the virtual and real worlds. Thus, artificial intelligence algorithms are able to meet QoS prediction in big data scenarios and discover more correlations between rules.[56]

3.4.3.2 Traffic Scheduling

The high variability of spatial and temporal traffic in modern networks requires the network to continuously change its processing strategy to maintain near-optimal network performance. Geyer et al. suggest that current telecommunications networks exhibit inherent variability in many different planes and time scales, such as unexpected fiber failures and rapid fluctuations in wireless channel quality due to multipath fading. Also, the increasing use of smartphones and tablets as the primary Internet access devices for users has caused traffic demand to change in response to the popularity of content. These and other factors lead to frequent and large fluctuations in traffic demand over time and space. As a result, traffic has the properties of variability and volatility. To ensure the stability of the network, it is necessary to maintain good system performance under different input (i.e., network and traffic) conditions. In addition, considering the occurrence of traffic surges, the actual performance of the system does not always follow the performance predicted by the optimization model. Therefore, online networking optimization (ONO) must satisfy that the performance of most of the predicted traffic conditions is optimal or at least stable when the actual traffic conditions deviate from the predicted conditions.[57]

The flow table matching strategy in SDN networks can reflect the dynamic processing of network traffic. Based on the classification method, Su et al. analyzed the structure of packets and proposed a field-based matching model for packets, F-OpenFlow. The method proposes: firstly, to improve the probability of matching table items by grouping matching fields; then, to analyze the structure of flow tables in existing networks by using metaspace search to find the same type of matching rules; then, to integrate the analysis model with dictionary tree by using metaspace method to process the fields in dynamic networks to obtain the corresponding rules and match the corresponding policies, thus achieving efficient and accurate network optimization. However, the above method does not use the historical data for matching, which leads to the inaccuracy of the relationship between the analyzed message location and the flow table, and does not guarantee the improvement of the hit rate and matching speed of the flow table.[58]

3.4.3.3 Traffic prediction

Network traffic is self-similar, multi-scale, long-range dependent, and highly non-linear (as modeled by Poisson and Gaussian models), and these statistical properties determine the predictability of traffic. Having accurate and timely traffic data is essential for most network operations management tasks, such as traffic computation, short-time traffic scheduling or rerouting, long-term capacity planning, network design, and network anomaly detection. For example, when network congestion occurs, traditional routing protocols do not respond immediately to adjust traffic distribution, resulting in high latency, packet loss and jitter. Especially in the case of high-volume traffic detection and DDoS prediction, proactive prediction-based approaches will be faster due to early warning. Similarly, after the network has been significantly affected, predicting network congestion is more effective than the reactive approach of detecting congestion through measurements.

Considering the above situation, Azzouni et al. proposed a dynamic routing framework called NeuRoute. In NeuRoute, the long short-term memory (LSTM) module is used to estimate future network traffic. The method trains the neural network model by inputting the network state and the estimated network traffic, and the corresponding routing solution computed by the heuristic algorithm is the output. Polson et al. developed a deep learning model to predict traffic, and their main contribution is to develop a linear model that combines the use of l-regularization and a series of hyperbolic tangent layers to solve the problem of sharp nonlinear transitions between free flow, failure, recovery, and congestion in predicted traffic, and to demonstrate that the deep learning architecture can capture these nonlinear spatiotemporal effects. Therefore, the deep learning approach to traffic prediction is used to perform traffic prediction while acquiring network traffic data to achieve intelligent routing.[59][60]

Although artificial intelligence methods can solve traffic prediction problems, it is difficult to say that one method is clearly superior to the other in any case. One reason is that the proposed model is developed using a small amount of individual traffic-specific data, and the accuracy of the traffic prediction method depends on the traffic characteristics embedded in the collected traffic data. Moreover, in general, when neural network related algorithms are applied to traffic prediction, the predictive power and robustness of the model are better than the general model. In general, existing traffic prediction methods mainly use shallow traffic prediction models and still do not satisfy many practical applications.

3.5 AI-Driven Operations (AIOps)

3.5.1 Stages of IT ops development

IT ops are divided into three stages, which are traditional ops, automated ops, and AIOps.

Traditional ops are the primary stage of IT Ops. It is a reactive, after-the-fact rescue approach. In traditional ops, after the system problem, the relevant departments will contact the operations and maintenance engineers, and the operations and maintenance engineers receive the information, use the VPN to log into the intranet to view the monitoring indicators, use their experience to troubleshoot, spend a lot of time to locate the fault, and then repair operations, and finally, the fault is restored. The traditional ops have the following problems: the system takes a long time to repair; the operation is prone to errors; as the business grows, the number of alarms increases and cannot be handled in a timely manner, leading to a decrease in website availability.

Automated operation and maintenance is the second stage of IT operation and maintenance, which is based on the generation of a large number of automation scripts, using automation scripts to monitor the system and resources. Automation scripts usually set some thresholds, when the script detects that a certain indicator has broken through the set reading value, it will trigger the relevant alarm, and then the automation script will call some set processes for troubleshooting, such as restarting the service, restarting the host, etc., to ensure that the system continues to run. The automation script can also perform some periodic work, such as virus check and kill, backup data, etc., in order to reduce human operation links and improve the efficiency of operation and maintenance. Although automated operations and maintenance compared to traditional operations and maintenance to reduce the human operation process, to a certain extent to improve efficiency, but is still an immature, intelligent degree of low operations and maintenance, such as still prone to serious leakage and false alarms, can not locate and solve the root cause of the failure, only through a simple restart way to restore services. [61]

Therefore, here comes the AIOps.

3.5.2 What is AIOps?

Artificial intelligence for IT operations, or AIOps, is a phrase coined by Gartner. It is the strategic application of artificial intelligence (AI), machine learning (ML), and machine reasoning (MR) technologies across IT operations to simplify and streamline processes, optimize the use of IT resources, and make faster, more accurate decisions and respond to network and system incidents more quickly. [62][63]

In real-time or near-real-time, AIOps contextualizes considerable telemetry and logs data throughout an organization's IT infrastructure. The data is then combined with relevant historical data to produce meaningful insights. AIOps is a virtual assistant with an extensive understanding of the IT and network environments, as well as the capacity to apply that information to deliver real-time analysis and execute or recommend next steps. [63]

The proliferation of gadgets, data, and people has made IT infrastructure more complicated than ever to maintain, prompting many to turn to AI and Machine Learning for assistance. By automating important processes, proactively addressing issues before they happen, and providing a unique insight into user, device, and application behavior, AIOps takes the complexity out of developing IT networks. [64]

3.5.3 Is AIOps a platform?

In order to install and operate AIOps, enterprises must synchronize multiple software and hardware components with AI and ML engines and specialized servers, as well as human knowledge.

Many service providers offer AIOps solutions that combine big data with AI, machine learning, and machine learning capabilities. These solutions make event monitoring, service administration, and other tasks easier and more automated. These solutions are commonly referred to as AIOps platforms by most providers.

AIOps is, above all, a method of modernizing IT operations in all areas—including network operations (NetOps), security operations (SecOps), and development operations (DevOps)—by integrating systems and data and intelligently automating IT using advanced technologies such as AI.

3.5.4 What else is required to implement AIOps?

Without the ability to integrate its IT systems so that those systems can share information and learn from one another, a company cannot implement AIOps. An open application programming interface (API) is required for systems integration; in other words, the product manufacturer makes the API publicly available to software developers.

Setting up AIOps also necessitates the use of software development kits (SDKs). These toolkits are used by developers to create custom applications that may be added to or connected to other programmers. [62]

3.5.5 Why Is AIOps Important?

Individual apps and services become more efficient and perform better as a result of AIOps. AIOps improves everything from security and outage issue reaction times to infrastructure purchasing for organizations that use it as part of their automated infrastructure and operations workflows. AIOps is viewed by those who are just getting started as an investment in performance analysis, anomaly detection, and event correlation that allows them to predict future network-impacting occurrences. [63]

3.5.6 Benefits of AIOps

Time and cost savings

IT departments waste a lot of time on processes that could be automated. IT personnel may, for example, stop spending hours resolving network failures and instead resolve them with a single click, thanks to AIOps.

Every minute saved through automation on a daily basis—10 minutes on one activity, 15 minutes on another—adds up to considerable annual IT cost savings for organizations.

Businesses that adopt an AIOps strategy may also detect and fix IT issues faster, prioritize issues more efficiently, and improve the overall performance of their IT organization and its many teams, such as SecOps, DevOps and NetOps.

All of the aforementioned factors can help a company's efficiency, productivity, and bottom line.

Force multiplying of IT capabilities

Instead of tiresome, manual labor, AIOps allows experienced engineers to devote their time and skills to more value-added activities, such as business innovation.

AIOps can also assist an IT organization in bridging skills gaps. Less-experienced team members can use AI, ML, or MR capabilities built into IT operations to swiftly troubleshoot issues without having to escalate to more experienced staff.

AIOps can also assist in providing insights that allow IT workers to make faster and more accurate decisions. AIOps can jointly notify those teams of problems or opportunities that they can act on together by sitting between diverse systems for SecOps, DevOps, NetOps, and other areas of IT.

Accelerating digital transformation

When a company incorporates AI, ML, and MR into its systems and connects them using APIs and SDKs, more information is shared across those systems. This allows AI, ML, and MR tools and solutions to become smarter over time and perform even better. These technologies must consume large amounts of data for learning.

Another advantage of establishing and extending AIOps is that it speeds up digital transformation. AIOps enables the company to make greater use of data, analytics, and automation across all aspects of IT, allowing it to do things like:

- Quickly develop new products and services
- Gain a better understanding of customers and provide them with unique experiences
- Lower risk and boost agility and resiliency

It gets easier to digitally transform the entire organization as more business sectors become digitized and interconnected. [62]

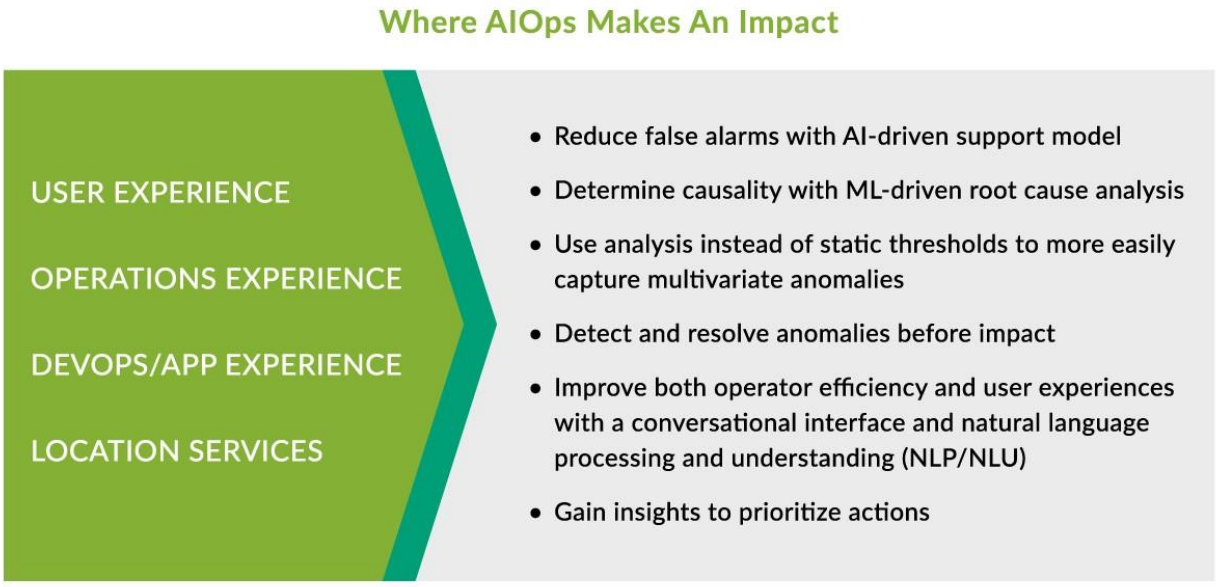

Figure 11. Where AIOps Makes An Impact [63]

3.5.7 Deployment of AIOps

Look for quick wins

AIOps is all about assisting IT teams in collaborating more effectively and optimizing IT operations. Look for obvious areas in IT where AI, ML, and MR could have a positive influence

by saving time and allowing IT workers to make faster choices. Because many operations are routine and maybe easily automated, IT technical assistance is frequently a starting point for AIOps.

Adopt open technology

The inability of legacy hardware and software to communicate with one another is a common roadblock to AIOps implementation. They are unable to share data because they were not meant to do so and cannot be configured to do so. Those looking to integrate AIOps into their IT operations should look for systems that follow open standards. They'll prefer to collaborate with providers who offer open APIs and SDKs for integrating systems and modifying them.

Organizations will also want to ensure that data telemetry is an open standard. Some suppliers regard their devices' telemetry to be confidential, and they charge customers a price to access it. This can make integrating some systems and data into AIOps difficult or expensive.

Start linking systems together

The next step is for the business to integrate and configure systems via APIs and SDKs once it has an initial AIOps plan and has integrated AI, ML, and MR into systems in a few areas of its IT operations. AIOps begins with the linking of these select systems so that they can begin sharing data and learning from one another. [62]

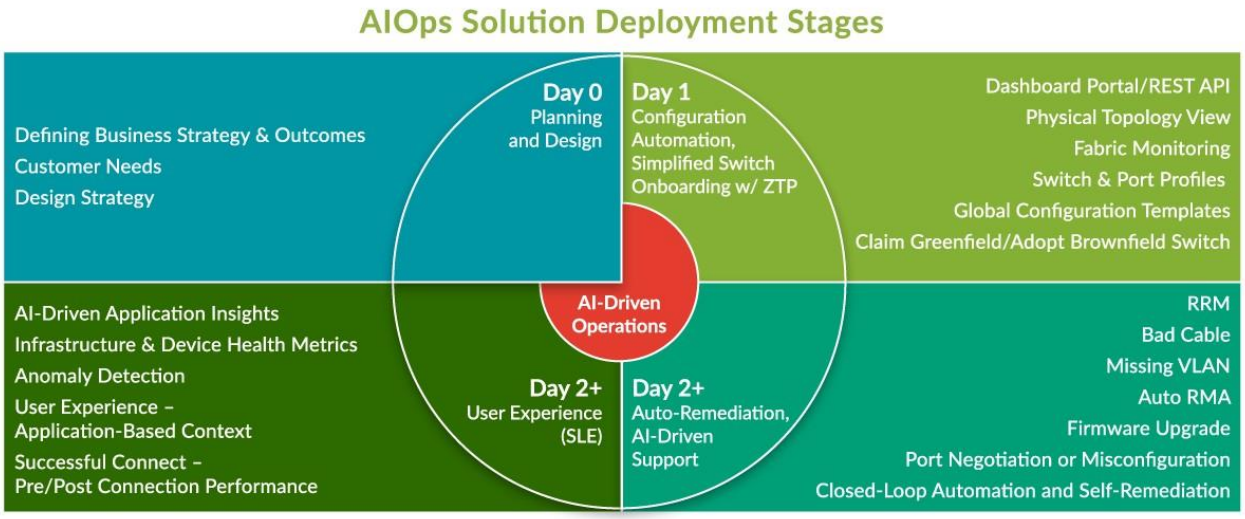

Figure 12. AIOps Solution Deployment Stage [63]

3.5.8 Open source vs. proprietary AIOps tools

The debate about open source versus proprietary tools is not new. But in the case of AIOps tools, there are other special factors to consider.

Not only is the AIOps tool market particularly complex, but the tools in question always have many unique qualities, such as the need to access sensitive data, often further influencing the specific judgment of the purchaser in terms of evaluation.

Open Source AIOps Tools

As of today, only a few open-source projects label themselves as AIOps, but many open-source platforms offer certain features that are fully compatible with the AIOps philosophy. For example, Kubernetes, which uses data analytics (to some extent) to automate workflow orchestration, is an important feature of AIOps platforms, and open source monitoring platforms such as Nagios and Zabbix can also provide some of the basic AIOps analytics functionality. In addition, various open-source programming language modules or frameworks, such as PyTorch and TensorFlow, also contribute to AIOps functionality, but these are clearly not complete AIOps platforms.

From all perspectives, the arguments in favor of open-source AIOps tools are largely along the same lines as those in favor of the open-source ecosystem as a whole, which tend to be less expensive and easier to modify or customize than proprietary alternatives, while also reducing the risk of vendor and platform lock-in.

Beyond that, there are some special considerations to keep in mind when evaluating open source AIOps tools. First, no end-to-end open source AIOps platform has emerged to date. In other words, no single open-source platform can directly provide enterprises with all the necessary AIOps functionality to streamline IT operations. Instead, a number of different open-source tools need to be integrated, each providing only a portion of the AIOps functionality. To use these open source tools and take full advantage of AIOps, IT operations teams are faced with a large number of tool options and, naturally, a lot of effort.

On top of that, AIOps tools, by their very nature, require access to large amounts of data, some of which can be quite sensitive or could be used by an attacker to launch an intrusion or even sabotage. This means that with proprietary AIOps tools, the buyer must trust the vendor and allow the latter to be a competent steward in extracting and analyzing data in the customer's systems and environment. In addition, compliance issues are important, and a number of laws now govern scenarios in which vendor tools move user data within their own infrastructure for processing or storage.

If the platform needs to leverage external infrastructure for data processing, then open source AIOps tools are subject to the same impact. But most open-source tools run primarily within a user's own data center, or at least on top of user-controlled public cloud infrastructure, and therefore pose generally less compliance or data privacy issues. After all, everyone can observe the source code of an open-source tool to determine how the project handles user information, enhancing the transparency and credibility of the data management process.

Proprietary AIOps Tools

In contrast to the open-source space, the proprietary software market has seen the emergence of a large number of tools that are explicitly labeled as AIOps. For example, as we will analyze below, both Cisco and Juniper have introduced enterprise networking solutions that apply AIOps. As an overall trend, a growing number of proprietary monitoring and incident response tools are using AIOps to strengthen their market presence.

The core reason for choosing proprietary AIOps tools is that they tend to be less difficult to use than open-source options. Proprietary tools are generally more user-friendly, and the former tend to offer a broader range of AIOps functionality than open-source options. In addition, a significant portion of proprietary AIOps tools run as hosted services, so users do not have to go through the trouble of setting up their own infrastructure to host these services.

However, for some proprietary AIOps tools, the above data management issues may pose new challenges. As a result, the average enterprise must carefully evaluate a vendor's compliance safeguards and ability to prevent misuse of data when selecting a vendor. The good news is that most vendors in the AIOps space have a strong business reputation and experience in managing customer data in a compliant and secure manner.[65]

3.6 Juniper AIOps solutions

Mist AI unifies Juniper's wired access, wireless access, and SD-WAN technologies. End-to-end troubleshooting, self-driving network operations, and client-to-cloud insight into customer experiences are simplified with the AIops solution. Marvis VNA is also the first AI-powered Virtual Network Assistant with an interactive conversational interface that offers simple solutions to complicated challenges. All of these technologies, which are powered by Mist AI, save time and money while enhancing the network's value.

In addition, AI and machine learning are key components in other Juniper product areas, enabling critical functions such as network health and diagnostics with corrective actions (Paragon

Insights), intent-based networking and closed-loop assurance (Apstra), and real-time actionable intel for threat prevention and protection (Connected Security). [64]

3.6.1 Mist AI and Cloud

Mist AI optimizes user experiences and streamlines operations across the wireless, wired, and SD-WAN domains by combining artificial intelligence, machine learning, and data science methodologies.

For end-to-end insight into user experiences, data is ingested from a variety of sources, including Juniper Mist Access Points, Session Smart Routers, Switches, and Firewalls. These devices collaborate with Mist AI to improve user experiences from client to cloud, providing automatic event correlation, Self-Driving Network operations, root cause analysis, network assurance, proactive anomaly detection, and more.

Mist AI is also used by Juniper for next-generation customer assistance. Marvis, the industry's first AI-driven Virtual Network Assistant, uses a natural language conversational interface to provide significant information and direction to IT workers.

Operators save time and money using Mist AI since problems are resolved faster and fewer onsite visits are required. Users gain from the more predictable, dependable, and measurable network infrastructure. [66]

3.6.2 Juniper Mist Wi-Fi Assurance

Juniper Mist is based on a new microservices cloud architecture that allows for elastic scalability to suit changing wired and wireless network market demands. The platform provides operational simplicity, API-based programmability, and consumer involvement via location-based services.

Wi-Fi Assurance automates wireless operations in place of manual troubleshooting. With outstanding visibility into user service levels, this subscription service makes Wi-Fi predictable, reliable, and measurable. The IT staff, for example, can set up and monitor service-level thresholds for critical wireless criteria.

With Radio Resource Management (RRM) at the client level, anomaly detection automates triggers to record packets for event correlation and creates network intelligence. These features provide IT teams with unprecedented access into each user's wireless network experience, allowing them to reliably extend Wi-Fi quality to end-users.

Juniper Mist cloud services are completely programmable, with all functionalities (provisioning, monitoring, and alarms) accessible via open APIs, allowing IT teams to interact with IT applications to automate network and line-of-business activities

Key Benefits of Wi-Fi Assurance

Maximize Wi-Fi User Experience	Minimize IT Support Costs
Proactively optimize performance	Dynamic packet capture for troubleshooting
Prioritize applications, resources, and users	Proactive root cause identification
Gain simple and secure access to resources	Network automation with APIs

Table 5. Key Benefits of Wi-Fi Assurance

Set, Monitor, and Enforce Service Levels

Set up and monitor service-level thresholds for critical wireless pre- and post-connection parameters, including time to connect, capacity, coverage, and throughput. With comprehensive visibility and geographical context into impacted users, applications, and devices, the IT team can evaluate how the network is functioning versus service level expectations (SLEs) at any moment.

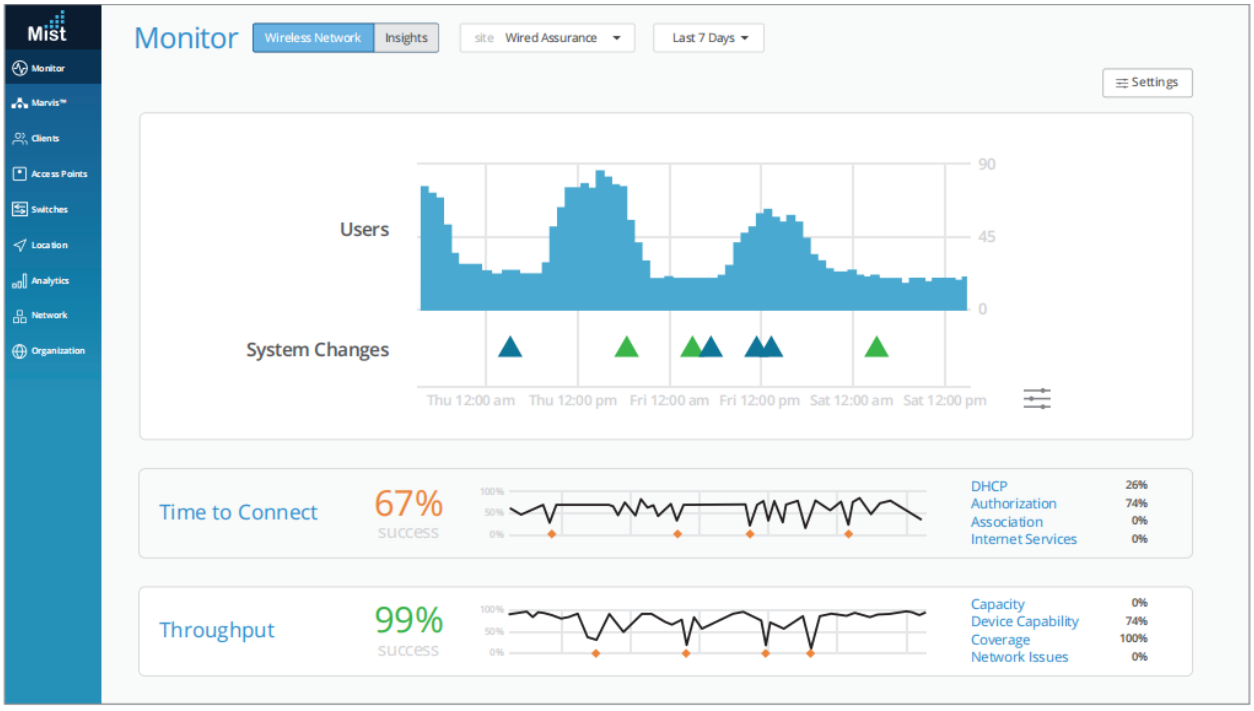

Figure13. Wi-Fi Assurance Monitor [67]

SLE Dashboard Analytics and Comprehensive Network Performance

The platform also gives a daily and weekly trend of the SLE metrics, in addition to proactively correlating events and delivering remediation advice. These reports provide unprecedented visibility into anomalies seen at the AP, device, application, and OS levels during the last week, allowing for longer-term trend research. The current set of available SLEs is Coverage, Capacity, WAN, Time to Connect, Successful Connects, AP Uptime, Throughput and Roaming.

Simple Root-Cause Analysis and Remediation

Juniper dynamically collects data from all endpoints and correlates it to quickly identify wireless, wired, and device issues. Every few seconds, over 150 state changes are recorded for each client device and access point. The IT team can swiftly address or avoid problems with predictive advice and automated workflows. This root cause analysis feature can be enhanced even more using the Marvis Virtual Network Assistant service.

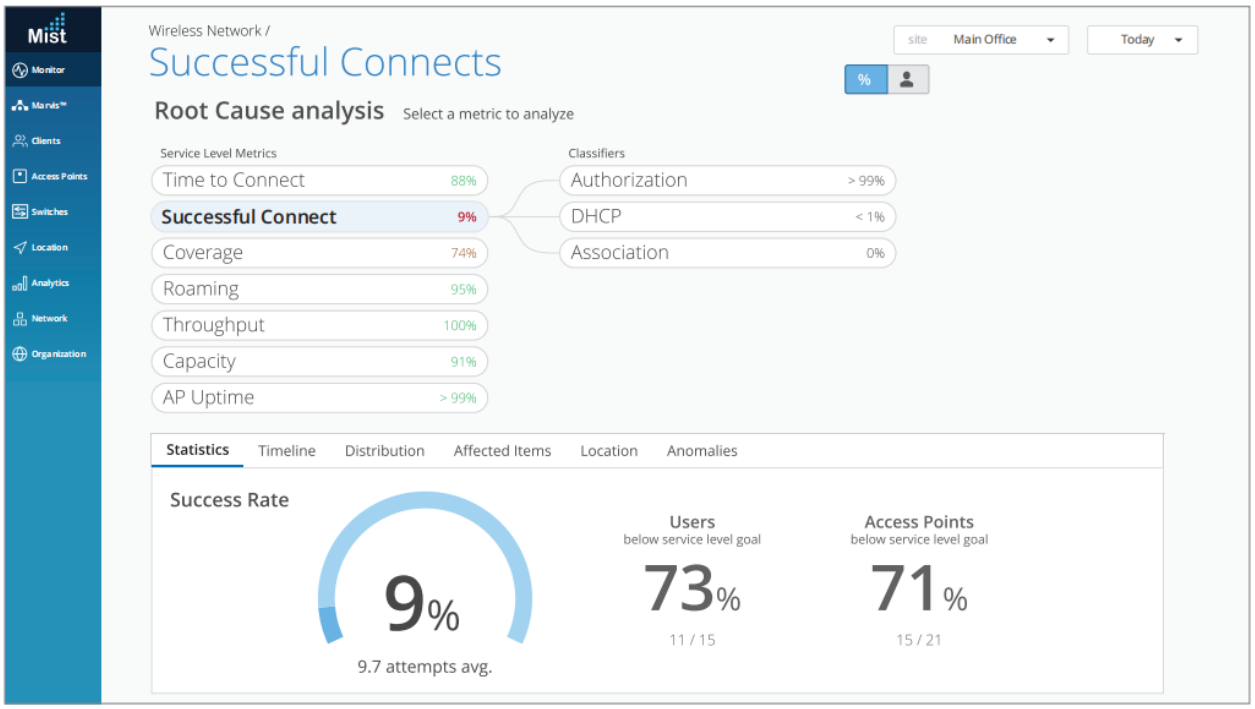

Figure14. Wi-Fi Assurance Root Cause analysis [67]

Automation for Deployment and Provisioning

The Juniper Mist platform is completely programmable, with open APIs allowing for full automation and seamless interaction with complementary products across the LAN, WAN, security, engagement, and asset location domains.

Network Rewind and Dynamic Packet Capture

When an anomaly is discovered, the Wi-Fi Assurance service instantly discovers and captures

packets. The IT staff can use this record to go back in time and check what was going on at the time the event occurred. It saves hours, if not days, of guesswork and time spent attempting to duplicate an issue.

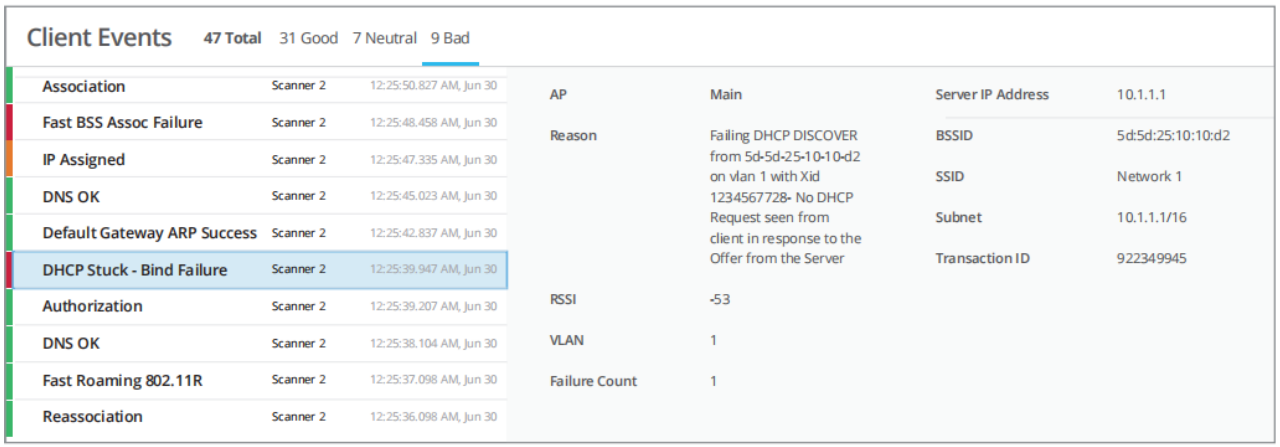

Figure15. Wi-Fi Assurance Client Events [67]

Client Profiling

Clients are profiled for device kinds, operating systems, applications, location, and user roles by Juniper Mist. It allows WxLAN to automatically detect printers, Apple TVs, and other IoT devices and categorize them for security and auditing purposes without the need for manual database management.

Risk Profiling Driven by Mist AI

The Risk Profiling solution includes WAN Assurance, which extends network security to the distributed network edge. Risk Profiling gives the Juniper Mist cloud visibility into infected wired or wireless clients and assigns a threat score assessed by the Juniper ATP cloud. The Juniper Mist cloud IT team can geospatially locate compromised devices and conduct one-touch mitigation measures like ban or de-authentication.

AI-Driven Radio Resource Management

Unlike previous systems, Mist learns and improves radio settings based on data science and cumulative SLE performance to ensure performance while also instantly reacting to sporadic outside interference. The AI-driven Radio Resource Management incorporates coverage and capacity anomalies based on client experience (SLE metrics) into RF decisions, allowing RF planning to improve and adapt over time.

WxLAN Policy Creation and Enforcement

With the inline policy engine, WxLAN, Juniper Mist provides operational simplicity by letting the IT team set policies for a role, device type, and user-based network access. Policies can be imposed at the edge of the access points thanks to global labels defined for physical and logical resources (users, AP, WLAN, IP addresses, IP subnets, and applications).

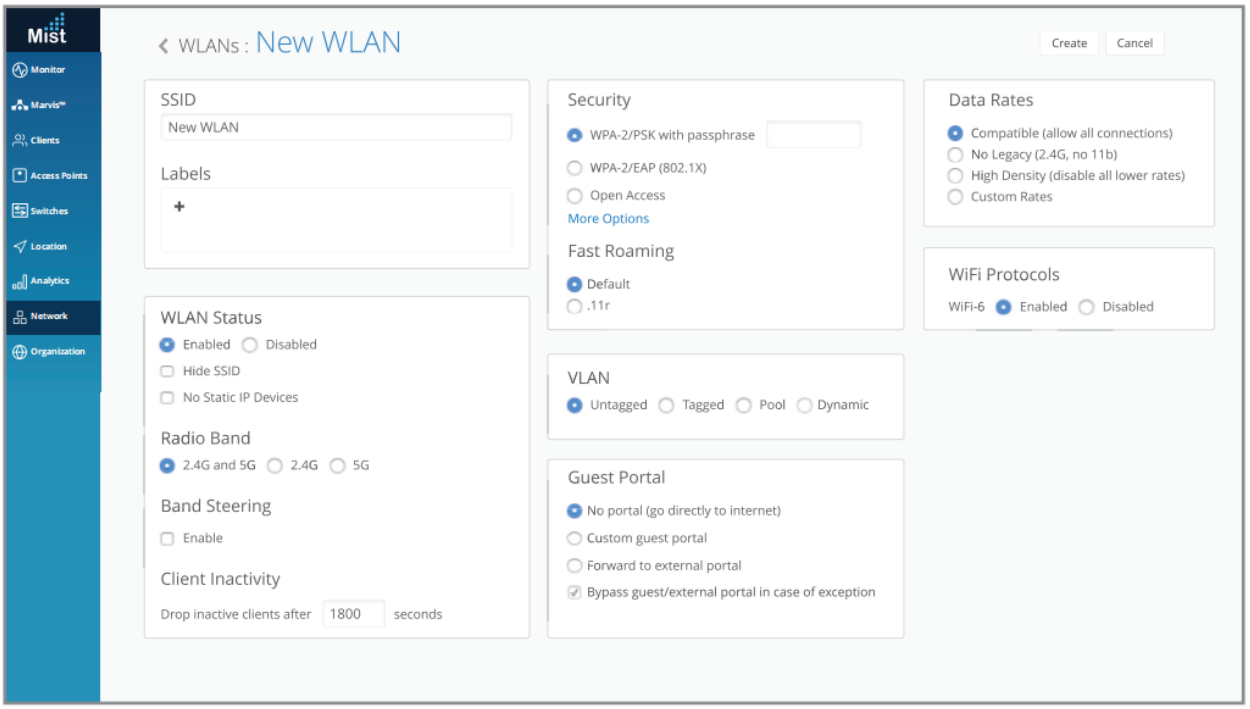

Figure16. Wi-Fi Assurance New WLAN [67]

Personal WLAN

Through a self-serve interface, create a personal wireless network (with a personalized preshared key). This functionality can be utilized to safeguard IoT and guest traffic, as well as provide a multitenant network with a scalable solution.

The Juniper Mist AI-driven WLAN solution is the gold standard for any digital deployment, with the Wi-Fi Assurance service helping the IT team deliver a dynamic user experience while simplifying management, planning, and troubleshooting. With a subscription, the customer may get comprehensive wireless, security, guest access, and network administration.

Guest Portal

Customers may use Juniper Mist to design personalized visitor portals that feature terms of service, email/text login, and even social media log in, all of which can help enhance client engagement. [67]

3.6.3 Juniper Mist Wired Assurance

Juniper Mist Wired Assurance is a cloud service that automates campus switches, access points, servers, IoT devices, printers, and other equipment. It streamlines every step of wired switching, from onboarding and auto-provisioning on Day 1 through operations and management on Day 2 and beyond. Through the Junos® operating system, Juniper EX and Juniper QFX Series Ethernet Switches deliver extensive streaming telemetry, allowing insight into what the switch is experiencing and how it is performing.

Wired Assurance is complemented by Marvis Virtual Network Assistant (VNA), which uses Mist AI to stream and troubleshoot network processes with self-driving actions that automatically correct faults. As part of the Self-Driving Network, Marvis helps teams to go from reactive troubleshooting to proactive remediation by translating insights into automated tasks.

Juniper Mist cloud services are completely programmable and use open APIs to automate and integrate with IT applications.

Day 0/Day 1: Single-Click Activation and Auto-provisioning of EX Switches

One-Step, Simplified Onboarding.

The wired switches can be onboarded by the cloud with a single activation code because they are real plug-and-play. In only a few minutes, network administrators can see switch metrics and service levels for wired devices.

Existing ("brownfield") EX deployments can also benefit from Wired Assurance once they've adapted to the cloud.

Configurations Models.

Using global templates in the cloud, create uniform setups while still having the freedom to customize specific switch and site attributes. The Juniper Mist cloud can instantly determine the type of device plugged into the switch and apply the appropriate port profiles using dynamic port profiles for colorless ports, bringing plug-and-play to a new level. It helps to ensure consistency and uniformity across multiple sites while expediting large-scale deployments rollouts.

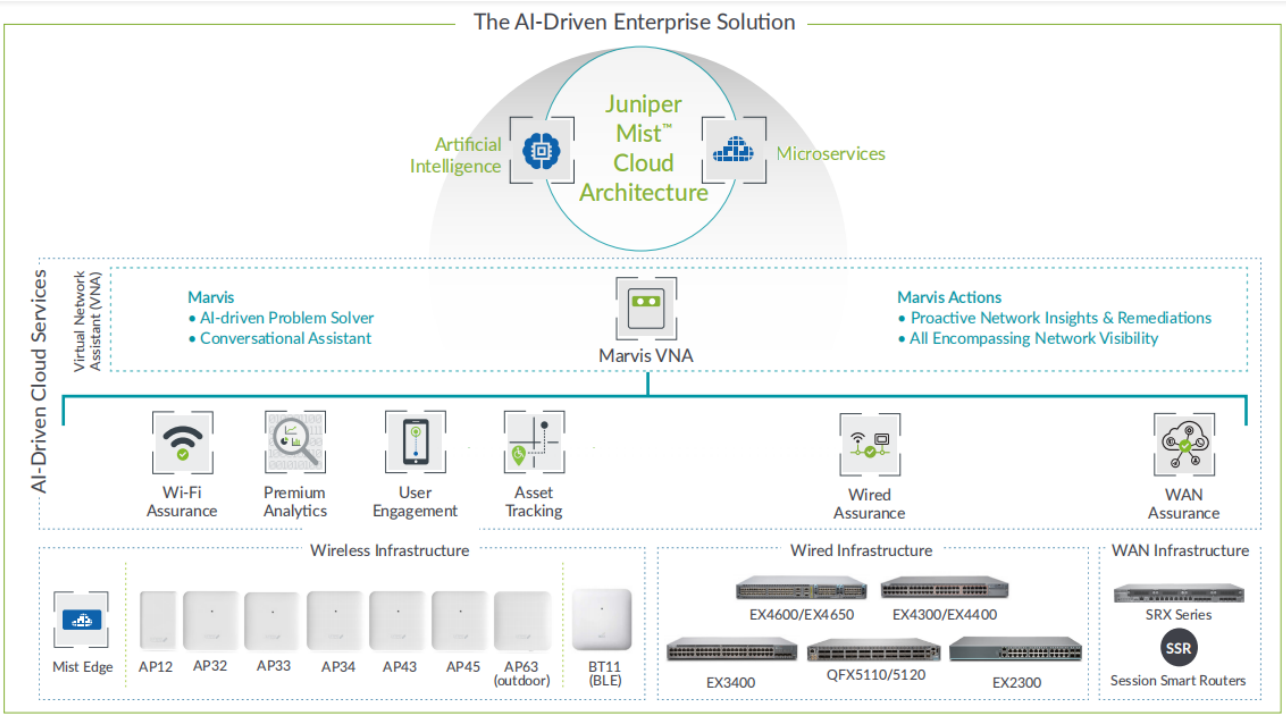

Figure17. AI-Driven Enterprise portfolio overview [68]

AI-Driven Campus Fabric with Juniper Mist Cloud.

Wired Assurance integrates cloud management and Mist AI into the campus fabric. It establishes new standards by moving away from traditional network management and toward AI-driven operations while improving connected device experiences.

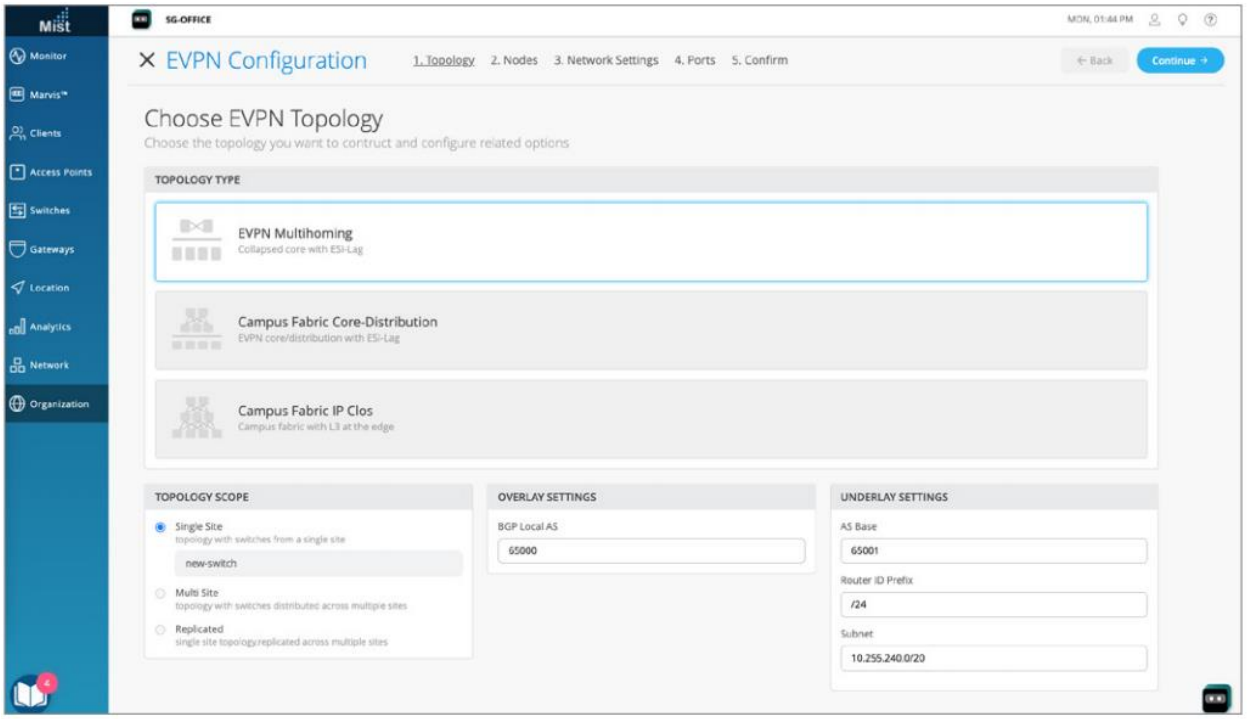

Figure18. AEVPN multihoming configuration via Juniper Mist cloud [68]

Device, Port, and Interface Profiles.

Port profiles make it easy to provision switch interfaces manually or automatically. Users can manually set profiles to specified port ranges and odd/even ports for static provisioning of color ports.

Users can plug the client device into any port with dynamic port profiles. Based on RADIUS name, LLDP, or manufacturer OUI properties, users can apply port profiles and policies to wired devices (access point, IoT device, corporate device, and others.) automatically.

Open APIs for Third-Party Integrations.

Use the power of 100 percent customizable APIs to monitor the network in real-time for fully automated activation, onboarding, and setup. Juniper Mist APIs are open and connect effortlessly with third-party systems such as Splunk and ServiceNow, which provide APIs with troubleshooting, automated ticketing, and other functions.

Day 2 and Beyond: AI-Driven Operations

Wired Service Level Expectations (SLEs).

Provide operational visibility into the wired experience SLEs for Juniper EX and QFX switches. With pre- and post-connection performance data, customers can ensure throughput, successful connections, and switch health. All in one dashboard, pre-connection displays the number and time of successful connects as well as authentication, while post-connection evaluates throughput and detects STP loops, congestion and interface problems. SLEs assist in the measurement and management of networks, allowing for easier troubleshooting and proactive anomaly identification.

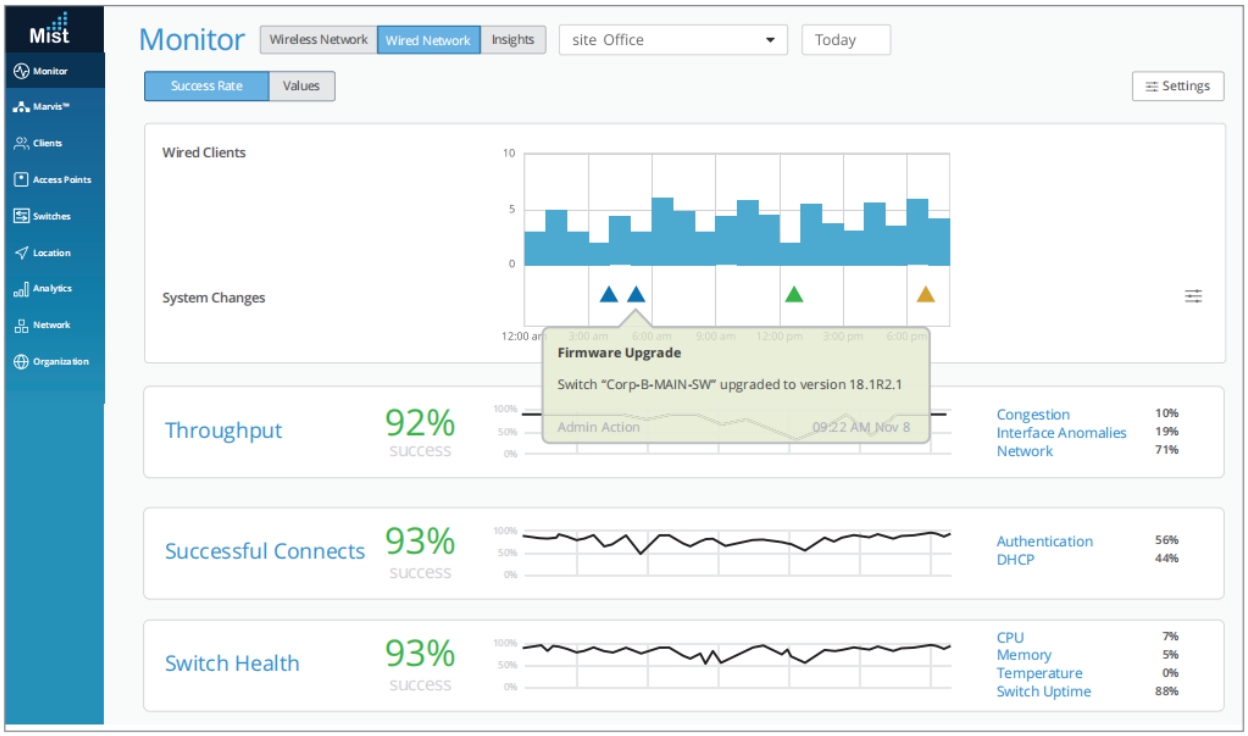

Figure19. Juniper Mist Wired Assurance service-level expectations [68]

AI-Driven Switch Insights.

Understand how Juniper EX and QFX Switches function with granular device-level switch data and insights such as CPU, memory consumption, and virtual chassis condition. The IT team can also examine information such as bytes transmitted, traffic utilization, and power draw down to the port level. For linked endpoints, the IT team will receive performance series data as well as real-time status data. Switch events like firmware updates, configuration changes and system alarms are also logged and correlated by Wired Assurance. When administrators hover their mouse over switch ports in the management interface, status information regarding access points, wired clients, and connections appears, including connection speed, PoE status, and throughput.

Figure20. Switch health metrics [68]

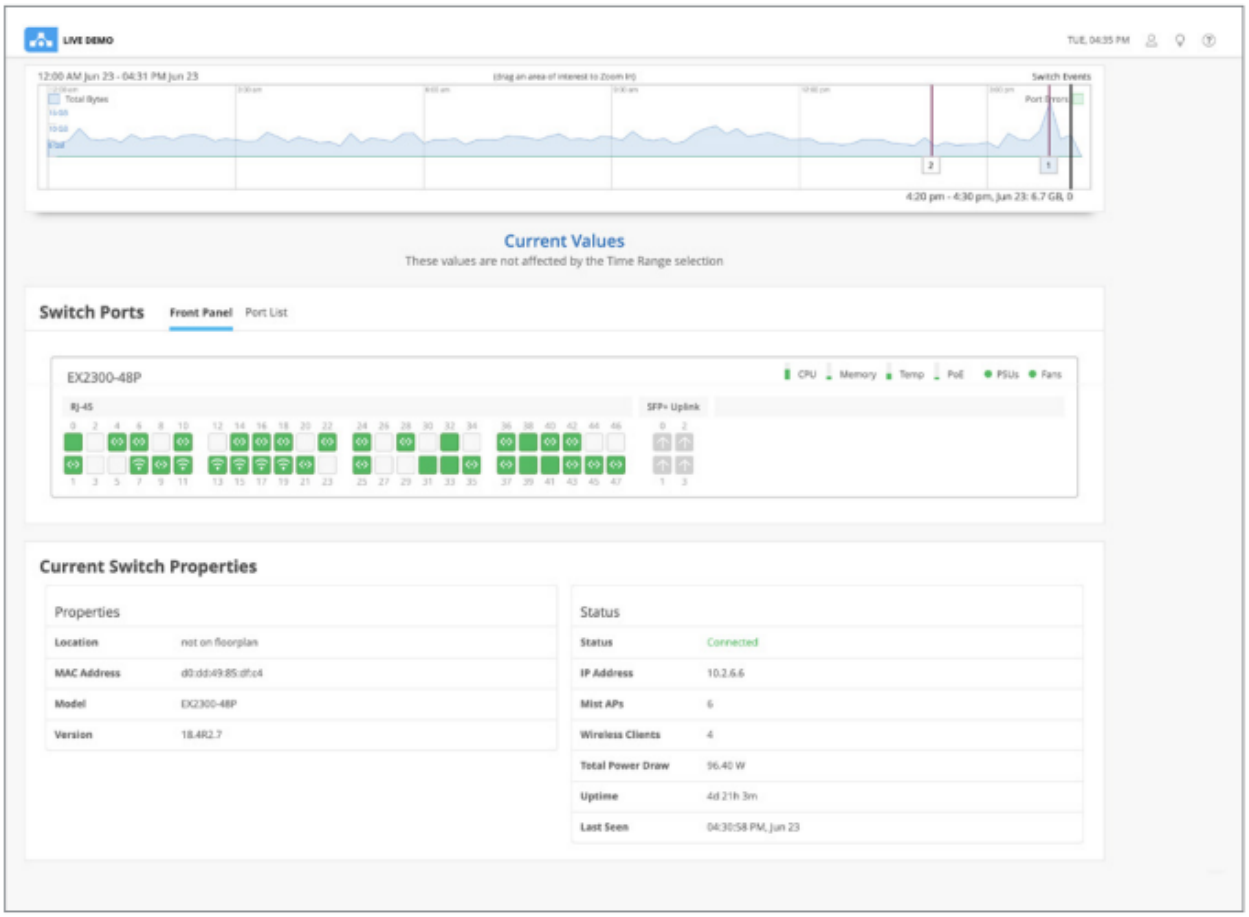

Figure21. Switch level insights [68]

Wired Client Health Metrics.

In a list, topology, or location view, customers can see an inventory of switches and wired devices. With important health parameters like switch firmware compliance, PoE compliance, switch AP affinity and missing VLANs, wired Assurance maintains effective network operations. These metrics are accessible for multivendor environments using Juniper access points and Marvis licences on third-party wired switches. The integration of BPDU Guard and MAC limit hit error detection simplifies administration port security at scale.

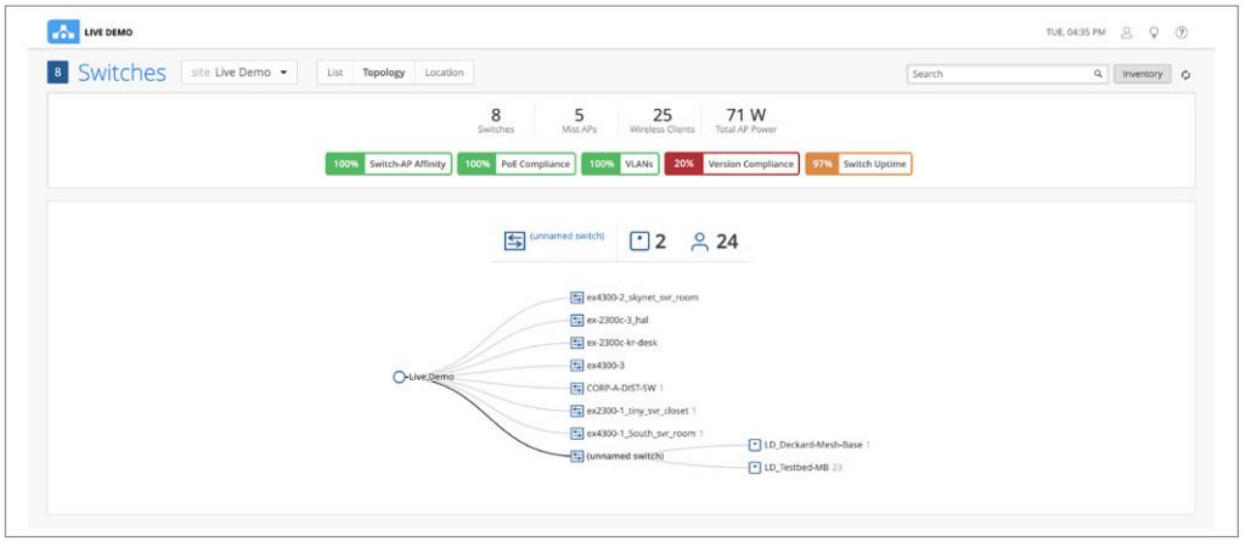

Figure22. Wired Assurance topology view [68]

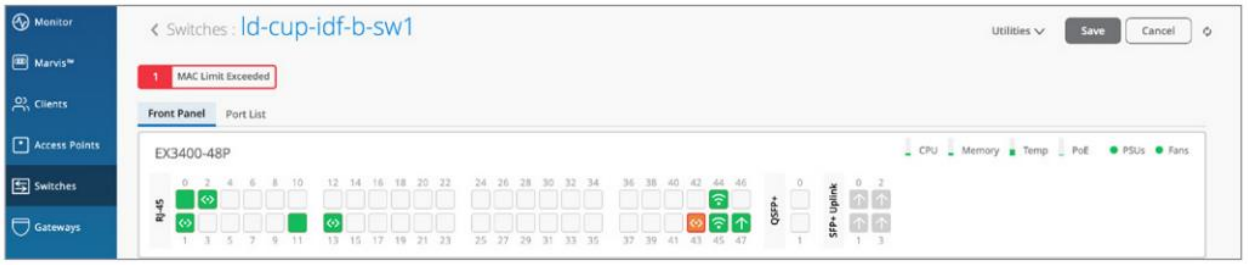

Figure23. Wired Assurance MAC limit exceeded warning [68]

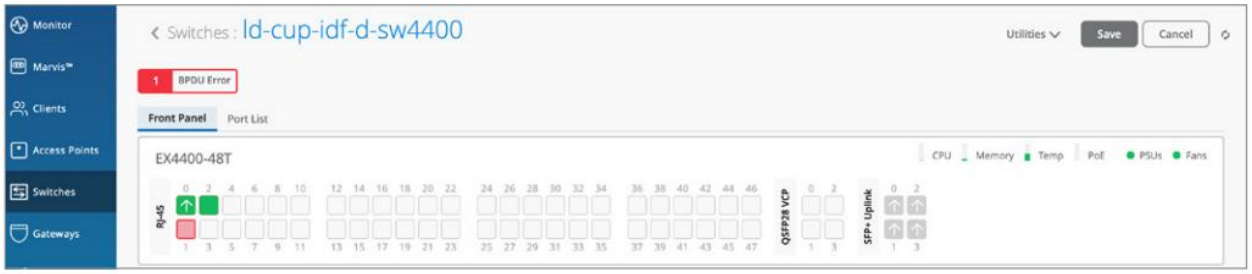

Figure24. Wired Assurance BPDU Guard error [68]

Marvis Virtual Network Assistant.

With simpler troubleshooting and performance analysis for helpdesk employees and network administrators, Marvis complements Wired Assurance and moves operations closer to The Self-Driving Network, obtaining useful information by simply asking a question in natural language. Users will be notified when there are deviations from set baselines thanks to Marvis' proactive anomaly detection in the SLE dashboard. Users can also get proactive advice for wired issues, including port negotiation mismatches, missing VLANs, faulty cables, repeatedly failing clients, and detection of L2 loops, via Marvis Actions.

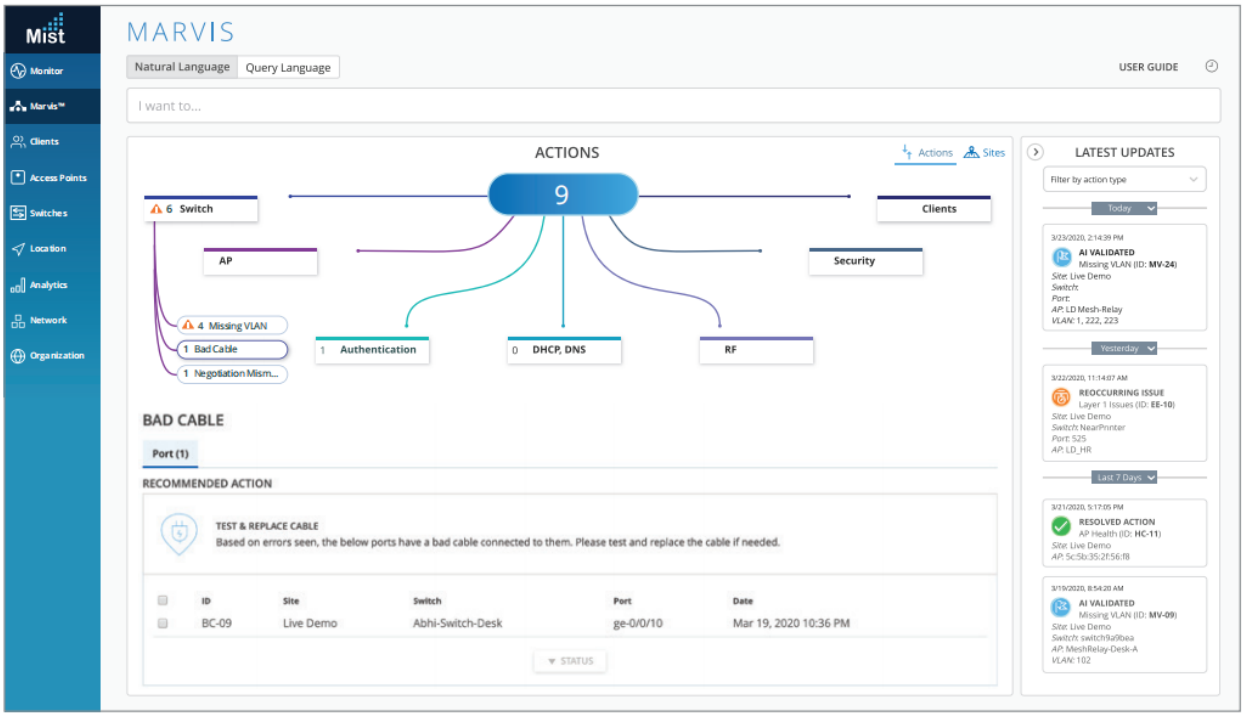

Figure25. Marvis Actions for wired switches [68]

Network Insights.

Wired Assurance offers a basic analytics capability that allows users to analyze up to 30 days of data, making it easier to derive network insights from data and analytics throughout the company. Examine the network throughput peaks to ensure that the support resources are properly aligned. Consider the IT team's desire to expand these capabilities to third-party network parts, consume up to a year's worth of data, and generate customized reports. Juniper Mist Premium Analytics is accessible as an add-on service in that instance.

Juniper EX and QFX switches.

The EX and QFX Switches are cloud-ready access with high performance and aggregation/core layer switches for data center, enterprise branch and campus installations. The feature-rich EX and QFX Switches provide simple and secure connectivity at scale, powered by Mist AI, as the infrastructure foundation for the network of the next decade. [68]

3.6.4 Marvis Virtual Network Assistant

A Conversational Assistant

Conversational interfaces, such as Siri, Cortana, and Alexa, have come a long way to become a part of people's daily lives, altering the way humans engage with computers. They've become a

hotbed of strategic investment across a variety of industries, including banking, retail, and healthcare, as companies seek to improve operations and provide users with individualized experiences. Now, powered by Mist AI, Juniper Mist is the first to provide a conversational interface to enterprise networking.

Marvis adds natural language understanding (NLU) to its natural language processing (NLP) capabilities to provide a conversational interface that understands user intent and improves the value and quality of delivered results. The Marvis conversational interface's strength is in its ability to contextualize requests in order to speed up troubleshooting workflows, answer product or feature-specific questions, offer network information, and assist in the discovery of any sort of network device. It can give recommendations to:

- In only a few clicks, get real-time network information.
- Use advanced NLP with NLU and NLG to deduce user intent from broad remarks and inquiries
- Learn from user feedback to improve individual user experiences
- Ask generalized questions beyond troubleshooting, such as "How to set up RRM?" and "Does AP have capacity?"

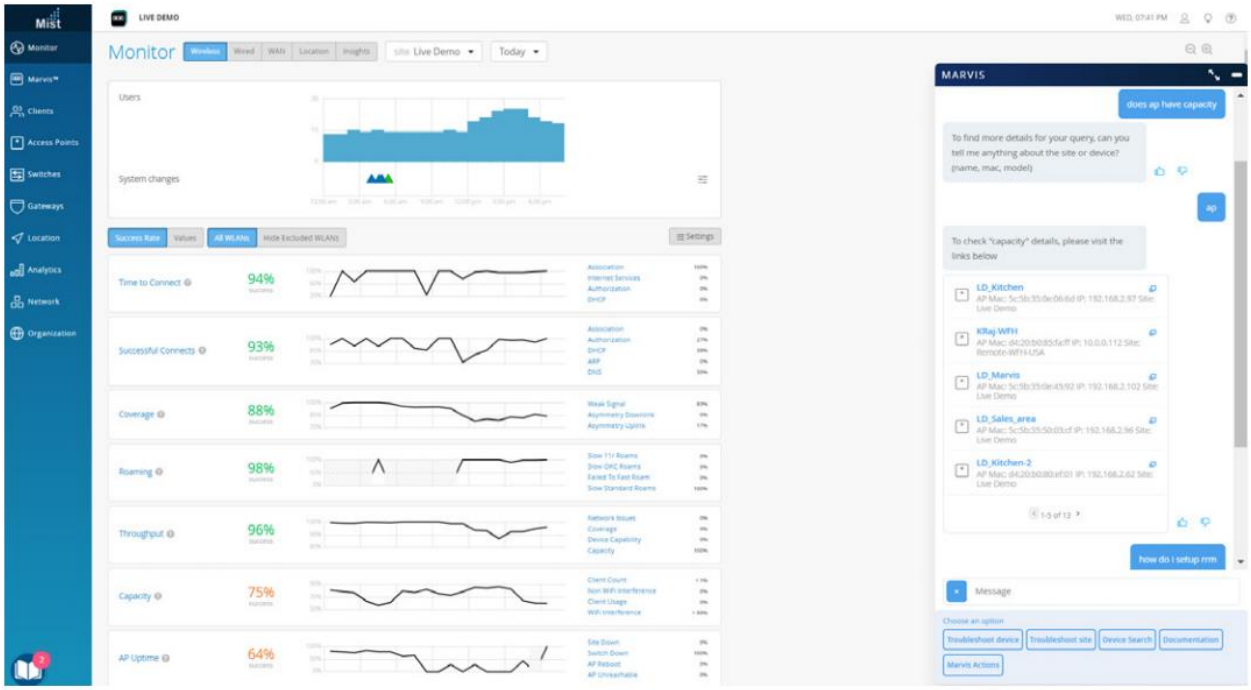

Figure26. Marvis conversational interface [69]

Marvis automates troubleshooting and support so that IT professionals can achieve a faster mean time to resolution and a higher level of innocence. It provides a complete network view with the user, client, and device details, removing the need to open several dashboards or know CLI commands. Marvis works as an extension of the IT team, sifting through data and logs to find root causes and providing high-quality responses in real-time.

Marvis is a one-stop-shop for IT teams who want to know how their network is doing. They don't have to remember CLI commands or which dashboards have the necessary data. It drastically transforms how IT personnel experience and interacts with the network now that they have answers at their fingertips.

Client-to-Cloud View Via Actions: Journey to a Self-Driving Network

Marvis Actions is all about simplifying operations and moving IT away from reactive troubleshooting and toward proactive remediation. It has a "morning cup of coffee" view that gives administrators visibility into high-impact network issues at an organizational level, so they know what to prioritize and focus on for the day. Marvis Actions expands easily as more sites are added because no further setup is required from the user.

Figure27. Marvis provides proactive return material authorizations [69]

With high efficacy, Marvis proactively discovers the root cause of issues across IT domains (WAN, security, WLAN, LAN and apps) to either automatically resolve issues (self-driving mode) or prescribe actions that require human interaction (driver-assist mode). Marvis completes the feedback loop by checking that the actions are proper in the Mist AI engine, allowing Marvis to learn while gaining the trust of the IT team.

Some Marvis Actions are listed here for Juniper Mist Wired Assurance. Marvis finds defective network cables attached to ports, incorrect port settings, L2 loops, and continual port flaps, and

separates wired clients failing to connect. It adds missing VLAN tags, corrects erroneous port mode setup, and isolates clients who are consistently failing. Marvis Actions assists Juniper Mist Wi-Fi Assurance in tracking and managing firmware upgrades, detecting coverage holes, identifying APs connected to a bad cable, detecting missing VLANs along with coverage holes and RF capacity failures, and identifying actions required to resolve EAP/802.1X authentication failures.

Marvis also recognizes AI-driven support for unhealthy Juniper access points with proactive return material authorization (RMA). It reduces support teams' manual troubleshooting checkpoints, resulting in considerable time and effort savings while improving users' overall experience, devices, and clients.

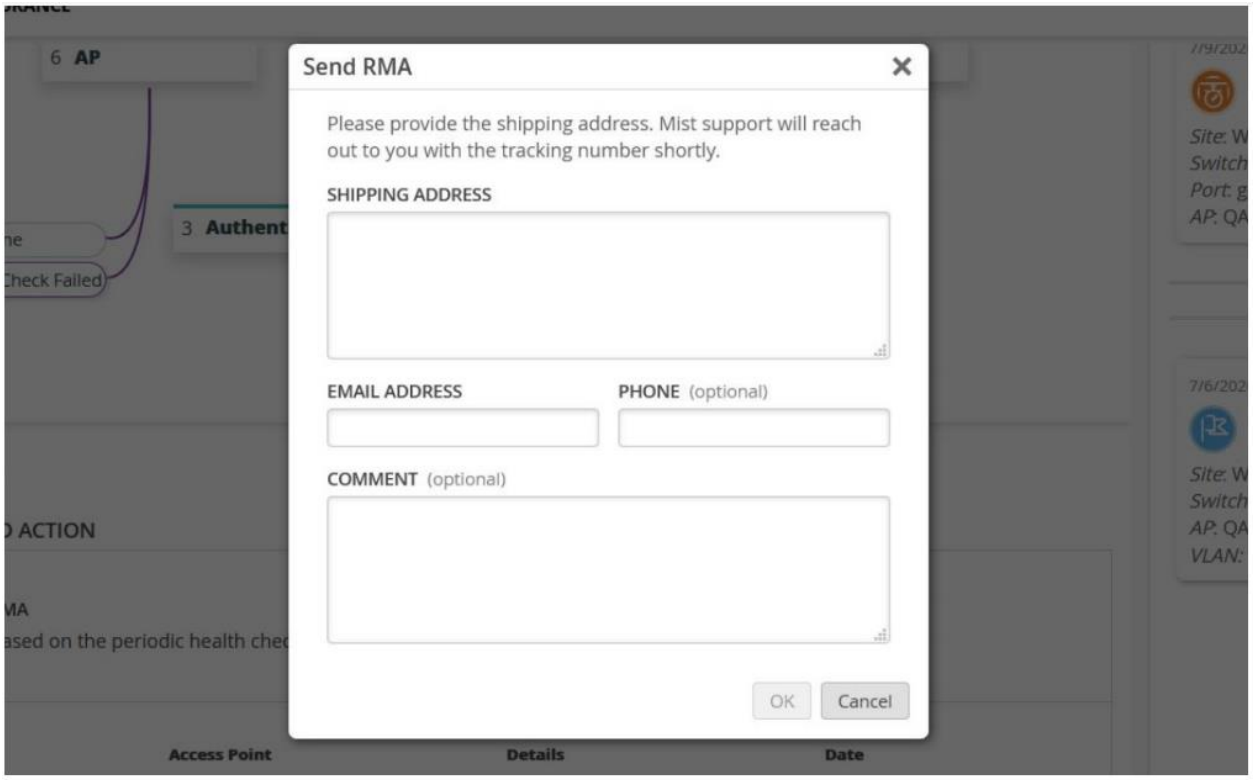

Figure28 . Marvis Actions [69]

Marvis can also trigger events using an API-driven interface, such as the automatic creation of a ticket on external support systems using email alerts and webhooks.

Marvis Client Application Performance Kit (APK)

The Marvis Android client is a software agent that sits on the end-user device and collects and displays detailed client-device information, such as client roaming behavior. The Marvis Client also recognizes device connection types, such as cellular or Wi-Fi, as well as signal strength. This

extra level of granularity allows administrators to gain a better understanding of the Wi-Fi experience from the client's perspective.

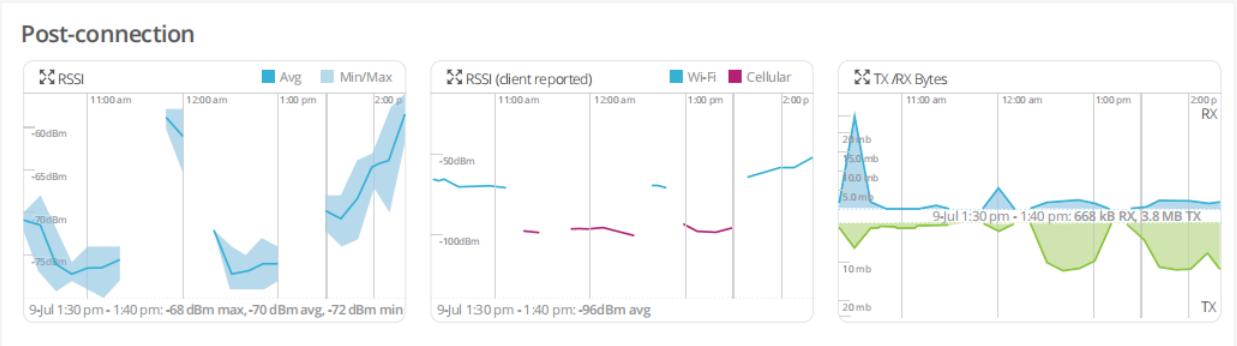

Figure29 . Post-connection details from Marvis client [69]

The Marvis client adds to the data on the client device. It goes beyond basic fingerprinting to provide extra information like device type, manufacturer, and different operating system versions. The more information the client APK can extract, the better the Mist AI engine can classify advanced devices. Marvis improves its capacity to discriminate between device-specific issues and generic device issues over time, such as specifically identifying that OS version 8.1.0 is harming certain customers.

Anomaly Detection

Anomaly detection is built into Marvis SLEs so that administrators are alerted to service-impacting occurrences and can swiftly identify and rectify the root cause of problems. Anomaly detection uses machine learning to automatically build service baselines and sends out notifications when they deviate from the norm. The feature employs the third generation of long-short-term memory (LSTM) and recurrent neural networks (RNN) algorithms to increase efficacy to over 95% while reducing false positives.

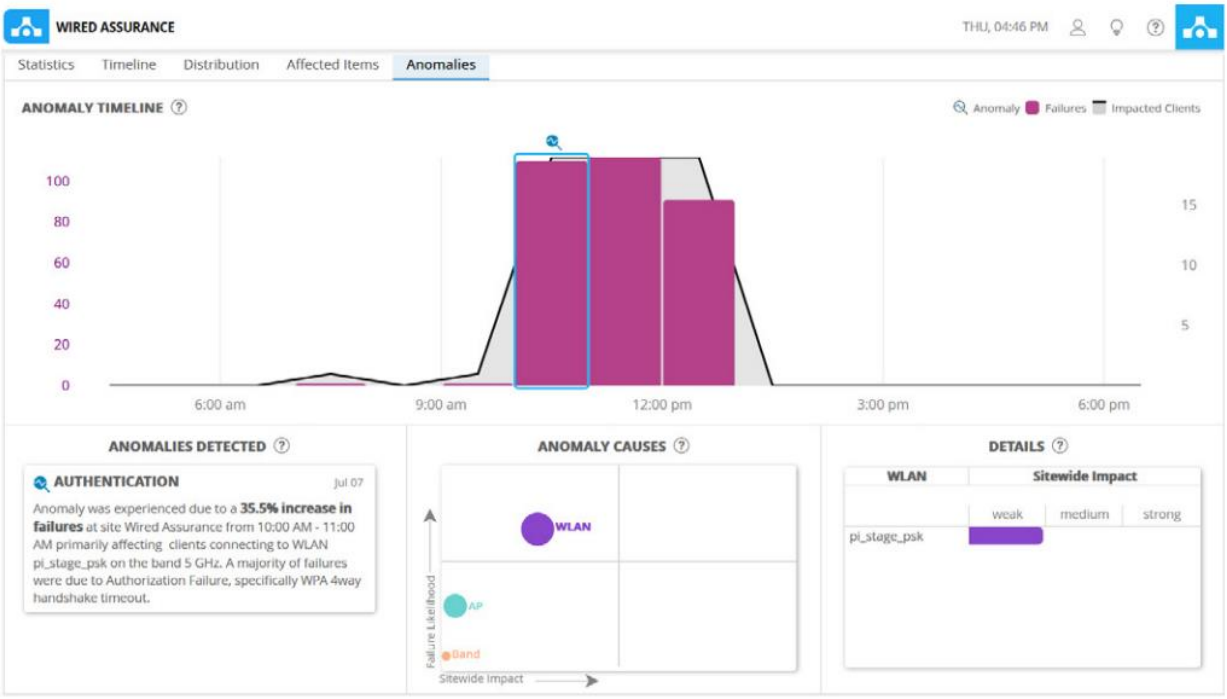

Figure30. Wired Assurance anomaly detection [69]

Client Service Level Expectations (SLEs)

Marvis is an add-on to the client SLE. With continuous behavioral analytics and network traffic monitoring, it uses machine learning to analyze and monitor client and device experiences. Understanding these trends provides IT with more information for troubleshooting and planning.

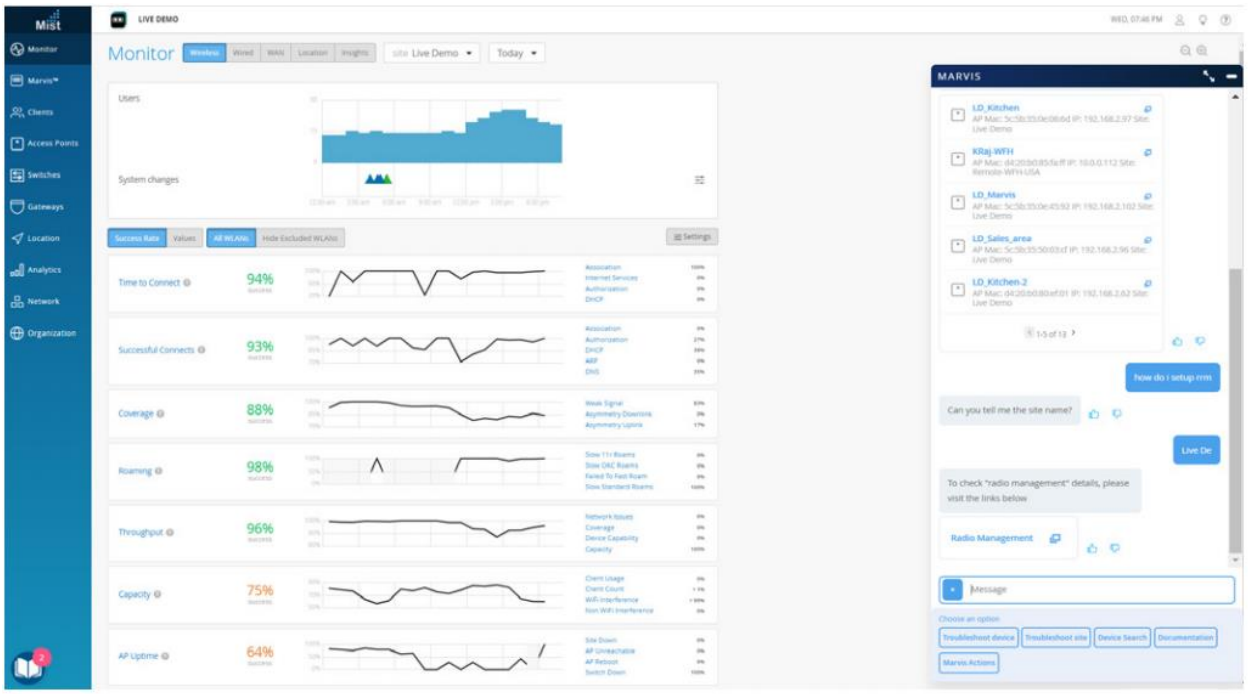

Figure31. Wi-Fi Assurance client service-level expectations [69]

Multivendor Switch Insights

IT teams can use Marvis to collect health statistics for Juniper and third-party switches that are connected to Juniper Access Points, such as:

- How many access points are connected to a switch
- PoE compliance status, which helps manage and balance the power draw of connected devices
- Identification of VLANs that are misconfigured on switch ports where APs are connected, but clients are getting blocked
- Version compliance for switches running dissimilar hardware
- Switch uptime

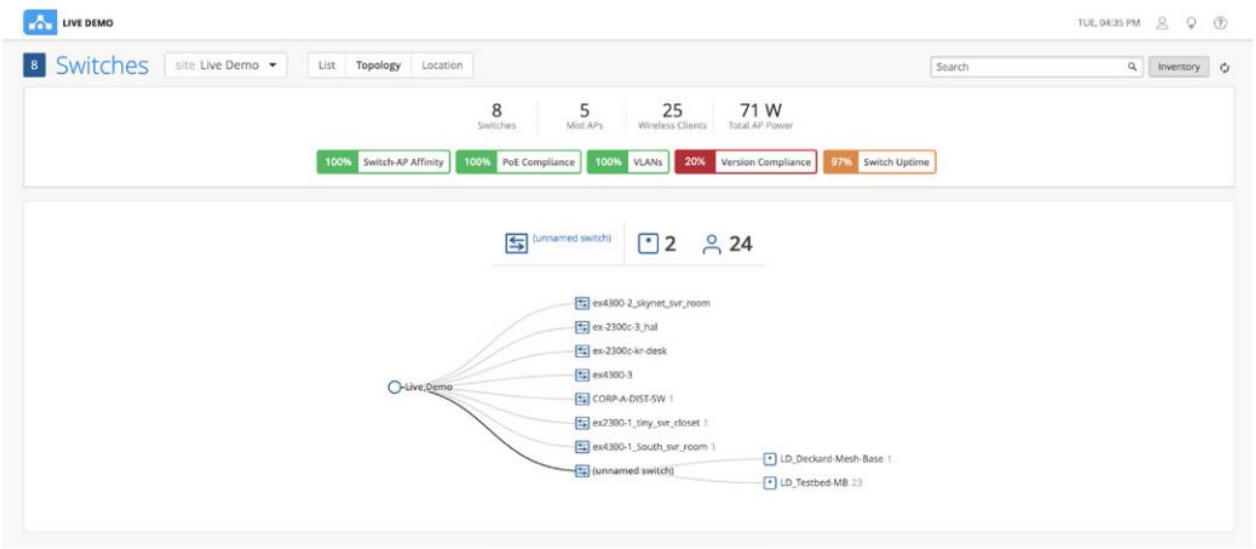

Figure32. Wired Assurance switch-level insight [69]

3.7 Cisco AIOps solutions

3.7.1 Cisco DNA Assurance

The increasing number of devices connected to the network and the Internet of Things (IoT) means that the IT staff must manage a growing, sophisticated network more efficiently than ever before. More customers, bandwidth-demanding applications, and services rely on reliable, consistent, and secure network systems, whether wired or wireless. However, IT expenses have not increased in parallel.

By minimizing manual troubleshooting processes and reducing the time spent resolving service faults, Cisco DNA Assurance with Artificial Intelligence (AI) and machine learning addresses these difficulties. Cisco DNA Assurance turns network devices into sensors, which are subsequently analyzed using AI and machine learning. The simple dashboard displays the general status and flags any issues. The process of performance enhancement and issue resolution is then automated through guided remediation, which keeps the user experience at its best while reducing the amount of time spent troubleshooting.

Benefits of Cisco DNA Assurance

- Boosts visibility: On a single screen, see the entire network status at a glance.
- Saves time: Noise and false positives are reduced while properly identifying issues that have the most significant impact on the network.
- Reduce workload: AI-powered technology can proactively identify the source of the most effective network issues.
- Facilitates troubleshooting: Remediation choices are automated using machine-reasoning techniques.
- Quick issue resolution
- Help IT staff excel: Spend less time on the network while simultaneously improving its performance.

How Cisco DNA Assurance works

Cisco DNA Assurance is a component of the Cisco DNA Center, which captures streaming data from applications, endpoints, devices, and users throughout the network. It then employs Cisco AI Network Analytics to determine what performance levels are required for the best user experience on the network and to generate recommendations for network improvement. These findings are compared to network policies in Cisco DNA Center's Automation section to ensure that network operations are in line with business goals. The IT staff may drill down for more detail on any section: wired devices, clients, services, apps, and wireless devices, using the minimalist client and device health dashboards. Issues that need to be addressed are highlighted, and the IT staff can click on them to see potential solutions. The Assurance dashboard has specialized sections to aid with more difficult issues:

- Device 360/client 360: View connection from any angle or context. Information on topology, throughput, and latency from various times and applications is included.
- Network time travel: Rather than trying to recreate a network problem in a lab, go back in time and investigate what caused it.
- Application experience: On a per-user basis, provide unrivaled visibility and performance control over the applications that are vital to the core business. Allow users to get the performance they need on the programs that are critical to their job.
- Wi-Fi 6 readiness: Visualize the wireless network's current state and which users and endpoints are having issues. Locate regions where upgrading the network makes sense and where the IT team can wait. [70]

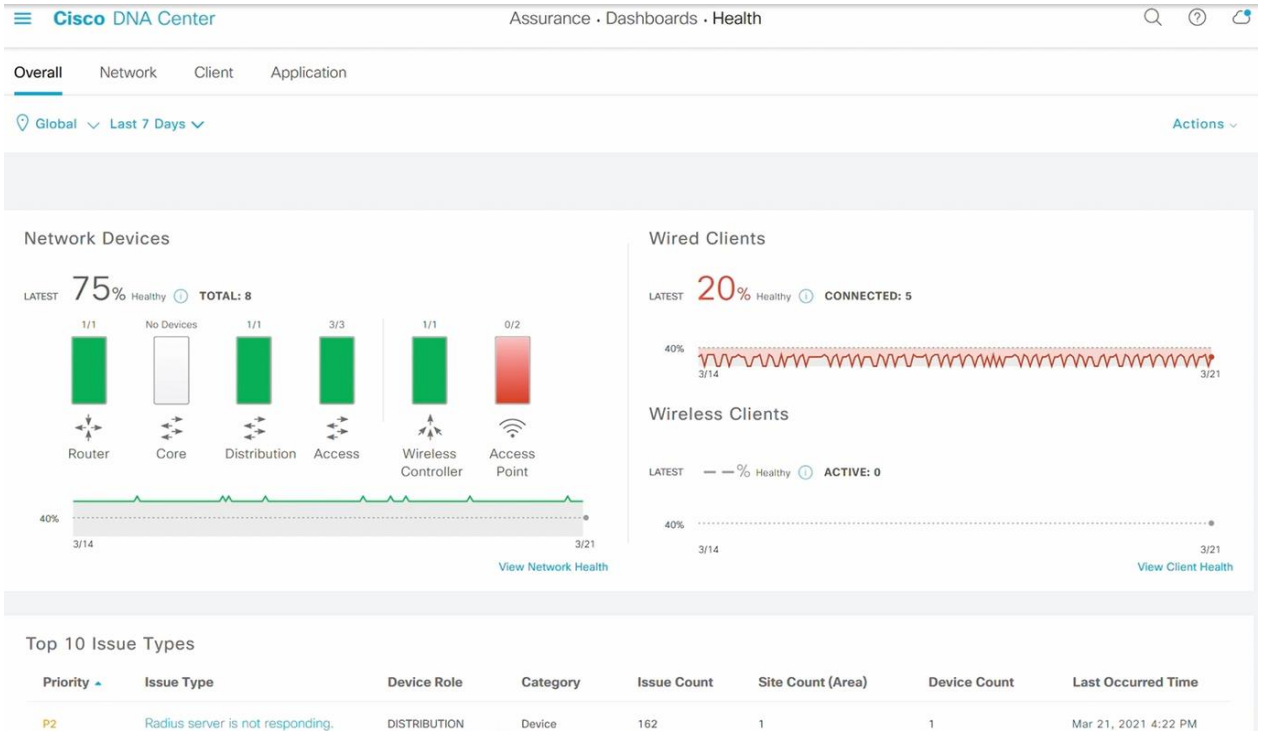

Figure33. Cisco DNA Assurance dashboard [71]

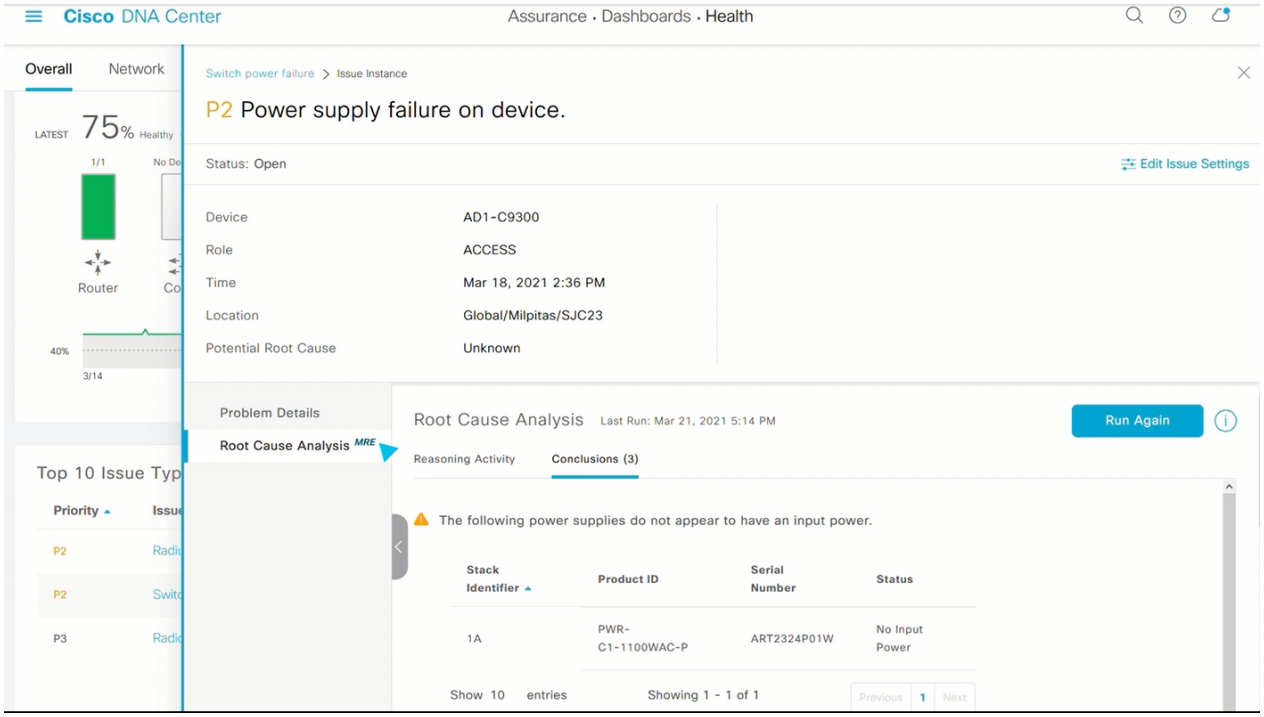

Figure34. Cisco DNA Assurance actions table [71]

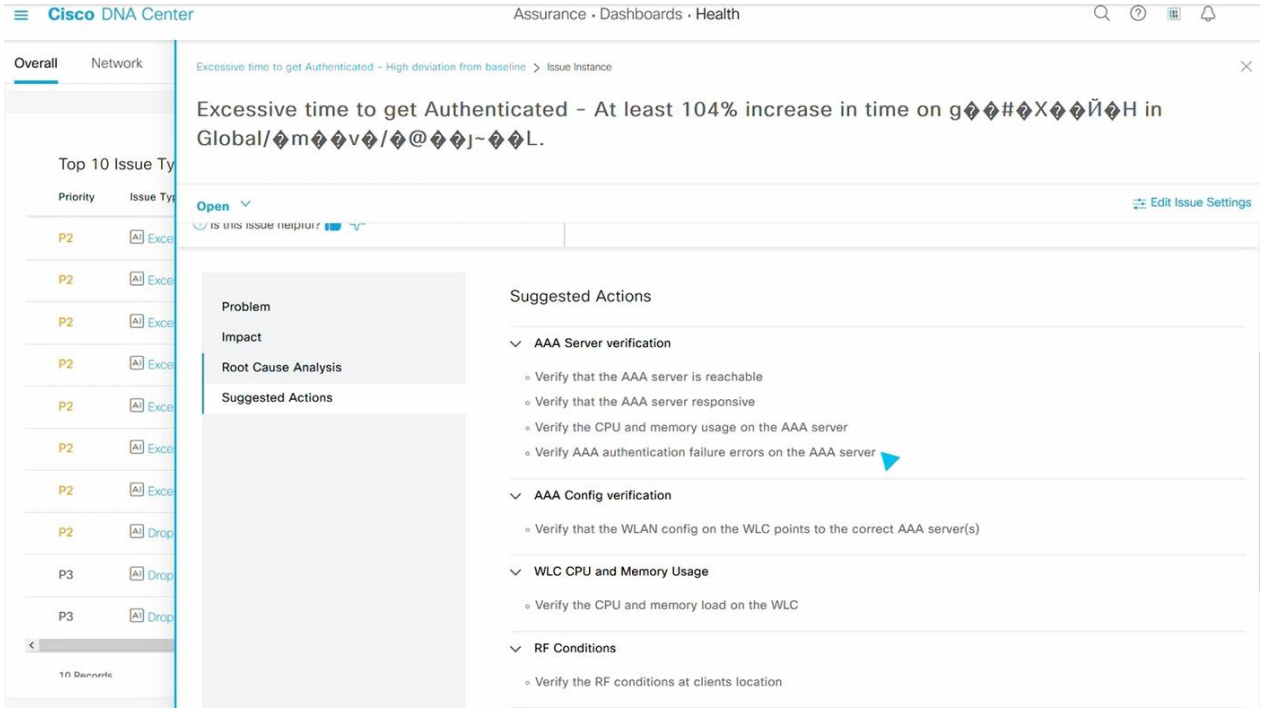

Figure35. Cisco DNA Assurance dynamic baseline [71]

3.7.2 Cisco AI network analytics

Within Cisco DNA Center, the Cisco AI Network Analytics solution provides highly tailored information to enterprise network settings, allowing IT professionals to spot problems sooner, handle problems faster, and reduce network noise. Both the Cisco AI Network Analytics cloud

(on safe and durable compute servers) and on-premises computing resources are used for Cisco AI Network Analytics (within the Cisco DNA Center appliance). Streaming telemetry and other data from network events on the customer's network is anonymized on-site before being sent to the Cisco cloud, where it is combined with anonymous data from networks all around the world. The technology will become more sophisticated as more networks use Cisco AI Network Analytics. Cisco also integrates human knowledge in its software, which includes decision-making from Cisco's greatest engineers. The system's decision-making algorithms incorporate all of the best practices and 35 years of networking experience. Cisco uses the industry's most advanced AI/ML algorithms to improve outcomes in the face of all this data. Based on the Cisco DNA Center parameters, the models are tailored to local network conditions and prioritized for greater relevance. The end outcome is accurate information that leads to greater performance.

Figure36. AI Network Analytics [72]

Visibility - Personalized baselining

There are no two networks alike. AI-driven systems can learn about the network's user trends, application metrics and services. After that, Cisco DNA Assurance can construct a bespoke performance curve for analytical judgments. As the network develops and changes, the AI-driven baseline for the network's unique performance characteristics is constantly adjusted.

Based on this tailored baseline, the AI-driven analytics engine (both on-premises and in the Cisco cloud) can make precise judgements about what is expected and what is not. This is

accomplished through the characteristics following:

Insight – Intelligent analysis

Any deviation from the AI-created tailored baseline for this network will be detected using AI-driven anomaly detection. It enables Cisco DNA Center to decipher any network data. The technology is capable of detecting performance issues with pinpoint accuracy while ignoring odd but harmless network noises. It lowers noise while properly identifying network anomalies that have the greatest impact. Users may foresee and prevent problems with AI-driven predictive analytics and proactive insights. The machine learning engine can predict increases in Wi-Fi interference, onboarding delays, office traffic load, and other factors in this situation. A benign event or set of events frequently precedes a troublesome occurrence in IP networks. Predictive analytics can assist network managers in anticipating the unexpected by learning how series of occurrences are related to one another.

There are kinds of proactive insights:

1. **System-generated insights** appear in Cisco DNA Center's Network Insights menu. These are the most important trends and departures from the network's regular performance trends. These insights can assist the IT team in determining the next stages in growing or preparing for network growth, allowing them to stay one step ahead of today's ever-increasing network demand.

2. **Proactive exploration**, in which the IT staff can look into any aspect of the network, service, or application that they'd like to learn more about. The network heat map is an example of proactive exploration, where a user may compare the performance of numerous wireless access points to identify areas for improvement. There are also site comparison features, which allow network administrators to compare different floors in a building or separate branch sites. The user can even compare their network performance to that of other similar and anonymous networks using anonymized and encrypted data.

Action – Accelerated remediation

Machine learning detects the most significant variables connected to the root cause of an issue, allowing Cisco AI Network Analytics to enable expedited remediation. It enables the IT staff to spot faults and vulnerabilities faster than ever before, undertake comprehensive root cause investigation, and implement corrective actions. Cisco will enable machine reasoning in future releases to implement the logical troubleshooting procedures that an engineer would take to address an issue. These features speed up the remediation, making the IT team's problem-solving

more precise and generally more productive.

Product usage telemetry

Using a Machine Reasoning Engine(MRE) can provide extra benefits to IT teams who use the Cisco DNA Center product usage telemetry option. The MRE may help IT teams with inventory management in general, as well as proactively uncover potential security risks, improve services and support, check the usage of new features that IT teams may not be aware of. The MRE from Cisco DNA Center can scan tens of thousands of network devices to ensure that all the devices have the most recent software image and to look for any vulnerabilities in device configuration. MRE can flag ideas if IT teams aren't making use of the most recent upgrade features. Product usage telemetry ensures that network devices are kept up to date and that the IT department is getting the most out of Cisco DNA Center. [72]

3.8 AIOps-based predictive algorithms

AIOps has various functions, among which the technical research in the prediction direction is also particularly important. Its prediction functions are mainly divided into fault prediction, performance prediction, capacity prediction and transaction volume prediction.

For fault prediction, by analyzing historical fault logs, machine learning algorithms are used to obtain the weights of each index related to faults, and various prediction models are combined to select the best prediction model for application to actual operation and maintenance work. Fault prediction technology can help O&M personnel reduce work pressure, avoid equipment failure to a certain extent, and make equipment life longer.

In terms of capacity and transaction volume prediction, time series prediction algorithms can be used to get the approximate demand in the following days, which facilitates resource planning and allocation. Intelligent capacity management can evaluate the system load ratio and upper limit and use prediction algorithms to derive the future trend of transaction volume or capacity usage, which can help the system expand appropriately during peak business periods to ensure performance and can also shrink appropriately during off-peak periods to save costs

Therefore, it is very meaningful to study AIOps-based prediction algorithms to improve the accuracy and stability of fault prediction, transaction volume prediction and capacity prediction, and thus improve the intelligence and efficiency of the operation and maintenance system. [73]

3.8.1 Base algorithm for time series prediction

3.8.1.1 Native

If we get a historical data set that does not fluctuate much throughout the time period, but basically tends to be stable, then we can simply use the Native method to predict future data. As shown in Figure 37, the price tends to stabilize without much fluctuation over a period of ten days, then we can directly use the real price of the last day of the historical data as the predicted value for the future day.

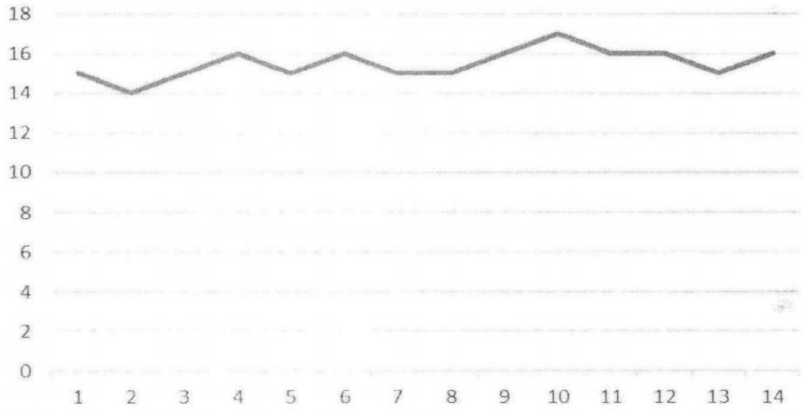

Figure37. Native Method Data Graph (x: days, y: price) [73]

This method of forecasting using the last historical data value as the next forecast value is called Native and its expression is shown in equation: [73]

$$\hat{y}_{T+1} = y_T$$

The Native prediction method is only applicable to scenarios where the data are stable throughout the time period and cannot be applied to data sets that change frequently.

3.8.1.2 Simple Mean Prediction Method

If we get a historical dataset that has little change in the mean value within each time period, although there are small fluctuations throughout the time period, then we can use the simple mean prediction method for prediction.

As shown in Figure 38, although the price has changed slightly upward and downward over a ten-day period, the average price remains almost unchanged, so we can use the average price of the historical data set as the forecast value.

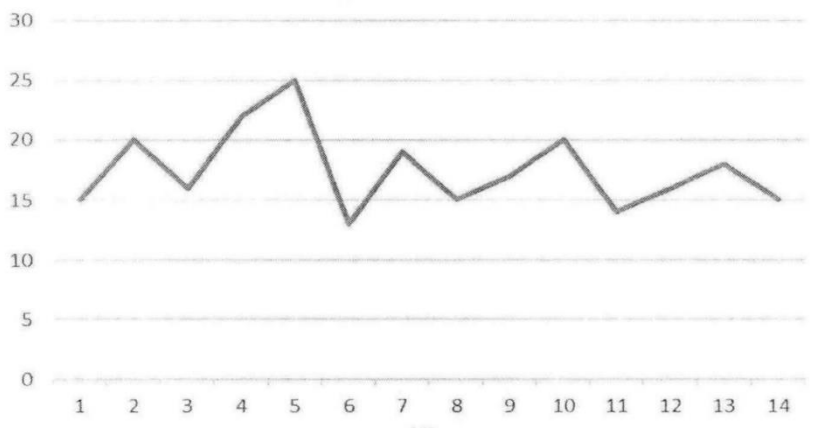

Figure38. Simple Mean Prediction Method Data Graph (x: days, y: price) [73]

The expression for the simple mean prediction method is shown in equation: [73]

$$\hat{y}_{T+1} = \frac{1}{T}\sum_{i=1}^{T} y_i$$

The simple mean prediction method predicts best in scenarios where the mean value of the entire historical data set is essentially stable.

3.8.1.3 Shifting Mean Method

If we get a data set that has stabilized in recent time periods but has particularly large changes in the initial time periods, then we can use an improved simple mean method, i.e., the moving mean method, to make predictions. As shown in Figure 39, the prices changed dramatically in the beginning days, and if we use these data for forecasting, we will definitely get very poor results, so we only use the average price of the last few time periods as the forecast value.

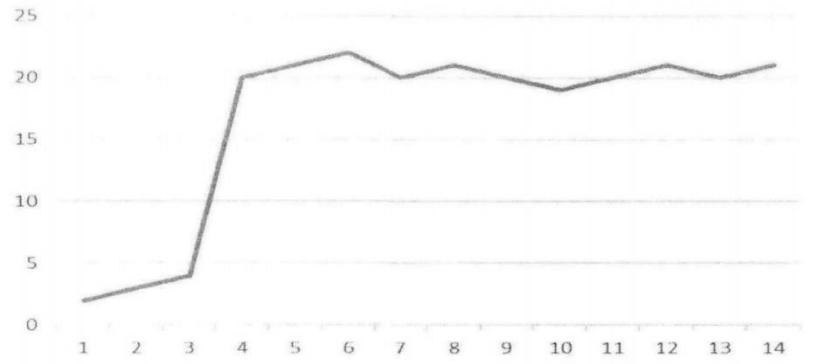

Figure39. Shifting Mean Method Data Graph (x: days, y: price) [73]

This method of using only the average of several time windows of historical data as the next predicted value is called the moving-mean method, where the next predicted value is obtained based on the average of the last p time windows, and its expression is shown in equation: [73]

$$\hat{y}_{T+1} = \frac{1}{p}(y_T + y_{T-1} \cdots + y_{T-p+1})$$

3.8.1.4 Weighted Shifted Mean Method

If we get a data set similar to the moving-mean method, the same moving-mean method is used for forecasting, but each time window has a different impact. This method of using several time windows of historical data with different weights to predict future values is called the weighted moving average method. The forecast value is obtained by averaging the P time windows with different weights, and the expression is shown in equation: [73]

$$\hat{y}_{T+1} = \frac{1}{p}(\omega_1 \bullet y_T + \omega_2 \bullet y_{T-1} \cdots + \omega_p \bullet y_{T-p+1})$$

3.8.1.4 Simple Index Smoothing Method

If we use all the historical data, only the weight of the data at different times is different. This method of forecasting is called simple exponential smoothing, and its expression is shown in equation: [73]

$$\hat{y}_{T+1} = \alpha y_T + \alpha(1-\alpha) y_{T-1} + \alpha(1-\alpha)^2 y_{T-2} + \cdots$$

3.8.2 Classical time series prediction models

3.8.2.1 Index Smoothing Model

The Index Smoothing Model is a traditional time series prediction method, which is improved from the moving average model.

The principle of the index smoothing model is to average the current actual values and the historical data values by a certain ratio, as well as to change the weights of the current values so as to obtain the smoothed values, which constitute the forecasting model by certain calculations. The index smoothing model will fit all the historical data, but will assign a weight to the decay of the index.

If the historical data set is available as: $X = \{x_1, x_2, \ldots, x_n\}$, $S_t^{(1)}$, $S_t^{(2)}$, $S_t^{(3)}$ denotes the smoothed values obtained after three index smoothing, respectively. The expressions are shown in equation: [73]

$$\begin{aligned} S_t^{(1)} &= \alpha x_t + (1-\alpha) S_{t-1}^{(1)} \\ S_t^{(2)} &= \alpha S_t^{(1)} + (1-\alpha) S_{t-1}^{(2)} \\ S_t^{(3)} &= \alpha S_t^{(2)} + (1-\alpha) S_{t-1}^{(3)} \end{aligned}$$

α is the weighting factor.

The smoothed values obtained above are processed and the prediction model can be obtained after certain calculations, whose expressions are shown in equation: [73]

$$Y_{t+T} = a_t + b_t T + c_t T^2$$

The expressions for the parameters a_t, b_t, c_t, are shown in equation: [73]

$$a_t = 2S_t^{(1)} - 3S_t^{(2)} + S_t^{(3)}$$
$$b_t = \frac{\alpha}{2(1-\alpha)^2}[(6-5\alpha)S_t^{(1)} - 2(5-4\alpha)S_t^{(2)} + (4-3\alpha)S_t^{(3)}]$$
$$c_t = \frac{\alpha^2}{2(1-\alpha)^2}(S_t^{(1)} - 2S_t^{(2)} + S_t^{(3)})$$

3.8.2.2 LSTM Model

Artificial neural networks are very effective in fitting non-stationary serial data, where the classical feedback neural network model first obtains the intrinsic regularity information from the continuous training of historical data, and then uses the error inverse feedback mechanism to obtain the most suitable model parameters, thus minimizing the fitting error. With the massive quantification and complexity of data, ordinary artificial neural networks are not enough to solve the problem, and then there are deep learning models that extract and learn the features of historical data to efficiently derive data patterns, among which RNN and LSTM models are the most classic.

The deep learning model RNN is optimized on the basis of feedback neural network model, which is characterized by the coherent interconnection between each neural layer and can make each hidden layer share the weights. However, although the RNN has improved the artificial neural network, the underlying principle is still the original gradient descent method, which may cause the gradient to disappear, and because of the limitations of the RNN structure, it is not very effective for long-term prediction of time series.

The LSTM model, also known as Long Short Term Memory Artificial Neural Network, is optimized from the RNN model, inheriting the advantages of the RNN model and solving the long-term dependency problem by adding GatedRNN. the LSTM model has the ability to fit the data for a long time, and eliminates the problem of gradient disappearance or expansion in the RNN model, so it is widely used in time series prediction problems.

3.8.2.3 ARIMA and SARIMA Model

ARIMA Introduction

The ARIMA model is a very widely used and classic traditional time series prediction model, which has a good ability to handle both smooth and unstable data, and has good results for most scenarios. The core idea of the ARIMA model is to first use the autoregressive algorithm to link the historical series values, current series values and external factors through a certain model, and then use certain statistical methods to derive the appropriate model parameters to integrate the three relationships.

Principles of the ARIMA model

The ARIMA model consists of three parts, which are the autoregressive model AR, the difference1, and the moving average model MA.

The idea of the autoregressive model is to fit the relationship between the historical data and the current value, and to use the historical data to predict the current value of itself, which requires the historical data to be smooth.

If the order of the autoregressive model is p, then its expression is shown in equation: [73]

$$y_t = \sum_{i=1}^{p} \gamma_i y_{t-i} + \varepsilon_t + C$$

Where, y_t represents the current data value, C represents the constant, ε_t represents the error term, and γ_i represents the autocorrelation coefficient.

MA fits the error term in the above equation and it reduces the stochastic fluctuation of the prediction very well.

If the order of the autoregressive model is q, then the expression of MA is shown in equation: [73]

$$y_t = \sum_{i=1}^{q} \theta_i \varepsilon_{t-i} + \varepsilon_t + C$$

The ARMA (p, q) model is a combination of the AR model and the MA model, whose expression is shown in equation: [73]

$$y_t = \sum_{i=1}^{q} \theta_i \varepsilon_{t-i} + \sum_{i=1}^{p} \gamma_i y_{t-i} + \varepsilon_t + C$$

The ARMA model is not combined with differencing, so it can only predict the smooth series. If it is necessary to predict the unstable data series, it is also necessary to properly differ the historical data to obtain the smooth series, and the model combined with differencing is the ARIMA model.

Principle of SARIMA model

SARIMA model is also known as seasonal difference autoregressive sliding average model. SARIMA model is modified from ARMA model by adding the principles of difference and seasonal difference.

The ARMA model has good modeling effect on smooth series data, and its basic form is shown in equation: [73]

$$\varphi(B)X_t = \theta(B)u_t$$

$\varphi(B)$ is the autoregressive coefficient polynomial of the smooth model; $\theta(B)$ is the moving average polynomial.

For non-stationary time series, differencing is required. If the series X_t, reaches a smooth state after differencing of order D, the series X_t, can be expressed as an ARIMA (p, d, q) model of the form shown in equation: [73]

$$\varphi(B)\nabla^d X_t = \theta(B)u_t$$

The period-by-period split of order d is $\nabla^d = (1-B)^d$.

If the series needs to undergo a D-order seasonal difference to reach smoothness after the d-order difference, then the series X_t requires a SARIMA (p, d, q) (P, D, Q, S) model, whose expression is shown in equation: [73]

$$\varphi(B)\Phi(B)^S\nabla^d\nabla_S^D X_t = \theta(B)\Theta(B)^S u_t$$

The seasonal differential of order D is denoted as $\nabla_S^D = (1-B^S)^D$, S is the seasonal period, $\Phi(B)^s$ is the seasonal autoregressive operator, and $\Theta(B)^S$ is the seasonal moving average operator.

3.8.2.4 Prophet Model

Prophet Model Introduction

The Prophet model, developed by FaceBook, is an interactive time series forecasting model that is very simple and practical. It can also automatically fill in missing values without the need for extensive data pre-processing, and has flexible periodic adjustment capabilities for different data forecasts.

Principle of Prophet Model

The Prophet time series prediction model is a four-part superposition of a trend term, a period term, a holiday term and an error term, and the model is composed as shown in equation : [73]

$$y(t) = g(t) + s(t) + h(t) + \varepsilon$$

g(t) is the trend term function to fit the non-periodic variation in the time series. s(t) is the periodic term function to fit the periodicity of a week or a year. h(t) represents the effect caused by special dates such as holidays. ε is the error term, representing the effect of errors that are not considered.

The basic trend term g(t) is often used in a logistic growth model, whose basic form is shown in equation: [73]

$$g(t) = \frac{\mathrm{C}}{1+e^{(-k(t-m))}}$$

C is the saturation value, k is the growth rate, and m is the bias parameter. In addition, the saturation value, growth rate and bias parameter are time-dependent functions that can be changed according to the specific prediction problem.

The periodic term s(t) is a periodic model constructed from the Fourier series, and the expression is shown in equation: [73]

$$s(t) = \sum_{n=1}^{N} [a_n \cos(\frac{2\pi nt}{P}) + b_n \sin(\frac{2\pi nt}{P})]$$

Where t represents the period and P represents the regular period length of the time series.

The step of fitting the period term is to determine the value of N and then the 2N parameters, i.e., $\beta = [a_1, b_1, ..., a_n, b_n]^{\mathrm{T}}$. Using the default value of N of the Prophet model (N = 10 is modeled for each year component), most practical problems with annual cycles can be coped with, and the specific expression is shown in equation: [73]

$$s(t) = X(t)\beta, \beta \sim Normal(0, \sigma)$$
$$X(t) = [\cos(\frac{2\pi(1)t}{365.25}), \sin(\frac{2\pi(1)t}{365.25}), ..., \cos(\frac{2\pi(10)t}{365.25}), \sin(\frac{2\pi(10)t}{365.25})]$$

h(t) is the holiday term, which represents the holiday or important event that will have an impact on the time series. The h(t) expression is shown in equation: [73]

$$h(t) = Z(t)\kappa_i, \kappa_i \sim Normal(0, \sigma)$$
$$Z(t) = [1(t \in D_1), ..., 1(t \in D_i), ..., 1(t \in D_L)]$$

Where i denotes holidays, D_i is the set of past and future holidays, and κ_i denotes the impact of each holiday on the forecast.

3.8.3 Combinatorial Prediction Models

3.8.3.1 Introduction to Combinatorial Prediction

In many forecasting scenarios, a single time series forecasting model has more or less many limitations and lacks stability. Considering the effectiveness of forecasting models, Buckland et al. proposed that the stability of model forecasting effectiveness should be the key factor in selecting forecasting models. In order to compensate for the shortcomings of single models, Bates and Granger proposed the concept of combination models, the core idea of which is to combine the prediction results of these single models by giving each model a certain weight to achieve a great degree of utilization of the advantages of single models and avoid their disadvantages as much as possible. After the idea of combining models was proposed, Clemen's research dispelled the doubts by verifying that the appropriate combination of prediction models has better prediction results and better stability.

The expression for the combination of forecasting models is shown in equation: [73]

$$Combine(t) = \sum_{i}^{n} f_i(t) * \omega_i$$

Where, f_i is the prediction result of the ith single model, ω_i is the weight occupied by the ith model, which indicates the influence of the single model on the combined prediction, and the sum of the weights of all single models is 1.

The combined prediction model combines the prediction results of different single models on data by some specific weighting methods, which can well solve the limitations of single model prediction and also improve the stability of prediction.

3.8.3.2 Combinatorial approach to time series prediction models

The core idea of the combinatorial prediction model is to combine the prediction results of these single models by assigning certain weights to each model to obtain new prediction results with the expectation of improving the accuracy and stability of the prediction.

In the combination of models, the method of assigning weights to different models is very critical, and if the weights are properly assigned, a combination model with much higher

prediction accuracy will be obtained. The most popular weight determination methods nowadays are described as follows.

(1) Equal weight method: The idea of this method is that each single prediction model is given the same weight. It is the most simple and intuitive method, but it is also the least reliable method because there is no other basis.

(2) Least variance method: The idea of this method is that the smaller the variance of the fitting error of a single prediction model, the greater the weight of the model. The minimum variance method is more reliable than the equal weight method, but it also has its limitations and cannot be applied to various scenarios.

(3) Advantage matrix method: Since each single prediction model has its own advantages and disadvantages, the accuracy of the prediction results are also different. If x1 indicates the number of times the first model is more accurate compared with the prediction results of the two models, and x2 indicates the number of times the second model is more accurate compared with the prediction results of the two models, then the weights of the two models are $\omega_1 = \frac{x_1}{x_1 + x_2}$ and $\omega_2 = \frac{x_2}{x_1 + x_2}$.[73]

3.8.3.3 A combinatorial DM-PS4DB prediction model based on the dominance matrix method

In studying the prediction of transaction volume and capacity in AIOps, it is found that the historical time series of both transaction volume and capacity are somewhat periodic and non-stationary by analyzing the dataset in general. The classical time series forecasting models, Prophet model and SARIMA model, have very good fitting effects for the periodic patterns in the time series. Among them, the Prophet model can not only fit the periodic pattern well, but also can fully consider the influence of special days such as holidays on the event series, while the SARIMA model is based on the ARIMA model with the added function of fitting for the periodicity, so it is also very accurate for fitting non-stationary series. In order to fully combine the advantages of a single model and avoid the instability of a single model, this paper proposes a combined DM-PS4DB forecasting model, which uses the weighted approach of the dominance matrix method to combine the forecasting results of Prophet model and SARIMA model to obtain new forecasting results, fully combining the advantages of both, and more accurate and stable forecasting of transaction volume and capacity.

The modeling and forecasting process of the DM-PS4DB forecasting model is as follows.

(1) Data analysis of the original time series and data pre-processing work.

(2) Apply the Prophet prediction model to model the original data, and get the Prophet model with the best effect by adjusting the model parameters and fitting the holiday impact and periodicity pattern of the data, and then perform data prediction and output the result P(t).

(3) Apply SARIMA prediction model to model the original data, and obtain the SARIMA model with the best effect after the process of smoothness test and model order fixing, and then perform data prediction and output the result S(t).

(4) Comparing the prediction results of Prophet model and SARIMA model, the number of times that the prediction results of the two models are more accurate is x1 and x2, respectively, and the respective weights are calculated as $\omega_1 = \frac{x_1}{x_1 + x_2}$ and $\omega_2 = \frac{x_2}{x_1 + x_2}$.

(5) Finally, the prediction results P(t) of the Prophet model and S(t) of the SARIMA model are weighted and combined according to the above weights to obtain the prediction results Y(t) of the DM-PS4DB model, whose expressions are shown in equation: [73]

$$Y(t) = \omega_1 P(t) + \omega_2 S(t)$$
$$\omega_1 = \frac{x_1}{x_1 + x_2}, \omega_2 = \frac{x_2}{x_1 + x_2}, \omega_1 + \omega_2 = 1$$

Chapter 4: Conclusion

As the construction of information technology becomes more and more complete, and the scale of the network becomes more and more massive, people's demand for the network is also increasing, making various industries need more efficient and stable IT systems to provide services, bringing higher requirements for the forward-looking and efficient system operation and maintenance, so the integration of AI and enterprise network is the general trend.

This report provides an overview analysis and study of the application of AI in enterprise networks. The first chapter introduces the definition of the enterprise network, design requirements, interconnection devices, types of enterprise network and their architecture topology and features, then also introduces some network terms, and analyzes the current challenges faced by enterprise network operation, and finally introduces some new generation technologies, which focus on SDN. The second chapter introduces AI and the direction of convergence between AI and computer networks from different perspectives, and finally introduces the current research results of applying AI in SDN. The third chapter introduces the application of AI in enterprise networks, the concept of AIOps, and specifically analyzes how AI Solves specific problems in SDN, the AIOps solutions between Cisco and Juniper, and finally introduces AIOps-based predictive algorithms.

As AIOps has extremely powerful functions such as anomaly detection, fault warning, fault location, and root cause analysis, and with the continuous development and increasing maturity of artificial intelligence technology, AIOps has become the ultimate development trend of IT operation and maintenance.

AIOps can integrate advanced technologies such as big data and machine learning with operations and maintenance scenarios to achieve autonomous learning and self-analysis of operations and maintenance systems. AIOps has an advanced big data platform, which is responsible for collecting various information on different indicators and dimensions and can gather a large amount of data information for artificial intelligence algorithms to analyze and combine, making the quality and efficiency of operations and maintenance greatly improved. AIOps can display and correlate all kinds of indicators of different dimensions in one system or platform through big data technology, realizing a global perspective to monitor and maintain system performance, extracting and reusing similar parts of algorithms in different scenarios, which can not only reduce the workload of operation and maintenance staff, but also improve the efficiency of troubleshooting, and ensure the stable and efficient operation of the system. AIOps can automatically collect data from various indicators for intelligent analysis integrate various scenarios, multiple data sources, and various algorithms to create a platform that is more

conducive to integrating application scenarios and required technologies and avoiding repetitive mechanical work for O&M staff. AIOps integrates knowledge from multiple fields and disciplines, and the diversification of its application scenarios and research of key technologies can trigger in-depth research and development of big data, machine learning, and other technologies, while increasingly mature technologies can, in turn, promote the exploration and refinement of key technologies of AIOps, thus forming a virtuous cycle of bad. In addition, it can get perfect artificial intelligence and other technologies and can promote the implementation of intelligent operation and maintenance as soon as possible.

The ultimate goal of AIOps is to realize the unattended intelligent operation and maintenance of the system, which has the incomparable advantages of the traditional operation and maintenance mode and is the inevitable development trend and the ultimate goal of IT operation and maintenance. Although the AIOps provider or major research institutions can only achieve part of the intelligent operation and maintenance functions, with the continuous maturity of artificial intelligence technology and the increasing number of companies investing in AIOps research, the companies that are currently investing in research and implementation of AIOps are distributed in all walks of life. We believe that it will not take too long to break through the difficulties and realize the many functions of AIOps step by step to achieve the perfect implementation of AIOps.

References

[1]. “What Is an Enterprise Network?” Cisco Inc.

https://www.cisco.com/c/en/us/solutions/enterprise-networks/what-is-an-enterprise-network.html

[2]. “What Is Network Provisioning?” Cisco Inc.

https://www.cisco.com/c/en/us/solutions/automation/what-is-network-provisioning.html

[3]. “What Is Network Management?” Cisco Inc.

https://www.cisco.com/c/en/us/solutions/enterprise-networks/what-is-network-management.html

[4]. Qingkuan, T. (2020). The Ultimate Guide to Enterprise Network Management. Computers & Networks, (13).

[5].“What Is Network Automation?” Cisco Inc.

https://www.cisco.com/c/en/us/solutions/automation/network-automation.html

[6]. “What Is Network Orchestration?” Cisco Inc.

https://www.cisco.com/c/en/us/solutions/enterprise-networks/what-is-network-orchestration.html

[7].“What Is Network Monitoring?” Cisco Inc.

https://www.cisco.com/c/en/us/solutions/automation/what-is-network-monitoring.html

[8].“What Is Network Analytics?” Cisco Inc.

https://www.cisco.com/c/en/us/solutions/analytics/what-is-network-analytics.html

[9].“What Is Network Troubleshooting?” Cisco Inc.

https://www.cisco.com/c/en/us/solutions/enterprise-networks/what-is-network-troubleshooting.html

[10]. Li KX, Wang XW, Yi B, Huang M, Liu XJ. (2021). Survey of intelligent software defined networking. Journal of Software, 2021,32(1)

[11]. Yu, J. (2021). Research on the Application of Artificial Intelligence in Computer Network Technology. Digital Communication World, (7).

[12]. "What is artificial intelligence for networking?" Juniper Inc.

https://www.juniper.net/us/en/research-topics/what-is-ai-for-networking.html

[13]. Yang, Z. (2021). Research on the Application of Artificial Intelligence in Computer Network Technology. Network Security Technology and Applications, (5).

[14]. Liu, T. (2021). Practical Application of Artificial Intelligence Technology in Computer Networks. Wireless Internet Technology, (12).

[15]. Zhang, L., & Liu, J. (2021). The application of artificial intelligence in computer network technology in the era of big data. Technology Wind, (20).

[16]. Chu, B. (2021). Application of the Artificial Intelligence in Computer Network Technology in Big Data Era. Internet + Innovation 2.0, (451).

[17]. Liu, Y. (2021). Analysis of Research Progress and Application of Computer Artificial Intelligence Technology. Management & Technology of SME, (9).

[18]. Shen, X. (2021). Research on the Application of Artificial Intelligence in Computer Network Technology. Computer Programming Skills and Maintenance, (7).

[19]. Xie J, Yu FR, Huang T, et al. (2018). A survey of machine learning techniques applied to software defined networking (SDN): Research issues and challenges. IEEE Communications Surveys & Tutorials, (99):1.

[20]. Rahimi R, Veeraraghavan M, Nakajima Y, et al. (2016). A high-performance

OpenFlow software switch. In: Proc. of the 17th IEEE Int'l Conf. on High Performance Switching and Routing (HPSR). IEEE, 93-99.

[21]. Rodriguez-Natal A, Portoles-Comeras M, Ermagan V, et al. (2015). LISP: A southbound SDN protocol. IEEE Communications Magazine, 53(7):201-207.

[22]. Zheng P, Hu CC, Li H. (2018). Reducing the southbound interface overhead for OpenFlow based on the flow volume characteristics. Journal of Computer Research and Development, 55(2):346-357.

[23]. Junhua B, Ying W, Zhong XX, et al. (2018). An SDN energy saving method based on topology switch and rerouting. In: Proc. of the 2018 IEEE/IFIP Network Operations and Management Symp. (NOMS), 1-5.

[24]. Tang F, Fadlullah ZM, Mao B, et al. (2018) An intelligent traffic load prediction based adaptive channel assignment algorithm in SDN-IoT: A deep learning approach. IEEE Internet of Things Journal, 1.

[25]. Leguay J, Maggi L, Draief M, et al. (2016). Admission control with online algorithms in SDN. In: Proc. of the Network Operations & Management Symp. IEEE, 718-721.

[26]. Nanda S, Zafari F, Decusatis C, et al. (2017). Predicting network attack patterns in SDN using machine learning approach. In: Proc. of the Network Function Virtualization & Software Defined Networks. IEEE, 167-172.

[27]. Jain S, Kumar A, Mandal S, et al. (2013). B4: Experience with a globally-deployed software defined WAN. In: Proc. of the ACM 2013 Conf. on SIGCOMM, 3-14.

[28]. Shi H, Li H, Zhang D, et al. (2017). Efficient and robust feature extraction and selection for traffic classification. Computer Networks, the Int'l Journal of Computer & Telecommunications Networking, 119(C):1-16.

[29]. Shi H, Li H, Zhang D, et al. (2018). An efficient feature generation approach

based on deep learning and feature selection techniques for traffic classification. Computer Networks, (26):81-98.

[30]. Ertam F, Engin A. (2017). A new approach for internet traffic classification: GA-WK-ELM. Measurement, 95:135-142.

[31]. Soysal M, Schmidt EG. (2010). Machine learning algorithms for accurate flow-based network traffic classification: Evaluation and comparison. Performance Evaluation, (6):451-467.

[32]. "AI and the Future of Networking" VMware Inc.

https://wcit2019.org/blog/ai-and-the-future-networking

[33]. "AIOps: Enterprise Network Evolution with ML" Jyoti Bose, 2020.

https://www.calsoftinc.com/blogs/2020/10/aiops-enterprise-network-evolution-with-ml.html

[34]. "What Is Artificial Intelligence in Networking?" Cisco Inc.

https://www.cisco.com/c/en/us/solutions/artificial-intelligence/artificial-intelligence-machine-learning-in-networking.html

[35]. Mhdawi AKA, Al-Raweshidy HS. (2018). iPRDR: Intelligent power reduction decision routing protocol for big traffic flood in hybrid-SDN architecture. IEEE Access, 1.

[36]. Kim S, Son J, Talukder A, et al. (2016). Congestion prevention mechanism based on Q-leaning for efficient routing in SDN. In: Proc. of the Int'l Conf. on Information Networking. IEEE Computer Society, 124-128.

[37]. Pasca STV, Prasad SS, Kataoka K. (2016). AMPF: Application-aware multipath packet forwarding using machine learning and SDN.

[38]. Tang F, Mao B, Fadlullah ZM, et al. (2017). On removing routing protocol from future wireless networks: A real-time deep learning approach for intelligent

traffic control. IEEE Wireless Communications, 99:1-7.

[39]. Mao B, Tang FX, Fadlullah ZM. (2018). A novel non-supervised deep-learning-based network traffic control method for software defined wireless networks. IEEE Wireless Communications, (4):74-81.

[40]. Pinto EMDL, Lachowski R, Pellenz ME, et al. (2018). A machine learning approach for detecting spoofing attacks in wireless sensor networks. In: Proc. of the 32nd IEEE Int'l Conf. on Advanced Information Networking and Applications (AINA). IEEE, 752-758.

[41]. Huang H, Guo S, Li P, Ye B, Stojmenovic I. (2015). Joint optimization of rule placement and traffic engineering for QoS provisioning in software defined network. IEEE Trans. on Computers, (12):3488-3499.

[42]. Mao B, Fadlullah ZM, Tang F, et al. (2017). Routing or computing. The paradigm shift towards intelligent computer network packet transmission based on deep learning. IEEE Trans. on Computers, 1.

[43]. Geyer F, Carle G. (2018). Learning and generating distributed routing protocols using graph-based deep learning. In: Proc. of the 2018 Workshop on Big Data Analytics and Machine Learning for Data Communication Networks, 40-45.

[44]. Lin I, Akyildiz F, Wang P, Luo M. (2016). QoS-aware adaptive routing in multi-layer hierarchical software defined networks: A reinforcement learning approach. In: Proc. of the 2016 IEEE Int'l Conf. on Services Computing (SCC). San Francisco, 25-33.

[45]. Nanda S, Zafari F, Decusatis C, et al. (2017). Predicting network attack patterns in SDN using machine learning approach. In: Proc. of the Network Function Virtualization & Software Defined Networks. IEEE, 167-172.

[46]. Song C, Park Y, Golani K, et al. (2017). Machine-learning based threat-aware system in software defined networks. In: Proc. of the 26th Int'l Conf. on Computer Communication and Networks (ICCCN). IEEE, 1-9.

[47]. Silva ASD. (2016). Atlantic: A framework for anomaly traffic detection, classification, and mitigation in SDN. In: Proc. of the Network Operations & Management Symp. IEEE, 27-35.

[48]. Bawany NZ, Shamsi JA, Salah K. (2017). DDoS attack detection and mitigation using SDN: Methods practices and solutions. Arabian Journal for Science and Engineering, 42(2):425-441.

[49]. Dayal N, Srivastava S. (2017). Analyzing behavior of DDoS attacks to identify DDoS detection features in SDN. In: Proc. of the Int'l Conf. on Communication Systems and Networks (COMSNETS), 274-281.

[50]. Niyaz Q, Sun W, Javd AY. (2016). A deep learning based DDoS detection system in software-defined networking (SDN).

[51]. Chen Z, Jiang F, Cheng Y, et al. (2018). XGBoost classifier for DDoS attack detection and analysis in SDN-based cloud. In: Proc. of the 2018 IEEE Int'l Conf. on Big Data and Smart Computing (BigComp). IEEE Computer Society, 251-256.

[52]. Hegde S, Koolagudi SG, Bhattacharya S. (2015). Scalable and fair forwarding of elephant and mice traffic in software defined networks. Computer Networks, 92(2).

[53]. Namdev N, Agrawal S, Silkari S. (2015). Recent advancement in machine learning based internet traffic classification. Procedia Computer Science, 60(1):784-791.

[54]. Li D, Hu G, Wang Y, et al. (2015). Network traffic classification via non-convex multi-task feature learning. Neurocomputing, 152: 322-332.

[55]. Tang F, Li L, Barolli L, et al. (2017). An efficient sampling and classification approach for flow detection in SDN-based big data centers. In: Proc. of the 31st IEEE Int'l Conf. on Advanced Information Networking and Applications (AINA). IEEE Computer Society, 1106-1115.

[56]. Jain S, Khandelwal M, Katkar A, et al. (2017). Applying big data technologies

to manage QoS in an SDN. In: Proc. of the Int'l Conf. on Network & Service Management. IEEE, 302-306.

[57]. Geyer F. (2017). Routing optimization for SDN networks based on pivoting rules for the simplex algorithm. In: Proc. of the 13th Int'l Conf. on Design of Reliable Communication Networks (DRCN 2017). Munich, 1-8.

[58]. Su Y, Peng T, Zhong X, et al. (2017). Matching model of flow table for networked big data.

[59]. Azzouni A, Boutaba R, Pujolle G. (2017). NeuRoute: Predictive dynamic routing for software-defined networks.

[60]. Polson NG, Sokolov VO. (2017). Deep learning for short-term traffic flow prediction. Transportation Research Part C: Emerging Technologies, 79:1-17.

[61]. Huang W. (2019). Research on AIOps Technologies Based on Machine Learning. Beijing Jiaotong University.

[62]. "What Is AIOps?" Cisco Inc.

https://www.cisco.com/c/en/us/solutions/artificial-intelligence/what-is-aiops.html

[63]. "What is AIOps?" Juniper Inc.

https://www.juniper.net/us/en/research-topics/what-is-aiops.html

[64]. "Artificial Intelligence For IT Operations - AIOps" Juniper Inc.

https://www.juniper.net/us/en/solutions/artificial-intelligence-for-it-operations-aiops.html

[65]. Du Y. (2021). AIOps a powerful tool for network operation and maintenance. Computers and Networks, 47(05):12-13.

[66]. "Mist AI and Cloud" Juniper Inc.

https://www.juniper.net/us/en/products/mist-ai.html

[67]. "Juniper Mist Wi-Fi Assurance" Juniper Inc.

https://www.juniper.net/us/en/products/cloud-services/wi-fi-assurance.html

[68]. "Juniper Mist Wired Assurance" Juniper Inc.

https://www.juniper.net/us/en/products/cloud-services/wired-assurance.html

[69]. "Marvis Virtual Network Assistant" Juniper Inc.

https://www.juniper.net/us/en/products/cloud-services/virtual-network-assistant.html

[70]. "Cisco DNA Assurance: AI/ML guided IT operations (AIOps) At-a-Glance" Cisco Inc.

https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/nb-06-dna-assurance-aag-cte-en.html?oid=aagen016863

[71]. "Cisco DNA Center" Cisco Inc.

https://www.cisco.com/c/en/us/products/cloud-systems-management/dna-center/index.html

[72]. "AI and Machine Learning" Cisco Inc.

https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/digital-network-architecture/nb-06-cisco-dna-ai-ml-primer-cte-en.html

[73]. Zhang C. (2021). Research and Application of Forecast Algorithm Based on AIOps. North China Electric Power University.