REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITE M'HAMED BOUGARA-BOUMERDES

Faculté de **T**echnologie
Département **I**ngénierie des **S**ystèmes **E**lectriques

Mémoire de Master

Présenté par

Bouderba Chems Eddine

Filière : Télécommunications

Spécialité : Réseaux ET Télécommunications

Study and Implementation of the Software-Defined Networking Approach in Branch Network

---

Organisme d'accueil : SARL COSYS

Soutenu le 02 /06 /2024 devant le jury composé de:

Akroum	Hamza	IMC	INGM	Président
Meriahi	Yassine	PROFESSOR	INGM	Encardreur
Belhabchia	Malik	ING	INGM	jury

Année Universitaire : 2023/2024

Acknowledgments

We thank God, Almighty Allah, for giving us health, courage, willpower, and patience to complete our final year project.

My sincere thanks and deep gratitude go to my supervisor, **Mr.yassine Meriahi**, for his availability, encouragement, and patience with me.

I would like to sincerely thank the members of the jury who honor me by evaluating my work.

My profound gratitude goes to my parents for their unwavering support, both moral and financial, throughout all the years of our studies.

I also wish to express our heartfelt thanks to our sisters, brothers, and all our relatives and friends who contributed to the realization of this thesis.

Finally, My thanks go to our entire class and to everyone who contributed, directly or indirectly, to the completion of this work.

Summary

Software-Defined Networking (SDN) represents a significant shift in network architecture, aiming to create networks that are more open, flexible, and simple by decoupling the control plane from the data plane. This separation allows for centralized control and dynamic management of network resources. SDN solutions, such as Huawei's iMaster NCE, exemplify the potential of this technology. iMaster NCE is an intelligent network automation platform that combines management, control, analysis, and AI capabilities to deliver comprehensive network solutions. It supports various applications, including data center management with iMaster NCE application ,These applications provide full lifecycle management, fast service provisioning, and intelligent operations and maintenance. Additionally, the simulation of branch networks using iMaster NCE demonstrates how SDN can streamline network deployment, optimize service provisioning, and enhance overall network performance, showcasing the transformative impact of SDN in enterprise environments.

Résumé

Le réseau défini par logiciel (SDN) représente un changement significatif dans l'architecture réseau, visant à créer des réseaux plus ouverts, flexibles et simples en dissociant le plan de contrôle du plan de données. Cette séparation permet un contrôle centralisé et une gestion dynamique des ressources réseau. Les solutions SDN, telles que iMaster NCE de Huawei, illustrent le potentiel de cette technologie. iMaster NCE est une plateforme d'automatisation de réseau intelligent qui combine des capacités de gestion, de contrôle, d'analyse et d'IA pour offrir des solutions réseau complètes. Elle prend en charge diverses applications, notamment la gestion des centres de données avec iMaster NCE application, Ces applications offrent une gestion du cycle de vie complet, un provisionnement rapide des services et des opérations et maintenances intelligentes. De plus, la simulation de réseaux de succursales utilisant iMaster NCE démontre comment le SDN peut rationaliser le déploiement du réseau, optimiser le provisionnement des services et améliorer les performances globales du réseau, montrant ainsi l'impact transformateur du SDN dans les environnements d'entreprise.

الملخص

تمثل تحولًا جذريًا في بنية الشبكات، حيث تهدف إلى إنشاء شبكات أكثر انفتاحًا (SDN) الشبكات المعرفة بالبرمجيات ومرونة وبساطة عن طريق فصل طبقة التحكم عن طبقة البيانات. يتيح هذا الفصل التحكم المركزي والإدارة الديناميكية .من هواوي، تُظهر الإمكانات الكبيرة لهذه التكنولوجيا iMaster NCE ، مثلSDN لموارد الشبكة. الحلول المعتمدة على هي منصة ذكية لأتمتة الشبكات تجمع بين قدرات الإدارة والتحكم والتحليل والذكاء الاصطناعي لتقديم iMaster NCE iMaster NCE حلول شاملة للشبكات. تدعم المنصة تطبيقات متنوعة، بما في ذلك إدارة مراكز البيانات باستخدام توفر هذه التطبيقات إدارة شاملة لدورة الحياة، وتوفير سريع للخدمات، وعمليات وصيانة ذكية. بالإضافة applications تبسيط نشر الشبكات، SDN كيف يمكن لتكنولوجيا iMaster NCE إلى ذلك، تُظهر محاكاة شبكات الفروع باستخدام في بيئات الشركات SDN وتحسين توفير الخدمات، وتحسين الأداء العام للشبكات، مما يبرز التأثير التحويلي لـ

List Of Content :

Table Of Figures

Table Of Tables :

List des Abbreviations:

- **API**: Application Programming Interface
- **BGP**: Border Gateway Protocol
- **Br**: Bridge
- **BYOD**: Bring Your Own Device
- **CLI**: Command Line Interface
- **Gb**: Giga Bit
- **HTTP**: Hyper Text Transfer Protocol (Protocole de Transfert Hyper Texte)
- **IP**: Internet Protocol
- **IPv4**: Internet Protocol version 4
- **LAN**: Local Area Network
- **MAC**: Media Access Control
- **MPLS**: Multiprotocol Label Switching
- **NETCONF**: NETwork CONFiguration protocol
- **ODL**: OpenDaylight
- **OF**: OpenFlow
- **OFM**: OpenFlow Manager
- **OVF**: Open View Finder
- **OVS**: Open Virtual Switch
- **Ovsdb**: Open Virtual Switch Database
- **QoS**: Quality of Service (Qualité de service)
- **RAM**: Random Access Memory
- **REST**: REpresentational State Transfer
- **SAL**: Service Abstraction Layer (Couche d'abstraction de service)
- **SDN**: Software Defined Network (Réseau défini par logiciel)
- **SNMP**: Simple Network Management Protocol (Protocole simple de gestion de réseau)
- **SSH**: Secure Shell
- **TCP**: Transmission Control Protocol
- **TLS**: Transport Layer Security
- **TTL**: Time To Live

- **UDP**: User Datagram Protocol
- **VLAN**: Virtual Local Area Network
- **VM**: Virtual Machine (Machine virtuelle)
- **WAN**: Wide Area Network
- **SD-WAN**: Software-Defined Wide Area Network
- **OSS/BSS**: Operations Support Systems / Business Support Systems
- **NFV**: Network Functions Virtualization
- **RIP**: Routing Information Protocol
- **OSPF**: Open Shortest Path First
- **RFCs**: Request for Comments
- **ACL**: Access Control List
- **RMON**: Remote Monitoring
- **EIGRP**: Enhanced Interior Gateway Routing Protocol
- **VoIP**: Voice over IP
- **LSPs**: Label Switched Paths
- **IETF**: Internet Engineering Task Force
- **VN**: Virtual Network
- **IoT**: Internet of Things
- **SBI**: Southbound Interface
- **NBI**: Northbound Interface
- **SSL**: Secure Sockets Layer
- **OFPT**: OpenFlow Protocol Type
- **VXLAN**: Virtual Extensible LAN
- **GUI**: Graphical User Interface
- **QR**: Quick Response (code)
- **HQ**: Headquarters
- **DHCP**: Dynamic Host Configuration Protocol
- **AC**: Alternating Current
- **ESN**: Electronic Serial Num

General Introduction :

The rapid evolution of networking technology has paved the way for Software-Defined Networking (SDN), a revolutionary paradigm that decouples the control plane from the data plane, thus enabling centralized and programmable management of network resources. SDN addresses the growing need for networks that are more open, flexible, and simple to manage. This project embarks on a comprehensive exploration of SDN, delving into its fundamental principles and practical applications, particularly within the context of enterprise networks. The objective is to elucidate the significant changes SDN brings to network design and administration, enhancing scalability, flexibility, and operational efficiency.

Through this project, we investigate various components that constitute the SDN ecosystem, including controllers, protocols, and interfaces such as OpenFlow, NETCONF, and OVSDB. A special focus is given to Huawei's iMaster NCE, an intelligent network automation platform that integrates management, control, analysis, and AI capabilities. The iMaster NCE exemplifies how advanced SDN solutions can streamline network operations, from initial deployment through to ongoing maintenance and optimization.

Additionally, a hands-on simulation of a branch network is conducted to illustrate the practical deployment and management capabilities of SDN. This simulation not only demonstrates the theoretical concepts but also provides a real-world scenario where the benefits of SDN, such as faster deployment times, improved management efficiency, and enhanced service quality, are clearly visible. By understanding both the theoretical and practical aspects of SDN, this project aims to provide a holistic view of how SDN is shaping the future of networking.

1 Traditional Network :

1.1 Background of Networking

1.1.1 Traditional Networking:

Traditional networking involves a hardware-centric approach where each network device (such as routers, switches, and firewalls) has its own dedicated control and data planes. This architecture has been the backbone of network infrastructure for decades.

Network Topologies:

Bus Topology: All devices are connected to a single central cable. Simple and cost-effective but prone to collisions and failures.
Star Topology: All devices are connected to a central hub or switch. Offers better performance and fault tolerance.
Ring Topology: Each device is connected to two other devices, forming a circular data path. Data travels in one direction, reducing collisions.
Mesh Topology: Devices are interconnected, providing multiple paths for data to travel. Highly reliable and fault-tolerant.

1.1.2 Evolution of networking technologies :

Over the past few decades, networking technologies have evolved significantly to address the limitations of traditional approaches and meet increasing demands for performance, scalability, and flexibility.

Ethernet:
Development: Ethernet has become the dominant wired networking technology, providing high-speed data transfer capabilities. From its inception in the 1970s, Ethernet standards have evolved from 10 Mbps to 100 Gbps and beyond.
Technologies like Gigabit Ethernet and 10 Gigabit Ethernet have extended Ethernet's capabilities to support modern data center and enterprise environments.
Suggested Picture: Diagram showing the evolution of Ethernet speeds and standards.

IP Addressing:

IPv4: The most widely used version of the Internet Protocol, with a 32-bit address space providing approximately 4.3 billion unique addresses.

IPv6: Developed to address IPv4 exhaustion, IPv6 uses a 128-bit address space, offering a virtually unlimited number of unique addresses.

RIP (Routing Information Protocol): A distance-vector protocol using hop count as a metric. Simple but limited in scalability.

OSPF (Open Shortest Path First): A link-state protocol that provides faster convergence and greater scalability, widely used in large enterprise networks.

BGP (Border Gateway Protocol): The protocol used to route data between different autonomous systems on the Internet, essential for global internet connectivity.

Network Management:

SNMP (Simple Network Management Protocol): A protocol used for managing and monitoring network devices. It provides a standardized way to collect and organize information about managed devices.

CLI (Command Line Interface): The traditional method for configuring network devices. While powerful, it requires manual input by network administrators and can be time-consuming.

1.2 Typical IP Network - Distributed Network

A typical IP network is characterized by its distributed nature, operating with peer-to-peer control. In this model, each network device (such as routers and switches) has independent forwarding, control, and management planes. This structure forms the backbone of traditional networking, ensuring robust and scalable network operations.

1.2.1 Independent Planes in Network Devices

In a typical IP network, each network device handles its own forwarding, control, and management functions independently. This autonomy allows for flexible and resilient network management.

1.2.1.1 Forwarding Plane

- **Function:** The forwarding plane, also known as the data plane, provides high-speed, non-blocking data channels for service switching between service modules. It processes and forwards various types of data on its interfaces.
- **Operations:** Specific data processing and forwarding tasks occur on the forwarding plane, including Layer 2 and Layer 3 switching, Access Control Lists (ACL), Quality of Service (QoS), multicast, and security protection.

1.2.1.2 Control Plane

- **Function:** The control plane is responsible for protocol processing, service processing, route calculation, forwarding control, service scheduling, traffic statistics collection, and system security.
- **Operations:** It manages all network protocols, providing the necessary network information and forwarding query entries required for data processing and forwarding on the data plane.

1.2.1.3 Management Plane

- **Function:** The management plane handles system monitoring, environment monitoring, log and alarm processing, system software loading, and system upgrades.
- **Operations:** It offers network management personnel tools like Telnet, web interfaces, SSH, SNMP, and RMON for device management. It supports, parses, and executes commands for setting network protocols and allows for the pre-configuration of parameters related to various protocols on the control plane.

1.3 Advantages of Typical IP Networks

Typical IP networks offer several benefits due to their distributed nature:

- **Protocol Decoupling:** Network devices are decoupled from specific protocols, allowing for flexibility and adaptability. This decoupling ensures that devices from different vendors can interoperate seamlessly.
- **Vendor Compatibility:** The adherence to standard protocols (e.g., TCP/IP) ensures that devices from various manufacturers can work together, promoting a multi-vendor environment.
- **Network Convergence:** In the event of network faults, distributed control mechanisms enable rapid convergence, minimizing downtime and maintaining network stability. Each device can independently reroute traffic based on updated routing information.

1.3.1 Fault Tolerance and Scalability

Distributed IP networks are inherently scalable and resilient:

- **Scalability:** The decentralized architecture allows the network to scale horizontally by adding more devices without significant changes to the existing infrastructure.
- **Fault Tolerance:** The independence of control planes across devices ensures that network failures are localized and do not propagate, enhancing overall network robustness.

1.3.2 Example: Switch Architecture

The switch is used as an example to describe the forwarding plane, control plane, and management plane.

- **Forwarding plane:** provides high-speed, non-blocking data channels for service switching between service modules. The basic task of a switch is to process and forward various types of data on its interfaces. Specific data processing and forwarding, such as Layer 2, Layer 3, ACL, QoS, multicast, and security protection, occur on the forwarding plane.

- **Control plane:** provides functions such as protocol processing, service processing, route calculation, forwarding control, service scheduling, traffic statistics collection, and system security. The control plane of a switch is used to control and manage the running of all network protocols. The control plane provides various network information and forwarding query entries required for data processing and forwarding on the data plane.
- **Management plane:** provides functions such as system monitoring, environment monitoring, log and alarm processing, system software loading, and system upgrade. The management plane of a switch provides network management personnel with Telnet, web, SSH, SNMP, and RMON to manage devices, and supports, parses, and executes the commands for setting network protocols. On the management plane, parameters related to various protocols on the control plane must be pre-configured, and the running of the control plane can be intervened if necessary.

1.4 Thinking in the Network Field: Problems Faced by Typical Networks :

As the demand for more robust and efficient networking solutions grows, traditional IP networks face numerous challenges that can hinder performance, scalability, and manageability. Despite their established architecture and widespread use, these networks are not without their limitations. This section explores the critical issues

encountered in typical network environments, shedding light on the complexities and inefficiencies that network administrators and engineers must navigate. By understanding these problems, we can better appreciate the innovations driving modern networking technologies such as Software-Defined Networking (SDN).

1.4.1 Frequent Network Congestion

Frequent network congestion is a common issue in traditional IP networks, often caused by the increasing volume of data traffic and the limitations of static routing protocols. When multiple devices and applications compete for limited bandwidth, bottlenecks occur, leading to reduced performance and slower data transmission. This congestion is exacerbated by the lack of dynamic adjustments in traditional networks, where static routes are predefined and do not account for real-time traffic conditions. As a result, some network paths become overloaded while others remain underutilized, further contributing to inefficiencies.

- **Bandwidth-Based Route Selection :**

- **Dynamic Routing Protocols:** Implement routing protocols such as OSPF (Open Shortest Path First) or EIGRP (Enhanced Interior Gateway Routing Protocol) that support dynamic adjustments based on network traffic.
- **Real-Time Traffic Monitoring:** Utilize tools that monitor network traffic in real-time, providing insights into which paths are congested and which are underutilized.
- **Load Balancing:** Distribute traffic more evenly across multiple paths to prevent any single route from becoming a bottleneck. Load balancing can be achieved through advanced routing techniques and algorithms.
- **Quality of Service (QoS):** Implement QoS policies to prioritize critical traffic, ensuring that essential services receive the necessary bandwidth even during peak times.

By adopting bandwidth-based route selection, traditional networks can achieve more efficient utilization of available resources, reducing congestion and improving overall network performance.

- **Tunnel Establishment Based on Fixed Sequence**

Another solution to address frequent network congestion is the use of tunnel establishment based on a fixed sequence. This technique involves setting up dedicated tunnels for specific types of traffic to ensure consistent and reliable data flow.

- **Fixed-Sequence Tunnels:** Establish fixed-sequence tunnels for critical traffic flows. These tunnels are predetermined paths that prioritize specific types of data, ensuring they have a reserved bandwidth and reduced latency.
- **Traffic Segmentation:** Segment traffic based on its priority and nature. For example, VoIP (Voice over IP) and video conferencing can be routed through dedicated tunnels to maintain quality and performance.
- **MPLS (Multiprotocol Label Switching):** Use MPLS technology to create these tunnels. MPLS can establish label-switched paths (LSPs) that direct traffic along predefined routes, optimizing the use of network resources.
- **Consistent Performance:** By using fixed-sequence tunnels, network administrators can provide a consistent performance for high-priority applications, reducing the impact of congestion on critical services.

- **Monitoring and Adjustment:** Regularly monitor the performance of these tunnels and adjust their configurations as necessary to respond to changing network conditions and traffic patterns.

By implementing tunnel establishment based on fixed sequences, traditional networks can significantly reduce congestion for high-priority traffic, ensuring reliable and efficient data transmission.

1.4.2 Complex Network Technologies :

Traditional IP networks are known for their robustness and reliability, but they also come with inherent complexities. These complexities can make network management and maintenance challenging. Two significant issues contributing to this complexity are the multitude of network protocols and the difficulty in network configuration.

- **Many Network Protocols :**

Network technology experts need to learn many RFCs (Request for Comments) related to network devices. RFCs are formal documents from the Internet Engineering Task Force (IETF) that describe the specifications, protocols, procedures, and standards for various aspects of networking. The understanding of these RFCs is essential for ensuring interoperability and proper network functioning.

- **Volume of RFCs:** The number of RFCs is continually growing as new technologies and standards are developed. This expansion requires network professionals to stay updated with the latest changes, which can be time-consuming and challenging.
- **Complexity of Protocols:** Different protocols serve different purposes and need to be configured to work together seamlessly. Each protocol, such as TCP/IP, OSPF, BGP, and MPLS, operates at different layers of the OSI model and has its own set of specifications.
- **Training and Expertise:** Network administrators and engineers must have extensive knowledge of each protocol's operation and configuration. The complexity of understanding and implementing these protocols increases the potential for misconfiguration and makes troubleshooting difficult.

- **Difficult network configuration:**

Configuring network devices in traditional IP networks can be a daunting task. Each vendor's devices come with their own unique set of commands and configuration procedures. To effectively manage these devices, network administrators need to master tens of thousands of commands. The number of commands continues to grow as new features and functionalities are added, further complicating the task.

- **Vendor-Specific Knowledge:** Each network equipment vendor has its own command-line interface (CLI) syntax and commands. Learning these commands requires significant time and effort.
- **Volume of Commands:** The sheer number of commands, which can range into the tens of thousands, is overwhelming. This complexity can lead to errors during configuration, which may result in network outages or security vulnerabilities.
- **Continuous Learning:** As vendors release new updates and devices, the command sets evolve, necessitating continuous learning and adaptation by network administrators.
- **Manual Configuration:** Traditional networks often require manual configuration of each device, which is time-consuming and prone to human error. This manual process is not scalable for large networks with numerous devices.

1.4.3 Difficulty in Locating and Analyzing Network Faults :

Traditional IP networks often struggle with efficiently identifying and resolving network faults, which can lead to prolonged downtime and negatively impact network performance and reliability. Here we explore the challenges associated with locating and analyzing faults in traditional networks.

- **Manual Fault Identification:** In many cases, network administrators must manually sift through logs and performance data to identify issues, a time-consuming and error-prone process. This manual approach lacks the efficiency needed to quickly resolve network issues.

- **Manual Packet Obtaining for Locating Faults** : In traditional IP networks, one of the key challenges in fault management is the manual process of obtaining packets to diagnose and locate faults. This method involves several steps that can be time-consuming and complex, making it difficult for network administrators to quickly and accurately identify issues.

- **Manual Fault Diagnosis :** Manual fault diagnosis is a critical but challenging aspect of traditional network management. This process involves identifying, isolating, and resolving network issues through manual intervention, which can be both time-consuming and error-prone. Here we explore the difficulties and implications of manual fault diagnosis in traditional IP networks.

Traditional O&M networks rely on manual fault identification, location, and diagnosis.
More than 85% of network faults are found only after service complaints. Problems cannot be proactively identified or analyzed.

1.4.4 Slow Network Service Deployment :

In traditional IP networks, deploying new network services is often slow and cumbersome. This section covers the challenges associated with various network policies, service networks, and the physical network infrastructure.

1.4.4.1 Network Policy:

- **Bandwidth Policy:** Managing bandwidth allocation manually is complex and time-consuming. Policies must be set on each device to ensure fair distribution and prevent congestion, which requires meticulous planning and ongoing adjustments.
- **QoS Policy:** Quality of Service (QoS) policies are essential for prioritizing critical traffic, but configuring QoS manually across a network is prone to errors and inconsistencies, impacting service quality.
- **Access Policy:** Implementing access policies to control who can access network resources involves configuring permissions on multiple devices. This manual process is error-prone and difficult to scale.

1.4.4.2 Service Network:

- **VN for Office Purposes:** Virtual Networks (VNs) for office use require configurations to support typical business applications and secure data transmission. Setting up these VNs manually is slow and resource-intensive.
- **VN for Scientific Research:** Research networks often need high bandwidth and low latency. Configuring these networks to meet specific scientific requirements can be complex and time-consuming.

- **VN for Video Surveillance:** VNs for video surveillance require reliable, high-bandwidth connections to ensure uninterrupted video streams. Manual setup of these networks to handle large volumes of data from multiple cameras is challenging.

1.4.4.3 Physical Network:

- **Device Configuration:** Physical network devices like routers and switches need to be manually configured for each new service deployment. This includes setting up interfaces, routing protocols, and security settings, which can be laborious.
- **Infrastructure Changes:** Adding new services often requires physical changes to the network infrastructure, such as installing new hardware or rewiring existing setups. These changes are time-consuming and can disrupt ongoing operations.
- **Scalability:** Scaling the physical network to accommodate new services involves significant planning and manual intervention, making it difficult to respond quickly to increasing demands

2 SDN network :

Software-Defined Networking (SDN) represents a significant shift in network architecture, fundamentally transforming how networks are designed, deployed, and managed. SDN was conceived as a solution to the limitations of traditional networking, driven by the need for more flexible, scalable, and manageable networks. The origin of SDN can be traced back to the innovative efforts of the Clean Slate Program at Stanford University, which aimed to reimagine network architecture from the ground up.

- **Birth of SDN: The Clean Slate Program**

The Clean Slate Program at Stanford University was initiated with the visionary goal of fundamentally rethinking the foundational principles of networking. Traditional networks, characterized by their rigid and complex configurations, were increasingly seen as obstacles to innovation and agility. The Clean Slate Program sought to address these limitations by developing a new network architecture that prioritized flexibility, scalability, and centralized control.

- The Clean Slate Program emphasized challenging existing networking assumptions and exploring novel approaches to improve network performance, security, and adaptability. The program aimed to create a network infrastructure capable of supporting the rapid evolution of applications and services, particularly in the context of cloud computing, mobile applications, and large-scale data centers.
- The program's research focused on creating a more dynamic and programmable network environment that could be easily managed and adapted to meet the changing needs of users and applications.

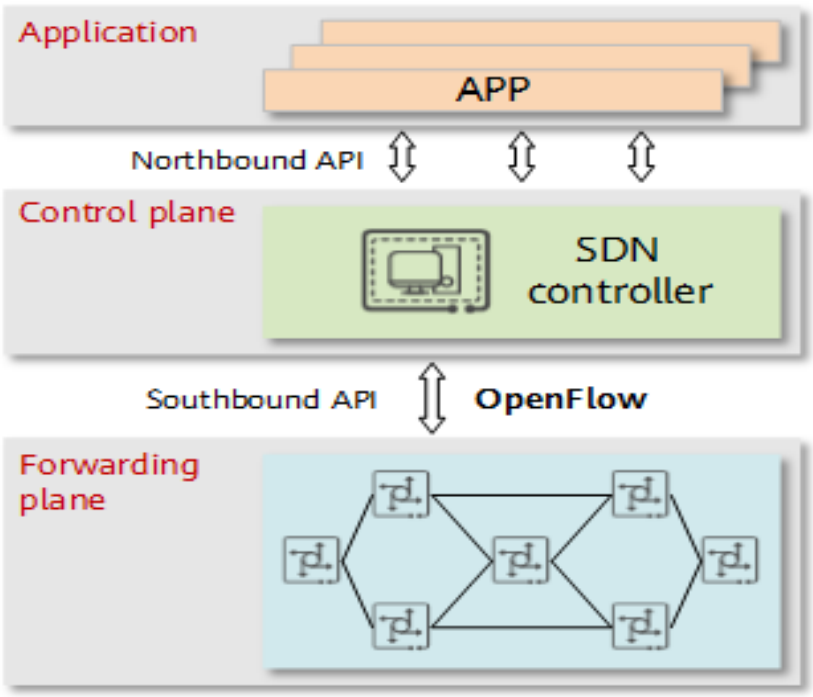


Figure 1Relationship between control plane, forwarding plane, and applications [1]

2.1 Core Principles of SDN

At the heart of SDN is the concept of decoupling the control plane from the data plane within network devices. This separation facilitates centralized control and programmability, providing a more efficient and dynamic approach to network management.

Control Plane vs. Data Plane:

- **Control Plane:** The control plane is responsible for decision-making processes, such as routing, traffic management, and policy enforcement. It determines the paths that data packets should take through the network based on a global view of the network state.
- **Data Plane:** The data plane executes the actual forwarding of data packets based on the decisions made by the control plane. It handles the high-speed transmission of data across the network infrastructure, ensuring efficient and reliable data delivery.

The separation of these two planes allows for centralized management and optimization of network resources, leading to significant improvements in network efficiency, flexibility, and scalability.

2.2 Early Characteristics of SDN

In its initial phase, SDN was defined by three key characteristics that differentiated it from traditional network architectures:

- **Forwarding-Control Separation:**

  - **Decoupling Functions:** SDN separates the network's control functions from its data forwarding functions. This decoupling allows the control plane to operate independently, providing centralized oversight and management of network resources.
  - **Enhanced Flexibility:** Network devices, such as switches and routers, become simple forwarding entities, while the control logic resides in a centralized SDN controller. This configuration allows for dynamic adjustments to network behavior based on real-time requirements and global network policies.
  - **Simplified Hardware:** By offloading control functions to a centralized controller, the hardware requirements for individual network devices are simplified. This reduces the complexity and cost of network equipment, making it easier to deploy and scale the network.

- **Centralized Control:**

  - **SDN Controller:** A central SDN controller manages the entire network, making global decisions and distributing forwarding rules to individual network devices. This centralization simplifies network management and ensures consistent policy enforcement across the network.
  - **Network Visibility:** Centralized control provides a comprehensive view of the network, enabling administrators to optimize resource utilization, enhance security, and quickly respond to changing network conditions. This visibility is crucial for troubleshooting, performance monitoring, and proactive network management.

- **Global Optimization:** With a centralized control plane, the SDN controller can optimize network performance globally, rather than on a per-device basis. This enables more efficient use of network resources and improves overall network performance.

➢ **Open Programmable Interfaces:**

- **OpenFlow Protocol:** OpenFlow was one of the first and most widely adopted protocols for communication between the SDN controller and network devices. It defines how the control plane interacts with the data plane, enabling programmability and allowing network administrators to implement custom forwarding rules.
- **API-Driven Management:** SDN promotes the use of open Application Programming Interfaces (APIs), allowing network administrators and developers to programmatically configure and manage the network. This programmability supports rapid innovation and customization of network functions and services.
- **Vendor Agnostic:** The use of open standards and APIs ensures that SDN solutions can be implemented across devices from different vendors, promoting interoperability and reducing vendor lock-in.

➢ **Evolution and Impact**

Since its inception, SDN has significantly evolved, influencing both academic research and commercial network solutions. The principles of SDN have been widely adopted, leading to the development of various SDN platforms and products that continue to transform networking practices.

- **Industry Adoption:**
  - Major technology companies, including Cisco, Juniper, VMware, and Google, have embraced SDN, integrating its principles into their products and services. These companies have developed SDN-based solutions that enhance network agility, reduce operational costs, and improve service delivery.
  - SDN has also found applications in various domains, including data centers, telecommunications, enterprise networks, and cloud computing. Its flexibility and programmability make it well-suited for diverse networking environments.
- **Commercial Implementations:**
  - **Google's B4:** One of the earliest large-scale implementations of SDN was Google's B4 network, which used SDN principles to manage its global data center interconnect network. B4 demonstrated the scalability and efficiency of SDN in a production environment, paving the way for broader adoption.
  - **AT&T's Network on Demand:** AT&T adopted SDN to offer flexible, on-demand network services to its customers. This initiative highlighted the potential of SDN to provide dynamic, customer-centric network services.
- **Ongoing Research:**
  - The SDN paradigm continues to be a focal point for research and development, driving innovations in network virtualization, automation, and security. Researchers are exploring new ways to leverage SDN to address emerging network challenges and opportunities.

- Network Function Virtualization (NFV): SDN is often used in conjunction with NFV, which virtualizes network functions traditionally carried out by dedicated hardware. This combination enhances network flexibility and reduces costs.
- Security Enhancements: Researchers are developing SDN-based solutions to enhance network security, such as dynamic threat detection and automated mitigation strategies.

2.3 Difference between Software Defined Network and Traditional Network :

Software Defined Network (SDN) is a modern networking architecture approach that enables the control and management of the network using software applications. It allows for the programming of the entire network's behavior in a centrally controlled manner through software applications using open APIs. SDN improves performance through network virtualization, making it possible to create virtual networks or control traditional networks with the help of software. Traditional networks refer to the conventional way of networking, which relies on fixed and dedicated hardware devices such as routers and switches to control network traffic. Traditional networks are static and based on hardware network appliances, and while they are well-established, they have limitations in scalability, flexibility, and automation compared to SDN. [2]

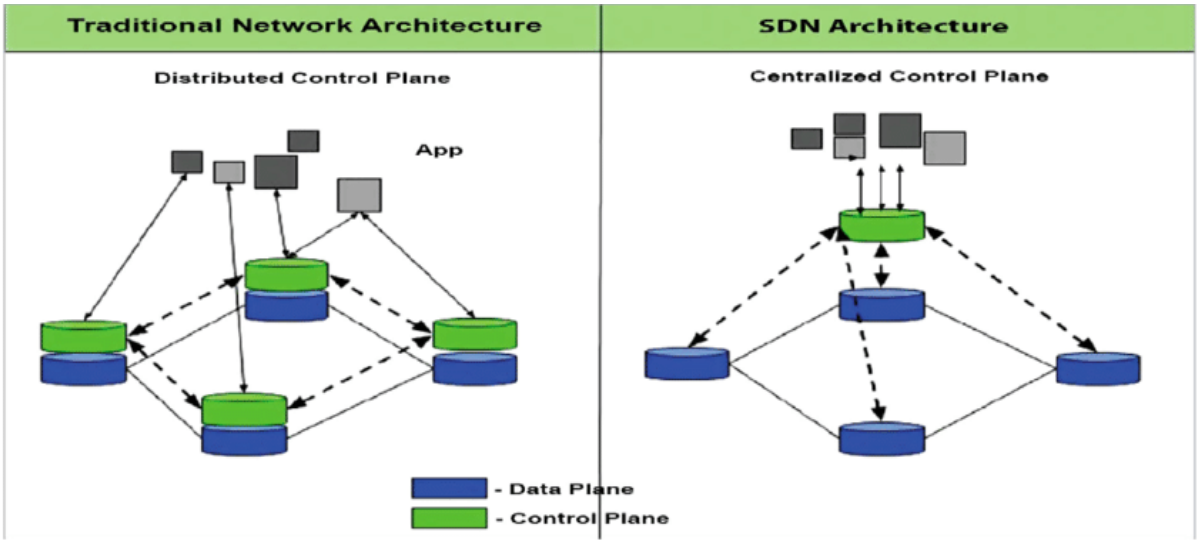


Figure 2diffrence between traditionnal network architecture and SDN architecture *[2]*

SDN comprises three key components: the data plane, the control plane, and the application layer. The data plane is responsible for forwarding network traffic, while the control plane manages network infrastructure and makes decisions about how network traffic should be handled. The application layer consists of software applications that run on top of the SDN infrastructure. On the other hand, traditional networks use physical network devices, such as routers, switches, and firewalls, to manage and direct network traffic. They rely on physical cabling to connect these devices and standard networking protocols like TCP/IP and Ethernet for communication between devices.

SDN offers several key benefits over traditional networking approaches. For example, SDN allows for more efficient network management, as network administrators can automate many tasks that would otherwise be done manually. SDN also allows for more flexible and customizable network configurations, as network infrastructure can be reconfigured on the fly, making it highly scalable and adaptable to changing network demands. Traditional networks have their own set of benefits, being well-established and widely used in various organizations. They

offer predictable performance as network devices are configured based on specific requirements and are familiar to network administrators, requiring minimal training.

SDN has a wide range of applications, from data center networking to wide area networks (WANs) and even the Internet of Things (IoT). It is particularly useful in situations where network infrastructure needs to be highly flexible and scalable. Traditional networks are ideal for legacy systems that require predictable and stable performance and are suitable for businesses with static network demands and minimal need for reconfiguration.

In comparison, SDN stands out with its scalability, extensive automation, and flexibility. It can easily scale to meet growing network demands, supports extensive automation, reducing the need for manual configuration and management, and allows for real-time reconfiguration and optimization of the network. Conversely, traditional networks provide consistent and predictable performance, are well-understood and trusted by network administrators, and are perceived as reliable due to their established use and well-understood technology

	SDN Network	Traditional Network
01	Software Defined Network is virtual networking approach.	Traditional network is the old conventional networking approach.
02	Software Defined Network is centralized control.	Traditional Network is distributed control.
03	This network is programmable	This network is non programmable.
04	Software Defined Network is open interface.	Traditional network is closed interface.
05	In Software Defined Network data plane and control plane are decoupled by software.	In traditional network data plane and control plane are mounted on same plane.
06	It supports automatic configuration so it takes less time.	It supports static/manual configuration so it takes more time.
07	It can prioritize and block specific network packets.	It leads all packets in the same way no prioritization support.
08	It is easy to program as per need.	It is difficult to program again and to replace existing program as per use.
09	Cost of Software Defined Network is low.	Cost of Traditional Network is high.
10	Structural complexity is low in Software Defined Network.	Structural complexity is high in Traditional Network.
11	Extensibility is high in Software Defined Network.	Extensibility is low in Traditional Network.
12	In SDN it is easy to troubleshooting and reporting as it is centralized controlled.	In Traditional network it is difficult to troubleshoot and report as it is distributed controlled.
13	Its maintenance cost is lower than traditional network.	Traditional network maintenance cost is higher than SDN.

Tableau 1comparison between SDN Network and Traditional Network

2.4 OpenFlow :

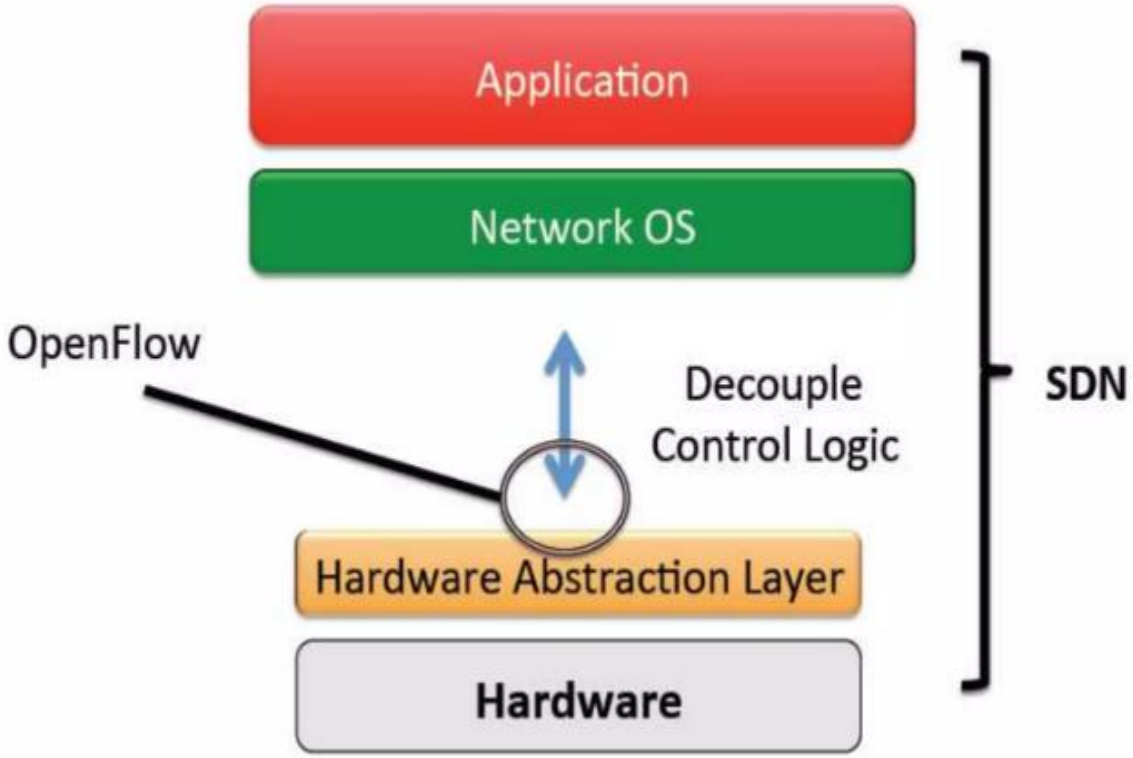


Figure 3 figure shows OpenFlow fucntion in the SBI interface

OpenFlow is a foundational protocol in Software-Defined Networking (SDN) that serves as a southbound interface (SBI) between the SDN controller and network devices such as switches and routers. It plays a crucial role in enabling the separation of the control plane from the data plane, which is a core tenet of SDN architecture.

OpenFlow defines a standardized method for an SDN controller to communicate with and manage the forwarding behavior of network devices. This is achieved through a well-defined set of messages that are exchanged between the controller and the switches. These messages are categorized into three main types:

- **Controller-to-Switch messages:**

  - Features message: After an SSL/TCP session is established, the controller sends Features messages to a switch to request switch information. The switch must send a response, including the interface name, MAC address, and interface rate

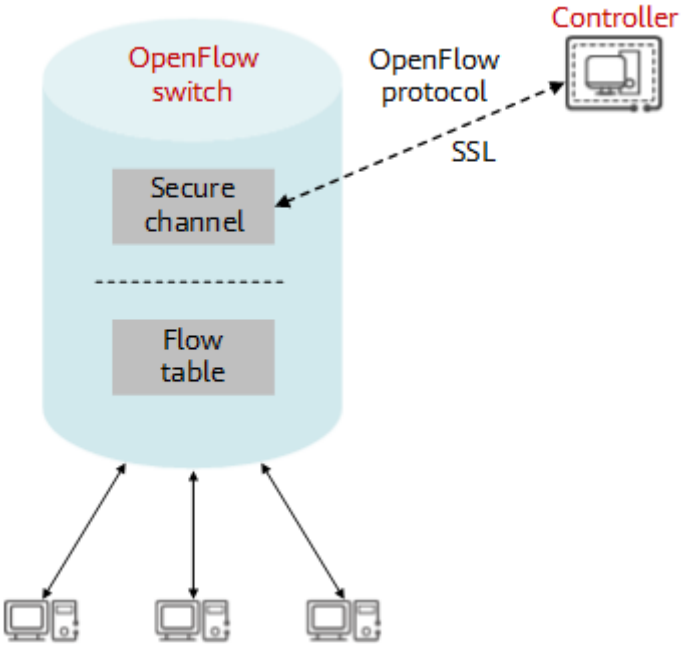


Figure 4Controller-to-Switch messages using SSL *[1]*

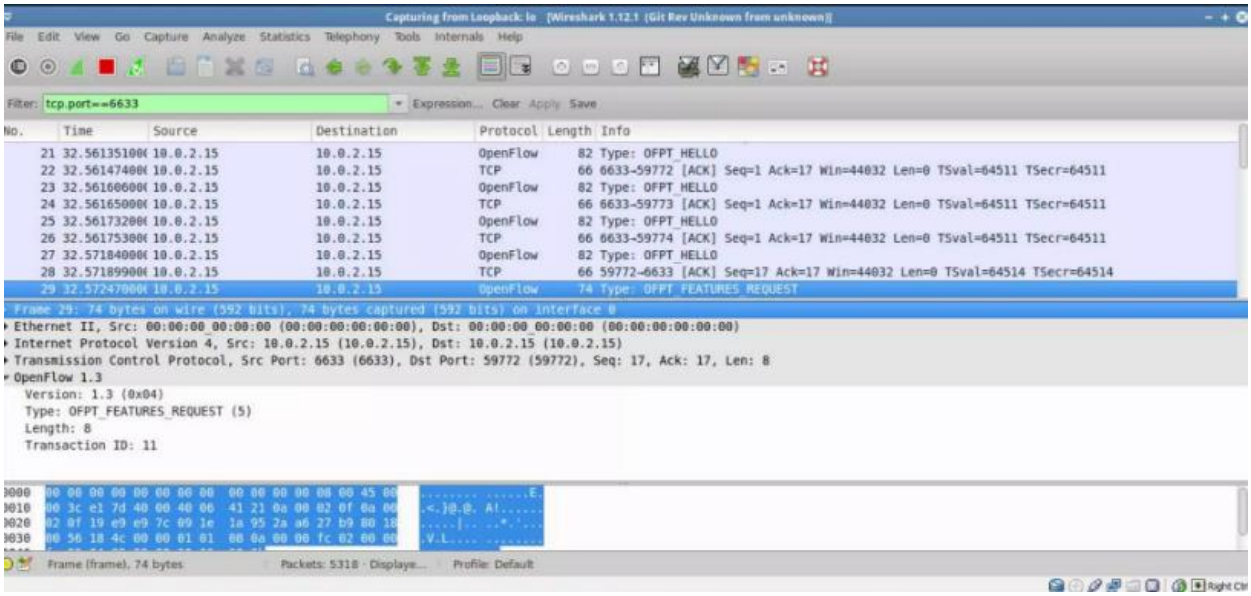


Figure 52OpenFlow-Feature Request(from Controller to Switch)

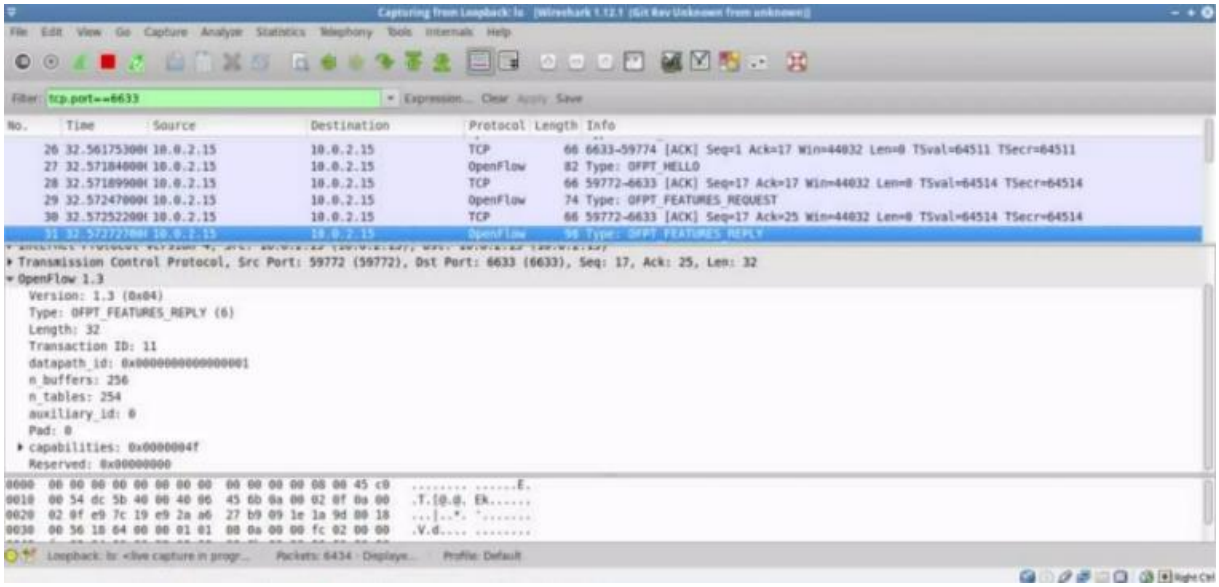


Figure 6OpenFlow-Feature Reply (from Controller to Switch)

- Configuration message: The controller can set or query the switch status.
- Modify-State message: The controller sends this message to a switch to manage the switch status, that is, to add, delete, or modify the flow table and set interface attributes of the switch.
- Read-State message: The controller sends this message to collect statistics on the switch.
- Send-Packet message: The controller sends the message to a specific interface of the switch.

➢ Asynchronous messages:

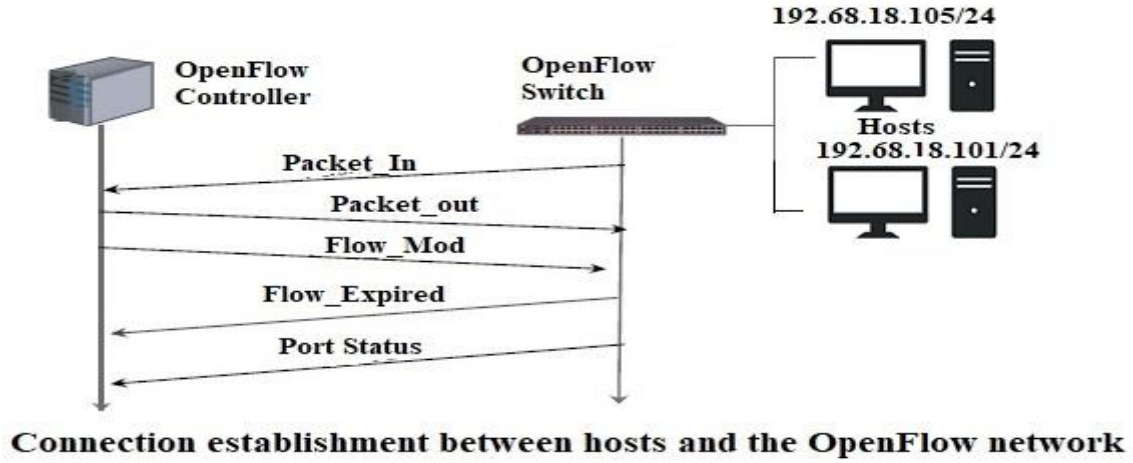
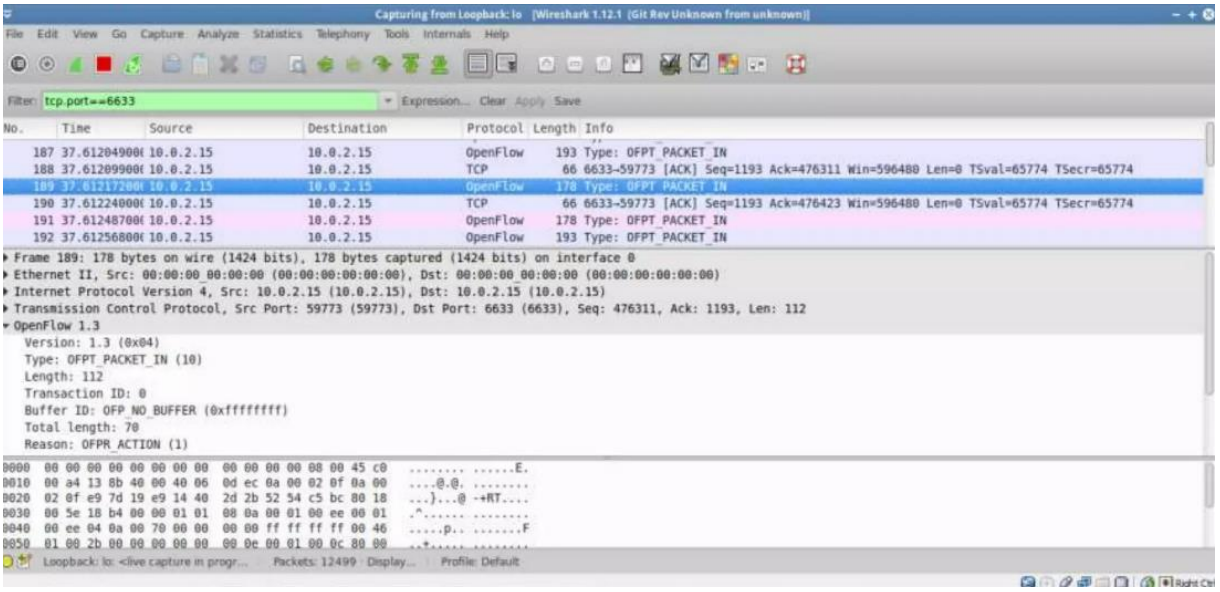


Figure 7 Connection establishment between hosts and the Openflow network *[3]*

- Packet-in message: If no matching entry exists in the flow table or the action "send-to-controller" is matched, the switch sends a packet-in message to the controller.

- Packet-out message: The controller sends this message to respond to a switch.

- Flow-Removed message: When an entry is added to a switch, the timeout interval is set. When the timeout interval is reached, the entry is deleted. The switch then sends a Flow-Removed message to the controller. When an entry in the flow table needs to be deleted, the switch also sends this message to the controller.



- Port-status message: A switch sends this message to notify the controller when the interface configuration or state changes.

➢ Symmetric messages:

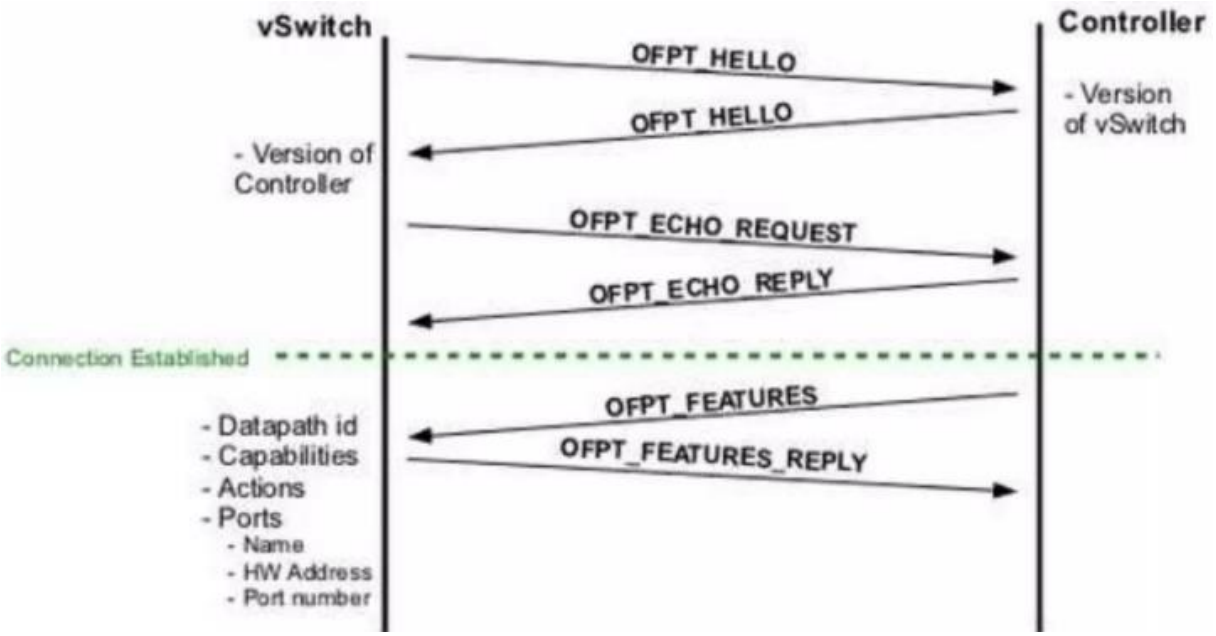


Figure 8 connection establishment between vswitch and Controller

- Hello message: When an OpenFlow connection is established, the controller and switch immediately send an OFPT_HELLO message to each other. The version field in the message is filled with the latest OpenFlow version supported by the sender. After receiving the message, the receiver calculates the protocol version number, that is, selects the smaller one between the versions supported by the sender and the receiver. If the receiver supports the version, connection requests are processed until the connection is successful. Otherwise, the receiver replies with an OFPT_ERROR message, in which the type field is filled with ofp error type OFPET HELLO FAILED

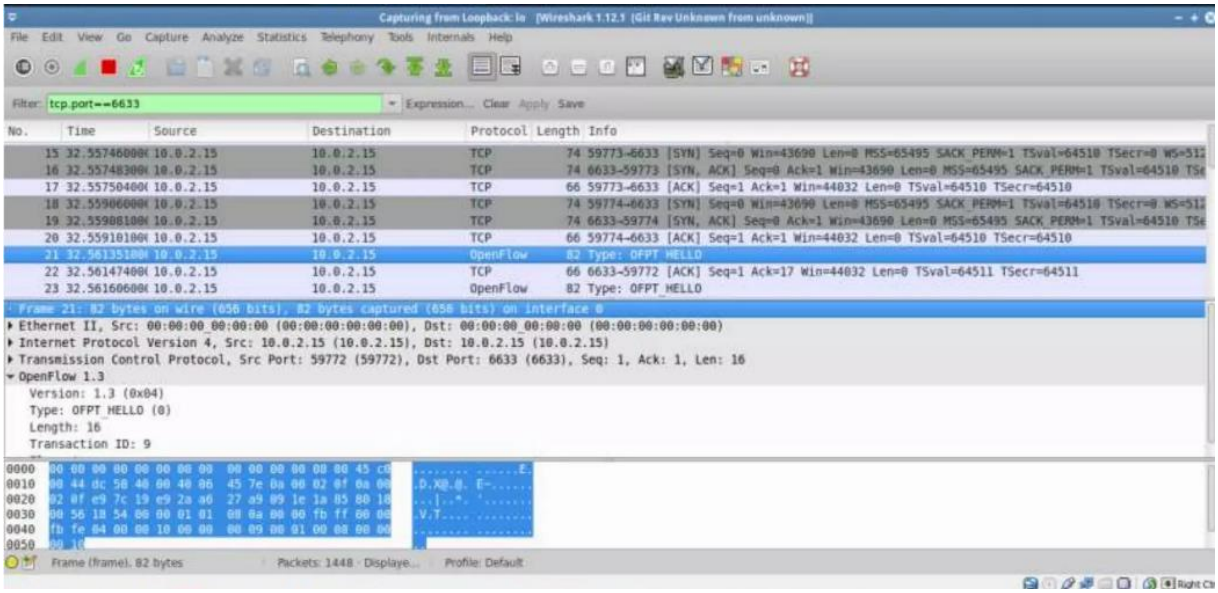


Figure 9OpenFlow-HELLO (from Switch to Controller)

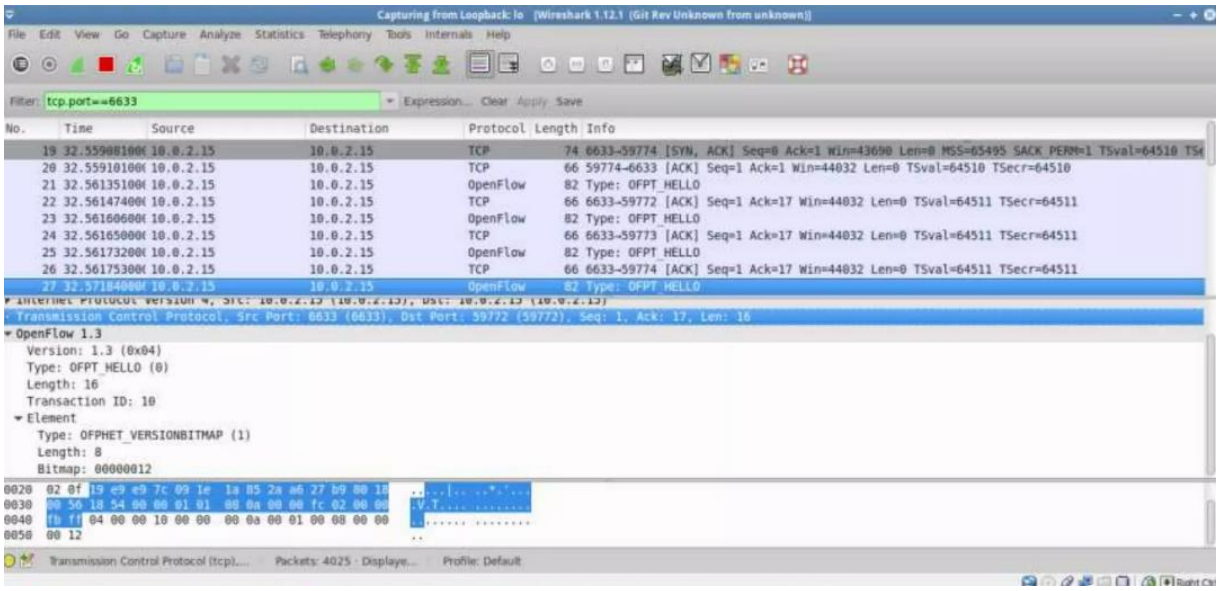


Figure 10OpenFlow-HELLO (from Controller to Switch)

- Echo message: Either a switch or controller can send an Echo Request message, but the receiver must reply with an Echo Reply message. This message can be used to measure the latency and connectivity between the controller and switch. That is, Echo messages are heartbeat messages.

- Error message: When a switch needs to notify the controller of a fault or error, the switch sends an Error message to the controller.

2.5 OpenFlow Table :

OpenFlow switches forward packets based on flow tables. These tables are composed of flow entries that determine how packets are handled within the network. Each flow entry includes several critical components: Match Fields, Priority, Counters, Instructions, Timeouts, Cookie, and Flags. Understanding these components in detail is essential for comprehending how OpenFlow enables flexible and precise network management.

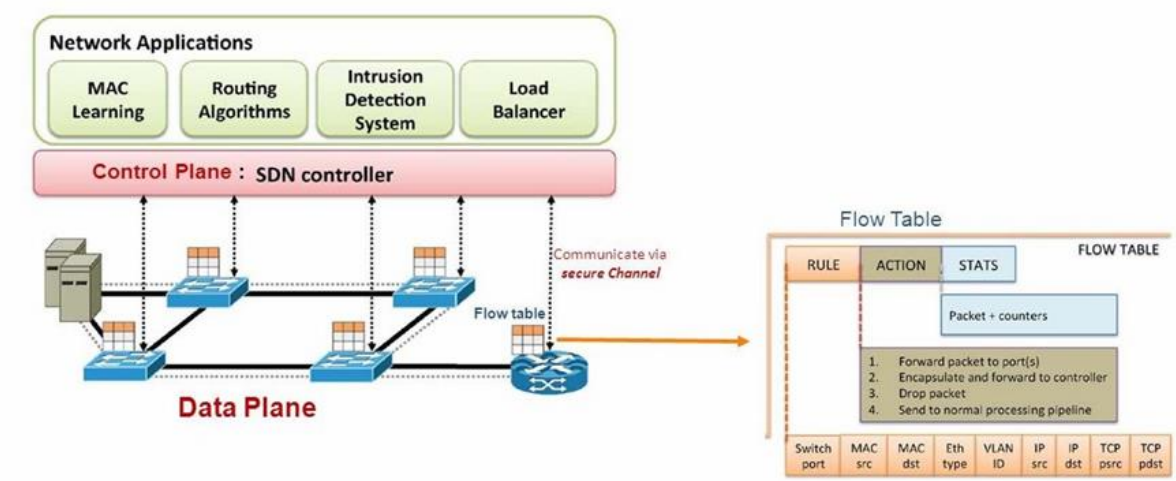


Figure 11 Pipeline OpenFlow

Match Fields	Priority	Counters	Instructions	Timeouts	Cookie	Flags

Flow table fields can be customized. The following table is an example.

Ingress Port	Ether Source	Ether Dst	Ether Type	VLAN ID	VLAN Priority	IP Src	IP Dst	TCP Src Port	TCP Dst Port
3	MAC1	MAC2	0x8100	10	7	IP1	IP2	5321	8080

Tableau 2 OpenFlow table

OpenFlow 1.5.1 supports 45 different match field options, offering extensive flexibility for network traffic classification and control.

2.5.1 OpenFlow Match Fields :

The Match Fields in an OpenFlow table entry are essential for identifying and categorizing network traffic based on various packet attributes. These fields enable fine-grained control and precise traffic management. Here, we'll discuss several key match fields that can be customized in OpenFlow:

2.5.1.1 Ingress Port

The ingress port is the physical or logical interface through which a packet enters the switch. Matching on the ingress port allows network administrators to apply specific rules based on the entry point of the traffic, which is useful for controlling access and directing traffic flows based on the source interface.

2.5.1.2 Ethernet Source (Ether Src)

The Ethernet source address, which is the MAC address of the device that sent the packet, is used to identify and manage traffic based on the originating device. This is essential for implementing security policies and tracking the source of network traffic.

2.5.1.3 Ethernet Destination (Ether Dst)

The Ethernet destination address, being the MAC address of the device to which the packet is being sent, is matched to forward packets to the correct network segment, ensuring proper delivery of frames within a local network.

2.5.1.4 Ethernet Type (Ether Type)

The Ethernet type field, which indicates the protocol encapsulated in the payload of the Ethernet frame, is used to distinguish between different types of traffic such as IPv4, IPv6, ARP, and more, enabling the application of protocol-specific rules.

2.5.1.5 VLAN ID

The VLAN ID specifies the Virtual Local Area Network to which the packet belongs, allowing for the segregation and management of traffic within different VLANs, thereby supporting network segmentation and improved traffic isolation.

2.5.1.6 VLAN Priority

The VLAN priority field indicates the priority level of the packet within a VLAN, used for implementing Quality of Service (QoS) policies, ensuring that high-priority traffic receives the appropriate level of service.

2.5.1.7 IP Source (IP Src)

The IP source address is the IP address of the device that sent the packet, which is crucial for routing, access control, and implementing source-based policies, allowing for the identification and management of traffic based on its origin.

2.5.1.8 IP Destination (IP Dst)

The IP destination address is the IP address of the device to which the packet is being sent, used to direct packets to their correct destination and apply destination-based policies, fundamental for routing and traffic engineering.

2.5.1.9 TCP Source Port (TCP Src Port)

The TCP source port identifies the application or process that sent the TCP segment on the source device, allowing for the control of traffic based on the originating application, enabling application-specific policies and traffic management.

2.5.1.10 TCP Destination Port (TCP Dst Port)

The TCP destination port identifies the application or process to which the TCP segment is addressed on the destination device, used to manage and direct traffic to specific applications, essential for implementing service-specific policies and ensuring proper delivery of application traffic.

2.5.1.11 Example Match Fields

To illustrate, here is an example of how these fields can be represented in a flow entry:

- **Ingress Port:** 3
- **Ether Src:** MAC1
- **Ether Dst:** MAC2
- **Ether Type:** 0x8100
- **VLAN ID:** 10
- **VLAN Priority:** 7
- **IP Src:** IP1
- **IP Dst:** IP2
- **TCP Src Port:** 5321
- **TCP Dst Port:** 808
-

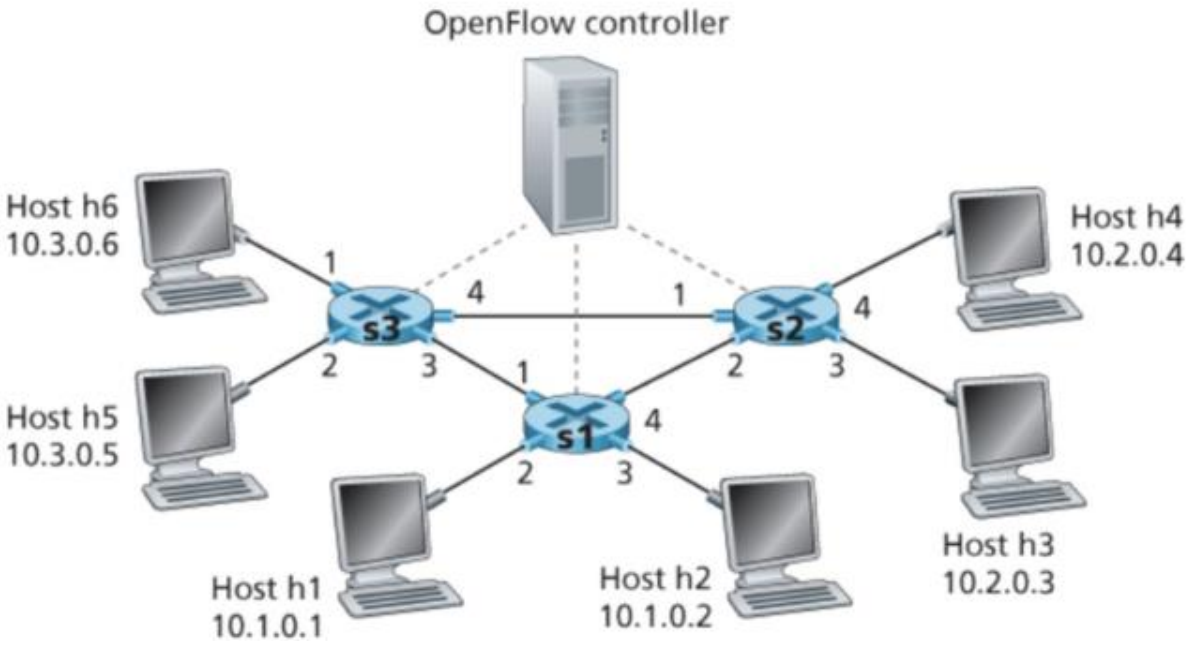


Figure 12OpenFlow controller *[4]*

2.5.2 Priority

The Priority field dictates the order in which flow entries are evaluated. Each flow entry is assigned a priority value, and entries with higher priority are matched before those with lower priority.

- **Significance of Priority:**
  - **Conflict Resolution:** In cases where multiple flow entries could match the same packet, the priority value ensures that the most critical or specific entry is selected.
  - **Fine-Grained Control:** Allows network administrators to define precise rules for packet handling, ensuring important traffic is managed appropriately.

2.5.3 Counters

Counters keep track of the number of packets and bytes that match a specific flow entry. They provide valuable statistics for monitoring and managing network performance.

- **Types of Counters:**
  - **Packet Counter:** Tracks the total number of packets that have matched the flow entry.
  - **Byte Counter:** Records the total number of bytes for packets that have matched the flow entry.

These counters enable network administrators to analyze traffic patterns, identify potential issues, and optimize network resource utilization.

2.5.4 Instructions

Instructions define the actions that an OpenFlow switch should take when a packet matches a flow entry. These actions can affect packets directly, modify action sets, or influence pipeline processing.

- **Key Instruction Types:**
  - **Apply-Actions:** Applies a set of actions immediately to the packet.
  - **Write-Actions:** Modifies the action set for later application.
  - **Clear-Actions:** Clears all actions in the action set.
  - **Write-Metadata:** Writes metadata values that can be used by subsequent flow tables.
  - **Goto-Table:** Directs the packet to another flow table for further processing.

Instructions provide the mechanism for implementing complex forwarding and processing behaviors, enhancing the versatility of the network.

2.5.5 Timeouts

Timeouts define the aging criteria for flow entries, determining how long they remain active within the flow table.

- **Types of Timeouts:**
  - **Idle Timeout:** Specifies the duration a flow entry remains in the table without matching any packets. If the entry is not matched within this period, it is removed.
  - **Hard Timeout:** Defines the absolute lifetime of a flow entry. Once this timer expires, the flow entry is removed regardless of whether it has been matched by any packets.

Timeouts ensure that flow tables are dynamically updated to reflect current network conditions, helping to optimize memory usage and processing efficiency.

2.5.6 Cookie

The Cookie is a unique identifier assigned to each flow entry by the SDN controller. It serves as a handle for the controller to manage and reference specific flow entries.

- **Uses of Cookie:**
  - **Flow Management:** Allows the controller to modify or delete specific flow entries.
  - **Statistics Collection:** Enables the controller to gather statistics for particular flows without affecting other entries.

Cookies provide an efficient mechanism for the controller to interact with flow entries, facilitating granular control and management.

2.5.7 Flags

Flags modify the management behavior of flow entries, offering additional control over how they are handled within the flow table.

- **Key Flags:**
  - **Send Flow Removed:** Instructs the switch to notify the controller when the flow entry is removed.
  - **Check Overlap:** Ensures that new flow entries do not overlap with existing ones, preventing conflicts.

Flags enhance the flexibility of flow table management, allowing for customized behavior and improved network reliability.

2.6 Comparison Between Forwarding Modes :

2.6.1 Typical Routing Protocol: Packet Forwarding Based on Routing Tables :

In traditional networking, packet forwarding is primarily based on routing tables, which are critical components for guiding traffic within a network. Here's a more detailed look at how this mode operates:

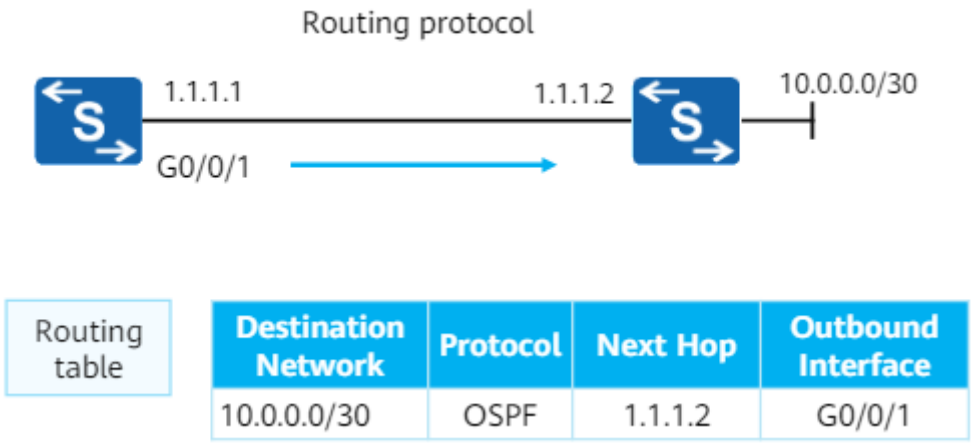


Figure 13Typical Routing Protocol: Packet Forwarding Based on Routing Tables

2.6.1.1 Routing Table Query for Traffic Forwarding

Network devices, such as routers, use routing tables to determine the next hop for forwarding packets. When a packet arrives, the device queries its routing table to find the most appropriate path based on the destination IP address.

2.6.1.2 Routing Table Entry Calculation

Entries in a routing table are calculated through the operation of routing protocols, such as OSPF (Open Shortest Path First), BGP (Border Gateway Protocol), or EIGRP (Enhanced Interior Gateway Routing Protocol). These protocols enable network devices to exchange routing information and dynamically calculate the best paths for traffic.

- **OSPF:** Utilizes a link-state routing algorithm to calculate the shortest path tree for each route.
- **BGP:** Manages how packets are routed across the internet through a path vector protocol, focusing on policy-based routing.
- **EIGRP:** A hybrid routing protocol that combines features of distance-vector and link-state protocols to provide efficient routing.

2.6.1.3 Fixed Length of Routing Tables

The structure of routing tables in traditional networks is fixed, meaning the format and length of each entry are predetermined. This rigidity can lead to limitations in scalability and flexibility as network demands grow.

2.6.1.4 Longest Match Rule

Packet forwarding in traditional networks relies on the longest match rule. When a routing device queries its table, it selects the entry with the longest matching prefix for the destination IP address. This ensures that the packet is forwarded as precisely as possible towards its intended destination.

2.6.1.5 Single Routing Table per Device

Typically, each network device maintains a single routing table, which simplifies the routing process but can also be a limitation in complex network environments. The reliance on a single table can lead to inefficiencies in handling diverse traffic types and applying nuanced traffic policies.

2.6.2 OpenFlow: Packet Forwarding Based on Flow Tables :

OpenFlow represents a revolutionary network protocol in Software Defined Networking (SDN), transforming how packet forwarding is orchestrated within networks.

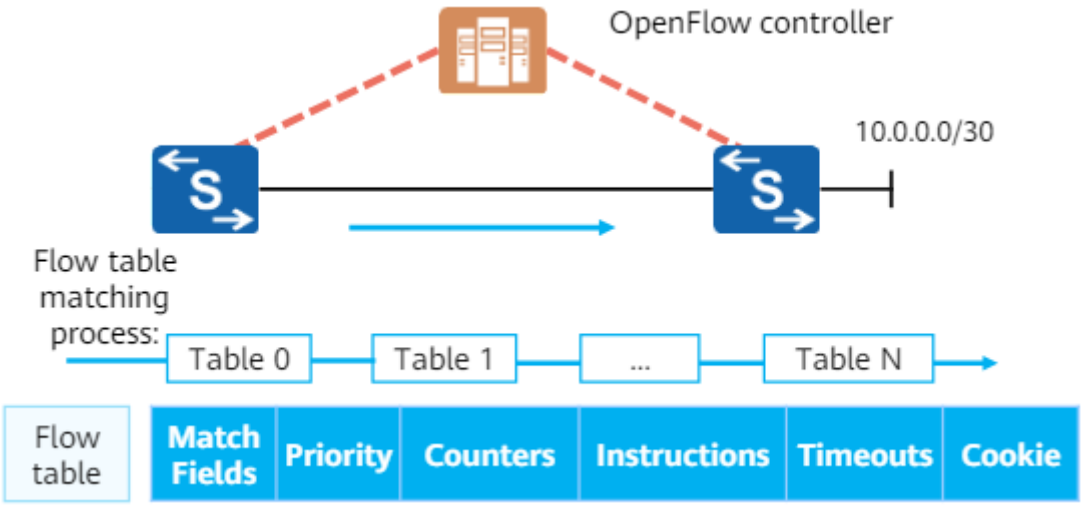


Figure 14OpenFlow: Packet Forwarding Based on Flow Tables

2.6.2.1 Flow Table Structure and Functionality

OpenFlow switches operate by utilizing dynamic flow tables that dictate the handling of incoming packets. Key aspects of flow tables include:

- **Calculation and Distribution:** Flow tables are computed centrally by an OpenFlow controller, which then disseminates these rules to the participating switches across the network.
- **Variable Length and Rules:** Each flow table can vary in size and defines specific criteria, known as match fields, which incoming packets must meet. These criteria typically include attributes such as ingress port, Ethernet addresses (source and destination), VLAN ID, IP addresses (source and destination), and TCP/UDP port numbers.
- **Multiple Flow Tables:** Unlike traditional networks that rely on a single routing table, OpenFlow-capable devices can manage multiple flow tables (typically indexed from 0 to 255). Each table processes packets according to predefined priorities, ensuring that higher-priority flow entries are processed before lower-priority ones.

2.6.2.2 Customization and Flexibility

One of the core advantages of OpenFlow is its flexibility in configuring flow tables. Administrators can tailor match fields, actions, timeouts, and other parameters to suit specific network requirements. This customization capability allows for efficient traffic management and fine-grained control over network behavior.

2.6.2.3 Software vs. Physical Switches

Presently, OpenFlow is predominantly deployed on software switches like Open vSwitch (OVS) and Cisco's CE1800V in data centers. Physical switches have yet to fully adopt OpenFlow, primarily due to challenges in separating the forwarding and control planes in hardware-based environments.

2.6.2.4 Applications and Use Cases

OpenFlow finds practical applications in diverse scenarios within SDN:

- **Data Center Networks (DCs):** Used for dynamic network provisioning, load balancing, and traffic engineering.
- **Campus Networks:** Facilitates efficient network management, security enforcement, and quality of service (QoS) policies.
- **Software-Defined WANs (SD-WANs):** Enables centralized management of WAN traffic, optimizing connectivity and application performance across distributed sites.

2.7 Essential Requirements of SDN :

oftware Defined Networking (SDN) revolutionizes traditional network architectures by introducing centralized control and programmability, aimed at enhancing network openness, flexibility, and simplicity.

2.7.1 Centralized Control and Global View

SDN fundamentally redefines network management by centralizing control through a unified, global view of the network. This centralized approach allows for:

- **Centralized Management:** Simplifies network operations and maintenance (O&M) by consolidating control over network devices and configurations into a single management entity.
- **Technical Abstraction:** Abstracts underlying hardware differences and complexities, streamlining network configuration and reducing O&M costs.

2.7.2 Automatic Optimization and Rapid Service Deployment

SDN facilitates dynamic network optimization and agile service deployment, offering:

- **Automatic Optimization:** Enhances network efficiency and resource utilization through automated traffic management and policy enforcement.
- **Rapid Service Deployment:** Accelerates the deployment of new services and applications by decoupling network control from hardware, allowing for swift configuration changes and service activation.

2.7.3 Open and Programmable Environment

SDN promotes an open and programmable networking environment, enabling:

- **Open Network:** Supports integration with third-party applications and services through open APIs, fostering innovation and interoperability.
- **Programmable Infrastructure:** Allows network operators and developers to create customized network behaviors and applications tailored to specific business needs.

2.8 SDN Network Architecture :

The SDN network architecture consists of the orchestration application layer, controller layer, and device layer. Different layers are connected through open interfaces. From the perspective of the controller layer, SBIs oriented to the device layer and NBIs oriented to the orchestration application layer are distinguished. OpenFlow is one of SBI protocols. [5]

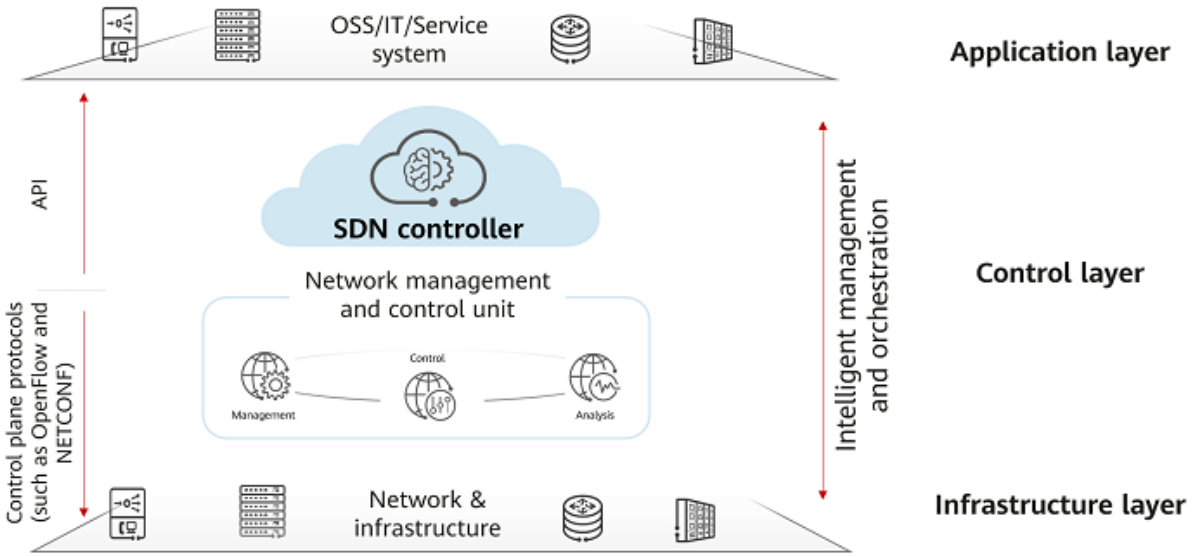


Figure 15 SDN Network Architecture

2.8.1 Orchestration Application Layer :

The Orchestration Application Layer encompasses several key components designed to streamline and automate network service provisioning:

- **Operations Support Systems (OSS):** Responsible for overseeing the end-to-end service orchestration across the entire network infrastructure. OSS ensures seamless integration of network services and operations.

- **OpenStack:** A widely adopted platform for cloud computing and SDN, OpenStack provides comprehensive service orchestration capabilities for managing network, compute, and storage resources within data centers (DCs).

2.8.2 Controller layer :

At the heart of SDN Network Architecture lies the Controller Layer, which serves as the central hub responsible for orchestrating network operations and services.

The Controller Layer in SDN represents the pivotal component that oversees and governs network behavior through centralized control:

- **Centralized Management:** Acts as the centralized intelligence or "brain" of the SDN system, consolidating control over network devices and services.

- **Network Service Orchestration:** Facilitates the orchestration of network services by translating high-level service requirements into specific configurations and actions that network devices execute.

The SDN controller is deployed within the Controller Layer, functioning as the nucleus of SDN operations:

Offers programmable interfaces (APIs) that allow for seamless integration with upper-layer orchestration applications and lower-layer network devices.

2.8.2.1 Controller Functions

The primary functions performed by the SDN controller include:

- **Topology Discovery:** Identifies and maps the network topology, understanding the interconnected relationships between network devices.
- **Flow Management:** Manages flow entries within network switches' flow tables, ensuring efficient packet forwarding based on predefined policies and traffic patterns.
- **Policy Enforcement:** Enforces network policies consistently across all network devices, ensuring compliance and security.
- **Dynamic Adjustment:** Responds dynamically to network changes, automatically adapting configurations and routing decisions based on real-time traffic and environmental conditions.

2.8.2.2 Integration with Orchestration Layer

Collaboration between the Controller Layer and the Orchestration Application Layer is crucial:

- **Service Orchestration:** Receives service deployment requests from orchestration applications (e.g., OSS, OpenStack) and translates them into actionable instructions for network devices.
- **Feedback Mechanism:** Provides feedback to orchestration applications regarding network status, performance metrics, and resource utilization.

2.8.3 Device Layer :

The Device Layer is the foundational layer in the SDN architecture, where network devices operate based on the instructions received from the SDN controller. This layer is crucial for executing the decisions made by the higher layers of the SDN architecture.

Network devices in the Device Layer are responsible for the actual data forwarding and execution of network policies as instructed by the SDN controller:

- **Packet Forwarding:** Devices such as switches and routers forward packets based on flow table entries delivered by the controller.
- **Policy Enforcement:** Enforce network policies (e.g., QoS, security rules) as specified by the flow entries in their flow tables.

The Device Layer comprises various network devices that function together to handle traffic within the network:

- **Switches:** Core devices that manage packet forwarding based on flow tables. Examples include software switches like Open vSwitch (OVS) and hardware switches supporting OpenFlow.
- **Routers:** Devices that direct data packets between different networks, working under the control of the SDN controller to manage routes dynamically.
- **Firewalls:** Security devices that enforce access control policies, filtering traffic based on rules set by the SDN controller.

2.8.3.1 Interaction with the Controller Layer

The devices at this layer interact closely with the SDN controller to ensure cohesive network operation:

- **Receiving Instructions:** Network devices receive flow entries and configuration instructions from the SDN controller through Service-Based Interface (SBI) protocols.
- **Reporting Status:** Devices provide real-time status updates and statistics back to the controller, enabling it to make informed decisions and adjustments.
- • **Flow Table Installation:** The SDN controller installs flow table entries in the network devices. These tables contain rules for packet matching and forwarding.
- • **Packet Matching:** When a packet arrives at a device, it is matched against the flow table entries. The highest priority match dictates the forwarding action.
- • **Action Execution:** Based on the matched flow entry, the device executes actions such as forwarding the packet to a specific port, dropping it, or modifying its headers.

In SDN architecture, **interfaces** play a crucial role in enabling communication and interaction between different layers. The two primary types of interfaces in SDN are the Northbound Interface (NBI) and the Southbound Interface (SBI). These interfaces facilitate the flow of information and instructions between the various components of the SDN system, ensuring seamless integration and efficient network management.

Northbound Interface (NBI) :

The Northbound Interface (NBI) is a critical component of the SDN architecture, providing the means for communication between the SDN controller and the upper-layer applications or orchestration systems. This interface allows applications to access network services and capabilities, enabling more dynamic and programmable network management.

Interconnection with Orchestration Layer:

- **Primary Role:** NBIs enable the SDN controller to communicate with the orchestration application layer. This connection is vital for integrating various network management and orchestration tools.
- **Orchestration Applications:** These can include OSS (Operations Support Systems), OpenStack, security applications, and other network management tools. Through NBIs, these applications can request resources, deploy services, and monitor network performance.

• **RESTful :** The most common protocol used for NBIs is RESTful (Representational State Transfer) API. RESTful APIs provide a standardized and efficient way for applications to interact with the SDN controller.

➢ **Advantages of RESTful :**

- **Simplicity and Flexibility:** RESTful APIs are easy to use and can handle various types of calls, return different data formats, and change structurally with minimal impact on the calling applications.
- **Scalability:** They are designed to be stateless, which helps in scaling the network management operations efficiently.
- **Interoperability:** RESTful APIs use standard HTTP methods, making them easily integrable with a wide range of applications and services.

Southbound Interface (SBI) :

The Southbound Interface (SBI) is a critical component in the Software-Defined Networking (SDN) architecture. It is the interface that enables the SDN controller to communicate and manage the underlying network devices. By using SBIs, the controller can configure, monitor, and manage network elements dynamically and efficiently.

- **OpenFlow :**

As one of the first protocols developed for SDN, OpenFlow plays a crucial role in enabling programmable networks. It allows for the separation of the control plane and data plane, providing centralized control and dynamic management of traffic flows.

OpenFlow defines how the SDN controller interacts with the flow tables of network devices. Each flow entry in the flow table specifies match fields, priorities, counters, instructions, timeouts, cookies, and flags. These entries determine how incoming packets are processed and forwarded.

- **NETCONF :**

NETCONF is an XML-based protocol that provides mechanisms to install, manipulate, and delete the configuration of network devices.

It offers operations for configuration management, including the ability to lock and edit configurations, commit changes, and roll back to previous configurations if necessary. NETCONF also supports capabilities discovery, allowing devices to advertise their supported features and capabilities to the controller.

- **SNMP :**

SNMP is a widely used protocol for network management, enabling the monitoring and configuration of network devices.

SNMP uses a hierarchical structure of objects (defined in MIBs - Management Information Bases) to manage devices. It supports operations such as retrieving and modifying the values of these objects, sending notifications (traps) about certain events, and querying the status of devices.

- **OVSDB :**

OVSDB is designed for managing Open vSwitch configurations and states.

The protocol operates on a database model where the SDN controller can query and update the state of Open vSwitch instances. OVSDB supports operations such as creating and deleting bridges and ports, configuring VLANs, and monitoring the operational state of switches.

• **Open vSwitch (OVS) :**

Open vSwitch is a production-quality, multi-layer virtual switch designed to enable network automation through programmatic extension while supporting standard management interfaces and protocols. OVS provides rich support for network virtualization and has become a critical component of many SDN and cloud deployments.

Open vSwitch (OVS) offers advanced networking features like VLAN tagging, traffic shaping, LACP, GRE, VXLAN tunneling, and monitoring through NetFlow, sFlow, and port mirroring. OVSDB, the management protocol, allows administrators to configure the switch, manage virtual devices, and monitor network status. This makes OVS a flexible and powerful tool for building scalable, efficient networks.

3 SDN SOLUTION Using Imaster Nce :

In this chapter, we delve into the practical aspects of implementing Software-Defined Networking (SDN) solutions. While the previous chapters provided a theoretical foundation and detailed the architecture and protocols underpinning SDN, this chapter will bridge the gap between theory and practice by exploring real-world applications and deployments. Specifically, we will discuss an SDN solution implemented in collaboration with an enterprise, highlighting the project's objectives, implementation details, and outcomes. [6]

One of the notable SDN solutions we will examine is Huawei's iMaster NCE (Network Cloud Engine). This solution exemplifies how SDN can be utilized to achieve enhanced network control, flexibility, and efficiency in a corporate environment. The iMaster NCE integrates cutting-edge technologies and practices to offer comprehensive network management and orchestration capabilities.

Huawei's iMaster NCE is a robust SDN solution designed to simplify network management and accelerate service deployment. By leveraging SDN principles, the iMaster NCE provides centralized control, automated operations, and enhanced network visibility. Here, we will explore the key features, components, and benefits of Huawei's iMaster NCE.

Huawei's iMaster NCE is an advanced network management and control platform that consolidates various functionalities into a single, cohesive solution. It is designed to support a wide range of network environments, from data centers to wide area networks (WANs), ensuring seamless integration and operation across different network segments.

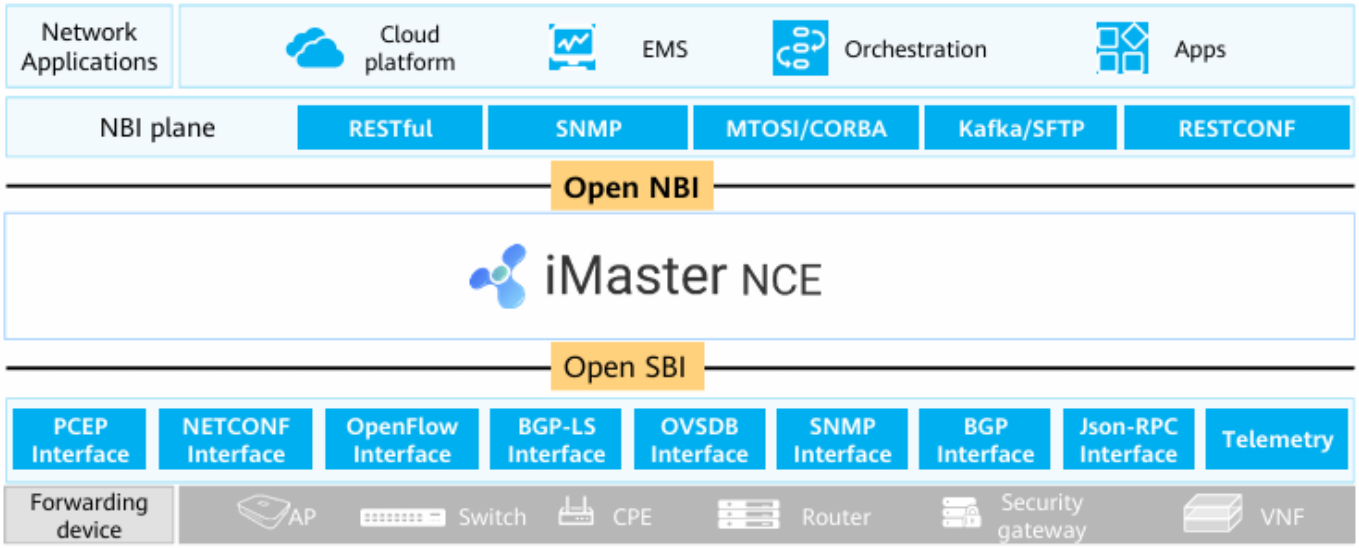


Figure 16 Huawei SDN Network Architecture

3.1 Cloud Platform Integration in SDN Architecture

Incorporating a cloud platform within the SDN architecture enhances resource management and orchestration, facilitating seamless control over network, compute, and storage resources. Here are the key components and tools involved in this integration:

- **Cloud Platform**:
  - The cloud platform serves as the resource management hub within a cloud data center (DC).
  - It manages network, compute, and storage resources, ensuring optimal allocation and utilization.
  - OpenStack is the most mainstream open-source cloud platform used for this purpose.

- **Element Management System (EMS)**:
  - EMS is responsible for managing one or more telecommunication network elements (NEs) of a specific type.
  - It provides a centralized interface for monitoring and controlling network elements, ensuring efficient operation and maintenance.
- **Orchestration (Container Orchestration)**:
  - The container orchestration tool provides network service orchestration functions, enabling automated deployment, scaling, and management of containerized applications.
  - Kubernetes is a mainstream tool widely used for container orchestration, offering robust features for managing containerized environments.
- **Integration with Business Support Systems (BSS) or Operations Support Systems (OSS)**:
  - MTOSI or CORBA protocols are used to interconnect with BSS or OSS, facilitating seamless communication and coordination.
  - Kafka or SFTP can be used to connect to a big data platform, enabling efficient data transfer and processing.

By integrating these components, the SDN architecture becomes more dynamic and capable of handling complex network environments. This setup allows for better resource management, automated orchestration, and improved overall efficiency.

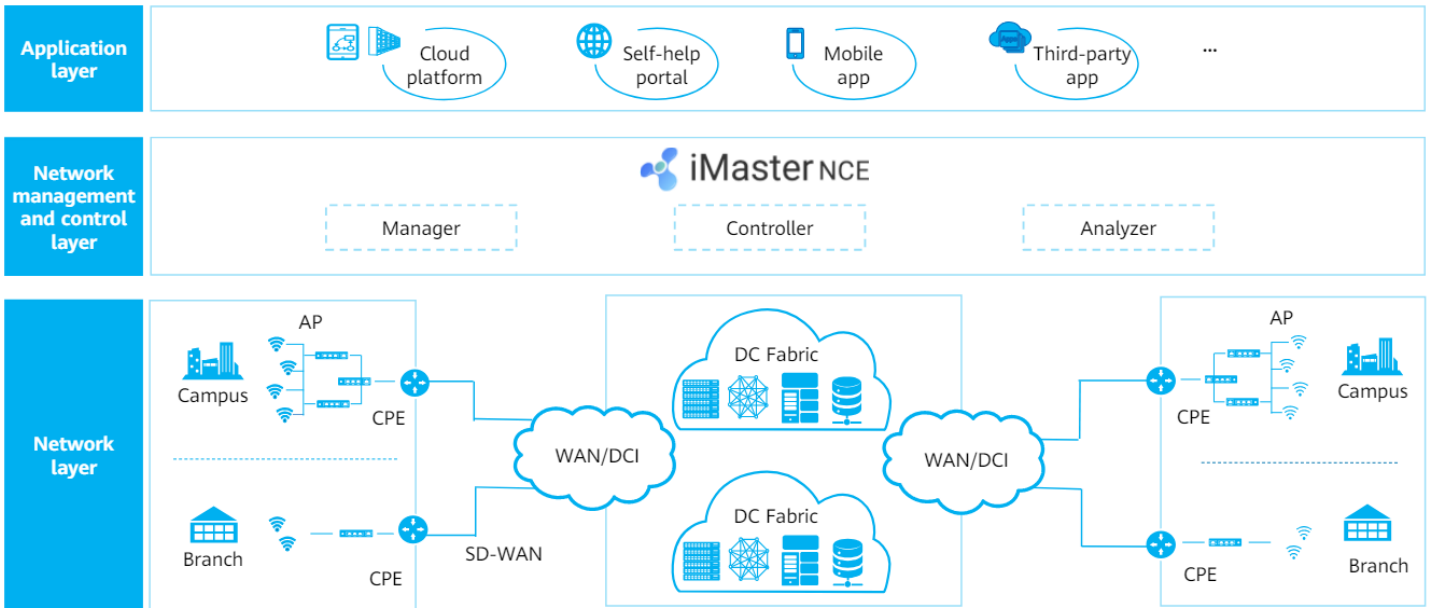


Figure 17 SDN Solution - Integrating Management, Control, and Analysis to Build an Intent-Driven Network

3.2 Introduction to iMaster NCE :

Huawei iMaster NCE is an advanced, industry-leading intelligent network automation platform. It integrates comprehensive capabilities across management, control, analysis, and artificial intelligence (AI). This platform is designed to streamline and enhance network operations, providing robust tools for centralized management, sophisticated network control, detailed analysis, and AI-driven optimization. With Huawei iMaster NCE, organizations can achieve greater efficiency, flexibility, and innovation in their network infrastructures, ensuring seamless operation and proactive problem solving.

3.2.1 Automation + Intelligence (2 IN 1) :

SDN-based automatic service configuration and deployment significantly streamline the process of setting up and managing network services, allowing for rapid and efficient provisioning with minimal manual intervention. Additionally, AI-based intelligent analysis, prediction, and troubleshooting provide advanced capabilities for monitoring network performance, identifying potential issues before they become critical, and resolving problems swiftly and accurately. These AI-driven features enhance the network's reliability and performance, ensuring optimal operation and continuous service availability.

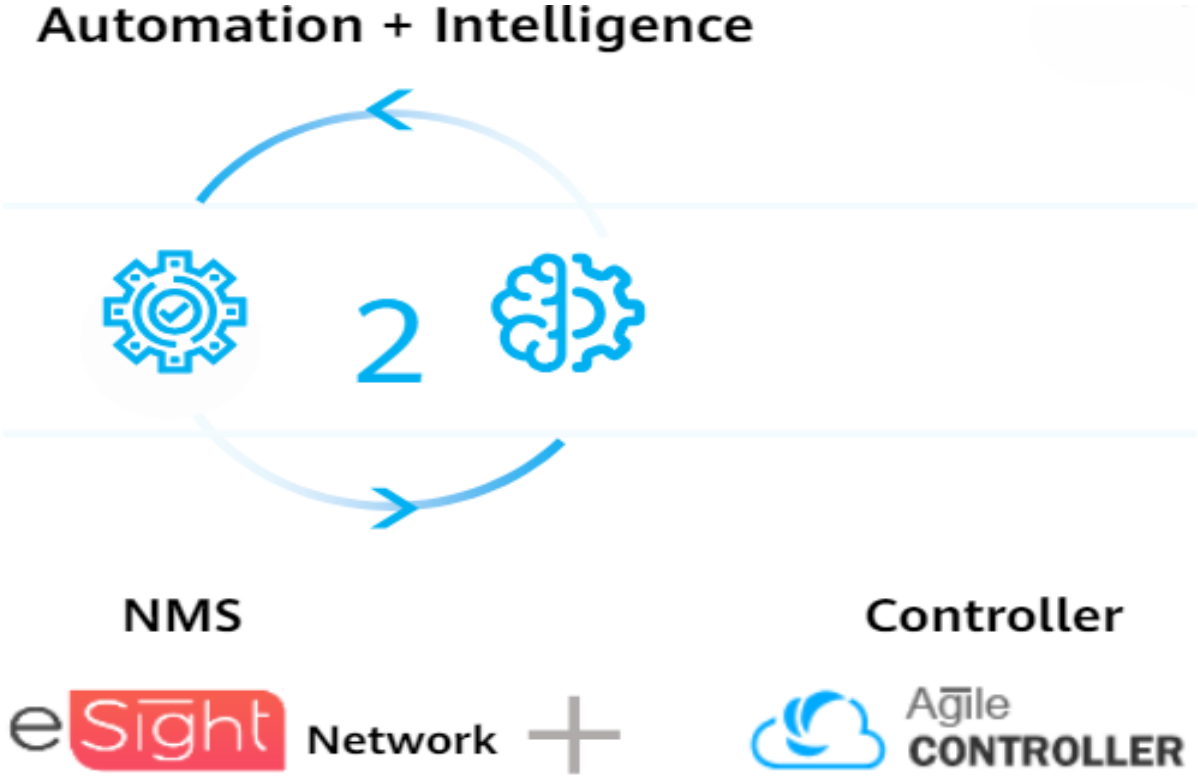


Figure 18 2 in 1 Solution (automation + intelligence) *[6]*

Combining the functionalities of Network Management Systems (NMS) such as eSight Network and controllers like Agile Controller creates a powerful, integrated solution that leverages both automation and intelligence. This synergy provides a comprehensive approach to network management and control, offering the following advantages:

3.2.1.1 Unified Management and Control:

- **eSight Network**: As an NMS, eSight provides centralized management, monitoring, and configuration of network devices. It ensures the smooth operation of network infrastructure through detailed visibility and control over all network components.
- **Agile Controller**: This SDN controller handles dynamic network configuration and real-time traffic management. It enables rapid deployment of network services, real-time network optimization, and seamless integration with various network applications.

3.2.1.2 Enhanced Efficiency and Simplification:

- Combining eSight Network and Agile Controller into a single solution reduces the complexity of managing separate systems. It provides a streamlined interface for administrators to handle both network management and control tasks, resulting in increased operational efficiency.

3.2.1.3 Intelligent Automation:

- The integration allows for sophisticated automation of network tasks. Automated service configuration and deployment minimize manual intervention, ensuring that network services are provisioned swiftly and accurately.
- AI-driven analysis, prediction, and troubleshooting capabilities enhance network reliability. The system can proactively identify and resolve potential issues, reducing downtime and maintaining optimal performance.

3.2.1.4 Improved Network Visibility:

- A combined NMS and SDN controller provide a holistic view of the network. This integrated perspective allows for better decision-making and more effective management of network resources.
- Detailed analytics and reporting tools offer insights into network performance, helping administrators to optimize network operations and plan for future growth.

3.2.1.5 Scalability and Flexibility:

- The 2-in-1 solution is designed to scale with the needs of the network. Whether managing a small enterprise network or a large data center, the combined capabilities of eSight Network and Agile Controller can adapt to varying demands.
- Flexible integration with other network systems and applications ensures that the solution remains relevant and effective in diverse network environments.

By merging the strengths of eSight Network and Agile Controller, organizations can achieve a robust, intelligent network management and control solution. This combination not only enhances the efficiency and reliability of network operations but also provides the foundation for future innovations in network automation and intelligence.

3.2.2 Manager + Controller + Analyzer (3 IN 1) :

integrating a unified database for detection, location, and troubleshooting significantly enhances the efficiency and effectiveness of network management. It enables real-time detection of issues, precise fault location, and streamlined troubleshooting processes, all of which contribute to improved network performance and reliability. [6]

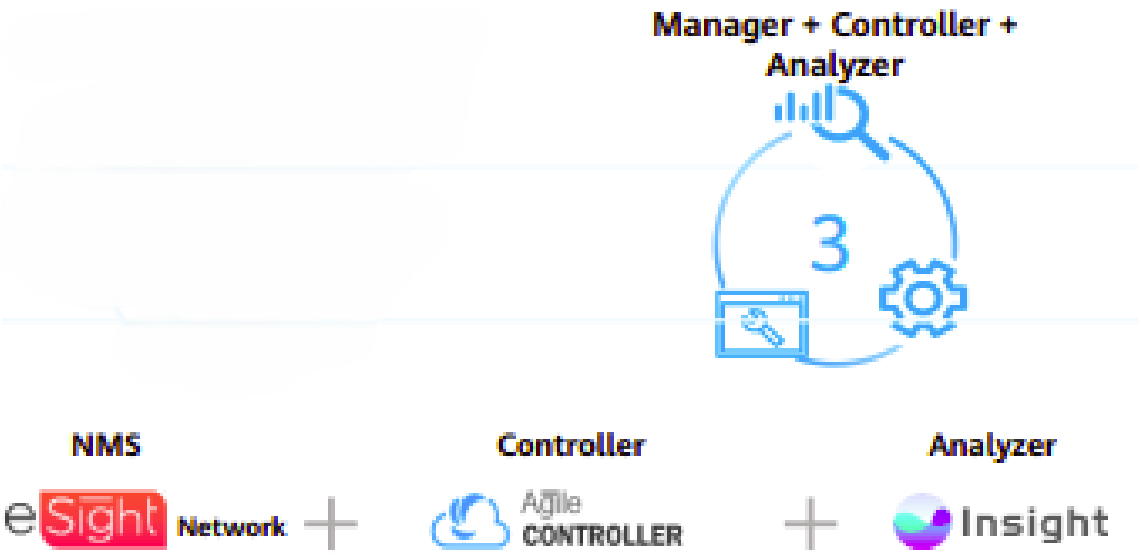


Figure 19 3 in 1 Solution (manager + controller+analyzer)

Combining a Network Management System (NMS) like eSight Network, a controller such as Agile Controller, and an analyzer like Insight into a single, unified platform enhances network management by integrating monitoring, control, and analysis.

3.2.2.1 Unified Database

- **Centralized Data**: Integrates all network information, ensuring consistency and accuracy.
- **Enhanced Access**: Simplifies data management and improves decision-making with real-time access.

3.2.2.2 Detection

- **Proactive Monitoring**: Real-time visibility into network status and performance, detecting issues early.
- **Automated Alerts**: Generates alerts for anomalies, enabling swift issue resolution.

3.2.2.3 Location

- **Fault Localization**: Pinpoints network faults precisely by analyzing traffic and performance data.
- **Intelligent Correlation**: Correlates events with control plane activities to identify root causes.

3.2.2.4 Troubleshooting

- **Automated Procedures**: Uses predefined workflows to diagnose and resolve problems quickly.
- **AI-Driven Insights**: Provides intelligent recommendations for effective problem-solving.

3.2.3 Solution Planning + Construction + Maintenance + Optimization(4 IN 1)：

3.2.3.1 Full Lifecycle Management

By integrating additional capabilities into the unified platform, we can achieve a comprehensive 4-in-1 solution that encompasses planning, construction, maintenance, and optimization. This advanced approach is embodied in Huawei's iMaster NCE, providing full lifecycle management for network operations

.

Figure 20iMaster NCE Solution 4 in 1 *[6]*

3.3 iMaster NCE Application :

Huawei's iMaster NCE is a comprehensive network automation and intelligence platform designed to streamline network operations across various domains. By integrating management, control, analysis, and AI capabilities, iMaster NCE delivers a unified solution that enhances network performance, reliability, and efficiency. Below, we explore the key applications of iMaster NCE and how they contribute to superior network management and optimization.

iMaster NCE

3.3.1 DC iMaster NCE-Fabric :

iMaster NCE-Fabric is Huawei's intelligent network management solution tailored for data centers (DCs). It offers a comprehensive suite of features designed to optimize the deployment, management, and operation of data center networks, ensuring high performance, reliability, and scalability.

- **Intelligent Traffic Management:** Leveraging AI and advanced algorithms, iMaster NCE-Fabric intelligently manages network traffic, ensuring optimal data flow within the data center. It dynamically adjusts traffic paths based on real-time network conditions, minimizing congestion and maximizing throughput.
- **Centralized Management and Control:** The platform provides a centralized interface for managing and controlling all network devices within the data center. This unified management approach simplifies operations and enhances visibility, allowing administrators to monitor and control network performance from a single point.
- **Enhanced Security:** iMaster NCE-Fabric integrates robust security features to protect data center networks from threats and vulnerabilities. It supports advanced security policies and real-time threat detection, ensuring the integrity and confidentiality of network data.
- **Scalability:** Designed to scale with the growth of data center networks, iMaster NCE-Fabric supports seamless integration of new devices and services. Its scalable architecture ensures that network performance remains consistent as the data center expands.
- **Simplified Troubleshooting:** With its powerful diagnostic tools, iMaster NCE-Fabric simplifies the process of identifying and resolving network issues. It provides detailed analytics and insights into network performance, helping administrators quickly pinpoint and address problems.

3.3.2 Enterprise campus iMaster NCE-Campus :

iMaster NCE-Campus from Huawei is an intelligent network management solution tailored for enterprise campus environments. It simplifies network deployment with automation, ensuring rapid setup and reducing configuration errors. The platform offers intelligent network management through AI-driven optimization and real-time analysis, enhancing performance and user experience. With centralized control and visibility, administrators can manage the entire campus network from a single interface, enforcing security policies and monitoring network health. iMaster NCE-Campus supports scalability, allowing seamless integration of new devices and services while maintaining network integrity. Open APIs enable integration with third-party applications, fostering flexibility and innovation in network management.

3.3.3 SD-WAN iMaster NCE-WAN:

Huawei's iMaster NCE-WAN is a robust SD-WAN solution that revolutionizes wide-area network management. It simplifies network deployment and management across distributed locations, leveraging automation to streamline operations and reduce configuration complexities. The platform enhances network performance by dynamically optimizing traffic routing based on application requirements and network conditions. Centralized control and visibility empower administrators to monitor and manage the entire SD-WAN infrastructure from a unified interface, ensuring consistent service delivery and proactive troubleshooting. iMaster NCE-WAN prioritizes security with integrated features for threat detection and policy enforcement, safeguarding data integrity and network resources. Scalable and flexible, the solution supports seamless expansion and integration of new services, while open APIs enable interoperability with existing IT ecosystems, facilitating customization and innovation in SD-WAN deployments.

3.3.4 IP WAN iMaster NCE-IP:

Huawei's iMaster NCE-IP is an advanced network management solution tailored for IP WAN environments. It simplifies the deployment and management of IP-based wide-area networks through automation, significantly reducing manual intervention and associated errors. The platform optimizes network performance by intelligently routing traffic, ensuring efficient use of network resources and enhancing the user experience. Centralized control provides administrators with comprehensive visibility and management capabilities, allowing for real-time monitoring and quick troubleshooting across the entire IP WAN infrastructure. iMaster NCE-IP also emphasizes security, integrating robust measures to detect threats and enforce policies, thereby protecting network integrity. Its scalable architecture supports the seamless addition of new devices and services, while open APIs facilitate integration with third-party applications, promoting flexibility and innovation in network management.

3.3.5 WAN Transmission iMaster NCE-T:

Huawei's iMaster NCE-T is a sophisticated management solution designed specifically for WAN transmission networks. It enhances operational efficiency by automating complex tasks, reducing manual efforts, and minimizing the risk of errors. The platform delivers superior network performance through intelligent traffic management and optimization, ensuring reliable and high-speed data transmission across wide areas. With centralized control, network administrators gain comprehensive visibility and management capabilities, enabling proactive monitoring and swift resolution of issues throughout the WAN transmission infrastructure. Security is a key focus, with integrated features to safeguard against threats and enforce stringent policies. iMaster NCE-T’s flexible and scalable design supports the integration of new transmission technologies and services, while its open APIs ensure compatibility with existing systems, fostering a seamless and innovative approach to WAN transmission management.

3.4 Huawei CloudFabric DCN Autonomous Driving Network Solution :

Based on the capabilities of iMaster NCE-Fabric, Data Center Networks (DCNs) deliver comprehensive, full-lifecycle services encompassing planning, construction, operation and maintenance (O&M), and optimization. During the planning phase, iMaster NCE-Fabric enables precise network design and resource allocation, ensuring the infrastructure meets current and future demands. In the construction phase, the platform streamlines the deployment process through automation, reducing setup time and minimizing configuration errors. For O&M, iMaster NCE-Fabric offers robust monitoring tools and automated workflows, facilitating real-time network management, quick fault detection, and efficient resolution. Additionally, its advanced analytics capabilities allow continuous network performance evaluation and optimization, adapting to evolving requirements and improving overall efficiency and reliability. This holistic approach ensures that DCNs are not only well-planned and swiftly deployed but also efficiently managed and continuously optimized throughout their lifecycle.

3.4.1 Integrated Planning and Construction:

Huawei's iMaster NCE-Fabric facilitates seamless integration of planning and construction phases within Data Center Networks (DCNs). By leveraging advanced planning tools that interconnect directly with iMaster NCE-Fabric, the platform enables precise and unified network design and deployment. This integration ensures that network resources are efficiently allocated and configured right from the outset, aligning with both current needs and future scalability requirements. A key feature of this integrated approach is Zero Touch Provisioning (ZTP), which significantly reduces manual intervention during network setup. With ZTP, devices can be automatically configured and deployed as soon as they are connected to the network, streamlining the entire construction process. This integrated methodology not only accelerates deployment times but also enhances accuracy and reliability, laying a strong foundation for ongoing network management and optimization.

3.4.2 Simplified Deployment:

Huawei's iMaster NCE-Fabric streamlines network deployment through advanced automation and intelligent features. The platform is capable of self-understanding and converting service intents, translating high-level service requirements into precise network configurations without manual intervention. This intelligent conversion ensures that the network setup aligns perfectly with the intended service objectives. Furthermore, iMaster NCE-Fabric includes sophisticated simulation and evaluation tools for network changes. These tools allow for the simulation of network modifications and their impacts before actual implementation, significantly reducing the risk of human errors. By evaluating potential changes in a controlled environment, administrators can ensure that deployments are error-free and optimized for performance and reliability. This combination of intelligent service intent conversion and robust simulation capabilities simplifies the deployment process, making it faster, more accurate, and highly efficient.

3.4.3 Intelligent O&M:

Huawei's iMaster NCE-Fabric enhances operational efficiency through its intelligent Operations and Maintenance (O&M) capabilities. Leveraging a knowledge graph and expert experience, the platform enables rapid fault detection and precise fault location, ensuring quick identification of issues within the network. This intelligent system can pinpoint faults faster than traditional methods, minimizing downtime and maintaining high service levels. Additionally, iMaster NCE-Fabric facilitates fast fault rectification by utilizing expert experiences and simulation analysis. By simulating fault scenarios and applying tried-and-tested solutions, the platform ensures swift and effective remediation, reducing the time needed to resolve issues and enhancing overall network reliability. These intelligent O&M features significantly improve the network's operational efficiency and resilience.

3.4.4 Real-time Optimization:

Huawei's iMaster NCE-Fabric employs advanced real-time optimization techniques to ensure optimal network performance and resource utilization. Utilizing AI-Fabric, the platform conducts local traffic inference and continuous online model training and optimization. This dynamic approach allows the network to adapt in real-time to changing traffic patterns, ensuring efficient data flow and reducing congestion. Additionally, iMaster NCE-Fabric predicts user behavior, providing actionable resource optimization suggestions. This predictive capability enables proactive adjustments to network resources, enhancing user experience and maximizing the efficiency of the network infrastructure. Through these real-time optimization features, the platform ensures that the network operates at peak performance, meeting the demands of modern data centers and enterprise environments.

Telemetry :

Telemetry refers to the automated process of collecting, transmitting, and analyzing data from remote sources to provide insights and facilitate decision-making. In the context of networking, telemetry involves gathering real-time data from network devices, such as routers, switches, and servers, and transmitting this data to a central location for analysis. This data can include metrics on traffic volume, packet loss, latency, device health, and more.

- **Real-Time Monitoring:** Telemetry provides real-time visibility into network performance and health, allowing network administrators to detect and respond to issues quickly.
- **Data Collection:** It collects a wide range of metrics, including traffic statistics, device status, and environmental conditions.
- **Data Transmission:** The collected data is transmitted to a centralized system, often using protocols like gRPC or HTTP/2 for efficient data transfer.
- **Analysis and Insights:** Advanced analytics tools process the telemetry data to provide insights, identify patterns, and predict potential issues.

Benefits:

- **Improved Network Performance:** By monitoring network performance in real-time, telemetry helps in maintaining optimal network operation.
- **Proactive Issue Detection:** Early detection of anomalies allows for proactive troubleshooting, reducing downtime and improving reliability.
- **Enhanced Security:** Continuous monitoring can help identify security threats and vulnerabilities as they occur.
- **Operational Efficiency:** Automation in data collection and analysis reduces the manual effort required for network management.

Encapsulated Remote SPAN (ERSPAN) :

Encapsulated Remote Switched Port Analyzer (ERSPAN) is a protocol used to mirror traffic from one or more source ports or VLANs and send the mirrored traffic to a destination port on a different device or across a network. ERSPAN extends the capabilities of the traditional SPAN (Switched Port Analyzer) by encapsulating the mirrored traffic in GRE (Generic Routing Encapsulation) packets, allowing it to be sent over an IP network.

- **Traffic Mirroring:** ERSPAN mirrors packets from specified source ports or VLANs on a switch.
- **Encapsulation:** The mirrored traffic is encapsulated in GRE packets, which include ERSPAN headers, making it routable across an IP network.

- **Remote Analysis:** The encapsulated traffic can be sent to a remote destination, such as a monitoring or analysis tool, which could be located on a different network or at a different site.

Benefits:

- **Centralized Monitoring:** Enables centralized traffic monitoring and analysis by aggregating mirrored traffic from multiple locations.
- **Flexible Deployment:** ERSPAN allows traffic to be captured and analyzed without being physically present at the source location.
- **Scalability:** Supports large-scale network monitoring by transporting mirrored traffic across IP networks.

Conclusion :

telemetry provides real-time insights into network performance and health through continuous data collection and analysis, while ERSPAN enables remote traffic mirroring and analysis by encapsulating mirrored traffic in GRE packets and transmitting it across an IP network. Both technologies are essential for modern network management, enhancing visibility, performance, and security.

SNMP VS TELEMTRY :

	SNMP	TELEMTRY
How it works	Polling mechanism collects device performance data and returns data to management platform	Push model continuously sends device operational data to management system
protocols	User datagram protocol	User datagram protocol or TCP
Use cases	Retrieving static data, such as inventory or neighboring devices	Collecting high-resolution performance data, sych as high-speed network interface statistics
benefits	Simple protocol and easy to perform ad hoc data collection ;Widely supported by network devices and monitoring platforms	Sends data at higher rate; more efficient and practical
challenges	Management system repeatedly creates and sends reauests to each device	Telemtry that relies on TCP connections can use large amounts of memory

Tableau 3 Comparison of SNMP and Telemetry Protocols

3.5 ZTP Deployment :

Zero Touch Provisioning (ZTP) is a modern network configuration and management technique designed to simplify and automate the deployment of network devices. By leveraging ZTP, organizations can streamline the process of configuring and provisioning new network equipment without the need for manual intervention. This approach significantly reduces deployment time, minimizes the potential for human error, and ensures consistent and accurate configuration across all network devices. [7]

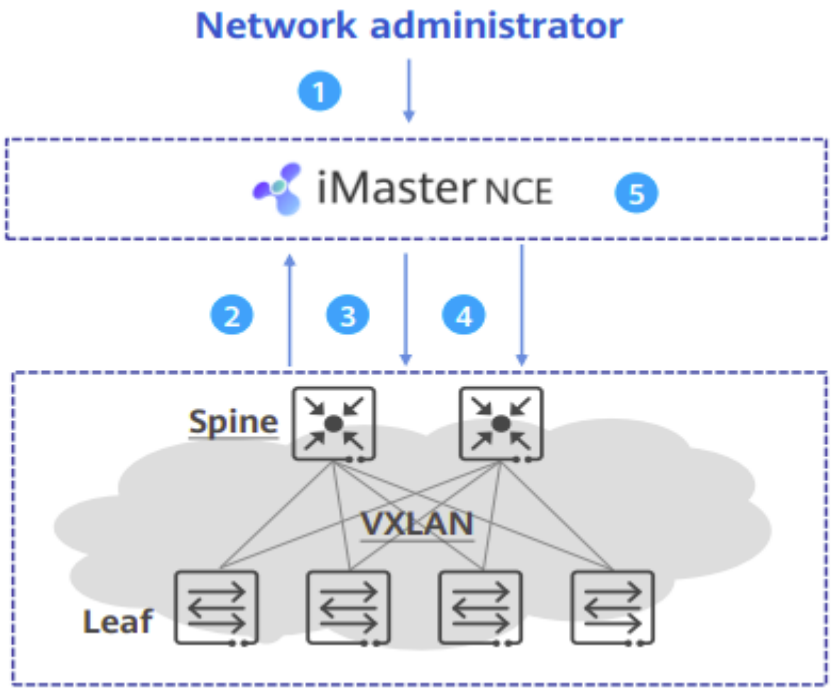


Figure 21Zero Touch Provisioning (ZTP) Deployment Overview

3.5.1 ZTP Deployment Process

Zero Touch Provisioning (ZTP) simplifies the process of network device deployment by automating the configuration steps. Here's a detailed breakdown of the ZTP deployment process:

- **Initiate ZTP Task:** The network administrator initiates the ZTP task by clicking the ZTP icon on the iMaster NCE interface. This action triggers the start of the automated provisioning process.
- **Device IP Address Acquisition:** New network devices automatically obtain an IP address using DHCP to establish initial communication with the iMaster NCE. This step ensures that each device can be uniquely identified and managed.
- **Role Determination and Initial Configuration:** Upon accessing iMaster NCE, the system determines the role of each device, whether it is a spine or leaf node in the network topology. Based on this role, iMaster NCE delivers the necessary configurations to the devices. These configurations include:
    - Management IP address
    - SNMP configuration for network monitoring
    - NETCONF configuration for remote management

  - The management IP address is used to manage the devices, ensuring they are correctly integrated into the network.
- **Global Configuration Delivery:** iMaster NCE then delivers global interconnection configurations, which may include OSPF or BGP configurations. These configurations enable the devices to communicate with each other and establish routing protocols necessary for network operation.
- **Device Online Status:** Once the configuration process is complete, the devices go online successfully. The network administrator can then view comprehensive network-wide information on the iMaster NCE interface, including the status and health of all network devices.
- This streamlined process allows for rapid, error-free deployment of network devices, significantly reducing the time and effort required for network expansion and maintenance. ZTP ensures that all devices are configured consistently, enhancing the overall reliability and performance of the network.

3.5.2 VXLAN :

VXLAN (Virtual Extensible LAN) is often used in conjunction with fabric network architectures to enhance the scalability, flexibility, and manageability of data center networks. Fabric networks, such as leaf-spine architectures, are designed to provide high-performance, low-latency, and reliable connectivity between a large number of network devices.

- **Leaf-Spine Architecture:**
  - A common type of fabric network where the network is divided into two layers: leaf switches and spine switches.
  - Leaf switches connect to the endpoints, such as servers and storage devices.
  - Spine switches provide high-speed interconnections between leaf switches, ensuring all leaf switches are only a single hop away from each other.
- **East-West Traffic Optimization:**
  - Fabric networks are optimized for east-west traffic, which is the communication between devices within the data center, as opposed to north-south traffic that flows in and out of the data center.
  - This optimization reduces latency and increases the performance of data center operations.
- **Scalability and Redundancy:**
  - Fabric networks can easily scale out by adding more leaf or spine switches.
  - Redundancy is built into the architecture, providing multiple paths for data to traverse, which enhances reliability and fault tolerance.

3.5.2.1 Benefits of Combining VXLAN with Fabric Networks:

- **High Performance:**
  - The leaf-spine architecture of fabric networks ensures low-latency, high-bandwidth connectivity, which is further enhanced by VXLAN's ability to efficiently forward traffic.

- **Simplified Network Management:**
  - Centralized control through SDN controllers simplifies the management of complex network environments, allowing for automated provisioning and policy enforcement.

- **Flexibility and Agility:**
  - The decoupling of the logical and physical networks enables rapid deployment of new services and applications, as well as dynamic reconfiguration of the network to meet changing demands.

- **Improved Resource Utilization:**
  - VXLAN allows for the better utilization of network resources by dynamically routing traffic through the most efficient paths in the fabric network.

3.6 Huawei CloudCampus Autonomous Driving Network Solution :

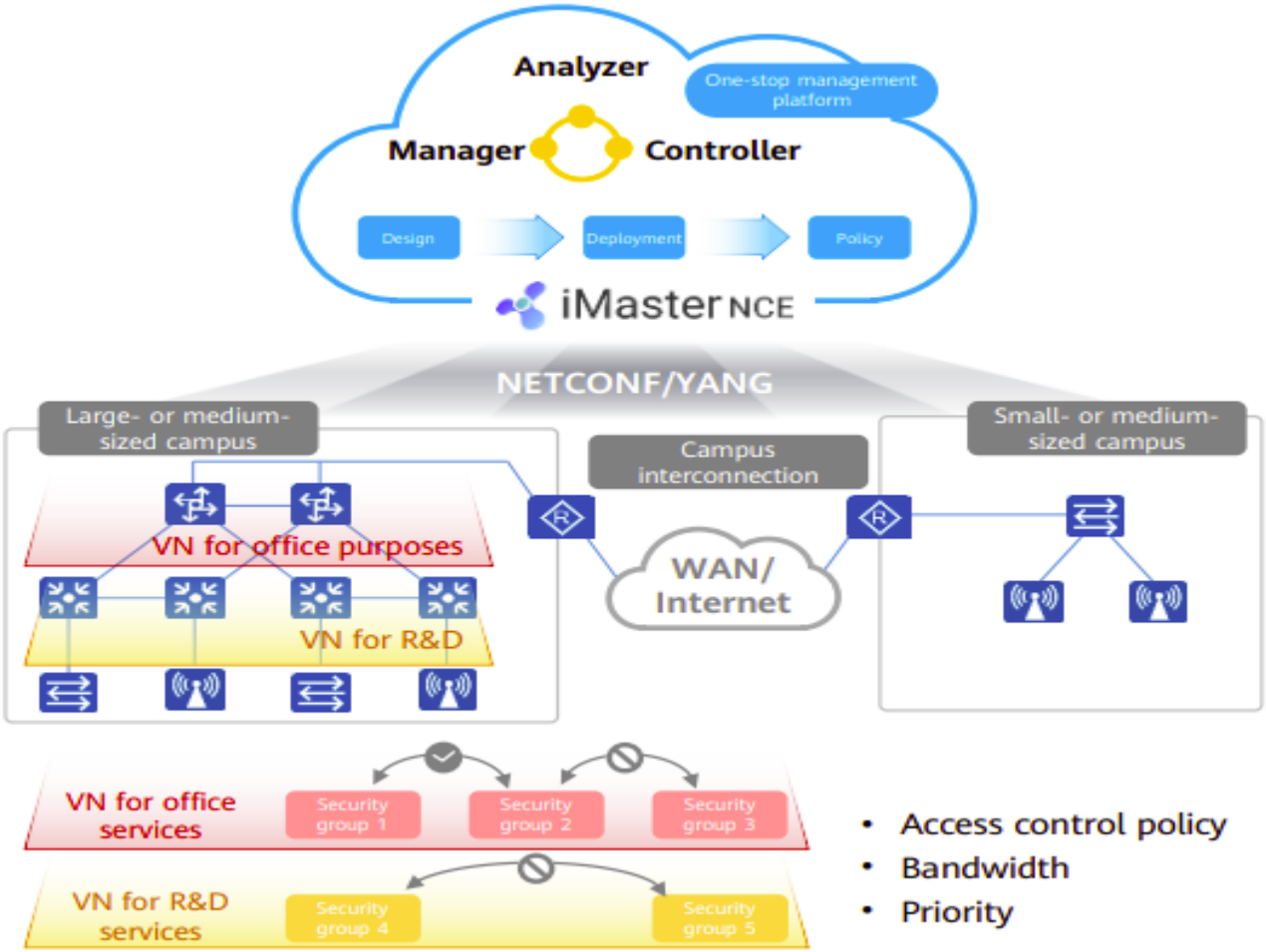


Figure 22CloudCampus Autonomous Driving Network Solution

3.6.1 Fast Network Deployment: Improving Deployment Efficiency by 600%

- **Device Plug-and-Play:**

  - **Simplified Device Deployment**: The process is streamlined so that new devices can be added to the network without complex setup procedures.
  - **Scenario Navigation**: Guided setup processes help ensure that devices are deployed correctly according to the specific requirements of different scenarios.
  - **Template-Based Configuration**: Reusable configuration templates simplify the setup of devices, reducing time and errors associated with manual configurations.

- **Simplified Network Deployment:**

  - **Network Resource Pooling**: Resources are pooled together to create a more flexible and efficient network, allowing for easier scaling and management.
  - **Multi-Purpose Network**: A single network infrastructure can support various types of services and applications, reducing the need for multiple specialized networks.
  - **Automatic Service Provisioning**: Services are provisioned automatically, eliminating the manual processes typically required and reducing deployment times significantly.

3.6.2 Fast Service Provisioning: Improving User Experience by 100%

- **Free Mobility:**

  - **GUI-Based Policy Configuration**: Network policies are configured through a graphical user interface, simplifying the process for administrators and allowing for quick adjustments.
  - **Uninterrupted User Access**: Users can access the network from any location without changes to their permissions or experience, ensuring seamless connectivity.

- **Intelligent Terminal Identification:**

  - **Anti-Spoofing Measures**: The system identifies and prevents unauthorized devices from accessing the network, enhancing security.
  - **High Identification Accuracy**: Intelligent algorithms achieve over 95% accuracy in identifying terminals, ensuring that legitimate devices are recognized and managed correctly.

- **Intelligent HQoS (Hierarchical Quality of Service):**

  - **Application-Based Scheduling and Shaping**: Network traffic is managed based on the specific requirements of different applications, ensuring optimal performance.
  - **Refined Bandwidth Management**: Bandwidth is allocated based on user and application needs, ensuring that key users have the resources they need for a high-quality experience.

3.6.3 Fast Intelligent O&M: Improving Network Performance by Over 50%

- **Real-Time Experience Visualization:**

  - **Telemetry-Based Monitoring**: Continuous monitoring of network performance provides real-time insights into user experiences across different areas and times.
  - **Detailed Visualizations**: Data is presented in an intuitive format, making it easier for administrators to understand and act on network performance metrics.

- **Precise Fault Analysis:**

  - **Proactive Issue Identification**: The system can identify 85% of typical network issues before they affect users, providing recommendations for resolution.
  - **Real-Time Data Analysis**: Continuous comparison and analysis of real-time data help predict potential faults, allowing for preemptive measures.

- **Intelligent Network Optimization:**

  - **Predictive Optimization**: Historical data is used to predict and optimize network performance, ensuring that resources are allocated efficiently.
  - **Performance Improvement**: Predictive measures improve overall network performance by over 50%, providing a better experience for all users.

3.7 Device Plug-and-Play:

3.7.1 Deployment by Scanning Bar Codes :

Using iMaster NCE, device plug-and-play is facilitated through three streamlined deployment modes—scanning QR code, DHCP-based deployment, and deployment through the registration center—ensuring quick and efficient network setup

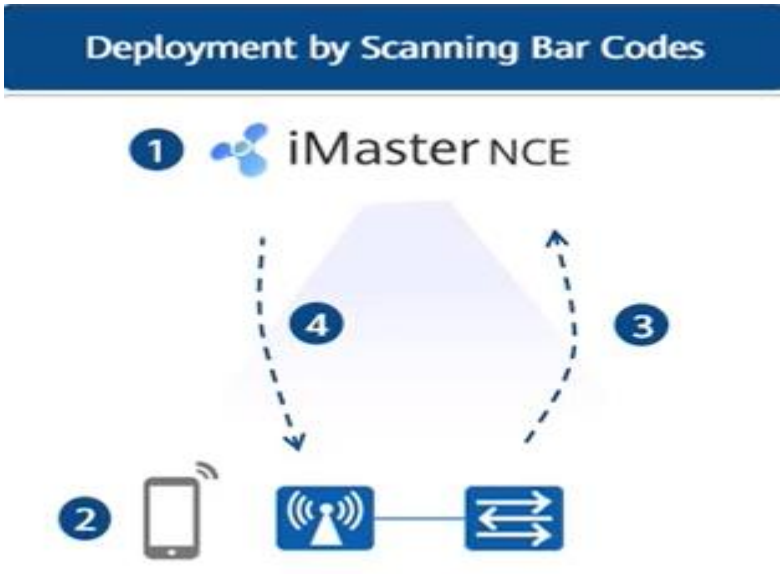


Figure 23Deployment by Scanning Bar Codes

Deployment by scanning QR codes is a straightforward process with four key steps: first, pre-configuration of device settings is completed to prepare for deployment; second, the actual deployment involves scanning bar codes on the devices, which simplifies and speeds up the registration process; third, devices automatically register and log in to the network, ensuring seamless integration; finally, automatic configuration delivery

Takes place, Where the network settings are pushed to the devices without manual intervention, streamlining the setup and reducing errors.

3.7.2 DHCP-based Deployment :

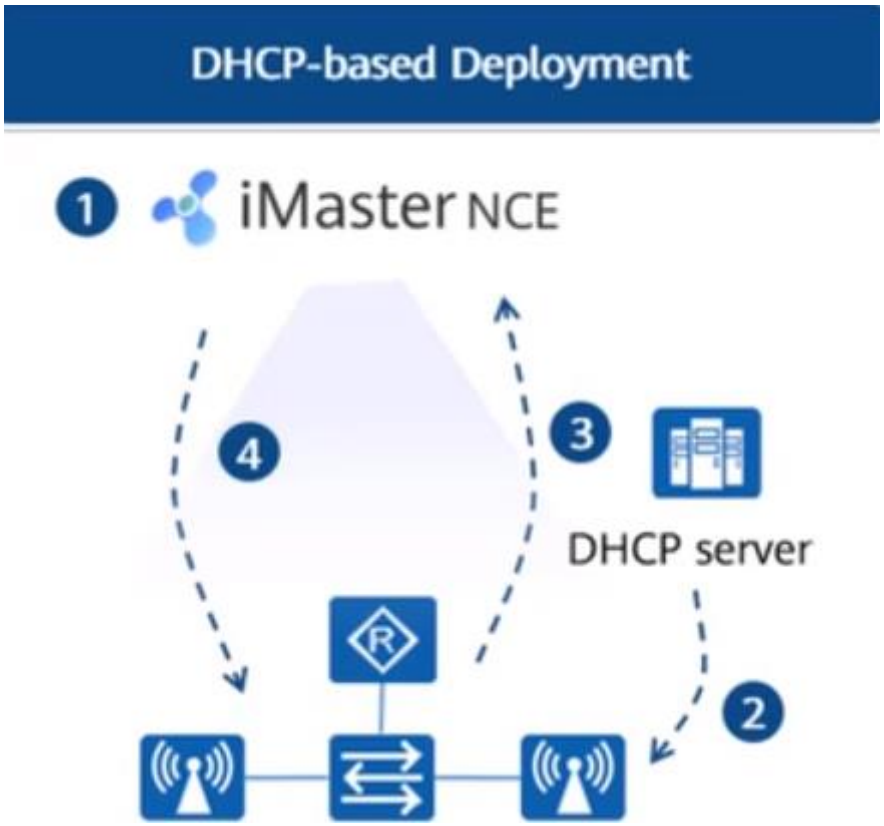


Figure 24 Diffrent steps for a DHCP based Deployment

DHCP-based deployment involves four main steps: first, pre-configuration of device settings is performed to ensure readiness for deployment; second, devices obtain registration information through the DHCP server, simplifying the initial network connection; third, devices automatically register and log in to the network, ensuring a smooth integration process; finally, automatic configuration delivery occurs, where network settings and policies are pushed to the devices without manual intervention, streamlining setup and minimizing errors.

3.7.3 Deployment through the Registration Center:

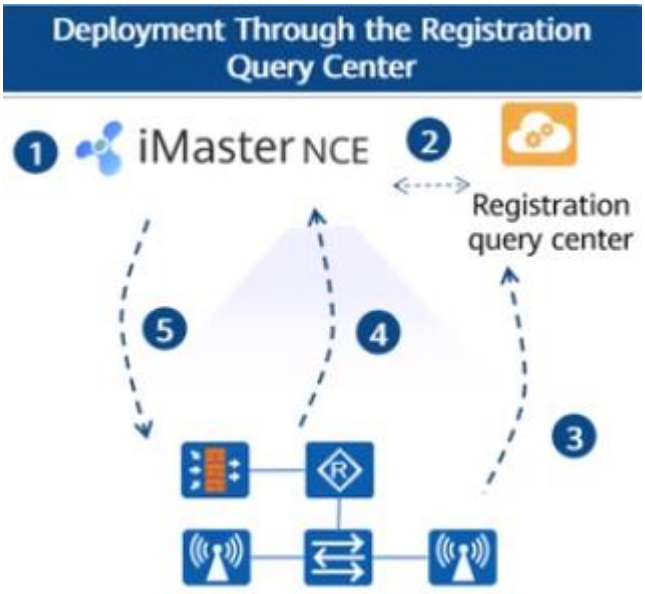


Figure 25Deployment through the Registration Center

Deployment through the registration center follows these steps: first, pre-configuration of devices is conducted to prepare them for deployment; second, information synchronization ensures that device and network settings are updated and aligned; third, devices obtain registration information through the registration center, facilitating their network integration; fourth, devices automatically register and log in to the network; finally, automatic configuration delivery pushes necessary network settings and policies to the devices, ensuring a seamless and efficient setup process.

3.8 Artifitial intelligence used in network part :

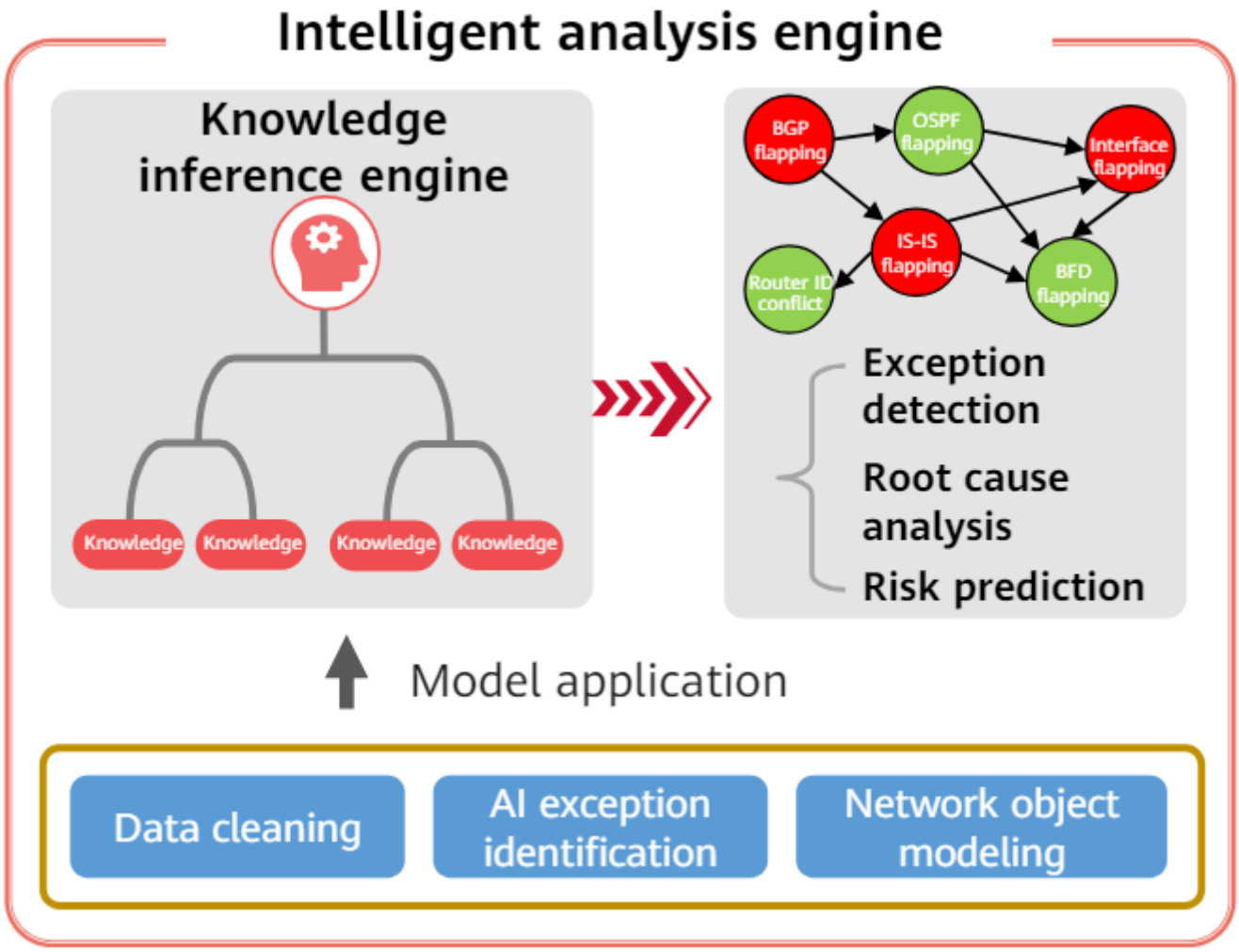


Figure 26AI-Driven Network Enhancement with iMaster NCE

3.8.1 AI-Powered Intelligent Network Management with iMaster NCE

The iMaster NCE platform integrates AI capabilities to enhance network management, providing an intelligent, automated solution for data center networks (DCNs) and radio calibration. Leveraging Huawei's extensive experience and continuous learning, iMaster NCE collects and processes holographic data and telemetry data to create a comprehensive understanding of the network.

3.8.2 Network Change Simulation and Risk Prediction

Using iMaster NCE, network changes can be simulated to predict and mitigate risks. The process involves collecting live network configuration, topology, and resource information, which is then modeled and analyzed using formal verification algorithms. This ensures that any changes to the network are thoroughly evaluated for resource sufficiency, access connectivity, and impact on existing services, thereby ensuring a seamless and secure transition.

3.8.3 AI-Powered Intelligent O&M for DCNs

iMaster NCE employs a knowledge inference engine for intelligent analysis, which includes data cleaning, AI exception identification, and network object modeling. This enables rapid fault detection, root cause analysis, and risk prediction. The system provides recommended emergency plans such as port isolation, configuration rollback, and capacity expansion recommendations, which aid in swift manual rectification and intent-based loop closing.

3.8.4 AI-Powered Intelligent Radio Calibration

Traditional manual and automatic calibration methods often fail to achieve optimal results due to their time-consuming nature and inability to account for real-time interference. iMaster NCE offers an AI-powered intelligent radio calibration process that uses real-time and historical data for calibration simulations and adjustments. This results in significant improvements in downlink rates per terminal and reductions in Wi-Fi channel interference, as verified by authoritative organizations like Tolly.

Together, these AI-driven capabilities of iMaster NCE ensure efficient network deployment, fast service provisioning, and intelligent O&M, thereby significantly enhancing overall network performance and user experience.

4 Small- and Medium-sized Campus Cloud Managed Network Comprehensive Lab - Reusing Virtual Environments

Preamble :

After familiarizing ourselves with the fundamentals of SDN, we will now focus on its implementation in the context of an enterprise network. The goal is to understand the changes this paradigm entails for network design and administration. Among other things, we will explore the methods of interaction with the elements involved in the proposed solution

Deploying and Managing Small- to Medium-Sized Campus Networks with Cloud Solutions :

The objective of this practical project is to demonstrate the deployment and management of a Branch network using cloud-managed solutions. This comprehensive simulation focuses on the reuse of virtual environments to streamline network setup, management, and operation processes. By leveraging advanced cloud management platforms, this project aims to showcase efficient, scalable, and flexible network configurations suitable for educational institutions. The simulation is structured to provide an approach to deploying and managing campus networks, highlighting the key functionalities and benefits of using cloud-managed solutions. A key aspect of this project is the reuse of virtual environments to enhance efficiency and scalability. By leveraging virtual environments, the project demonstrates how network administrators can quickly deploy, test, and manage network configurations without the need for extensive physical infrastructure. This approach not only saves time and resources but also allows for more flexible and adaptable network management practices. This comprehensive simulation provides a thorough introduction to the deployment and management of small- to medium-sized campus networks using cloud-managed solutions.

4.1 Introduction to Comprehensive Experiments

4.1.1 Content Description

- **This simulation includes these 5 modules**
    - Module 1 is the preconfiguration planning of the cloud management platform and management switches.
    - Module 2: Creating sites and bringing devices online. By creating site HQ on iMaster NCE- Campus, you can manage devices in the HQ.
    - Module 3: describes wired and wireless service configuration at the HQ site. This module helps master wired and wireless configuration on the NCE-Campus and the wired and wireless convergence deployment solution.
    - Module 4: is admission authentication. By configuring 802.1X authentication for wired terminals and Portal authentication for wireless terminals on iMaster NCE-Campus, you can configure authentication and policies for wired and wireless terminals to access the network on the controller.
    - Module 5: is about result verification. By testing service connectivity and viewing user login and logout logs on iMaster NCE-Campus, mastering basic network O&M methods based on iMaster NCE-Campus.

Lab Networking

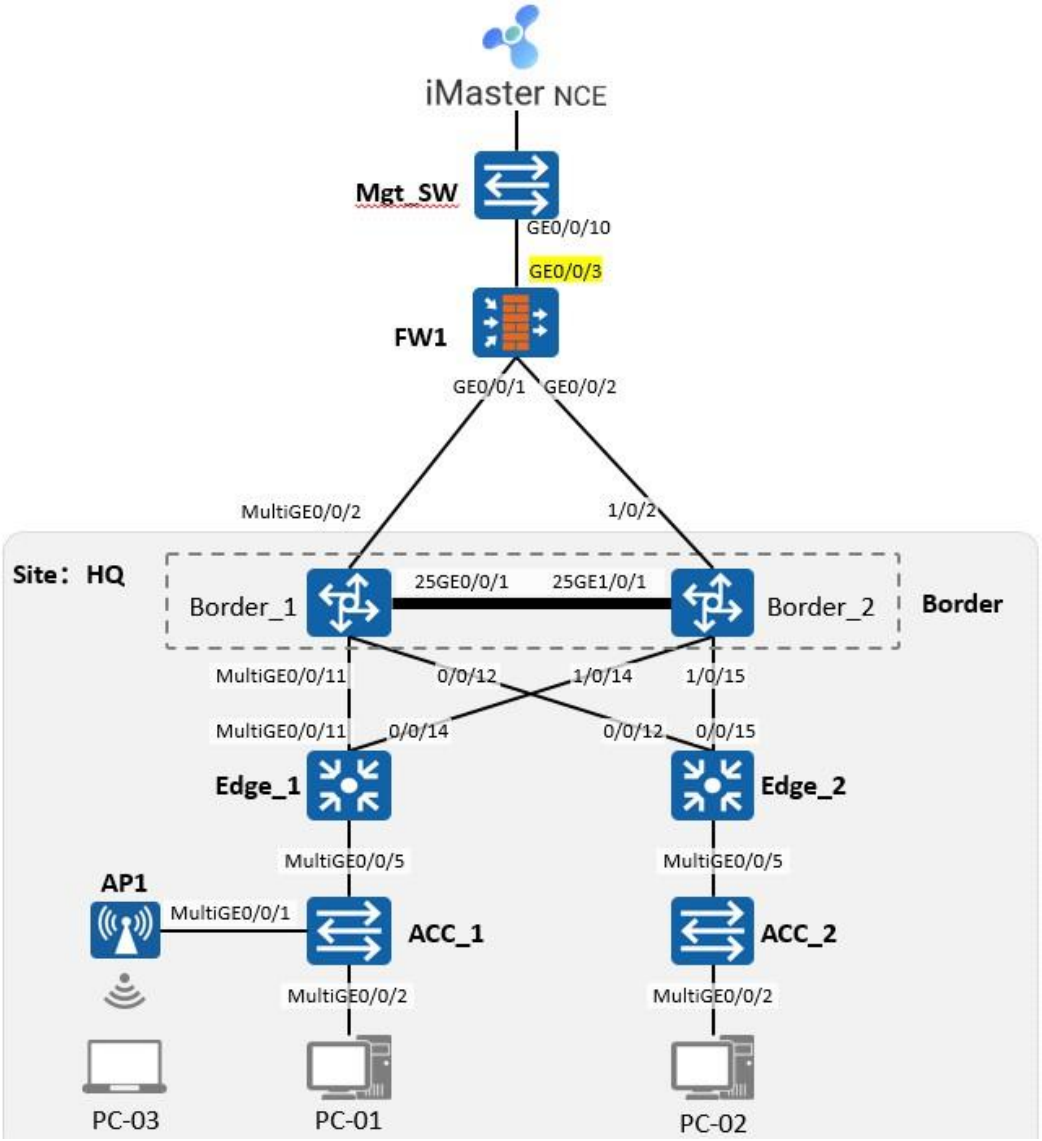


Figure 27 Branch Network topologie

As shown in the figure, the network consists of the HQ, egress zone, network service zone, and cloud management platform.

Site HQ: ACC_1 and ACC_2 are connected to wired terminals to provide network services for wired users. ACC_1 connects to APs to provide network services for wireless users. Edge_1 and Edge_2 function as aggregation devices, and Border functions as core devices and consists of two stacked core switches.

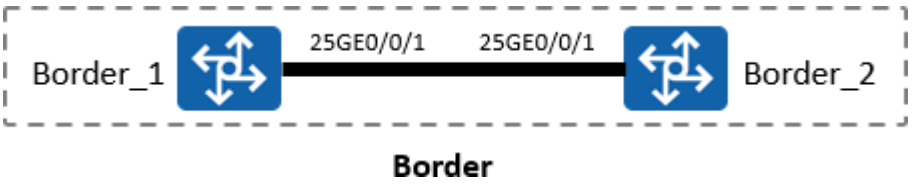
Egress zone: FW1 functions as the campus egress and provides the external network service connection function for the campus intranet.

NCE-Campus: connects the egress zone and the NCE-Campus controller to provide the campus network management function.

4.2 Creating a Site and Bringing a Device Online :

4.2.1 Configuring Stacking on Border Switches :

4.2.1.1 Networking Overview



4.2.1.2 Network planning

Equipment	Port	Logical Interface
Border_1	25GE0/0/1	stack-port 0/1
Border_2	25GE0/0/1	stack-port 0/2

4.2.1.3 Configuration roadmap

- Configure a logical stack port on Border_1, add it to a physical port, and configure the stack ID and stack priority.
- Configure a logical stack port on Border_2, add it to a physical port, and configure a stack ID.

4.2.1.4 Configuration Procedure

➢ **Configure service port stacking on Border_1.**

Configure service port 25GE0/0/1 on Border_1 as a physical member port and add it to the corresponding logical stack port.

<HUAWEI> system-
view [HUAWEI]
sysname Border_1
[Border_1] interface stack-port 0/1
[Border_1-stack-port0/1] port interface 25GE 0/0/1 enable
Warning: Enabling stack function may cause configuration loss on the interface. Continue? [Y/N]: y.

Disable the interconnection interface between Border_1 and Border_2 and enable it after Border_2 restarts.

[Border_1-stack-port0/1] shutdown
interface 25GE 0/0/1 [Border_1-stack-
port0/1] quit

Set the stack ID of Border_1 to 0 and the stack priority to 200.

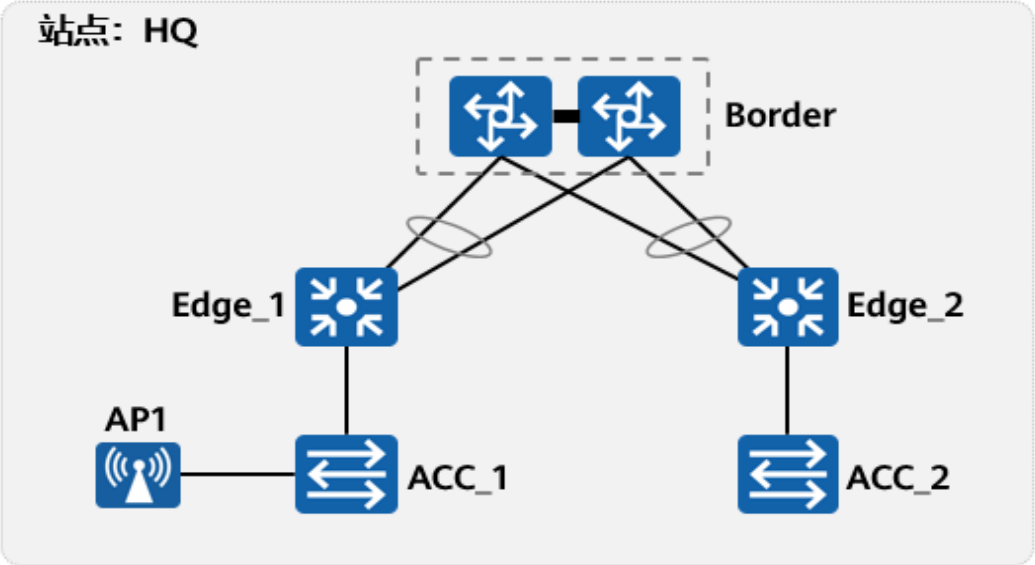
[Border_1] stack slot 0 priority 200
Warning: Do not frequently modify the Priority because it will make the stack split. Continue? [Y/N]: y

Important: We do the same thing for Border_2 except for the stack port we set it to stack-port 0/1.

Enable the interconnection between Border_1 and Border_2.
[Border_1] interface stack-port 0/1
[Border_1-stack-port0/1] undo shutdown interface 25GE 0/0/1 [Border_1-stack-port0/1] quit

4.3 Creating a Site and Adding Devices

4.3.1.1 Networking Overview



4.3.1.2 Network planning

Stacking system planning

Parameter	Value
Stack name	Border
Site	HQ
Roles	core
Creation mode	Manually created
Members of the	Border_1 and Border_2

Tableau 4Stacking system planning

4.3.1.3 Configuration roadmap

- Log in to the iMaster NCE-Campus controller.
- Creating a Site and Adding Devices
- Creating a Stack

4.3.1.4 Configuration Procedure

Log in to the iMaster NCE-Campus controller and start the deployment.

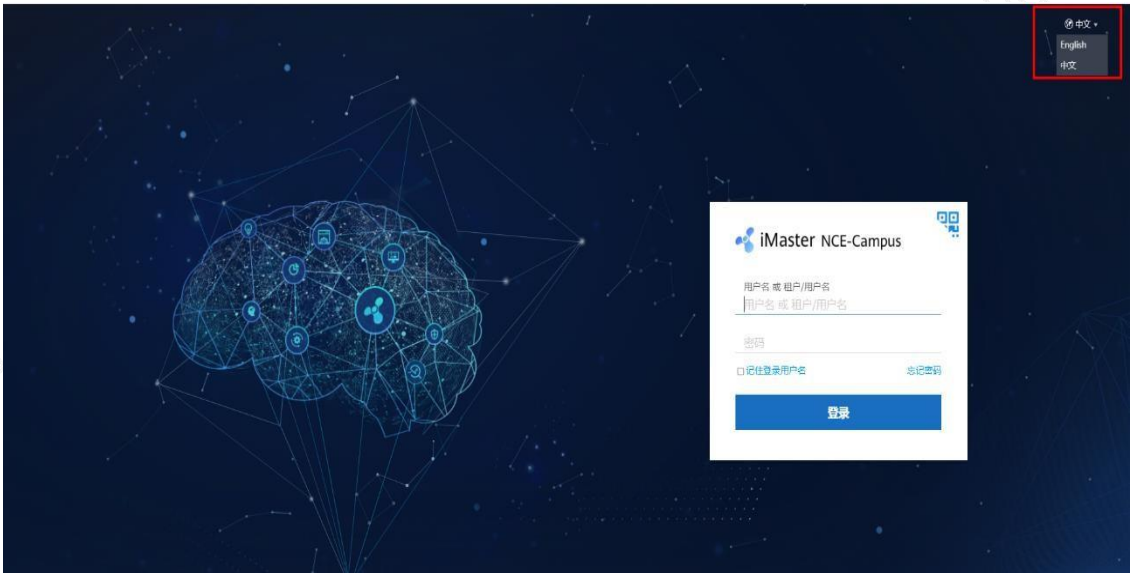
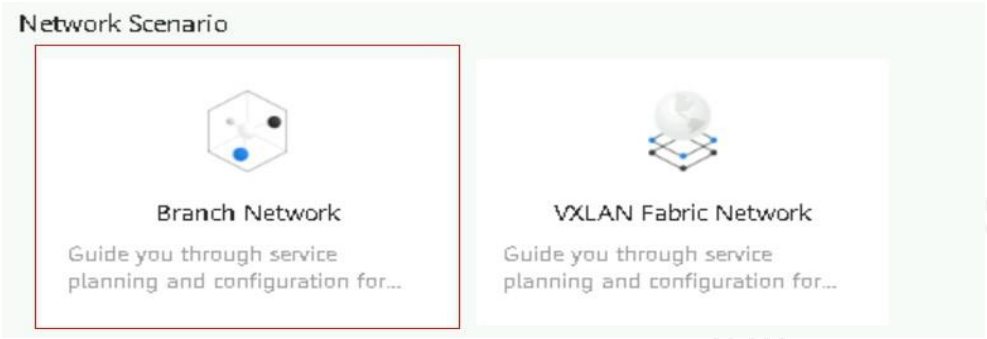
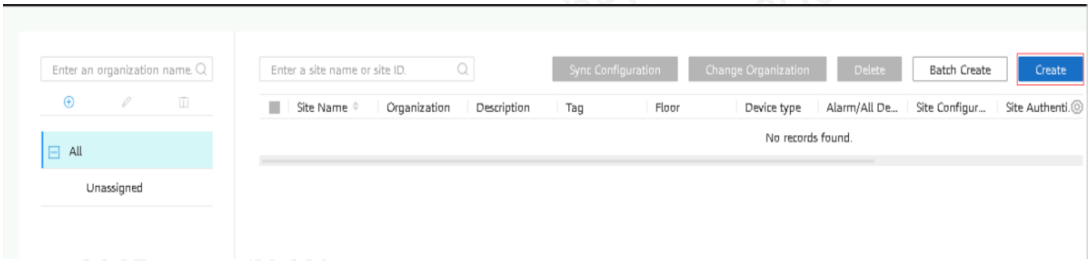


Figure 28 iMaster NCE login page

On the home page of iMaster NCE-Campus, Networking Scenario > Branch Network. The Fabric network configuration page is displayed, as shown in the following figure.





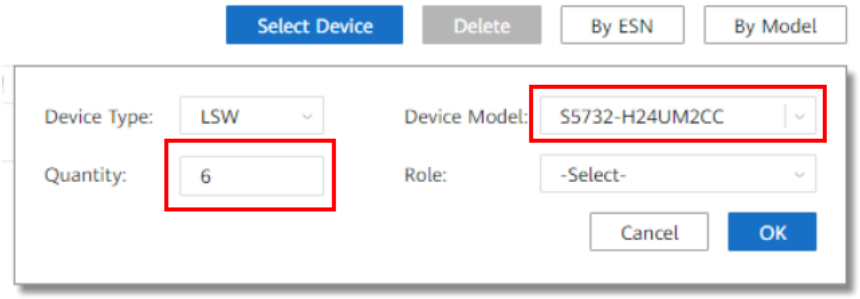
➢ Creating a Site and Adding Devices

Create a site.

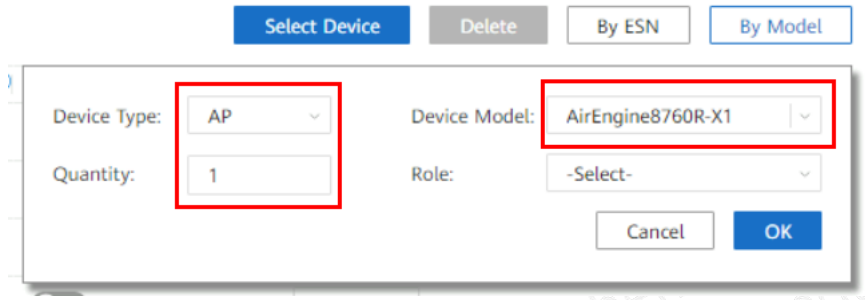
Site created.

we select some basic site information and select a device type.

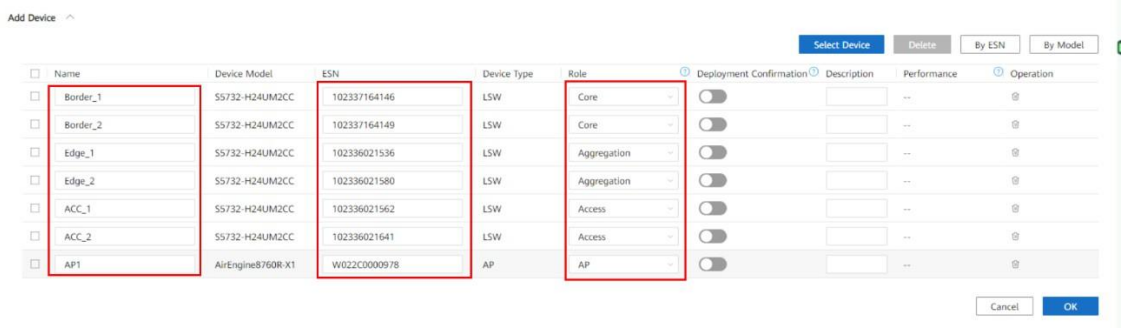
Add six S5732-H24UM2CCs by device model.



Add an AirEngine8760R-X1 by device model.

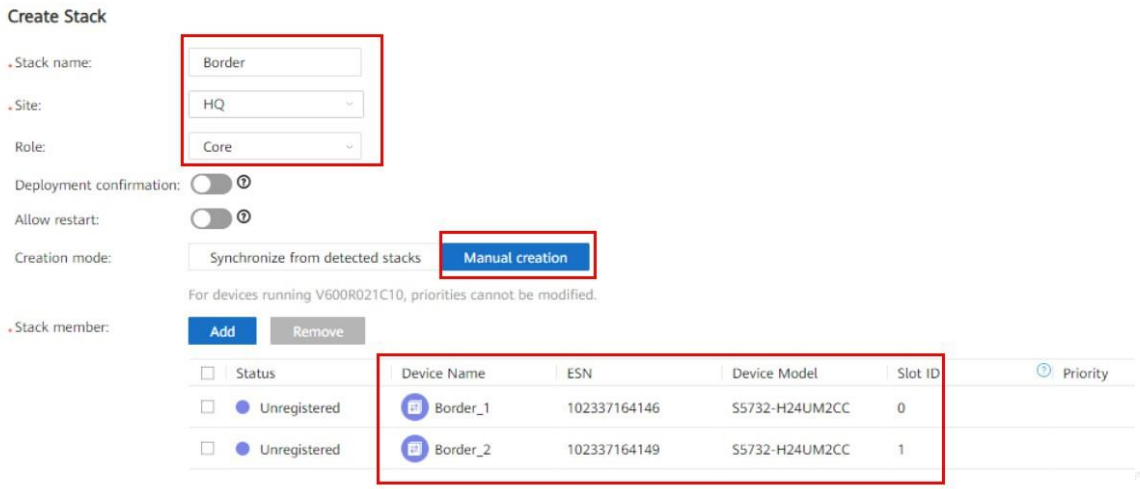


Set the device name and role and add the ESN of the device according to the planning table.



➢ Adding a stack

Choose Network Planning > Device Resource > Device Management. On the Device Management page, choose Device Group > Stack.



.

- **The device management configuration has not been completed. Therefore, all devices are offline.**

4.4 Configuring Border Switch Management

4.4.1 Networking Overview

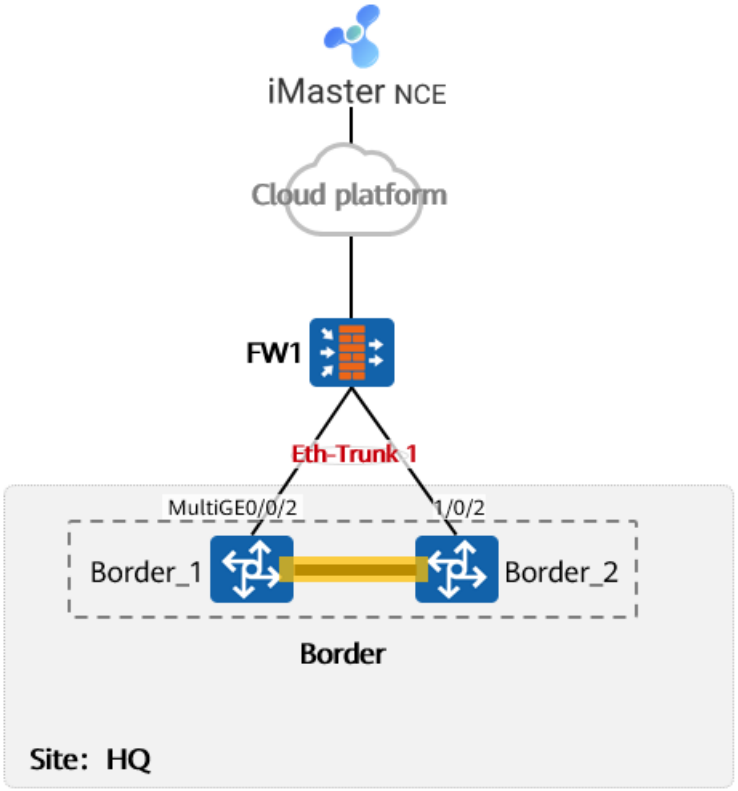


Figure 29 Border Switch Management

Network Planning

Parameter	Value
Interconnection Between Border and NCE-Campus L2 Interface	Border switch interconnection port: Eth-Trunk 1 Border switch interconnection interface type: Trunk Allow-Pass VLAN 2 to allow packets to pass through the interconnection ports of core switches.
Interconnection Between Border and NCE-Campus L3 Interface	Border switch interconnection interface: VLANIF 2 IP address and subnet mask for interconnection with the core switch: 172.16.2.254/24 Southbound IP address and port number of iMaster NCE-Campus: 10.175.205.137:10020

Tableau 5Border Switch Management Planning

Equipment	Eth-Trunk interface ID	Member interface	Parameter Description
Border	Eth-Trunk 1	MultiGE0/0/2 MultiGE1/0/2	Administrative status: enabled Working mode: manual mode Link type: Trunk Allowed VLAN: 2

Tableau 6Eth-Trunk Planning for Border Switches

4.4.1.1 Configuration roadmap

- Configure the VLAN and IP address used by the core switch to interconnect with NCE-Campus.
- Configuring a Southbound Static Route from the Border Switch to iMaster NCE-Campus
- Configuring the Border Switch to Communicate with iMaster NCE-Campus in NETCONF Over SSH Callhome Mode
- Configuring Uplink Aggregation on Border Switches

4.4.1.2 Configuration Procedure

Stack management means that the stack system goes online on NCE-Campus, the stack system needs to obtain the southbound IP address of NCE-Campus and establish the network between the stack system and NCE-Campus.

➢ Configuring VLANs and IP Addresses for Border Interfaces

```
[Border] vlan 2
[Border-vlan-2] quit
[Border] interface Eth-Trunk 1
[Border-Eth-Trunk1] port link-type trunk
[Border-Eth-Trunk1] port trunk allow-pass vlan 2
[Border-Eth-Trunk1] quit
[Border] interface MultiGE 0/0/2
[Border-MultiGE0/0/2] eth-trunk 1
[Border-MultiGE0/0/2] quit
[Border] interface MultiGE 1/0/2
[Border-MultiGE1/0/2] eth-trunk 1
[Border-MultiGE1/0/2] quit
[Border] interface vlanif 2
[Border-Vlanif2] ip address 172.16.2.254 24
[Border-Vlanif2] quit
```

➢ Configuring a Static Route to the Southbound Interface of NCE-Campus

```
[Border] ip route-static 10.175.205.137 24 172.16.2.1
```

Configuring the NETCONF Function on the Border Node

```
[Border] netconf
Warning: Enabling NETCONF will cause LNP to be disabled and STP to be enabled. Continue? [Y/N]:y
[Border-netconf] source ip 172.16.2.254
[Border-netconf] callhome imaster-campus
[Border-netconf-callhome-imaster-campus] ip address 10.175.205.137 port 10020
[Border-netconf-callhome-imaster-campus] return
```

4.5 Configuring Aggregation and Access Switch Management

4.5.1 Networking Overview

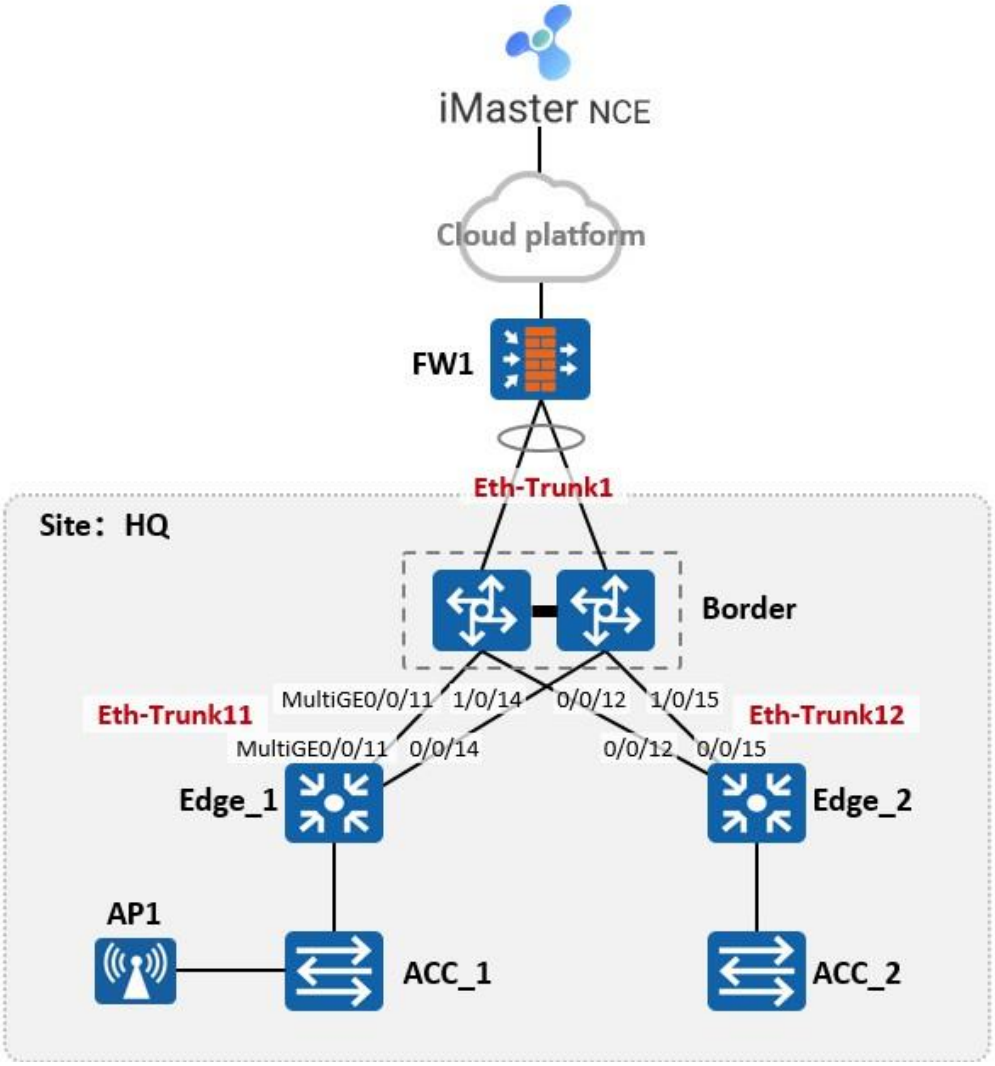


Figure 30Configuring Aggregation and Access Switch Management

Network planning

Parameter	Value
Aggregation/Access Device Goes Online (Border as DHCP)	Device: Border Subnet name: Manage_Net Management VLAN ID in wired auto-negotiation mode: VLAN 3 IP address obtaining mode: manual IP address/mask: 172.16.3.254 / 24 DHCP: enabled DHCP mode: server

	Management network: enabled AP mode: Fit AP Auto-negotiate controller address: On Controller address type: IP
APs go online. (Border as native AC)	Management VLAN with auto-negotiation: VLAN 4

Tableau 7Aggregation and Access Switch Management Planning

Equipment	Eth-Trunk Interface ID	Member interface	Parameter Description
Border	Eth-Trunk 11	MultiGE0/0/11 MultiGE1/0/14	Administrative status: enabled Eth-Trunk auto-negotiation: enabled Working mode: manual mode Link type: default
Edge_1	Auto-negotiation	MultiGE0/0/11 MultiGE0/0/14	
Border	Eth-Trunk 12	MultiGE0/0/12 MultiGE1/0/15	
Edge_2	Auto-negotiation	MultiGE0/0/12 MultiGE0/0/15	

Tableau 8and aggregation switch Eth-Trunk Planning

Configuration roadmap

- Restore the aggregation or access switch to factory settings.
- Configuring the Border Switch as the Management Subnet Gateway of Aggregation/Access Switches
- Configure the auto-negotiation management VLAN with the core switch as the root device.
- Create an Eth-Trunk interface connecting the core switch and aggregation switch, and enable the auto-negotiation function on the Eth-Trunk interface.

➢ Restoring the Device to Factory Settings

Log in to Edge_1, Edge_2, ACC_1, and ACC_2 respectively and run the following command to restore the devices to their factory settings:

```
<Edge_1> system-view
Enter system view, return user view with Ctrl+Z.
[Edge_1] reset netconf db-configuration
Warning: This operation will clear the database configuration and saved configuration file and restart the device. Continue? [Y/N]: y
```

4.6 Configuring Fit APs to Go Online on the AC (Border)

4.6.1 Networking Overview

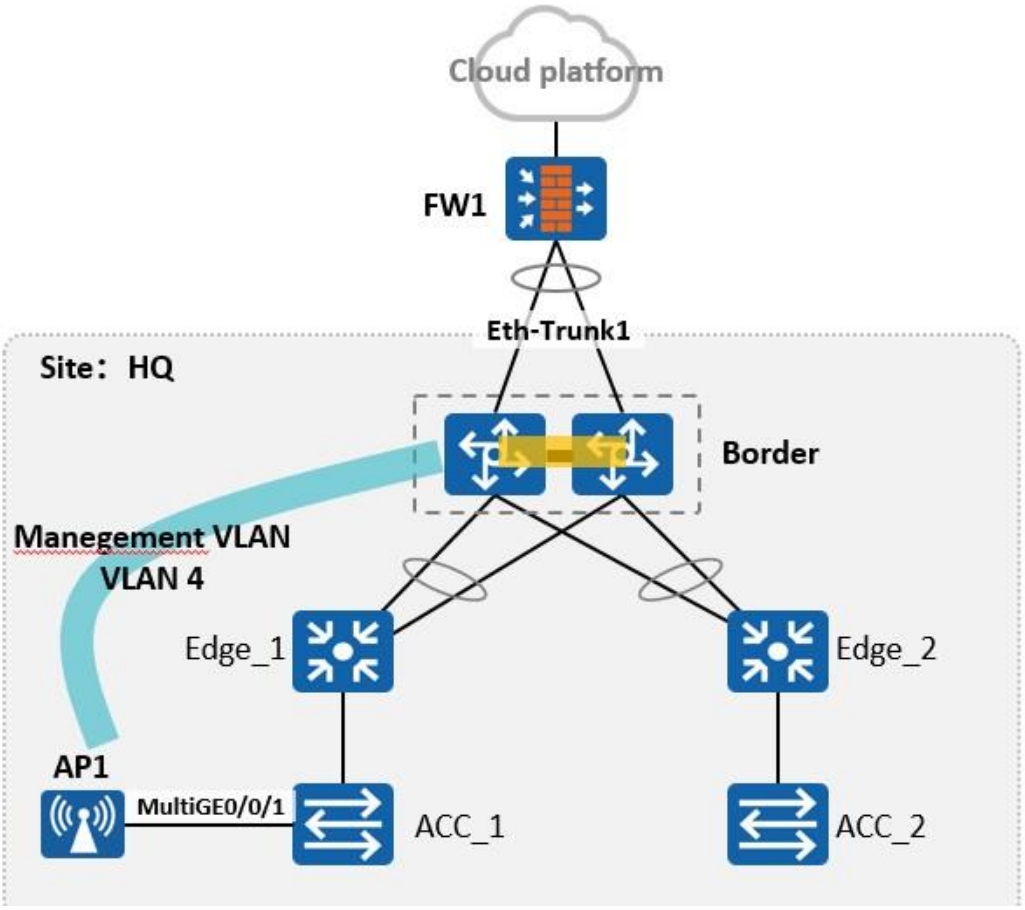


Figure 31Configuring Fit APs to Go Online on the AC

Network planning

AP Management

Parameter	Value
AP goes online. (Border as native AC)	Device: Border Subnet name: AP_Manage_Net Management VLAN ID in auto-negotiation mode: VLAN 4 IP address obtaining mode: manual IP address/mask: 172.16.4.254 / 24 DHCP: enabled DHCP mode: server Management network: enabled AP mode: Fit AP Auto-negotiate controller address: On

	Auto-Negotiation WAC Address: On WAC Address: 172.16.4.254

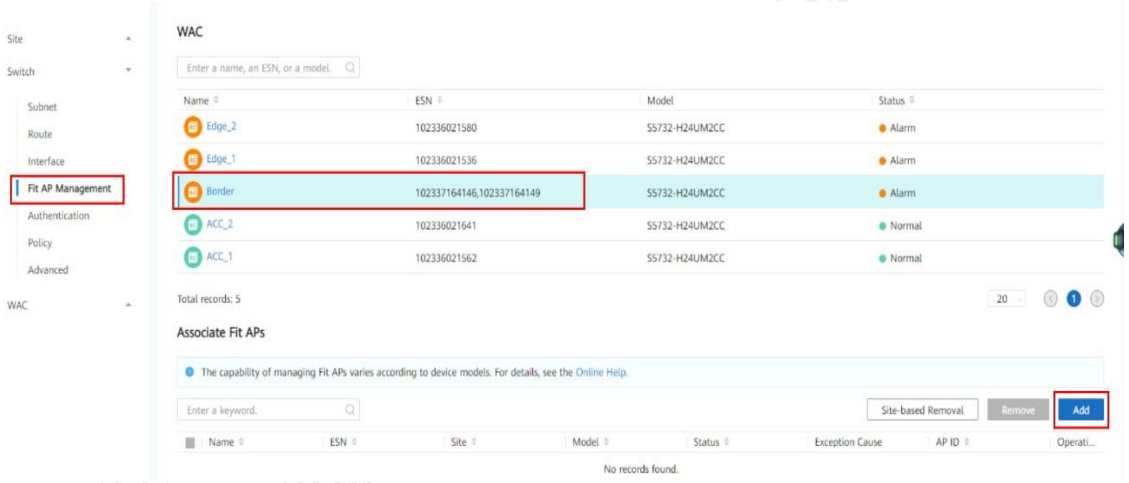
Tableau 9AP Management Planning

4.6.1.1 Configuration roadmap

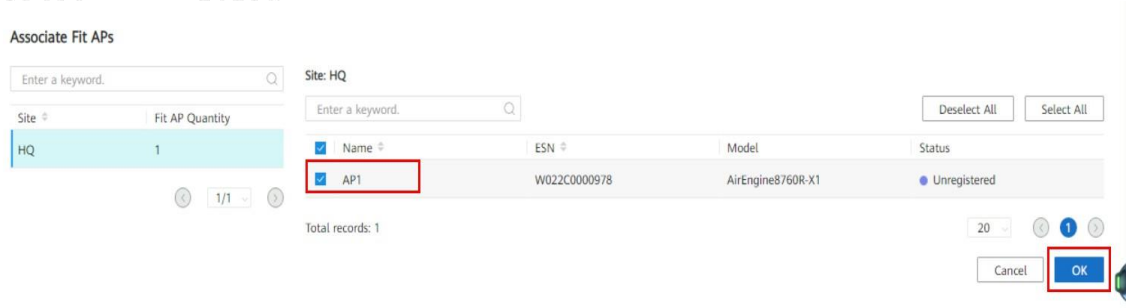
- Assign APs to Border in Site Configuration
- Configuring the Border Switch as the Management Subnet Gateway of APs
- Set the wireless auto-negotiation management VLAN of the core switch to VLAN 4.
- On the border web page or CLI, manually set the CAPWAP tunnel source interface to VLANIF 4.

4.6.1.2 Configuration Procedure

On the NCE-Campus home page we go to Manage Fit AP, then We click the Border column and then click Add to allocate AP1 to the border.



Select AP1 and click OK.



- **Set the source address of the CAPWAP tunnel.**

  # On the border CLI, we set the source address of the CAPWAP tunnel:

  Set the CAPWAP communication source interface to VLANIF 4. Configure the user name and password (admin and Huawei@123) for logging in to the Fit AP. the access password (Huawei@123) for the global offline management VAP. The password is used to connect to the offline management SSID of the fit AP in wireless mode.

  [Border] capwap source interface Vlanif 4

  Warning: This command may cause a configuration conflict in NETCONF mode. Continue? [Y/N]:y

  Set the user name for FIT APs(The value is a string of 4 to 31 characters, which can contain letters, underscores, and digits, and must start with a letter): admin

  Set the password for FIT APs(plain-text password of 8-128 characters or cipher-text password of 48-188 characters that must be a combination of at least three of the following: lowercase letters a to z, uppercase letters A to Z, digits, and special characters): Huawei@123

  Confirm password: Huawei@123

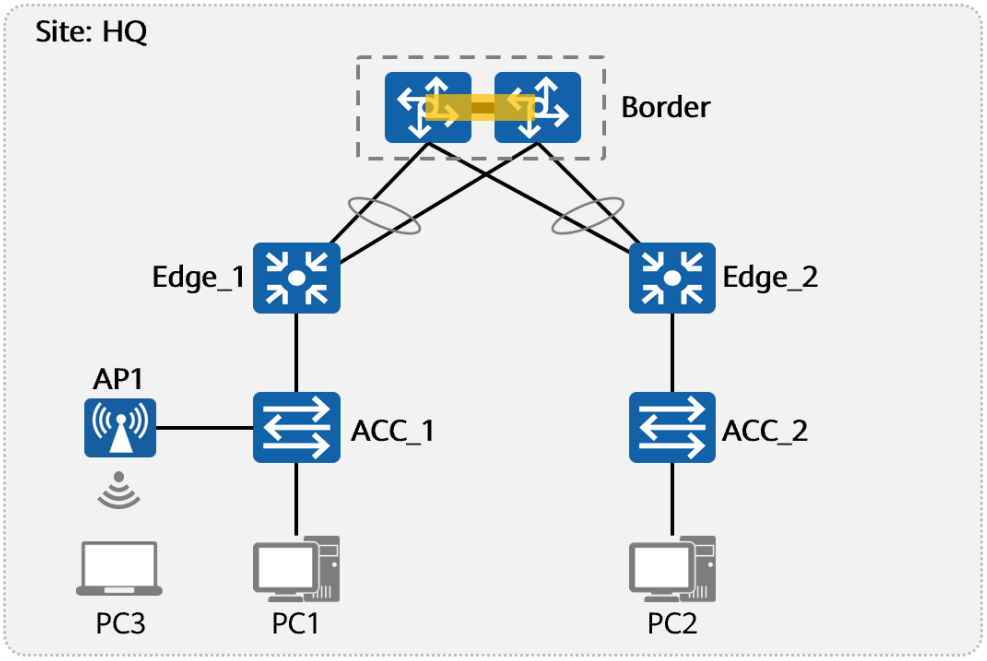
  Set the global temporary-management psk(contains 8-63 plain-text characters, or 48-108 cipher-text characters that must be a combination of at least two of the following: lowercase letters a to z, uppercase letters A to Z, digits, and special characters): Huawei@123

  Confirm PSK: Huawei@123

4.7 Service network planning and configuration

4.7.1 Configuring Wired Services

Networking Overview



Network planning

Parameter	Value
Wired service address	Device: Border Subnet name: Wired_Net Management VLAN ID in wired auto-negotiation mode: VLAN 100 IP address obtaining mode: manual IP address/mask: 172.27.10.254/24 DHCP: enabled DHCP mode: server

	Management network: Off

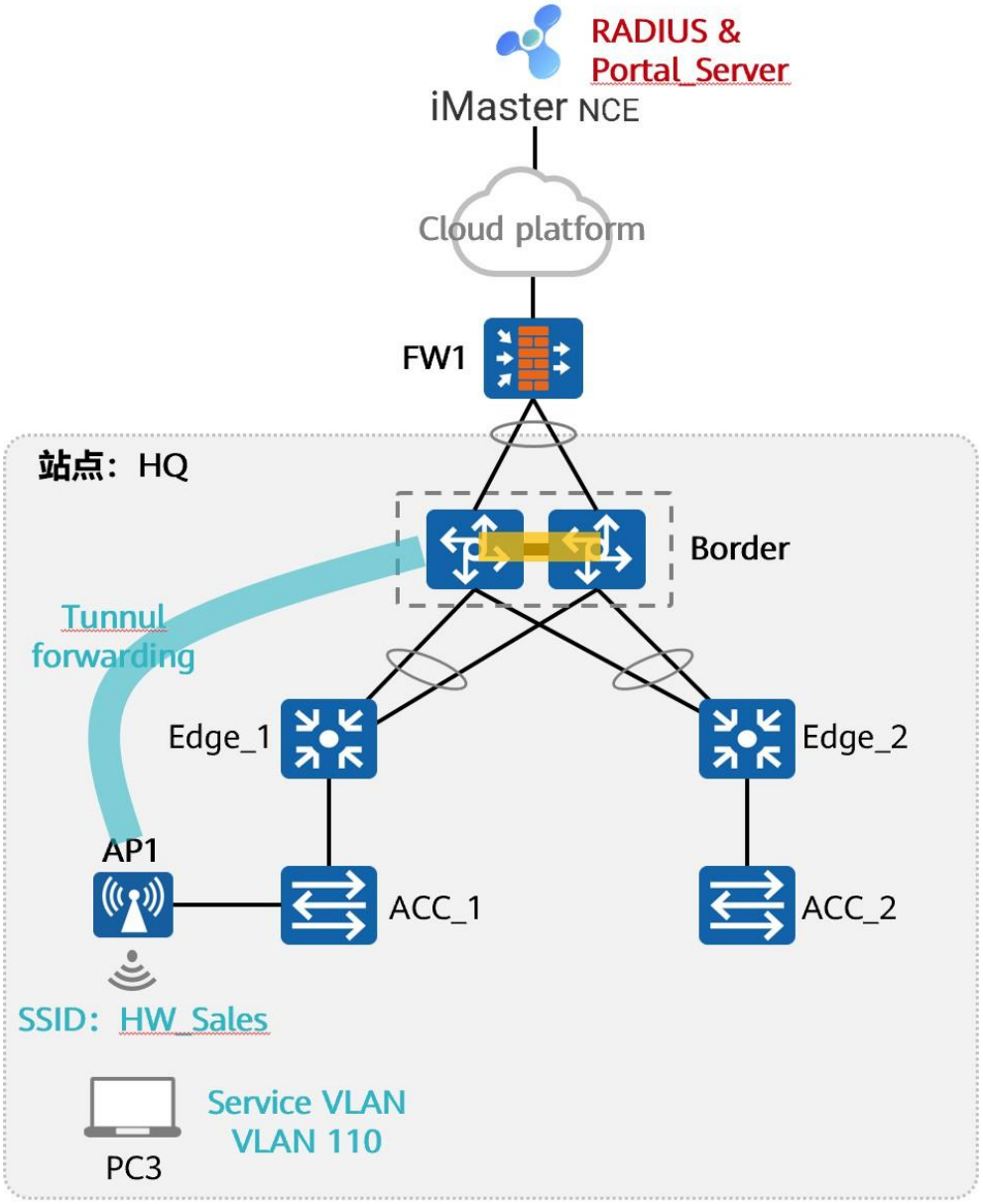
Tableau 10Wired and Wireless Service Address Planning

Equipment	Eth-Trunk Interface Number	Member interface	Parameter Description
Border	Eth-Trunk 11	MultiGE0/0/11 MultiGE1/0/14	Administrative status: enabled Eth-Trunk auto-negotiation: enabled Working mode: manual mode Link type: Trunk Default VLAN: 1 Allowed VLANs: 1, 3, 4, 100, 110
	Eth-Trunk 12	MultiGE0/0/12 MultiGE1/0/15	
Edge_1	Eth-Trunk 0	MultiGE0/0/11 MultiGE1/0/14	Link type: Trunk Default VLAN: 1 Allowed VLANs: 1, 3, 4, 100, 110
		MultiGE0/0/5	
Edge_2	Eth-Trunk 0	MultiGE0/0/12 MultiGE1/0/15	Link type: Trunk Default VLAN: 1 Allowed VLANs: 1, 3, 4, 100, 110
		MultiGE0/0/5	
ACC_1		MultiGE0/0/5	Link type: Trunk Default VLAN: 1 Allowed VLANs: 1, 3, 4, 100, 110
		MultiGE0/0/2	Link type: Access VLAN ID：100
ACC_2		MultiGE0/0/5	Link type: Trunk Default VLAN: 1 Allowed VLANs: 1, 3, 4, 100, 110
		MultiGE0/0/2	Link type: Access VLAN ID：100

Tableau 11planning for core and access switches

4.8 Configuring the WLAN Service

4.8.1 Networking Overview



4.8.2 Network planning

Parameter	Value
Wireless service address	Device: Border Subnet name: wireless_Net Management VLAN ID in wired auto-negotiation mode: VLAN 110 IP address obtaining mode: manual

	IP address/mask: 172.27.11.254/24 DHCP: enabled DHCP mode: server Management network: Off

Table 21 Wireless Service Address Planning

Equipment	Eth-Trunk Interface Number	Member interface	Parameter Description
Border	Eth-Trunk 11	MultiGE0/0/11 MultiGE1/0/14	Administrative status: enabled Eth-Trunk auto-negotiation: enabled Working mode: manual mode Link type: Trunk Default VLAN: 1 Allowed VLANs: 1, 3, 4, 100, 110
	Eth-Trunk 12	MultiGE0/0/12 MultiGE1/0/15	
Edge_1	Eth-Trunk 0	MultiGE0/0/11 MultiGE1/0/14	Link type: Trunk Default VLAN: 1 Allowed VLANs: 1, 3, 4, 100, 110
		MultiGE0/0/5	
Edge_2	Eth-Trunk 0	MultiGE0/0/12 MultiGE1/0/15	Link type: Trunk Default VLAN: 1 Allowed VLANs: 1, 3, 4, 100, 110
		MultiGE0/0/5	
ACC_1		MultiGE0/0/5	Link type: Trunk Default VLAN: 1 Allowed VLANs: 1, 3, 4, 100, 110
		MultiGE0/0/1	Link type: Trunk Default VLAN: 4 Allowed VLANs: 1

Table22 Interface planning for core and access switches

Parameter	Value
Service name: HW_Sales08	
Service VLAN	110

SSID Profile	Name: YG SSID name: HW_Sales08
Security Profile	Name: default Security policy: Open (portal authentication will be used later)
VAP profile	Name: YG Service VLAN: VLAN 110 Forwarding mode: tunnel forwarding Referenced profile: SSID profile YG, authentication profile configured on the NCE-Campus
AP group	Name: default Referenced profile: VAP profile "YG"

Table23 AC-side wireless service planning

4.8.2.1 Configuration roadmap

- Configuring a Wireless Service Subnet
- Configuring Interface Attributes
- Configuring the SSID Profile, Security Profile, and VAP Profile for Wireless Services

Result Verification

The WLAN service configuration is automatically delivered to AP1. After the configuration is complete, run the display vap ssid HW_Sales08 command on the border plane to view the following information. If Status is ON, a VAP has been created on the radio corresponding to AP1. [Border]dis vap ssid HW_Sales08

Info: This operation may take a few seconds,

please wait. WID : WLAN ID

AP ID	AP name	RfID	WID	BSSID	Status	Auth type	STA	SSID
0	AP	0	1	C4E2-87DB-65F0	Open	0		HW_Sales08
				ON				
0	AP	1	1	C4E2-87DB-6600	Open	0		HW_Sales08
				ON				

Total: 2

4.9 Admission certification

4.9.1 Wired Access 802.1X Authentication

Network planning

Parameter	Value
Wired_employee_group user group	
User name	wired_employee_01
Password	Huawei@123
Change the password at the next login.	Shuts off
Allowed Login Mode	802.1X & Portal 2.0

Table24 User Account Planning

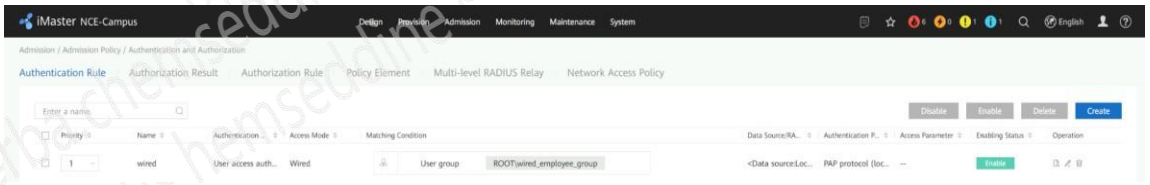
4.9.1.1 Configuration roadmap

- Creating a built-in RADIUS server
- User Access Authentication Configuration (Wired Access Control Point Side)
- User Access Authentication Configuration (On the Authentication Server Side

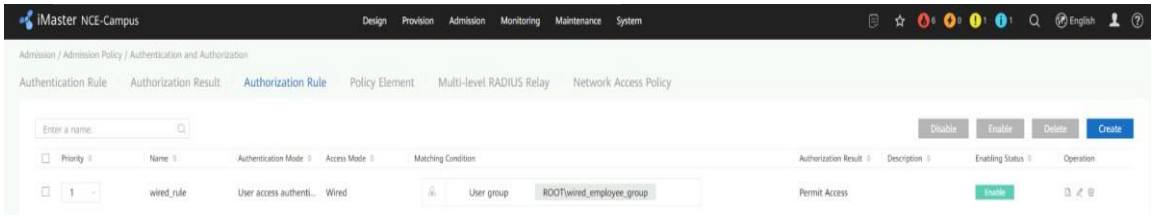
On iMaster NCE-Campus, check the completed authentication rules and authorization rules, as shown in the following figure. If the configuration is successful, the configuration is successful.

Note: The output information in the following figure is only an example. Parameters such as the name and information are subject to the actual data plan.

Authentication rule



authorization rule



Portal authentication for wireless access

Network planning

Parameter	Value
wireless_employee_group user group	
User name	wireless_employee_01
Password	Huawei@123
Change the password at the next login.	Shuts off
Allowed Login Mode	Portal, 802.1X & Portal 2.0

Table25 User Account Planning

5.2.2 Configuration roadmap

- Creating a built-in Portal server
- User Access Authentication Configuration (On the Authentication Server Side)
- User Access Authentication Configuration

5.2.3 Configuration Procedure

Creating a built-in Portal server

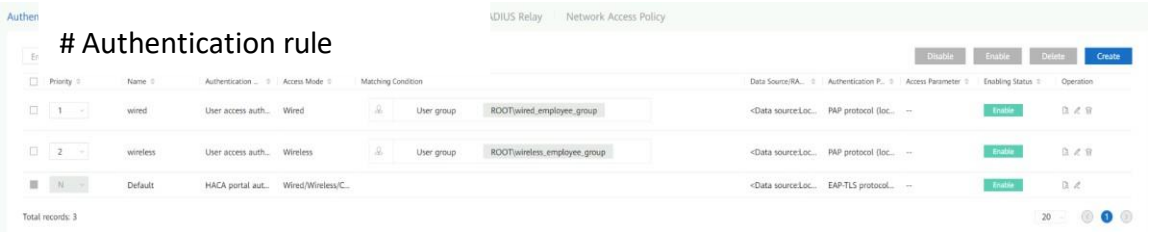
Create a built-in Portal server.

On the home page of the iMaster NCE-Campus controller, choose Design > Network Design > Template Management. On Portal Server tab. Set the key to Huawei@123.

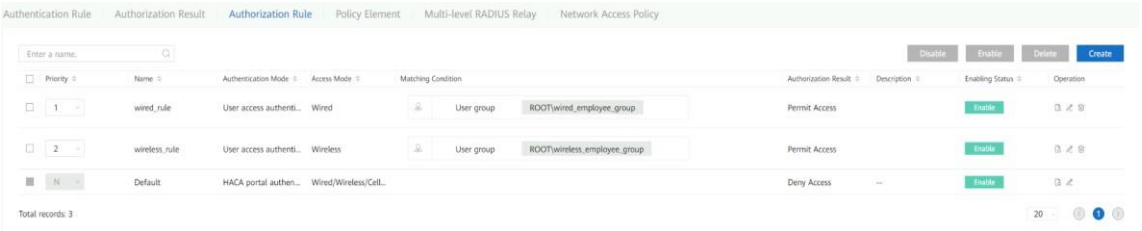
Result Verification

On iMaster NCE-Campus, check the authentication rules and authorization rules. If the following figure shows the authentication rules and authorization rules, the configuration is successful.

Authentication rule



Authorization rule



The WLAN service configuration is automatically delivered to the AP. After the configuration is complete, run the display vap ssid HW_Sales08 command on the Border to view the following information. If Auth type is Open+Portal/MAC, Indicates that the VAP on the radio corresponding to the AP has successfully invoked the Portal authentication profile.

[Border]dis vap ssid HW_Sales08

Info: This operation may take a few seconds, please wait.

WID : WLAN ID

AP ID	AP name	RfID	WID		Status	Auth type	STA	
0	AP	0	1	C4E2-87DB-65F0	ON	Open+Portal/MAC	0	HW_Sales08
0	AP	1	1	C4E2-87DB-6600	ON	Open+Portal/MAC	0	HW_Sales08

Total: 2

4.10 Verification of comprehensive experimental results

4.10.1 Admission authentication verification

Network planning

Parameter	Value
Corresponding test terminal	PC1 PC2
User Account	wired_employee_01/Huawei@123
Service VLAN	100
IPv4 subnet	172.27.10.0/24
IPv4 gateway address	172.27.10.254
Authentication mode	802.1X authentication

Table26 Wired User

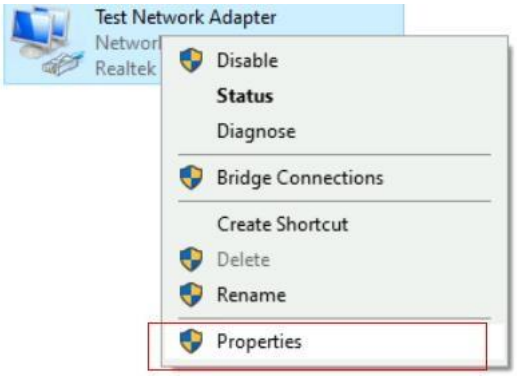
Parameter	Value
Corresponding test terminal	PC3
Name	wireless_employee_01/Huawei@123
Service VLAN	110
IPv4 subnet	172.27.11.0/24
IPv4 gateway address	172.27.11.254
Authentication mode	Portal authentication

Table27 Wireless User

802.1X authentication

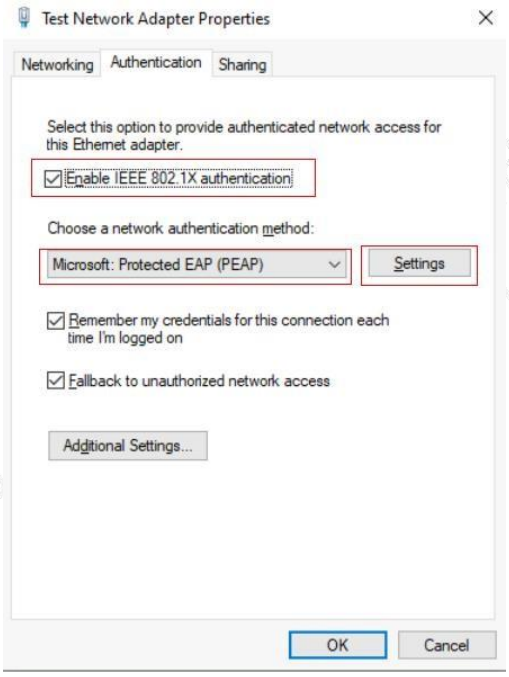
We use PC2 to perform authentication. Then we check the obtained IP address and the authorization result of the switch.

Take PC2 as an example. Control Panel > Network and Internet > Network and Sharing Center > View Network Status and Tasks > Change Adapter Settings.

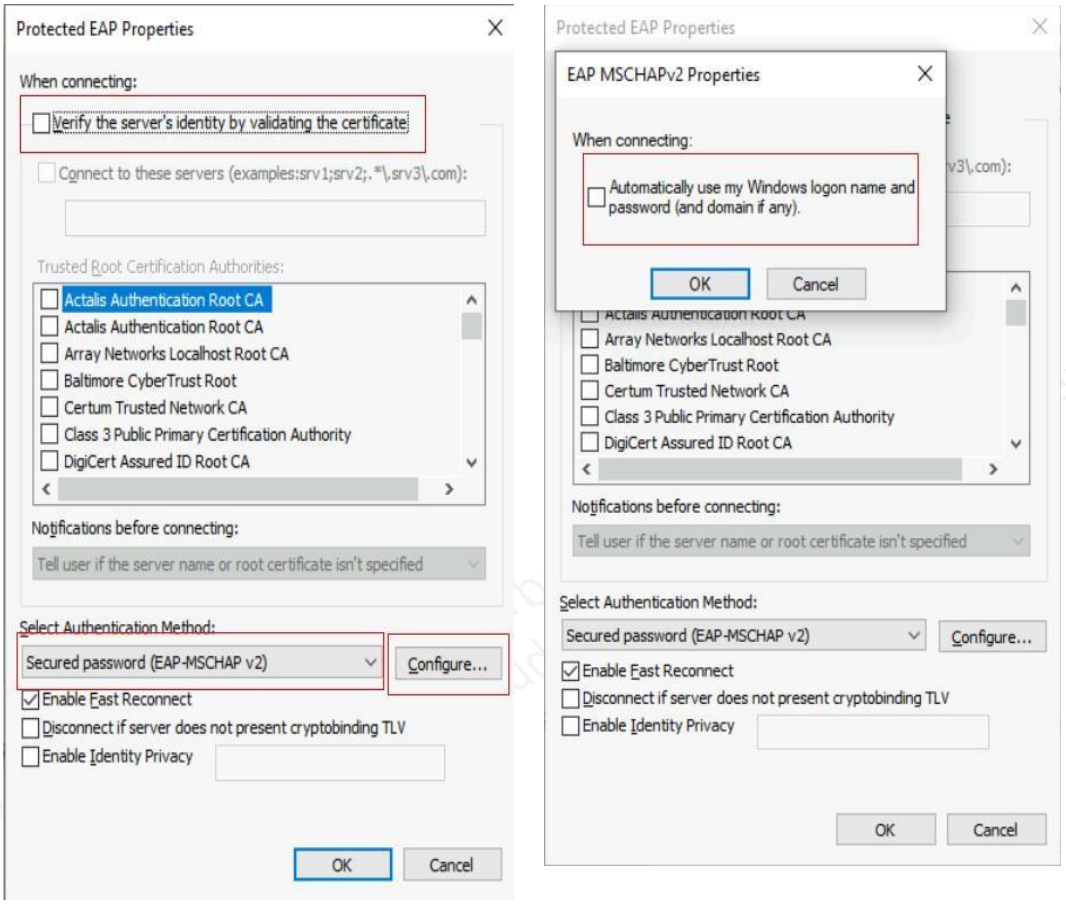


(Optional) Initializing 802.1X Authentication on Terminals

In the Authentication tab, we select Enable IEEE 802.1X authentication, set Network authentication method to Microsoft: Protected EAP (PEAP) > Settings.

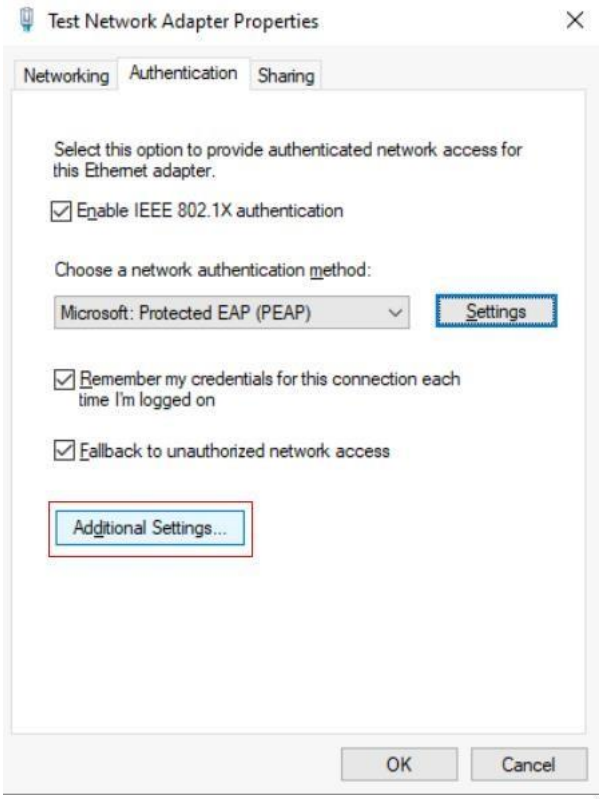


Deselect Verify server identity by verifying certificate, set Authentication method to Secure password (EAP-MSCHAP v2), and click Configure. In the dialog box that is displayed, Deselect Automatically use Windows login name and password.

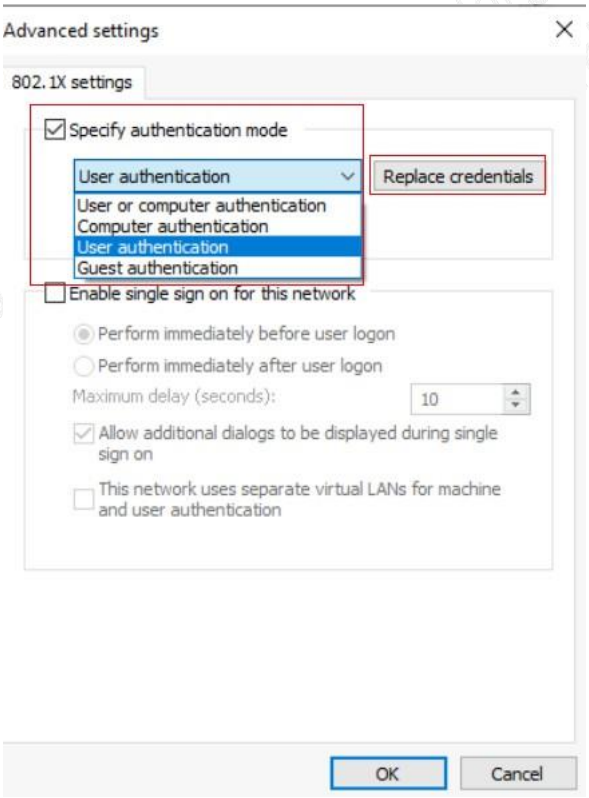


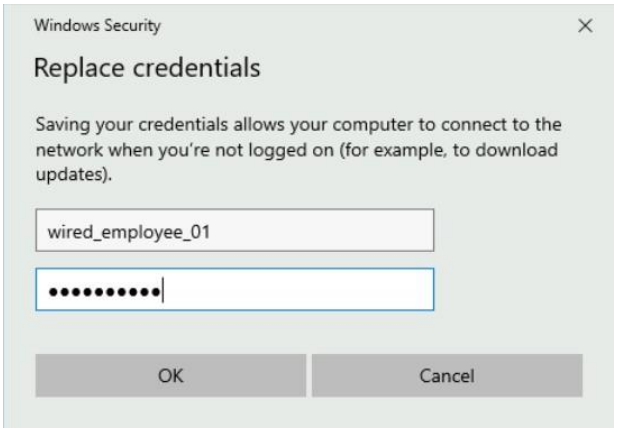
- **Identity authentication**

  # PC2 is authenticated.



In the pop-up window, select User Authentication and click Alternate Credentials (the first click will display as Save Credentials).





Check the information obtained by PC2.

Check the information obtained by PC2. The obtained IP address is 172.27.10.0/24 and the gateway address is 172.27.10.254, which matches the Wired service network segment.

```
C:\Users\phiclc2019002>ipconfig
Ethernet adapter Test Network Adapter:

Connection-specific DNS Suffix. :
IPv4 Address.....: 172.27.10.62
Subnet Mask.....: 255.255.255.0
Default Gateway.....: 172.27.10.254
```

Check the online users on ACC_2.

View online users on ACC_2, which is the authentication control point.

```
<ACC-2>dis access-user
------------------------------------------------------------------------------
UserID Username IP address MAC Status
------------------------------------------------------------------------------
5 admin - - Success
16402 wired_employee_01 172.27.10.62 bc5f-f4f9-df70 Success
------------------------------------------------------------------------------
Total: 2, printed: 2
```

Display detailed information about wired_employee_01.

```
<ACC-2>display access-user username wired_employee_01 detail

Basic:
User ID: 16402
User name: wired_employee_01
  Domain-name                  : aaa4f4a837d25fd5a90aa13
  User MAC                     : bc5f-f4f9-df70
  User IP address              : 172.27.10.62
  User vpn-instance            : -
  User IPv6 address            : -
```

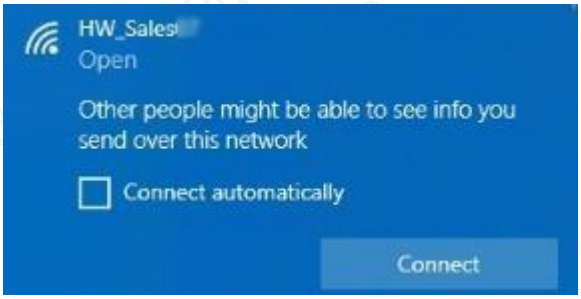
```
  User access Interface          : MultiGE0/0/2
  User vlan event                : Success
  QinQVlan/UserVlan              : 0/100
  User vlan source               : user request
  User access time               : 2023/06/12 17:15:36
  User accounting session ID     :                                ACC-
  20001200000010016****0100012 User access type                   :
  802.1x
  Terminal Device Type           : Data Terminal
  User inbound data flow(Packet) : 5,273
  User inbound data flow(Byte)   : 452,083
  User outbound data flow(Packet) : 12
  User outbound data flow(Byte)  : 1,204
  Service Scheme Priority         0

AAA:
  User authentication type       : 802.1x authentication
Current authentication method: RADIUS
Current authorization method: - Current
accounting method: RADIUS

------------------------------------------------------
```

Portal authentication

Use PC3 to perform Portal authentication and check whether the Portal authentication succeeds and whether the PC3 can obtain authorization information.

Connect PC3 to the SSID HW_Sales08.

Expand the Wi-Fi list on PC3, find the previously defined SSID HW_Sales, and connect to the SSID.



View the obtained IP address.

```
C:\Users\phiclc2019002>ipconfig
Wireless LAN adapter Wi-Fi:

Connection-specific DNS Suffix. :
IPv4 Address .....: 172.27.11.165
Subnet Mask. .....: 255.255.255.0
```

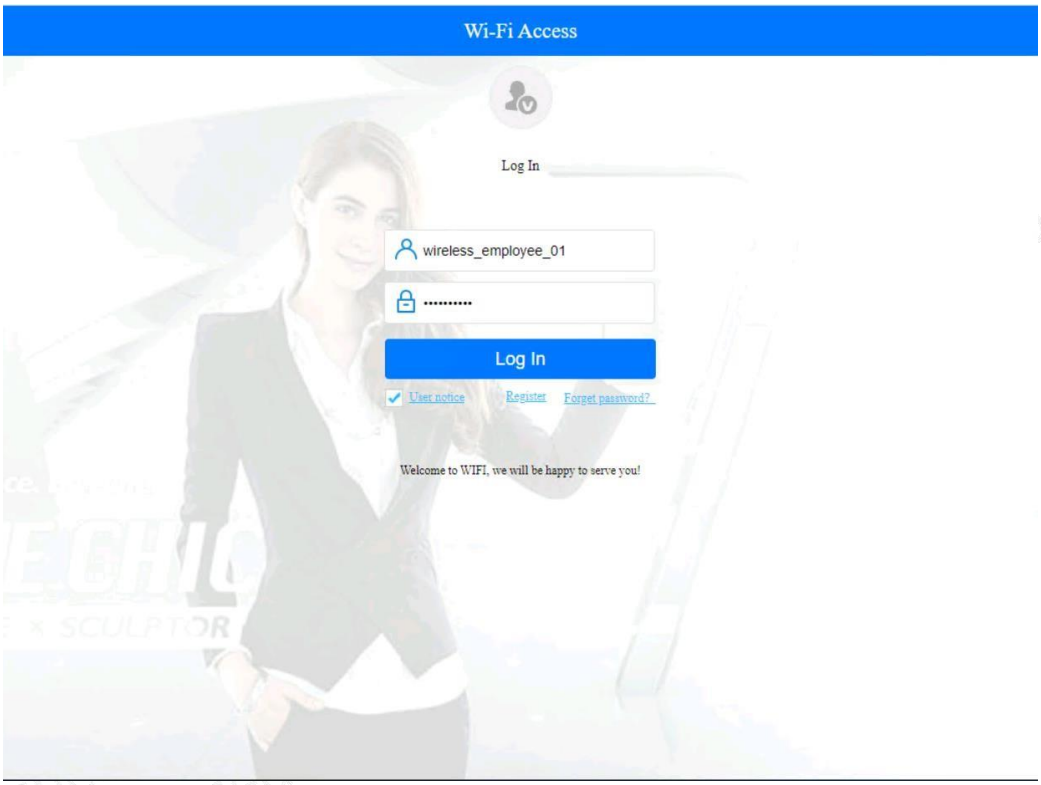
Default Gateway. .....: 172.27.11.254

The obtained IP address is on the 172.27.11.0/24 network segment, and the gateway address is on the 172.27.11.254 network segment, which complies with the Wireless_Net service network segment.

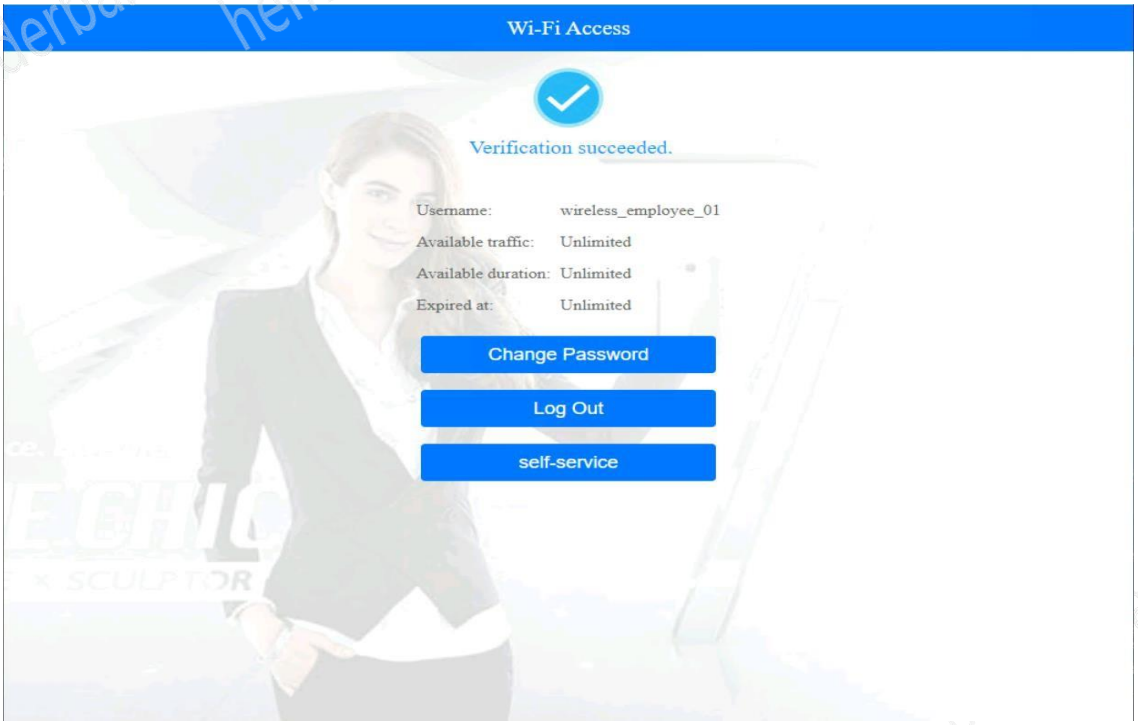
- **Identity authentication**

A user can open a browser and access any IP address, such as 1.1.1.1. (In this lab, DNS is not deployed, so you can enter only IP addresses.) The user fails to be authenticated. Therefore, the authentication point (Border switch) redirects the user to the Portal authentication page.

Enter the account wireless_employee_01 and Huawei@123, we select Notice to Users, and click Log In.



If the login succeeds, Portal authentication succeeds.



- **Query online users on the Border.**

View online users on the core when the core functions as the native AC and is the authentication point for wireless users.

<Border>display access-user username wireless_employee_01 detail

Basic:
User ID: 16409
User name: wireless_employee_01
Domain-name: aaa403fbd72717838894469
User MAC: 502b-7318-2886
User IP address: 172.27.11.165
User vpn-instance: -
User IPv6 address: -
User access Interface: Wlan-Dbss2277
User vlan event: Success
QinQVlan/UserVlan: 0/110
User vlan source: user request
User access time: 2023/06/12 19:48:06
User accounting session ID: Border09211000000110cc****0100019
User access type: WEB
AP name: AP
Radio ID: 0
AP MAC: c4e2-87db-65f0
SSID: HW_Sales08
Online time: 84(s)
Web-server IP address: 10.175.205.137
User inbound data flow(Packet): 197 User inbound data flow(Byte): 30,699 User outbound data flow(Packet): 257 User outbound data flow(Byte): 284,399
Service Scheme Priority: 0

AAA:
User authentication type: WEB authentication
Current authentication method: RADIUS
Current authorization method: -
Current accounting method :RADIUS

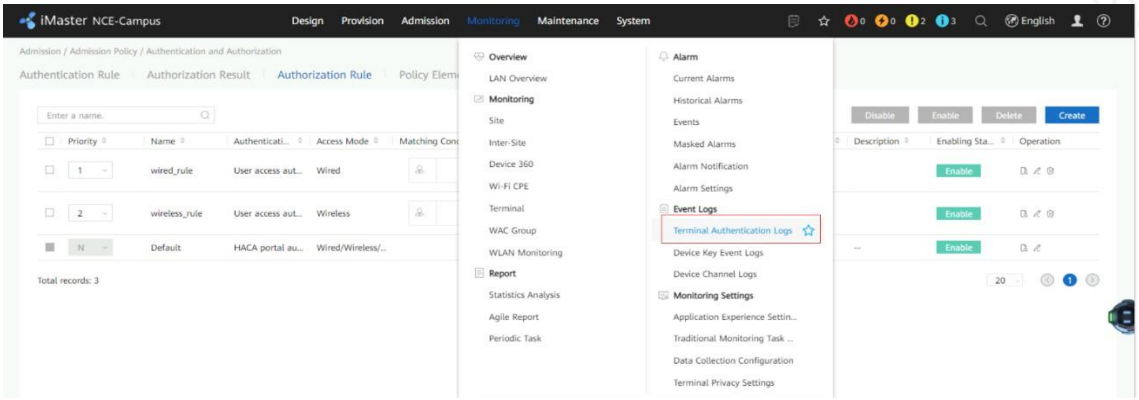
Total: 1, Printed: 1

.

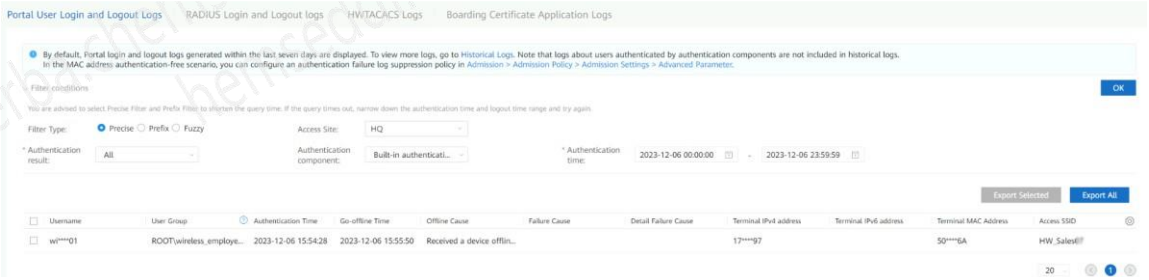
Viewing Authentication Logs

On the iMaster NCE-Campus, view Portal logs and RADIUS logs.

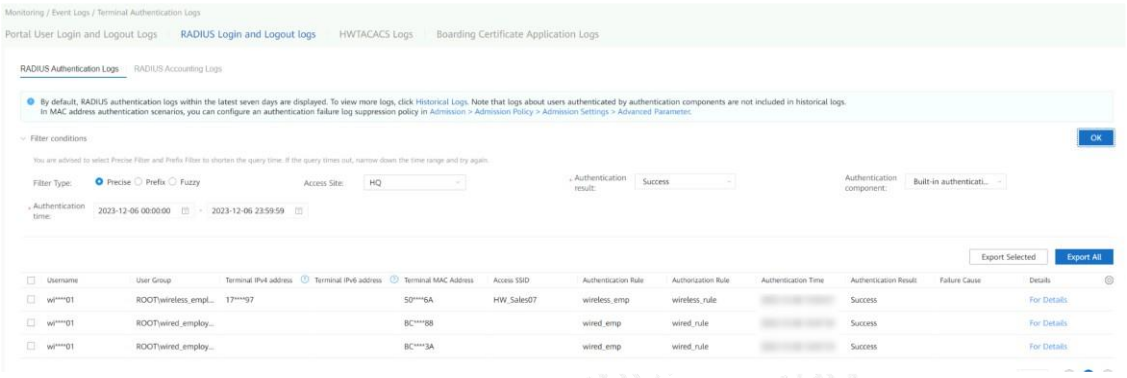
On iMaster NCE-Campus, we choose Monitor > Event Logs > Terminal Authentication Logs. The terminal authentication log page is displayed.



Click Portal online and offline logs to view the online and offline logs of all portals.



Click RADIUS online and offline logs to view all RADIUS online and offline logs



Verifying the Network Connectivity

Verify the network connectivity.

Use PC2 to perform 802.1X authentication. Log in to PC2 as wired_employee_01. Connect PC3 to the SSID HW_Sales08, and log in to PC3 with the account wireless_employee_01.

Note: Unless otherwise specified, the output information in this experiment is for reference only. The actual service IP address obtained by the device prevails.

Wired and wireless users access each other

PC2 ping PC3

The service IP address of the PC is automatically obtained through DHCP. The output information in this module is only an example. The service IP address obtained by the device depends on the actual environment.

C:\Users\phiclc2019002>ping 172.27.11.165

Pinging 172.27.11.165 with 32 bytes of data:
Reply from 172.27.11.165: bytes=32 time=5ms TTL=127 Reply from 172.27.11.165: bytes=32 time=4ms TTL=127 Reply from 172.27.11.165: bytes=32 time=3ms TTL=127 Reply from 172.27.11.165: bytes=32 time=4ms TTL=127

Ping statistics for 172.27.11.165:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 3ms, Maximum = 5ms, Average = 4 ms

Access the southbound login address of the NCE-Campus as a wired user (simulated access to the public network)

PC2 ping 10.175.205.136

C:\Users\phiclc2019002>ping 10.175.205.136

Pinging 10.175.205.136 with 32 bytes of data:
Reply from 10.175.205.136: bytes=32 time<1ms TTL=253 Reply from 10.175.205.136: bytes=32 time<1ms TTL=253 Reply from 10.175.205.136: bytes=32 time<1ms TTL=253 Reply from 10.175.205.136: bytes=32 time<1ms TTL=253

Ping statistics for 10.175.205.136:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0 ms

Access the southbound login address of the NCE-Campus as a wireless user (simulated access to the public network)

PC3 ping 10.175.205.136

C:\Users\phiclc2019002>ping 10.175.205.136

Pinging 10.175.205.136 with 32 bytes of data:
Reply from 10.175.205.136: bytes=32 time=3ms TTL=253 Reply from 10.175.205.136: bytes=32 time=3ms TTL=253 Reply from 10.175.205.136: bytes=32 time=3ms TTL=253 Reply from 10.175.205.136: bytes=32 time=6ms TTL=253

```
Ping statistics for 10.175.205.136:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 3ms, Maximum = 6ms, Average = 3ms
```

General Conclusion :

In conclusion, this project has thoroughly examined the transformative impact of Software-Defined Networking (SDN) on modern network infrastructures. By decoupling the control and data planes, SDN introduces a level of flexibility and centralized control that significantly enhances network management and optimization capabilities. The exploration covered the fundamental technologies and protocols that form the backbone of SDN, such as OpenFlow, NETCONF, and OVSDB, highlighting their roles in enabling dynamic and programmable network configurations.

The implementation and analysis of Huawei's iMaster NCE further exemplified the practical advantages of SDN. The iMaster NCE integrates management, control, analysis, and AI, thereby streamlining network operations from deployment to ongoing maintenance and optimization. The platform's capabilities in automating service configuration, performing intelligent analysis, and ensuring robust network performance underscore the benefits of adopting SDN in enterprise environments.

The practical simulation of a branch network within this project demonstrated the tangible benefits of SDN, including significantly faster deployment times, improved operational efficiency, and enhanced service quality. The ability to manage the entire lifecycle of the network—from planning and construction to maintenance and optimization—through a single integrated platform underscores the revolutionary potential of SDN.

Overall, SDN represents a pivotal shift towards more dynamic, responsive, and intelligent network architectures. It offers a scalable solution to the growing complexities of modern networks, ensuring that they can meet the demands of increasingly data-driven and interconnected environments. This project not only highlights the theoretical underpinnings of SDN but also provides a clear roadmap for its practical implementation, showcasing its potential to drive future innovations in networking technology.

Bibliographiy

5 Bibliographie

[1] G. Yangyang, «info.support.huawei,» 30 09 2021. [En ligne]. Available: https://info.support.huawei.com/info-finder/encyclopedia/en/OpenFlow.html.

[2] j. satyabrata, «geeksforgeeks,» 11 05 2023. [En ligne]. Available: https://www.geeksforgeeks.org/difference-between-software-defined-network-and-traditional-network/. [Accès le 09 05 2024].

[3] «TutorialsWeb,» [En ligne]. Available: https://www.tutorialsweb.com/SDN/open-flow-protocol-1.htm.

[4] «StudyX,» [En ligne]. Available: https://studyx.ai/homework/100267038-onsider-again-the-sdn-openflow-network-in-the-attached-figure-suppose-we-want-switch-s2.

[5] Funstuff, «HUAWEI,» 18 08 2023. [En ligne]. Available: https://forum.huawei.com/enterprise/en/Software-Defined-Networking-SDN/thread/692676040658403328-667213856029683712.

[6] 667213003285733380, «HAUWEI,» 20 07 2021. [En ligne]. Available: https://forum.huawei.com/enterprise/en/network-management-sdn/thread/667246680887672832-667213856029683712.

[7] Leslie, «QSFPTEK,» 13 12 2023. [En ligne]. Available: https://www.qsfptek.com/qt-news/what-is-vxlan-and-why-do-we-need-it.html.

[8] M. Badareen, «Linkedin,» 30 12 2023. [En ligne]. Available: https://www.linkedin.com/pulse/understanding-snmp-telemetry-network-management-mohammad-albadarin-0guif/.

[9] K. M. Sivalingam, «ReasearchGate,» 04 2021. [En ligne]. Available: https://www.researchgate.net/publication/352016764_Applications_of_Artificial_Intelligence_Machine_Learning_and_related_techniques_for_Computer_Networking_Systems.