Network Innovation and Development Alliance

World WLAN Application Alliance

IEEE United Arab Emirates Section

High-Quality 10Gbps AI Campus Technical and Standard White Paper

Preface

Rapid developments in the digital economy, combined with breakthroughs in digital technology innovation and significant advancements in artificial intelligence (AI), have enabled the implementation of comprehensive AI-powered campus networks that seamlessly connect everything in the digital and physical environments while providing users with more personalized and warmer proactive services.

With the surge of Internet of Things (IoT) devices, popularization of HD video streams, and widespread use of immersive collaboration (AR/VR), data on campus networks is growing exponentially. Large model applications are penetrating deeply into industry scenarios, with both inference and training rapidly shifting toward the edge, closer to data sources and business operations. Campuses and enterprises are accelerating carbon reduction and efficiency improvement, upgrading campus infrastructure to build zero-carbon campuses, and helping achieve the carbon peak and carbon neutrality goals. All of the above poses higher requirements on campus network infrastructure.

Building a high-quality 10 Gbps AI campus network extends beyond mere bandwidth enhancement; it reshapes the infrastructure paradigm for the intelligent era, and serves as a pivotal foundation for fostering new quality productive forces. In 2024, the industry published the High-Quality 10 Gbps Campus Network Technology Development Research Report, which proposed the concept and key technologies for building high-quality 10 Gbps campus networks, and reached broad industry consensus. Based on this, the Network Innovation and Development Alliance (NIDA), World WLAN Application Alliance (WAA), IEEE UAE Section, Internet Association of Kazakhstan, and other organizations jointly compiled the High-Quality 10 Gbps AI Campus Technical and Standard White Paper in 2026, which defines the application architecture, technical architecture, and physical architecture of high-quality 10 Gbps AI campus networks. The white paper specifies six fundamental capabilities of high-quality 10 Gbps AI campus networks: "autonomous network", "broadband access 10 Gbps", "connect everything", "deterministic experience", "energy-saving", and "full-scope security". It further illustrates the networking architecture and applications of high-quality 10 Gbps AI campus networks in industries such as education, government, finance, and healthcare. The white paper serves as a reference for organizations engaged in campus digital transformation and network infrastructure construction, including related agencies, construction and operations enterprises, and research institutions, aiming to offer insights into the digital transformation of enterprises.

The completion of this white paper has been made possible by the support of many parties, to whom we extend our sincere appreciation for their contributions.

Contents

01

Trends and Challenges in Campus Services

As the basic unit of a city, a campus is the main place where people live and carry out production activities, an important carrier to boost digital economy development, and a key point to realize green and low-carbon transformation. Emerging technologies, such as 5.5G, artificial intelligence (AI), and digital twins, are rapidly advancing, driving campuses to evolve towards full intelligence and creating new scenarios and applications. In recent years, extensive exploration and practice have been carried out for developing intelligent campuses, which has entered a critical phase.

Campuses cover most work and production scenarios. More than 80% of the gross domestic product (GDP) and more than 90% of innovation are generated in campuses. Campus networks are an important carrier and necessary tool for campus services. The development trends of campus services can be used to infer the evolution trends of campus networks. Campus service development exhibits the following trends.

1.1 Wireless

There are two main types of wireless terminals connected to campus networks. One type includes smart terminals such as personal computers and smartphones; the other includes Internet of Things (IoT) terminals such as smart locks and electronic shelf labels (ESLs), and is expected to encompass augmented reality (AR) devices, watches, and naked-eye 3D displays.

The number of smart terminals and IoT terminals connected to networks has increased by nearly 2.5 times in the past decade (2015 to 2025). According to statistics and forecasts from Gartner and ABI Research, the number of personal terminals has increased by three to five times in the past three years, with users now accessing campus networks via multiple terminals simultaneously instead of just one. Higher demands for concurrent connections necessitate the creation of high-performance, high-concurrency Wi-Fi networks in campuses.

The usage of IoT terminals in campuses has become commonplace. According to IoT Analytics, the number of connected devices worldwide has exceeded 17 billion. Besides the vast number of smart terminals such as smartphones, tablets, laptops, and landline phones, the number of IoT terminals has reached 7 billion. This data is widely acknowledged and reflects the rapid development of IoT technologies worldwide. About 80% of IoT terminals are connected to networks wirelessly, and their number is still growing annually by 17%.

Table 1-1 Key challenges posed by terminals to campus networks

Challenge Dimension	Data Support	Network Requirement
Terminal density	3–5 terminals per person (in 2025)	High concurrent access capability (for example, Wi-Fi 7/8 required)
Traffic pressure	Popularization of new terminals such as AR devices and naked-eye 3D displays	10 Gbps-level wireless bandwidth and low latency
Large number of IoT terminals	7 billion IoT terminals worldwide	Multi-protocol compatibility (Wi-Fi/BT/ZigBee/RFID)
Network management	80% IoT terminals depending on wireless connections; annual growth rate of 17% in wireless IoT terminals	Automatic O&M and intelligent terminal identification

1.2 Digital and Intelligent

Independent construction of campus infrastructure results in isolated systems and data, failing to meet the sustainable development needs of the campus digital economy industry. Future-proof campuses should deploy high-quality and moderately advanced new IoT sensing networks and network infrastructure, leveraging 10 Gbps connections to genuinely usher in an era of comprehensive sensing and intelligent connectivity of everything.

By 2030, the total number of connections worldwide will exceed 200 billion, and 10 Gbps connections will become the norm. The next-generation Net5.5G technology will help campuses achieve precise positioning, high-speed network coverage, and borderless information transmission. In addition, campuses will deploy ubiquitous IoT sensing devices to collect and monitor the running status data of the infrastructure, and will build campus digital twins based on massive data and AI foundation models. In this way, campuses will become highly intelligent with capabilities of comprehensive sensing, human-machine collaboration, and always-on connectivity, and support self-learning, self-diagnosis, self-decision-making, and self-execution. Innovative capabilities, such as unattended operations, automatic control, and adaptive learning are developed by integrating digital technologies into robots and other intelligent devices, fully boosting the campus construction and operations efficiency. Thus, campuses can automatically perceive user behavior and preferences and respond in real time to meet personalized user requirements.

In addition, technologies such as AI, big data, digital twins, knowledge graph, and deep learning are used to build autonomous network infrastructure for campuses: Network policies and their impacts are simulated in real time, and network parameters are continuously optimized through intelligent decision-making to ensure optimal services. For each fault, campus networks can quickly infer and locate the root cause, analyze the impacts, and recommend the optimal handling solution. Automatic O&M is implemented through human-machine collaboration to guarantee continuous service experience and O&M efficiency, laying a solid foundation for digital and intelligent development of campus networks.

1.3 Converged

Traditional campuses adopt a fragmented subsystem construction mode. As a result, their security protection, energy efficiency, and conferencing subsystems run independently of each other, causing data silos, difficult service collaboration, low management efficiency, and high system maintenance costs:

Resource fragmentation:

The separate network construction for office, production, security protection, IoT, and other systems leads to repetitive investments, redundant cabling, difficult maintenance, and a more than 40% increase in capital expenditure (CAPEX) and operating expenditure (OPEX).

Complex O&M:

Multiple networks running concurrently cause policy conflicts and difficult fault locating. The mean time to repair (MTTR) exceeds 4 hours.

Building infrastructure	Information-based application system	1	Public services
		2	Smartcard application
		3	Property management
		4	Information facility operation management
		5	Information security management
		6	Guest system
		7	Parking lot management
	Information facility system	8	Information access system
		9	Cabling system
		10	Indoor mobile communication signal coverage system
		11	Satellite communication system
		12	Subscriber telephone switching system
		13	Wireless intercom system
		14	Information network system
		15	Cable and satellite television reception system
		16	Public address system
		17	Conference system
		18	Information guidance and release system
		19	Clock system
	Building equipment management system	20	Building equipment monitoring system
		21	Building energy efficiency monitoring system
		22	Cooling and heating system
		23	Air conditioning and ventilation system
		24	Water supply and drainage system
		25	Lighting system
		26	Elevator and escalator system
		27	Power supply and distribution system
		28	Environment monitoring system
		29	Heating and ventilation system
	Public security system	30	Automatic fire alarm system
		31	Security management system
		32	Emergency response system
		33	Video security center
		34	Video surveillance system
		35	Access control system
		36	Intrusion alarm system
Municipal infrastructure		37	Lamp management system
		38	Manhole cover detection system
...			

Figure 1-1 Resource fragmentation

Network architecture upgrade integrates vertical service networks to implement "one network for multiple purposes and multiple capabilities", significantly improving network resource efficiency and seamless service interconnection capabilities. Driven by digital and intelligent transformation, campuses are evolving from static spaces to "organic life forms" with self-evolution capabilities. They leverage deep AI collaboration for sensing of data and network resources to implement automatic resource adjustment, service requirement prediction, and instantaneous response, providing ubiquitous intelligent connections for innovative services. A vast number of devices and sensors break information silos and build intelligent conference/building/campus ecosystems, which fundamentally rely on the infrastructure capabilities of real-time data collection, analysis, and transfer. During this process, the full lifecycle management of data as a core asset drives two convergence transformations:

Communication and sensing collaboration for network optimization:

Sensing data such as the personnel distribution heat map dynamically drives the adjustment of network slice bandwidth.

AI-powered network:

Sensing and network resources are automatically scheduled based on service priorities. This cuts the service rollout period from months to hours and lowers the OPEX by 30%.

ABI Research predicts that architecture upgrade and converged digital and intelligent transformation can not only achieve the core goal of reducing the OPEX by 30%, but also drive the enterprise WLAN market to reach a scale of USD 14.5 billion by 2028.

Table 1-2 Comparison of key metrics between the traditional architecture and the upgraded architecture

Metrics	Traditional Architecture	Upgraded Architecture	Improvement
Service rollout period	3–6 months	2–8 hours	98% ↑
Resource utilization	30%–40%	70%–85%	100% ↑
Fault rectification duration	4–12 hours	< 1 hour	85% ↑
O&M manpower input	High (professional team required)	Low (mainly automation)	60% ↑

1.4 Energy-Saving

In recent years, climate change has intensified, resulting in more extreme weather conditions that threaten global sustainability. As a result, managing climate change is now a top strategic goal for many countries. Ten years after the Paris Agreement, more than 160 countries have established targets for carbon neutrality.

Campuses generate over 60% of urban carbon emissions and play a critical role in achieving the goal of carbon peak/carbon neutrality. Under the guidance of this goal, green transformation is now central to campus strategies, shifting from individual energy-saving measures to systematic zero-carbon operations.

Zero-carbon/Near-zero-carbon campuses are important spatial carriers to implement the "carbon peak/carbon neutrality" strategy. In compliance with the policies for green, clean, and cyclic development, campuses are encouraged to explore zero-carbon transformation throughout the lifecycle, such as construction, O&M, and management. Through "bits manage watts", campuses must strike a balance between digital development and the goal of carbon peak/carbon neutrality: They must provide sufficient power for IoT and network devices that implement campus intelligence, while using digital technologies to promote clean energy structure, efficient energy management, and green production and living activities.

Zero-carbon transformation in the campus production field is a complex systematic project covering multiple dimensions. It requires the collaboration of the campus ecosystem to improve information infrastructure and management services, intelligent and high-quality development of industries, and intelligent integration of campuses and cities. Networks help campuses explore a green and low-carbon construction path that suits their own characteristics, so as to scientifically implement the goal of dynamic zero carbon.

1.5 Secure

The IoT trend and multi-network convergence (5G/Wi-Fi and cloud-edge synergy) have completely broken the traditional "castle-and-moat" security boundary model that implements physical isolation, resulting in exponential expansion of the attack surface and ubiquitous security threats. Network security has evolved from a support system to a core productivity element, and become equally important as the services it protects. Therefore, campus networks must build a full-chain, all-scenario security protection system covering terminal access, network transmission, and service data, to provide multi-dimensional in-depth defense in a converged network environment.

Table 1-3 Security service scenarios and typical risks

Service Scenario	Specific Scenario/Risk	Typical Risk	Key Feature/Challenge
Terminal access	IoT devices: • IoT devices deployed in public places are prone to unauthorized access and spoofing. • Firmware of cameras and sensors is not updated in a timely manner (high-risk vulnerabilities exist, CVSS ≥ 9.0). • Industrial systems such as PLC and SCADA use default or weak passwords. • The OTA upgrade mechanism of the in-vehicle system has vulnerabilities.	• Ransomware infection (causing device suspension and data encryption) • DDoS botnet (devices are controlled to launch attacks) • Key infrastructure suspension (industrial control devices are damaged) • Vehicle control hijacking (endangering personal safety)	• Massive heterogeneous devices: Numerous types and unclear ledgers make management difficult. • Long lifecycle/Difficult update: Firmware update is delayed or impossible, leaving numerous vulnerabilities unaddressed. • Physical exposure: Devices are often deployed in unattended or open environments and are prone to unauthorized access and spoofing. • Lack of security baselines: The default configurations are insecure, and no unified security standards are available.
	Smart terminals: • Remote office terminals (laptops and mobile phones) access an enterprise network through insecure public Wi-Fi. • BYOD devices access sensitive services without installing compliant security software or being managed by MDM.	• Ransomware spread (entering the intranet through infected terminals) • Sensitive data leakage (device missing or theft) • Pivot for lateral movement in internal networks	• BYOD management difficulty: Devices are owned by individuals, leading to weak security controls. • Complex access environment: Enterprise core resources are accessed through untrusted networks.
Network transmission	Blurred network boundaries: • 5G and Wi-Fi 6/7 are deeply integrated with wired networks. • Data is frequently exchanged between cloud data centers (DCs), edge nodes, and terminals (east-west traffic). • The microservice architecture greatly increases the complexity of internal network communication.	• Lateral movement attack (attacker moves freely inside the network) • APT stealthy propagation (using complex network topologies to hide traces) • Cross-domain ransomware infection (from the IT domain to the OT domain or different cloud environments) • Network sniffing and man-in-the-middle (MITM) attacks (listening to or tampering with data on transmission links)	• Physical isolation failure: 5G/Wi-Fi hybrid networking, cloud-edge synergy, and multi-cloud interconnection make the separation between internal and external networks disappear. • Surge in east-west traffic: Traditional border firewalls struggle to effectively monitor the high-volume, complex communication traffic between servers, applications, and microservices. • Traffic encryption: Deep inspection is harder due to the significant volume of encrypted traffic (such as TLS traffic).
Service data	Increased data mobility and exposure: • Sensitive data frequently flows between terminals, edge nodes, clouds, and different service systems. • Data is stored on hybrid clouds, edge nodes, and even terminals. • Microservice-based applications complicate data access permission management.	• Data theft through MITM attacks (sensitive information intercepted during transmission) • Phishing for credentials (for unauthorized access to data) • Internal data leakage (caused by malicious internal personnel or incorrect configurations) • Data encryption by ransomware (causing service interruption and data asset loss) • Not meeting data compliance requirements (such as GDPR and CCPA)	• Ubiquitous data: Data is distributed on terminals, edges, and clouds, and the data flow paths are complex. • Multi-environment storage: Data is stored in public clouds, private clouds, local DCs, edge devices, and other environments. • Complex permission management: Fine-grained permission control is difficult to implement across networks, environments, and applications. • Data lifecycle management: Data creation, storage, use, transmission, and destruction need to be protected.

According to Gartner, by 2026, 60% of enterprises will be forced to deploy the zero trust architecture due to service interruptions caused by security gaps. The security of converged networks is the cornerstone of service continuity. Embedding security capabilities into networks is the only way to build a future-proof campus featuring both intelligence and reliability in the digital wave.

02

Concept and Connotations of High-Quality 10 Gbps AI Campus

2.1 Architecture Definition for High-Quality 10 Gbps AI Campus

Based on the analysis of campus service characteristics, key network capabilities, and networking characteristics, the high-quality 10 Gbps AI campus architecture is defined from aspects of application architecture, technical architecture, and physical architecture, aiming to provide a better campus network solution.

2.1.1 Application Architecture

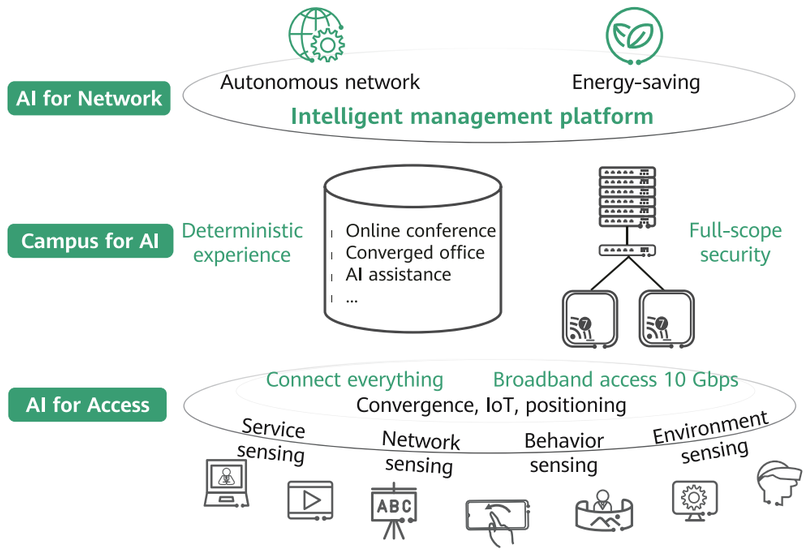


Figure 2-1 Logical architecture and key capabilities of a future-oriented AI campus

AI for Network: network management upgraded with the AI brain

New technologies such as large-scale models and natural language translation are introduced to help networks evolve towards L4 autonomous driving. On one hand, campus networks can provide more information for AI, such as information about terminals, services, traffic, locations, and environments, to help AI improve its overall capabilities. For instance, sensing information can be utilized to implement intelligent energy saving in buildings, including collaboration with the building management system to control air conditioners and lights. On the other hand, large-scale models help implement automatic check and maintenance, provide real-time visibility at the device, network, and application levels, support real-time user and application journey playback, and enable minute-level fault demarcation and locating. The network intelligent agent automatically analyzes the root cause of each fault based on the fault analysis model, achieving detection and auto-solving of 90% wireless faults.

Campus for AI: network experience upgraded for AI applications

As AI agents become widespread, how to use them securely and efficiently becomes a key challenge for networks. Based on intelligent AI application identification and assurance technologies, AI application sessions are guaranteed millisecond-level deterministic latency and 1E-9 packet loss rate. This meets the high-quality and high-standard network requirements of new AI terminals, agents, and services (such as embodied AI and AI operating systems). With AI-based traffic collection, identification, and analysis capabilities, networks can provide differentiated experience for AI applications of different users and services, and provide real-time service capabilities for AI. In addition, campus networks can provide comprehensive security assurance for AI terminals and agents through physical encryption of wireless and wired links.

AI for Access: terminal management capability upgrade using AI technologies

Terminals of various types are the main service recipients but are also a key source of threats. Therefore, achieving visibility, manageability, and security control at the network access layer is also a key challenge for campus networks. AI technologies can be used to identify terminal types and control terminal behaviors, and implement functions such as automatic configuration and protection policy. Moreover, spatial sensing extends security from connections to the physical environment.

2.1.2 Technical Architecture

There are six primary technical focuses for campus networks, determined by service scenarios and capabilities.

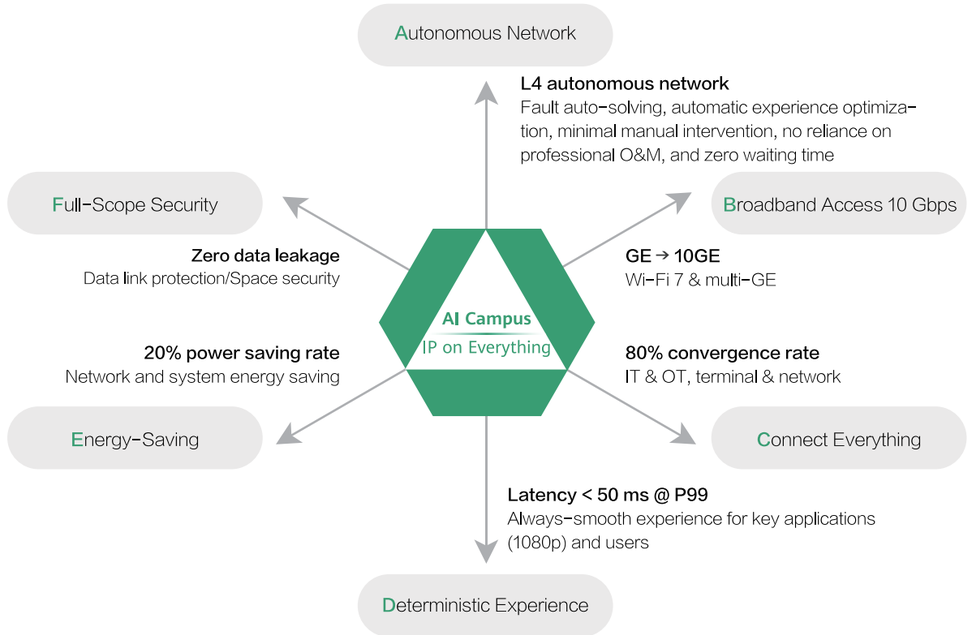


Figure 2-2 Key technologies of AI-driven campuses

Autonomous network: According to the YD/T 6764-2025 industry standard for the autonomous network architecture, networks are categorized into six levels from L0 to L5 based on their degree of automation. For each level, the standard defines clear, unambiguous generational characteristics of technological maturity and service application effectiveness indicators. The key technologies of L4 are generative AI and AI agents. Dialog-based O&M is supported through natural language interfaces. Intelligent task planning and execution enable the system to proactively optimize user experience and detect exceptions. Except for a few scenarios that must be manually handled, most O&M scenarios can be handled by the system automatically or with minor human assistance. That is, L4 supports dialog-based proactive O&M on the basis of L3's visualized O&M, further reducing manual operations during O&M. The benefits include 100% success of remote site-visit-free deployment, 100% auto-solving of faults that do not require site visits, automatic detection and solving of 80% wireless issues, and AI-based user experience scoring. This achieves one-stop management of networks, security, and users, one-map visibility of terminals, and quality visualization and locating.

Broadband access 10 Gbps: Wi-Fi 7 technology drives the upgrade of access bandwidth to 2.5GE–10GE, enables 10-meter high-performance Wi-Fi coverage, and brings 60%–80% capacity increase with converged scheduling, spatial reuse, and dynamic-zoom smart antennas. High-reliability continuous networking ensures zero packet loss. The bearer network is simplified from three layers to one layer, achieving "One Device, One Network".

Connect everything: Ubiquitous wireless connections ("WLAN + X") serve as the key technology basis for varied campus access requirements. Wi-Fi supports long-distance (> 15 m) integrated sensing and communication. Objects are precisely sensed through fine timing measurement (FTM), channel state information (CSI) sensing, and mmWave sensing, integrating sensing into security protection and energy saving solutions. From the distributed passive solution to the centralized solution, Wi-Fi IoT supports co-site deployment with a radius of 10 m to further simplify IoT convergence in industry scenarios such as asset management, healthcare, retail, and industrial production, helping next-generation production to meet flexible manufacturing and security requirements.

Deterministic experience: With the popularization of AI terminals, embodied AI, smart manufacturing, and other smart applications, campus networks are required to ensure deterministic network experience. This can be achieved through a series of functions: Intelligent application identification helps identify key applications such as audio, video, cloud desktop, and collaborative office based on traffic characteristics. Intelligent all-flow scheduling implements network-wide E2E slicing and device-network synergy to achieve a freeze rate of less than 1% for AI and XR services. Intelligent all-flow poor-QoE analysis provides insights into the experience by analyzing millions of flows, enabling application-level journey playback and network-wide visualization. Exclusive service assurance enables VIP users and terminals to access the network anytime and anywhere with a deterministic latency of less than 50 ms and guaranteed bandwidth. Other capabilities include proactive care for VIP users, real-time experience evaluation, and timely fault warning.

Energy-saving: Energy saving is now a common mission in the industry. For campuses, this means reducing both device power usage and overall campus energy consumption. AI-based tidal traffic prediction, new energy-saving protocol standards, and intelligent chip sleep modes can reduce 20% energy consumption of network devices. Wireless sensing technologies enable campus networks to sense the personnel presence status so as to control equipment such as air conditioners and lights, implementing "bits control watts" and reducing the campus overall energy consumption by 20%.

Full-scope security: In campus scenarios where personnel activities are dense, inadequate security infrastructure is a major vulnerability of the entire system. For example, ransomware can easily propagate through internal campus devices. Therefore, campuses must prioritize enhancing their network security system. An example is zero trust network access (ZTNA), or zero trust architecture (ZTA), which leverages AI to implement zero trust on user access and detects more than 95% of abnormal behaviors in real time. Wired and wireless link-layer encryption technologies ensure zero data leakage from end to end. Especially, anti-eavesdropping technology at the link layer of the wireless air interface can fundamentally solve wireless security risks. CSI sensing and other Wi-Fi spatial sensing and detection technologies implement detection of personnel intrusions and unauthorized devices (such as rogue cameras) within seconds. Terminal and NE side security is ensured through a systematic device security protection architecture and situational awareness capability.

2.1.3 Physical Architecture

As shown in the figure, a campus network consists of the terminal layer, access/aggregation/core layer, WAN layer, and management-control-analysis layer. The terminal layer consists of various smart terminals and IoT terminals. The access layer consists of wired and wireless network access devices. The aggregation/core layer consists of fixed or modular switches. The WAN layer consists of routers and firewalls. The management-control-analysis layer consists of the software-defined networking (SDN) controller and analyzer, and is the brain of network management.

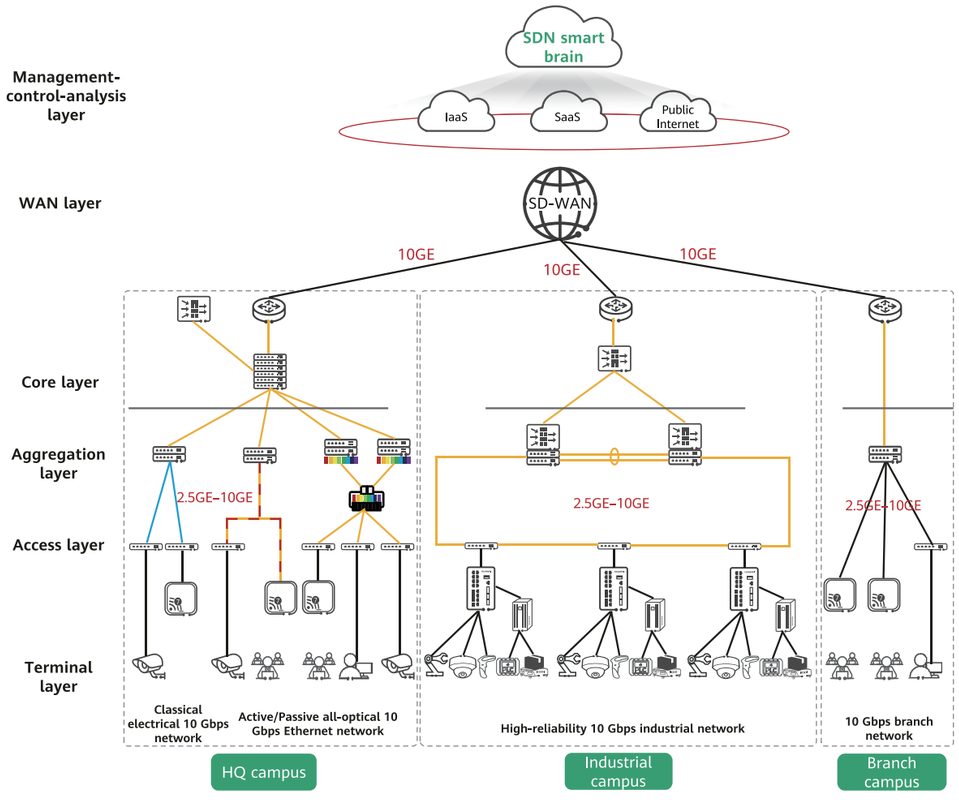


Figure 2-3 Physical architecture of a high-quality 10 Gbps AI campus network

Terminal layer: includes various access terminals for campus office and production, such as smart terminals and IoT terminals.

Access layer: includes network devices that connect terminals to the network and provides 2.5GE to 10GE access capabilities. The access layer provides access modes including Wi-Fi 7 wireless access and 2.5GE/10GE wired access.

Aggregation layer: includes network devices located between the access layer and core layer. Being highly active and providing rich features, the aggregation layer supports 10GE access and provides two mainstream solutions: Ethernet electrical solution and Ethernet optical solution.

Core layer: usually has core switches deployed to connect to firewalls, routers, and aggregation switches. The core layer features high performance, high density, and high scalability, and bears services of the entire campus network.

WAN layer: provides egress routing capabilities for the campus network. In the multi-branch campus scenario, it provides high-performance interconnection capabilities for branch campuses. The WAN layer also provides network security protection capabilities to ensure the security of campus network devices and services.

Management-control-analysis layer: functions as the brain in the campus SDN solution. This layer manages and controls campus network devices, and analyzes and ensures campus services, serving as the core of an intelligent campus.

2.2 Autonomous Network

2.2.1 Definition

According to the autonomous network architecture standard, an autonomous network is a network consisting of intelligent and automated network infrastructure, operations and management systems, and service systems. With the Intelligent World 2035 vision, enterprises are accelerating the intelligent upgrade of multi-agent collaborative decision-making and autonomous task execution. In the AI agent era, guided by the objectives of high availability, optimal experience, and simplified operations, enterprises are building the new ICT infrastructure from three aspects: intelligent-native capability and resilience of the underlying ICT infrastructure, AI agent autonomy capability of O&M systems, and self-adaptability and self-evolution of swarm intelligence.

2.2.2 Key Technologies

2.2.2.1 Digital Twin Network

Enterprise O&M digital twin technologies are classified into four types: multi-dimensional sensing, predictive analytics, simulation and deduction, and interconnection protocols. AI agents are used together with high-precision models to implement closed-loop decision-making and verification, for example, to perform the prediction-simulation-optimization process.

Multi-dimensional digital twin sensing

Multi-dimensional O&M views from networks to applications are provided, including the network view, application view, and user view. The network view focuses on multi-dimensional sensing and visualization of network resources, network performance, configuration forwarding, and network exceptions. The application view focuses on multi-dimensional sensing and visualization of the performance, load, and exceptions of application flows.

Predictive digital twin technology

The surge of AI terminals drives the requirements for failure prediction of IoT modules on wireless networks and optical modules on fixed networks. Optical module failures frequently interrupt training, which requires networks to predict such risks in advance. In terms of hard disks, HDD/SDD faults will cause data loss. This also requires predictive risk management and disk replacement window planning. The multi-source component failure data is integrated based on the Transformer architecture to build a professional prediction algorithm model, which can accurately predict the failure risks of optical modules and hard disks, ensuring service continuity and optimizing spare parts management.

Digital twin simulation technology

Digital twin simulation displays key indicators that are difficult to obtain and provides what-if analysis. For example, Wi-Fi 3D coverage simulation can be used to plan the coverage of directional antennas in high-density and warehouse campus scenarios, discover coverage holes in the routine O&M process, and verify and deliver radio calibration configurations; simulation also applies to Wi-Fi FTM location and CSI sensing of personnel presence and quantity, helping engineers determine the deployment locations of sensing APs to ensure the optimal sensing performance across the network.

Digital twin interconnection protocol

O&M systems of multiple vendors and domains coexist in enterprise campus O&M scenarios, necessitating a set of digital twin interconnection protocols to implement lightweight data interconnection and seamless operations and support unified networking cognition for agents and easy manual intervention. From the technical perspective, fully simplified networking, capability negotiation, and governance capabilities should be provided, and a unified pan-ICT infrastructure model should be defined.

2.2.2.2 AI Agent

The typical AI agent architecture consists of four core modules: **LLM engine, planning and execution system, tool service matrix, and knowledge-memory augmentation unit**. Take the fault AI agent as an example. The input is the fault symptom description. The planning and execution system identifies the intent of the input, divides the task into individual steps, plans, and executes each step by invoking the corresponding tool. Reflection and optimization are required when an error or interruption occurs. The key technologies are as follows:

Planning and reflection: Planning is the core mechanism of dynamic decision-making throughout the AI agent process. Currently, the mainstream solutions in the industry include SOP planning and free planning. For some known problems, the SOP mode can be used to preset the handling process. For some unknown scenarios, the free planning mode will be used in the future. The core of the reflection mechanism is to iteratively optimize policies through self-evaluation and environment feedback. For example, the Reflexion framework uses dynamic memory to store key decision nodes. When an execution exception is triggered, the reflection process is started to generate a correction policy.

Knowledge and memory: Enhanced prompts are generated by integrating external knowledge bases and context information, building the dual-memory system. Short-term memory stores interaction information (such as historical user instructions) in real time based on the model context window to keep conversations coherent and track task progress. Long-term memory uses vector databases to retain user profiles, behavior

patterns, and domain knowledge, implementing cross-session knowledge reuse (for example, the O&M Q&A copilot provides personalized services by invoking historical interaction records).

Foundation model: In terms of the architecture, both fast thinking and slow thinking models are necessary. When to use the slow thinking model and when to use the fast thinking model can be determined through intelligent routing, which can be implemented by training dedicated embedding models considering the query difficulty and task type.

2.2.2.3 Intelligent Collaboration

Challenges of intelligent collaboration include cross-agent objective decomposition and task orchestration, conflict resolution, and multi-agent interaction. The technical implementation is described as follows:

Objective decomposition and task orchestration: Decompose a cross-domain task into sub-objectives that can be understood within a single domain based on the LLM and process knowledge. The main technical challenges to be addressed include: differentiated understanding capabilities, which may cause inconsistent understanding of objectives; dependency between sub-objectives of multiple agents; strong autonomy of agents with their respective high-priority objectives/tasks, which makes it difficult to forcibly deliver/execute objectives.

Conflict resolution: The main scenarios include execution objective deviation, cross-domain diagnosis conflict, and collaboration obstacles caused by information inconsistency. Solution technologies include case-based reasoning (CBR) and multi-agent debate. In CBR, historical cases are searched and adapted to new scenarios. For example, the old solution is adjusted to resolve similar faults. In multi-agent debate, after each agent proposes a proposition from the domain perspective, the judge agent comprehensively evaluates the propositions and makes a decision. For example, a consensus is reached on the root cause of a network fault after a debate between the protocol-layer and device-layer agents.

Multi-agent communication protocol: The core challenges of multi-agent interaction include semantic gap (language/understanding deviation), LLM processing exceptions caused by long context, and token processing capability differences. A task-oriented protocol system needs to be developed, which defines E2E interaction process standards covering registration, coalition formation, negotiation, execution, and feedback, and standardizes transmission protocols, interfaces, and information models. The system implements efficient communication across agents (for example, resolving semantic conflicts between device agents and policy agents at the protocol level), ensuring high reliability and security of autonomous collaboration in the multi-agent system.

2.2.3 Key Metrics

An autonomous network aims to reduce the network complexity and skill demands, changing O&M and delivery by professional personnel to automated processes with little or no human involvement. This cannot be achieved overnight. Networks will gradually evolve from conditional autonomous to highly autonomous and full autonomous. The following table provides suggestions on key metrics.

Table 2-1 Key metrics

Category	Metric	Excellent: Highly Autonomous	Good: Conditional Autonomous
Planning and construction	Intelligent WLAN planning	CAD drawing and 3D simulation, supporting AI-based identification and drawing of obstacles and automatic AP deployment	Image (PDF, JPG, etc.) and 2D simulation; manual obstacle drawing and manual AP deployment
	LAN-WAN convergence	Simplified and automatic LAN & WAN deployment based on branch scenarios; one-click batch deployment of multiple branches	Separate automatic deployment of LANs and WANs; configuration and deployment on a per-site basis
	Automation efficiency	Single-site provisioning: minute-level	Single-site provisioning: hour-level/day-level
	Device plug-and-play	Zero Touch Provisioning (ZTP) and Secure Zero Touch Provisioning (SZTP)	ZTP
Maintenance and optimization	Digital twin: multi-layer map visualization for networks, users, terminals, and applications	Accurate sensing of the network status and actual experience of users, terminals, and applications, with multi-layer visibility	Multi-layer KPI visualization of networks, users, and applications
	Auto-solving of wireless network faults	Automatic detection of wireless faults and auto-solving of 80% wireless faults	Detection of faults but without auto-solving
	Automatic handling of user access and experience faults	Auto-solving of 85% user access and experience faults; minute-level fault demarcation and locating	Demarcation of faults but without auto-solving; hour-level or day-level fault locating
	Intelligent O&M based on AI foundation models	Foundation model-based natural language interaction, status inspection, and intelligent fault auto-solving by agents	Basic intelligent O&M and limited intelligent interaction, unable to automatically resolve faults

2.3 Broadband Access 10 Gbps

2.3.1 Definition

"Broadband access 10 Gbps" aims to achieve 10 Gbps user access and represents the evolution direction of next-generation campus access. With the high-bandwidth and high-concurrency access capabilities of wireless networks (Wi-Fi 7) and the high-performance bearing capabilities of wired networks, campus networks provide high-speed connections for users and meet the stringent requirements of new applications on network bandwidth, latency, and concurrency performance. Campus network connections are the bridges between the physical and digital worlds,

helping build a converged communications network infrastructure featuring wide coverage, high bandwidth, and high scalability. The key technologies are as follows:

- Wireless side: Wi-Fi 7, continuous networking, smart roaming, etc.
- Wired side: optical and electrical Ethernet technologies. All-optical Ethernet includes active Ethernet optical and passive Ethernet optical technologies.

2.3.1.1 10 Gbps Wireless

10 Gbps wireless refers to the high bandwidth, high concurrency, and seamless roaming capabilities provided by the Wi-Fi 7 protocol and collaboration between APs, which meet the requirements of emerging applications on campus networks for network bandwidth and latency.

The Wi-Fi 7 standard introduces technologies such as the 6 GHz frequency band, 320 MHz frequency bandwidth, 4096-QAM modulation, Multiple Resource Unit (MRU), and Multi-Link Operation (MLO) to increase the throughput of Wi-Fi networks to 23 Gbps and provide low-latency access assurance for users, helping high-quality 10 Gbps AI campus networks improve user experience.

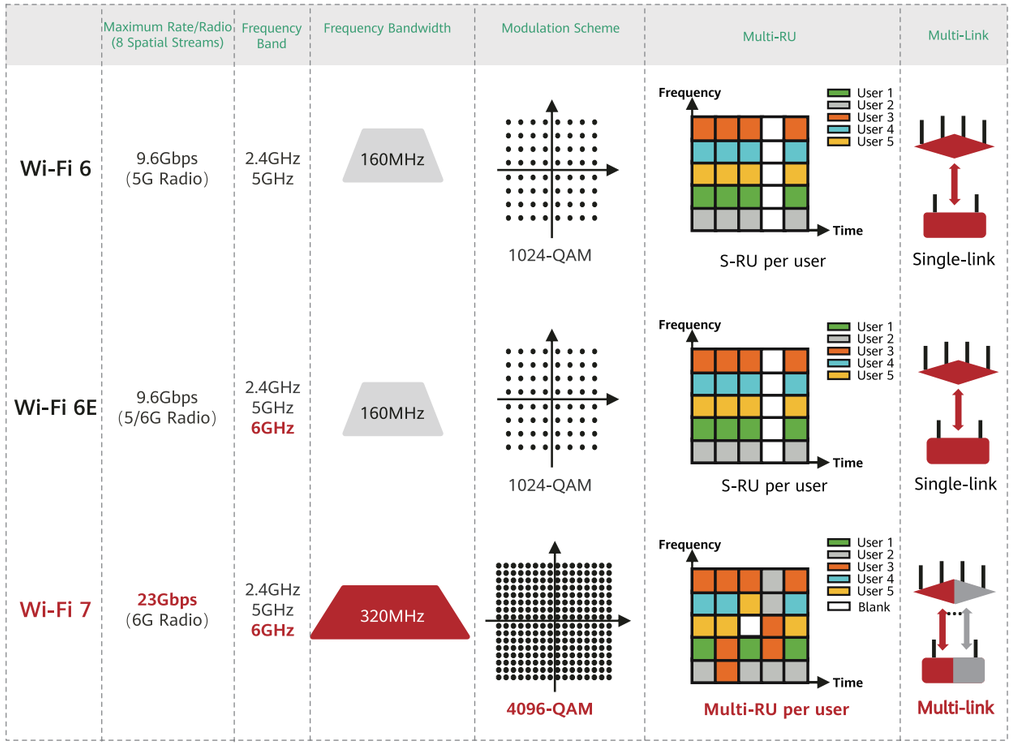


Figure 2-4 Comparison between Wi-Fi standards

2.3.1.2 10 Gbps Wired

10 Gbps wired means that access-side switches support 10GE connection with wired terminals, or the uplink bandwidth of APs is upgraded to 10GE. It can be implemented through the classic Ethernet solution and all-optical Ethernet solution. The all-optical Ethernet solution is further classified into active Ethernet network and passive Ethernet network (PEN) solutions.

Table 2-2 10 Gbps wired capabilities

	Classic Ethernet	Classic All-Optical Ethernet	All-Optical Ethernet: Active	All-Optical Ethernet: PEN
Bandwidth	2.5 Gbps to 10 Gbps	2.5 Gbps to 10 Gbps, 25 Gbps to 400 Gbps	2.5 Gbps to 10 Gbps	2.5 Gbps to 10 Gbps
PoE	Y	N	Y	N
Passive architecture	N	N	N	Y

1. The key to selecting a wired solution is the cable type. If electrical cables are used, as shown in Figure 2-5, cables of Cat6A or higher must be deployed if 5 Gbps or 10 Gbps bandwidth is required, so as to meet the high-performance access requirements of Wi-Fi 7. However, this solution increases the cable deployment cost by about 30%. A more economical solution is to reuse the existing Cat5E/Cat6 cables: Through access switch reconstruction, the transmission rate can be increased to 2.5 Gbps to meet the basic performance requirements of Wi-Fi 7.

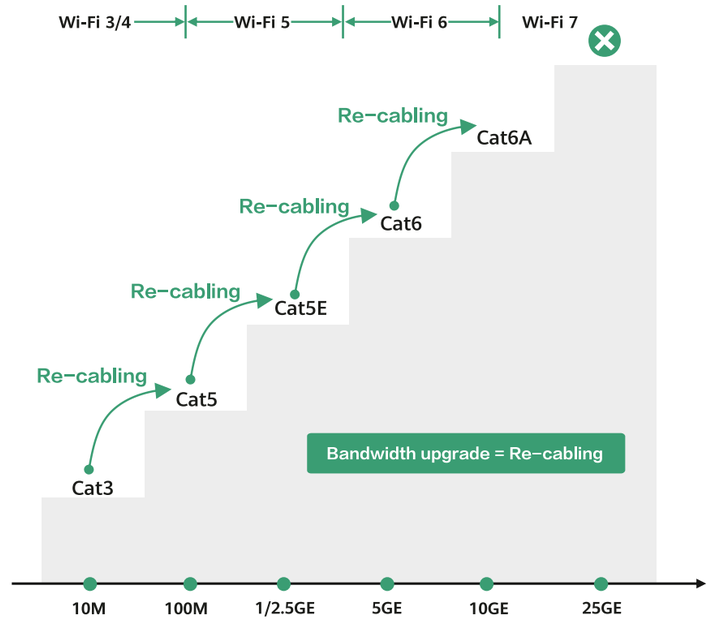


Figure 2-5 How cables evolve with Wi-Fi generations

2. In all-optical scenarios, hybrid copper-fiber cables (hybrid cables for short, as shown in Figure 2-6) can provide both long-distance power supply and high-speed access capabilities. This integration significantly simplifies network deployment.

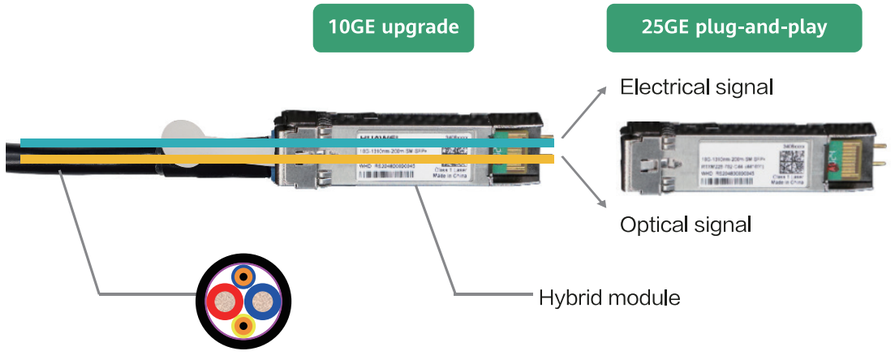


Figure 2-6 Hybrid cable and optical module composition

Table 2-3 Key capabilities of hybrid cables

Cable Specifications	Cable Diameter	PoE Power Supply Distance (15.4 W)	PoE+ Power Supply Distance (30 W)	PoE++ Power Supply Distance (60 W)
Hybrid cable-17AWG	6.2 mm	1280 m	500 m	250 m
Hybrid cable-21AWG	5.7 mm	500 m	200 m	100 m
Hybrid cable-24AWG	4.4 mm	200 m	100 m	50 m

* The American Wire Gauge (AWG) is a standard unit for measuring the diameter of an electrically conducting wire. A smaller AWG value indicates a thicker wire diameter and higher current carrying capacity.

2.3.2 Key Technologies

2.3.2.1 Continuous Networking

Continuous networking allows a WLAN with multiple APs to provide seamless signal coverage and ensure optimal service experience for users. Key technologies of continuous networking include smart antennas and multi-AP coordination.

Continuous networking implements AP grouping and priority division by synchronizing data between AP radio chips at the microsecond (μs) level. After an AP preempts a channel, it becomes the primary AP through negotiation, and instructs secondary APs to adjust the coverage angles of their smart antennas and send data packets synchronously. In this way, multiple APs can work on the same channel, significantly improving spectrum efficiency and system capacity.

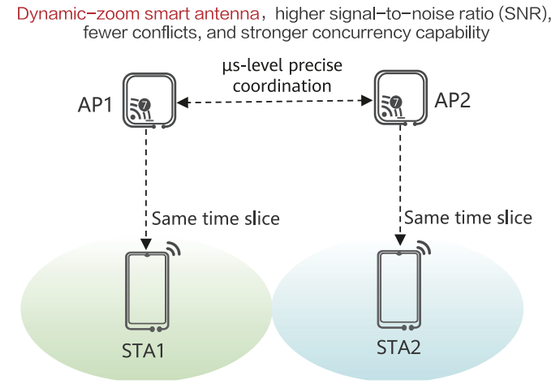


Figure 2-7 Smart antennas and multi-AP coordination

2.3.2.2 Smart Roaming

Smart roaming uses the network AI capability to profile the roaming behaviors of STAs and steer STA roaming in a differentiated manner. This solves problems in traditional roaming such as sticky STAs, long channel scanning time, and poor roaming compatibility, improving the roaming experience of STAs. Key technologies of smart roaming include STA identification, STA profiling, STA quality data learning, and roaming steering.

Smart roaming replaces STA-triggered roaming with network-steered roaming, optimizes roaming handover opportunities, and shortens the roaming time. It supports the personalized roaming parameter settings for each type of STA, and minimizes the possible adverse impacts caused by STAs' protocol compatibility and implementation differences.

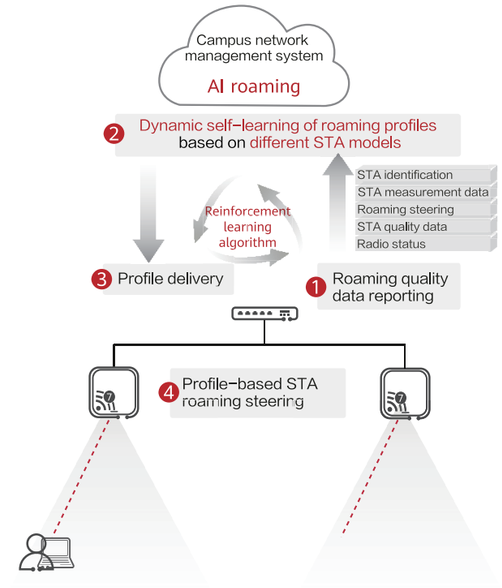


Figure 2-8 Smart roaming handover

2.3.2.3 10 Gigabit Ethernet

A cost-effective network acceleration solution is to reuse the existing Cat5E/Cat6 cables to increase the rate to 2.5 Gbps (as shown in Figure 2-9), which meets the basic requirements of Wi-Fi 7.

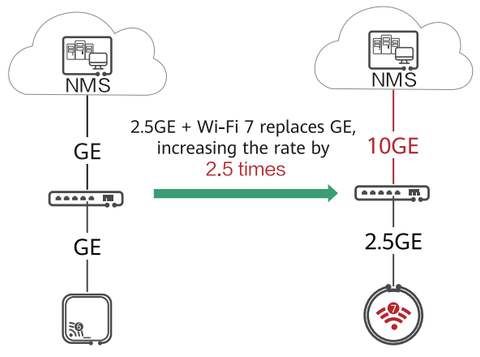


Figure 2-9 2.5GE Wi-Fi 7 traditional network

When the bandwidth requirement exceeds 2.5 Gbps, another option is optical cables, which can support future bandwidth requirements of over 10 Gbps. The following solutions are available based on the evolution of all-optical Ethernet technologies:

· Active Ethernet Network Solution: uses hybrid cables to provide long-distance PoE power supply and high-speed access capabilities, as shown in Figure 2-10.

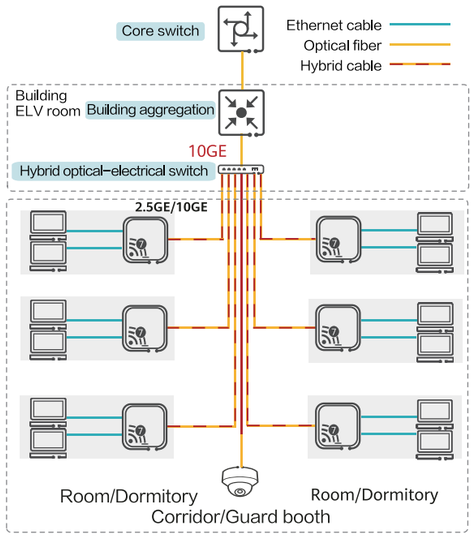


Figure 2-10 Active Ethernet Network Solution

· Passive Ethernet Network (PEN) Solution: uses passive all-optical technology to build a simplified 10 Gbps all-optical network with high performance. The solution extends high-speed 10GE optical fibers to rooms to meet the future service evolution needs, and saves the deployment of active ELV rooms, providing security and reliability. Figure 2-11 shows the solution networking.

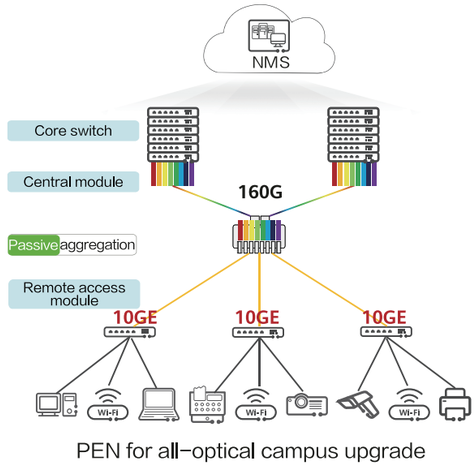


Figure 2-11 PEN Solution

2.3.3 Key Metrics

According to standards proposed by the World WLAN Application Alliance (WAA), a 10 Gbps ultra-broadband campus network should meet the following criteria.

Table 2-4 Key metrics

Category	Metric	Excellent	Good
Bandwidth	(Wireless) Single-user maximum rate	≥ 3.5 Gbps	≤ 3.5 Gbps
	(Wireless) Total throughput of three-AP 80 MHz intra-frequency networking with 18 STAs	960 Mbps	700 Mbps
	(Wired) High bandwidth at the access side (access device uplink)	Exclusive 10GE	Exclusive GE
	(Wired) High bandwidth based on the passive, simplified architecture (aggregation/core device downlink)	Single module: > 100 Gbps	Single module: 10 Gbps
Concurrency	Number of 4K HD video channels	60	40
	Passive high-density access	96/PCS	80/PCS
Architecture	(Wireless) Distributed architecture	Continuous large-scale networking and SSID sharing	Single-AP working, no continuous networking or zero roaming
	(Wired) Integrated networking of aggregation and access devices and unified management	Unified management	Not supported
Long-distance access	Long-distance PoE++ capability	≥ 250 m	≥ 200 m

2.4 Connect Everything

2.4.1 Definition

Emerging industry applications in campuses require not only high-quality wireless connections, but also the support for a wide range of access scenarios, including high-precision wireless positioning, wireless integrated sensing and communication, and IoT convergence. The unified wireless infrastructure (such as high frequency band and large-scale antenna array) enables both high-quality communication (such as Wi-Fi IoT) and environment sensing (such as positioning and imaging) to achieve seamless sensing and service coverage in physical space, extending beyond mere communication.

2.4.2 Key Technologies

2.4.2.1 Overview of Wireless Integrated Sensing and Communication

The Institute of Electrical and Electronics Engineers (IEEE) clearly defines the industry evolution direction of WLAN-based integrated sensing and communication in IEEE 802.11bf. That is, wireless signals received by STAs with WLAN sensing capabilities are used to determine target characteristics in specific environments; the collaboration between the WLAN and campus digital platforms enables real-time monitoring and intelligent analysis of campus environments and devices and ensures quick response. This provides strong technical support for smart campus construction and development.

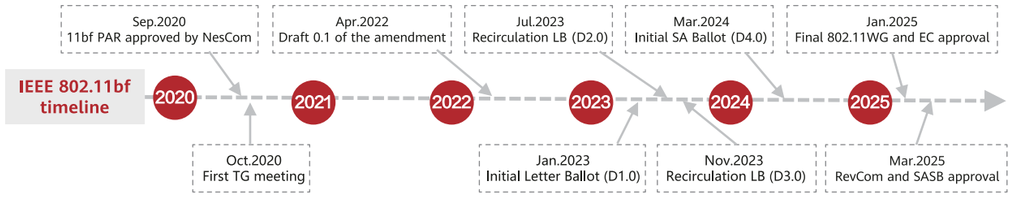


Figure 2-12 IEEE 802.11bf timeline

Wi-Fi-integrated intelligence: To build a new paradigm of "integrated sensing and communication" for campus networks, WLAN works as the ubiquitous sensing carrier with the following commercial advantages:

- Ubiquitous presence and cost advantages: After the COVID-19 pandemic, as the world widely accepts mobile distributed office and cloud-based services, WLAN continues to be the information system with the widest coverage in campuses. A WLAN serving as the sensing end offers significant advantages in digitizing, processing, and analyzing the physical world information.

- Privacy protection and data security: In the digital era, privacy protection and data security are becoming increasingly important. Integrated sensing implemented based on traditional visual sensing and WLAN technologies can provide low-cost coverage and multi-dimensional accurate judgment while effectively guaranteeing privacy security and information security.

In the process of digital and intelligent transformation in smart campuses, campus infrastructure is evolving from "connection pipes" to "intelligent platforms". With Wi-Fi as the unified foundation, the "Wi-Fi+X" converged system, which natively integrates IoT access, environment sensing, and precise positioning capabilities, is building an intelligent network that covers connections, sensing, and physical space based on the core concept of "integrated sensing and communication". This provides a new path for refined operations and service innovation in smart campuses.

2.4.2.2 Short-Range Communication Technologies

Campus terminals are the sensing end of smart campuses and play an important role in campus information and monitoring. Various sensors and monitoring terminals, such as detectors and cameras, are deployed to monitor the temperature, humidity, and other environmental information of the campus in real time, and detect potential security risks. The key trends at the terminal layer are intelligence (built-in edge computing capability), IP connectivity (direct network access), and multi-function integration. Campus terminals are both the sources of data and the execution points of intelligent instructions. Their coverage range and level of intelligence directly affect the overall sensing accuracy and response speed.

NearLink: a revolutionary Chinese native standard for a wide range of application fields such as vehicle, industrial control, and whole-house intelligence. The alliance has more than 1200 members, and the chip shipment volume reached 85 million in 2024 and is expected to exceed 100 million in 2025, covering over 20 vehicle models such as AITO M9 and Stelato S9. In 2025, the number of product categories will reach 500.

Bluetooth: The new channel detection technology improves the indoor positioning precision to sub-meter level. The "NearLink + Bluetooth" dynamic switching solution can be used to reduce cross-device interference. However, Bluetooth lags behind NearLink/UWB in terms of the positioning precision (1–3 m) and delay.

UWB: ultra-wideband, supporting centimeter-level high-precision positioning. With nanosecond-level narrow pulses (bandwidth ≥ 500 MHz), UWB uses time-of-flight (TOF) ranging and trilateration algorithm to achieve a 10-cm-level precision. It is mainly used in industrial automation and warehousing logistics scenarios and has the advantage of being secure against relay attacks.

NFC: near field communication, indispensable for secure near-field interaction within 10 cm. It prevents eavesdropping and unauthorized access and is suitable for financial payment and access control systems. NFC connects with just one tap, which simplifies the Bluetooth pairing process and improves the consumer experience.

As a popular new technology, NearLink faces both opportunities and challenges when being integrated with existing technologies.

- NearLink works on open frequency bands such as 2.4 GHz, 5 GHz, and 6 GHz, risking spectrum overlap with Wi-Fi. Co-channel interference between NearLink and Wi-Fi 7 can be avoided using the dynamic spectrum sensing technology, which monitors channel utilization in real time and dynamically allocates frequency band resources. In this way, Wi-Fi 7 is responsible for large-bandwidth data transmission, and NearLink focuses on transmitting control instructions with low latency (such as robot arm operations), achieving time division multiplexing (TDM).

- NearLink and Wi-Fi can be used together based on dynamic spectrum sensing, achieving a latency of 10 ms in industrial scenarios, 60% lower than Bluetooth's 25–100 ms.

2.4.2.3 Integrated IoT

With high concurrency and low latency, Wi-Fi has become an ideal unified IoT access platform, effectively collaborating with mainstream protocols such as Bluetooth and Radio Frequency Identification (RFID). By implementing unified access and management on the network side, this solution significantly lowers the architecture complexity and O&M costs brought by traditional multi-protocol IoT deployment, providing an efficient and cost-effective path for asset digitalization.

- In smart business scenarios, the solution efficiently supports real-time information synchronization and centralized management of numerous ESLs, enabling dynamic pricing and inventory visualization.
- In the asset management field, integrated RFID and Bluetooth capabilities enable automatic stocktaking of fixed assets and track management of mobile assets, improving asset utilization efficiency.
- In industrial interconnection scenarios, stable and reliable wireless access is provided for numerous devices including production line sensors, smart meters, and environment monitoring terminals, with the capabilities of real-time backhaul of production and energy consumption data.

2.4.2.4 Integrated Sensing

Wi-Fi signals have evolved beyond basic connectivity into a significant sensing medium. Combined with dedicated sensors such as mmWave radars, Wi-Fi signals enable the transition from "connection" to "cognition" and truly implement "integrated sensing and communication".

- Spatial and environmental intelligence: Wi-Fi channel state information (CSI) can be intelligently parsed to seamlessly detect space occupancy and identify group behaviors. The lighting and air conditioning systems can then be automatically and accurately adjusted according to the detection results, driving refined energy saving and reducing operating costs.
- Health and safety guarding: Sensing nodes equipped with mmWave radars are deployed in key areas to continuously monitor breathing and heart rate, evaluate sleep quality, and provide instant warnings for risks such as falls and bed exits, all in a non-contact manner. This provides round-the-clock, privacy-friendly care for scenarios such as elderly care and health management.
- Proactive security protection: The characteristics of wireless signals are used to detect intrusions and implement non-intrusive electronic perimeter protection, and can be used to detect hidden cameras in specific solutions, building a new dimension of proactive security protection covering both physical and network spaces.

Wi-Fi sensing is an effective and economical method for wireless sensing, and can be used for room-level presence detection (10 m), AI-assisted positioning and tracking (2–5 m), sub-meter-level body activity identification, centimeter-level vital sign detection (breathing/heartbeat), medical imaging, and more scenarios. Compared with infrared/mmWave solutions, Wi-Fi sensing leverages the integrated sensing and communication architecture that does not require cabling and integrates multiple systems, significantly reducing deployment and O&M costs.

Table 2-5 Application scenarios of Wi-Fi sensing

Application Scenario	Technical Means	KPI or Recommended Frequency Band
Human presence detection	The channel CSI fluctuates in the time domain corresponding to different human body states, based on which human presence or absence can be identified. This method is applicable to both movement and stationary scenarios.	Maximum coverage range: 10 m to 15 m Distance resolution: 0.5 m to 2 m Distance precision: < 0.2 m
Activity identification	The Doppler spectrum, target moving speed, and CSI amplitude change are extracted based on the CSI.	Large-scale activity: sub-7 GHz Small-scale activity: 60 GHz
Target positioning and tracking	Fingerprinting-based method (commonly used): Database-based positioning and tracking Geometric model-based method: Multi-parameter joint estimation is used to improve the positioning and tracking performance in multipath channel scenarios. The performance is limited by the number of antennas and bandwidth.	Distance resolution: 0.5 m Distance precision: < 0.2 m
Vital sign detection	The channel CSI amplitude and phase changes are estimated.	Heartbeat detection: 60 GHz

2.4.2.5 Integrated Positioning

Based on the unified Wi-Fi infrastructure, the network provides positioning capabilities ranging from region-level statistics collection to centimeter-level tracking on demand, accurately empowering diversified service scenarios and maximizing infrastructure investment returns.

- RSSI-based positioning (with a precision of 5–10 meters) provides an ultra-low-cost solution ideal for business insight and operations optimization scenarios, such as heat map analysis of customer flow in shopping malls and supermarkets and macro-level building footfall statistics collection.
- FTM-based positioning (with a precision of 1–3 meters) is built on international standards and is natively supported by smartphones. It provides seamless personnel/asset positioning, indoor navigation, and geo-fencing management, improving the efficiency of guest services and security management.
- UWB fused positioning (with centimeter-level precision) uses Wi-Fi networks for synchronization and backhaul and provides reliable support for high-precision scenarios, such as safety monitoring for high-risk operation personnel (e.g., based on positioning safety lights), precise positioning of valuable assets, and navigation for AGVs and robots.

2.4.3 Key Metrics

Table 2-6 Key metrics

Metric	Excellent	Good
IoT capability	Wi-Fi 7, NearLink, Bluetooth, ZigBee, etc.	Wi-Fi 6/7, Bluetooth, ZigBee, etc. (NearLink or mmWave radar not supported)
Positioning	UWB, FTM, BLE, and RSSI	BLE and RSSI
Container	Wi-Fi built-in container	Not supported
IoT scalability	USB, built-in IoT radio, and PCIe	USB
Sensing	Wi-Fi CSI sensing, mmWave radar, and unauthorized camera detection	mmWave radar
Coverage point quantity	No need to increase	Adding sensor coverage points (one sensor added per 10–15 m^2)
Cabling	Reusing existing Ethernet cables	Adding dedicated cables (such as RS485 cables) for sensors
Communication system O&M	O&M through one system	O&M through multiple systems

2.5 Deterministic Experience

2.5.1 Definition

As the digital economy continues to evolve and industries undergo intelligent transformation, campuses have emerged as key hubs for economic activity and innovation. Consequently, the demands on campus networks have shifted from basic connectivity to delivering superior user experiences. Traditional networks rely on "best-effort" data transmission, which is inherently unreliable and often results in packet loss and transmission jitter. The deterministic experience capability improves user experience by delivering deterministic priority, bandwidth, and latency, as well as high reliability, meeting network quality requirements in different scenarios.

2.5.2 Key Technologies

2.5.2.1 Deterministic Priority

Deterministic priority means that both application forwarding and user network resource allocation follow predefined, deterministic priority rules.

2.5.2.1.1 Application Priority

Deterministic application packet priority ensures that packets of key applications, such as video conferencing and cloud desktop, are preferentially forwarded by dynamically adjusting their priorities. This involves the following key technologies:

- Application identification: On the basis of IP header analysis, Layer 4 to Layer 7 content and protocol fields of packets are extracted and analyzed to identify the application name.
- Intelligent multimedia scheduling: Technologies such as congestion control and differentiated quality of service (QoS) are used to accurately suppress bandwidth-hungry service traffic and preferentially schedule audio and video traffic, ensuring the quality of high-priority services and improving bandwidth utilization.

2.5.2.1.2 User Priority

Deterministic user priority means that key users receive prioritized access to network services. Key users include important enterprise users and important terminals on the network, such as video conferencing terminals in conference rooms. Technologies such as preferential access, wireless signal enhancement, and wireless preferential forwarding are used to ensure the wireless network experience of key users.

- Preferential access guarantees the access experience of key users by allowing them to access the network and disconnecting online non-key users when the number of access users reaches the threshold.
- Wireless signal enhancement means to enhance the signal strength at locations of key users to resolve poor and unstable connectivity caused by distance from APs or user mobility.
- Wireless preferential forwarding allows APs to reserve air interface resources for key users. This function improves air interface experience of key users when APs are congested by high-bandwidth services (such as large file download/upload and HD video) of some greedy STAs with non-standard preemption capabilities.

2.5.2.2 Deterministic Bandwidth

Deterministic bandwidth means that bandwidths to be occupied by different services can be isolated from each other, preventing interference during data transmission. On a network that carries numerous services, network slicing can be used to guarantee bandwidth for key services to prevent packet loss due to insufficient bandwidth during service concurrency.

Network slicing technology allocates resources of a physical network to multiple logical networks, with each logical network serving a specific type of service or industry. The logical topology, SLA requirements, reliability, and security level of each network slice can be flexibly defined, thereby meeting diverse requirements of services, industries, and users.

2.5.2.3 Deterministic Latency

Deterministic latency refers to a definite time required for end-to-end data transmission. In addition to the inherent physical latency, traditional networks have uncertain latency caused by processes such as queue-based transmission and table lookup-based forwarding. Moreover, the best-effort communication mechanism used on traditional networks lacks determinism and real-time performance — capabilities that are critical in fields such as industrial manufacturing. To solve the problem of uncertain latency, technologies such as time-sensitive networking (TSN) are developed.

Leveraging high-precision time synchronization, TSN identifies key service traffic based on flow rules and performs deterministic traffic scheduling at precisely defined time points. In this way, the single-hop forwarding latency of key service traffic is controlled within microseconds. The involved key technologies include high-precision time synchronization (such as IEEE 1588v2) and traffic scheduling mechanism (such as 802.1Qbv gate control list scheduling).

2.5.2.4 High Reliability

High reliability prevents unreliable transmission caused by factors such as packet loss and delay during data forwarding. As technology advances, more and more services (such as payment service and PLC control information transmission for industrial equipment) have become highly sensitive to packet loss and require higher network reliability. A common technology for reducing the packet loss rate is dual fed and selective receiving.

In dual fed and selective receiving, the ingress device replicates received data, and sends the original data and its copy to the egress device through different paths. The egress device then forwards the data that arrives first. Dual fed and selective receiving mainly solves the problem of packet loss caused by single points of failure on forwarding paths, significantly improving network reliability.

2.5.3 Key Metrics

After the preceding functions are deployed on a campus network, the following performance can be achieved.

Table 2-7 Key metrics of experience assurance

Category	Metric	Excellent	Good
Application assurance	Resolution of audio and video services without downgrading or video freezing upon link congestion	4K	720p
	Time taken to insert a 10 MB image in the collaborative office scenario	6s	20s
	Performance for 15-channel video playing and 15-channel PPT slide switching on cloud desktops	1080p, latency < 100 ms	720p, latency < 1000 ms
Industrial assurance	Hitless upgrade	M-LAG, 50 ms service switchover	Not supported
	High-performance industrial ring network	10 ms to 20 ms switchover upon a fault	> 50 ms switchover upon a fault
	Dual fed and selective receiving for redundancy	Supported	Not supported
User assurance	Latency when the air interface channel utilization is greater than 80%	< 50 ms	< 200 ms
	Less than –68 dBm downlink signal strength of a STA (or about 10 m horizontal distance between a STA and an AP, without blocking)	Bandwidth increased by 30%	No bandwidth increase
	Fault alarm function	Supported	Not supported

2.6 Energy-Saving

2.6.1 Definition

Campus network energy saving includes multiple dimensions, including device-level energy saving, network-level energy saving, and smart building energy saving. Smart building energy saving uses the CSI sensing capability of WLANs to monitor and identify environment changes. CSI sensing collaborates with the building management system to significantly reduce the energy consumption of facilities such as air conditioners and lighting, thereby reducing energy waste in campuses and achieving the goal of green buildings.

2.6.2 Key Technologies

2.6.2.1 Device-Level Energy Saving

In device-level energy saving, energy saving modes are defined on single devices based on different loads. For example, a device enters the sleep/standby mode when it is unloaded, and enters the low power consumption mode when lightly loaded.

APs are the most numerous nodes on a WLAN, and their working status becomes the focus of an energy-saving solution. APs are usually powered by PoE switches. In addition to entering the sleep mode or low power consumption mode, APs can achieve energy saving through PoE OFF operations.

- PoE OFF mode: The PoE switch disables the port from supplying power to the AP. In this case, the AP does not consume any power. When the AP is started, the port provides power to the AP again.
- Sleep mode: Key hardware such as the CPU runs at extremely low power, and other components are shut down. The sleep mode saves 80% to 90% energy for a single AP, and the AP can resume operation within one minute.

2.6.2.2 Network-Level Energy Saving

Network-level dynamic energy saving is implemented on demand through intelligent SDN measures. Specifically, shutdown can be performed by group at a scheduled time and by role for each region, so that the network intelligently shuts down some devices by time segment and device role to achieve network-level energy saving.

AI analyzes network tidal characteristics and configures energy-saving policies for each region. The following figure shows the network traffic statistics of a teaching building in a university over five days. It can be seen that the network usage increases significantly at 07:00, reaches the peak in the morning and afternoon, and drops to near zero after 00:00.

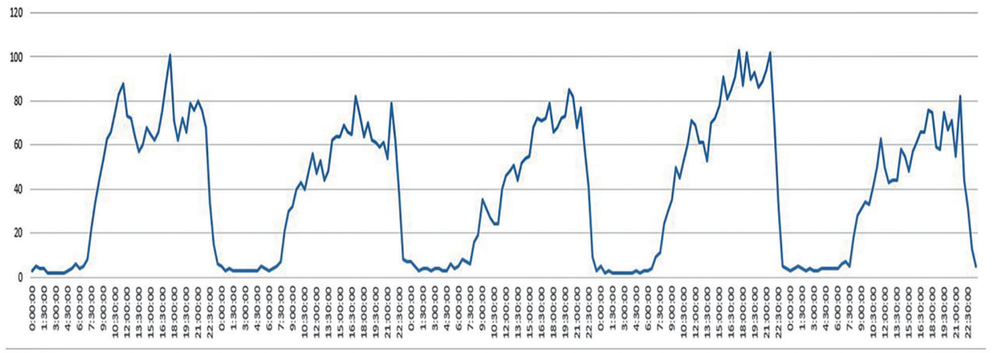


Figure 2-13 Network traffic statistics of a teaching building in a university

Network energy consumption visualization refers to collecting energy consumption information reported by devices such as APs to monitor the energy usage of the campus network, buildings, floors, and specific APs in real time. The information is analyzed and displayed on the intelligent analysis system — usually a component of the NMS or SDN controller. As shown in the following figure, the system can display the network status at the region level, including regional overall energy consumption by day or hour, regional network usage (channel utilization), and regional overall network quality by day or hour. This visualized management helps network administrators easily grasp the overall energy usage and implement time- and region-specific energy-saving measures.

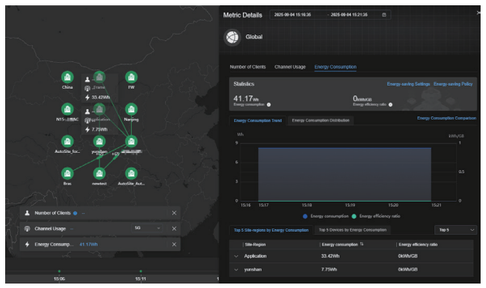


Figure 2-14 Campus energy consumption monitoring through the WLAN visualization system

Energy saving can also be achieved by simplifying the network architecture. For example, making the access layer lightweight and the aggregation layer passive enables lightweight operation and reduces energy consumption.

- The passive architecture saves the deployment of active devices at the aggregation layer, saving energy at the aggregation layer.
- The access layer uses the simplified architecture, replacing the original access devices that consume dozens of watts with lightweight devices that consume only several watts.

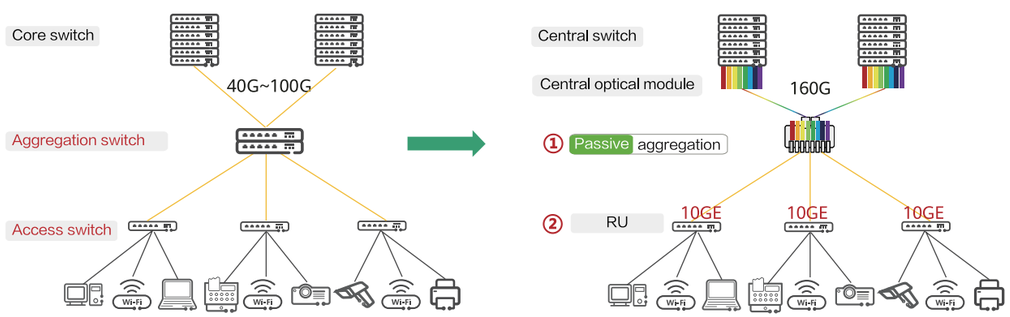


Figure 2-15 Simplified network architecture

2.6.2.3 Intelligent Building Collaboration

Intelligent building collaboration is a solution in which the WLAN collaborates with the building management system to save energy on building facilities such as air conditioners and lights. Over 75% of building energy consumption comes from air conditioning and lighting. As air conditioners and lights are mainly for people's use, they can be turned off at night when no one uses them to save energy. As technology advances, in addition to communication functions, a WLAN now supports spatial and personnel sensing based on channel state information (CSI), providing information input for the building management system to take decisions on energy saving.

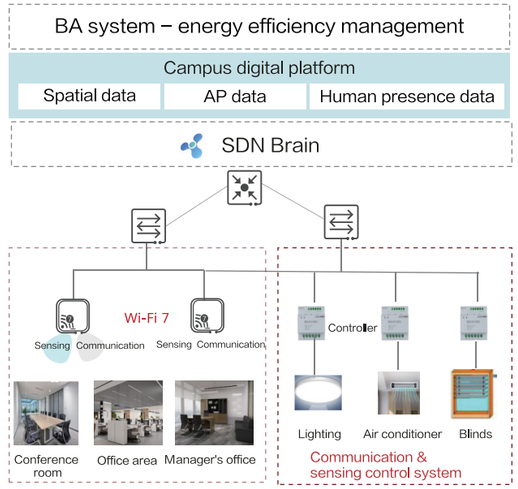


Figure 2-16 Intelligent building collaboration

As the WLAN collaborates with the building management system to save energy, the running time of the air conditioning and lighting systems is significantly reduced, lowering their energy consumption by 15% to 30%. This lowers power costs for building operators and offers substantial economic and environmental benefits.

2.6.3 Key Metrics

Table 2-8 Key metrics for energy saving

Category	Metric	Excellent	Good
Device energy saving	Chip-level dynamic energy saving	Supported, saving more than 10% in energy consumption	Not supported
Network energy saving	Energy saving based on NE tidal prediction	AI-based prediction	Manual prediction
	Shutdown when unoccupied, sleep mode under low load	Supported	Not supported
	Wake-up time	Seconds	Minutes
	Energy-saving benefit	30%	10%
Smart building energy saving	Energy saving based on CSI sensing: human presence detection through Wi-Fi for linked turn-off of building equipment such as air conditioners and lights	Supported	Not supported

2.7 Full-Scope Security

2.7.1 Definition

In campus scenarios, full-scope security aims to build a dynamic, intelligent comprehensive protection system. The system is centered around a unified policy platform, integrates various security capabilities, and provides closed-loop protection for all domains of the campus (including physical and virtual assets, users, service flows, data, and applications), ensuring service continuity and data security. Full-scope security firmly follows the concepts of zero trust, in-depth defense, and continuous self-adaptation. Through the deep integration and collaboration of technologies, it guarantees security for all space (physical/virtual), all objects (assets/users/data), and all processes (access/transmission/processing), serving as a key solution to cope with complex network threats.

Zero-trust architecture:

As a revolutionary paradigm in security defense, the campus security solution based on the concept of zero trust provides comprehensive security protection across terminal security, terminal compliant access, link security, microsegmentation, resilience, and trustworthiness.

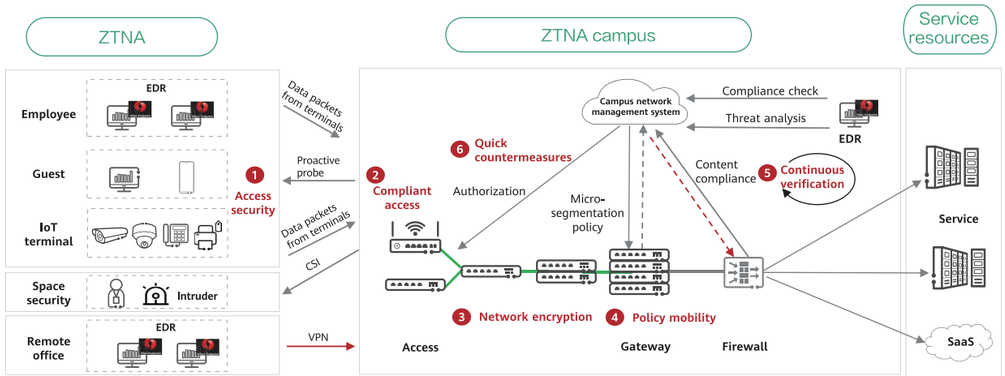


Figure 2-17 Campus network security architecture

Zero-trust network security:

1. Access security: provides overall secure access capabilities in terms of connection and space anytime, anywhere, covering scenarios such as terminal security, space security, and remote secure access.
2. Identity and access management: implements unified identity governance, multi-factor authentication, and attribute-based dynamic access control.
3. Link security: enables link-layer anti-eavesdropping for transmission over the wireless air interface and wired backhaul for APs and switches (through MACsec).
4. Microsegmentation: implements fine-grained isolation policies on the network (especially east-west traffic) to limit the lateral movement scope of attacks.
5. Continuous threat detection: uses AI and machine learning (ML) technologies to quickly detect advanced threats through network traffic analysis, endpoint detection and response (EDR), and user and entity behavior analytics.
6. Threat risk response: accurately identifies risk sources based on continuous threat detection, and automatically responds to risks near the point of network access to block the network access of risky terminals.

2.7.2 Key Technologies

2.7.2.1 Access Security

Asset visualization and management: Terminal identification and visualization capabilities, including EDR asset collection on the terminal side and terminal fingerprint analysis on the network side, are used to accurately identify terminals and control network access, implementing secure access.

Terminal identification on the network side is to analyze and extract terminal characteristics based on the digest fields of protocol packets to identify information such as the terminal type, model, and vendor. Terminal identification methods include passive fingerprint collection, proactive scanning, and AI clustering.

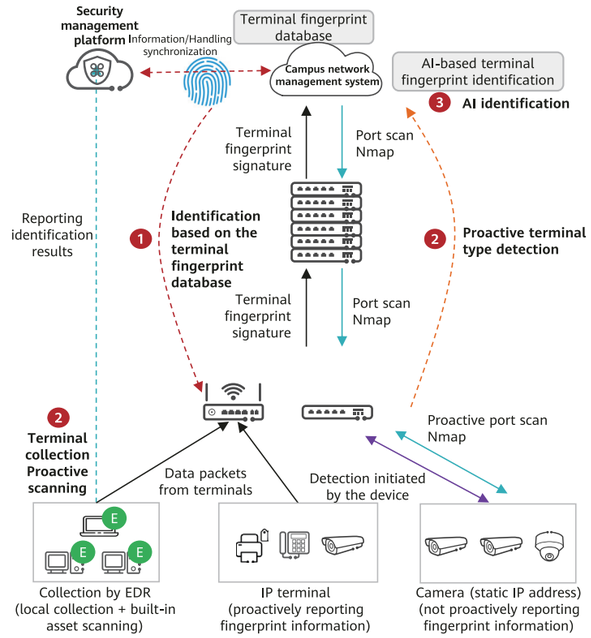


Figure 2-18 Terminal identification process

With the popularization of AI agents, smart terminals pose higher security protection requirements and challenges, making it essential for the industry to provide more powerful terminal-side protection capabilities. An example is the EDR hierarchical advanced threat protection system, which can defend against various attacks such as ransomware, zero-day, and fileless attacks, and implement integrated cloud-network-edge-device protection through network-security collaboration.

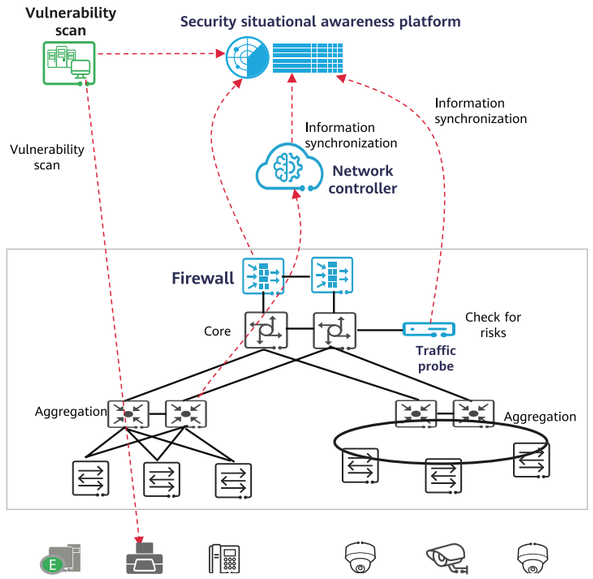
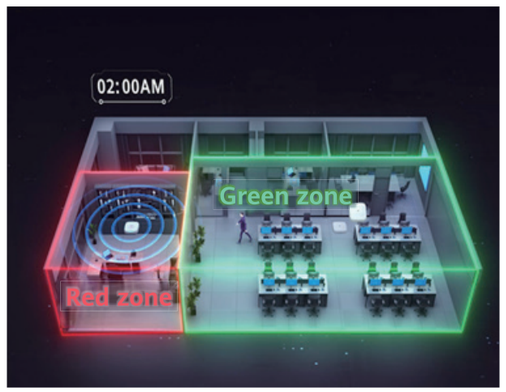


Figure 2-19 EDR security protection

The campus physical space is also secured. Technologies such as Wi-Fi 7 and mmWave radar implement personnel and object sensing in areas, which can be used in scenarios such as personnel intrusion analysis, special event monitoring, and indoor unauthorized device detection. With technological maturity and industry development, more scenario-specific solutions will emerge.

Office: unauthorized access to key areas



Hotel: camera detection, abnormal room use (intrusion), etc.

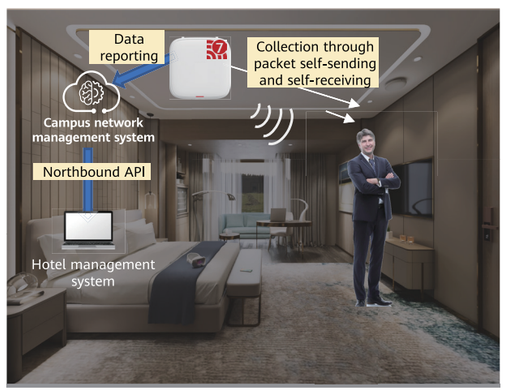


Figure 2-20 Spatial security detection

2.7.2.2 Compliant Access

Compliant access: Only compliant, authorized terminals are allowed to access the campus network, and different network permissions are assigned to terminals based on the identity and compliance status. The terminal compliance mechanism includes host security check, secure access authentication (such as 802.1X and Portal authentication), dumb terminal identification and anti-spoofing, and unauthorized access prevention. RADIUS and TACACS+ authentication protocols are used together to implement single sign-on (SSO) for network access, service access, and O&M operations, eliminating privilege escalation risks.

Microsegmentation: is a network security architecture approach that focuses on dividing the network into granular security zones (micro-segments) and enforcing stringent access control policies between these zones to limit attacker lateral movement, thereby enhancing overall security.

Security groups

Group	ID
Sales	1
R&D	2
Marketing	3
...	...

Security group–based policy control matrix

	Sales	R&D	Marketing	...
Sales	√	×	√	...
R&D	×	√	√	...
Marketing	√	√	√	...
...	...	...	...	...

Figure 2-21 Security groups

2.7.2.3 Link Security

Encryption algorithms such as WPA2 and WPA3 are used to encrypt the transmission over the air interface, ensuring that data captured by unauthorized users is encrypted and can be parsed into valid information only after decryption. In wireless scenarios with high security requirements, scrambling is performed for air interface transmission, making it impossible for unauthorized users to obtain any valid information over the air interface. In terms of wired links, MACsec is used to implement physical layer encryption.

Wi-Fi Protected Access (WPA), which includes WPA, WPA2, and WPA3, is a set of security standards developed by the Wi-Fi Alliance to safeguard wireless network access, and supports authentication modes such as EAP-PEAP and EAP-TLS.

Air interface signal scrambling technology draws on multi-user multiple-input multiple-output (MU-MIMO) and leverages idle antennas of APs to send extra electromagnetic wave noise, protecting the communication path of STAs. Within the location range of a target STA, the actual data is not affected by interference signals, ensuring that the data can be correctly demodulated. However, outside the location range of a target STA, the actual data is affected by the interference signals, meaning unauthorized users cannot demodulate Wi-Fi signals. As shown in the following figure, outside the location range of a target STA, only meaningless noises can be captured when someone attempts to eavesdrop or capture wireless packets.

When the target STA moves, the information can be quickly updated to ensure the accuracy of air interface scrambling.

Figure 2-22 Signals received by different users after air interface scrambling

MACsec is a Layer 2 encryption technology that ensures hop-by-hop link-level secure data transmission. With a series of security functions including data encryption, integrity check, and replay protection, MACsec applies to scenarios that require high data confidentiality, such as government and finance.

2.7.2.4 Resilience and Trustworthiness

Resilient systems refer to the security and trustworthiness of network devices. That is, network devices not only ensure security (confidentiality, integrity, and availability) but also enable users to trust their privacy protection, reliability, and stability. From the perspective of campus network threats, it is essential to focus on protecting key objects such as software, data, and hardware on terminals and servers, and the capabilities extend to management and control platforms, routers, firewalls, switches, and WLAN products.

Through analysis of the entire lifecycle, the following key capabilities are required: factory-level trustworthiness, protocol security, O&M trustworthiness, and system trustworthiness.

In terms of device and supply chain security, it is necessary to start from the manufacturing process, such as establishing a device firmware whitelist mechanism and formulating admission standards for imported chips to prevent backdoor risks.

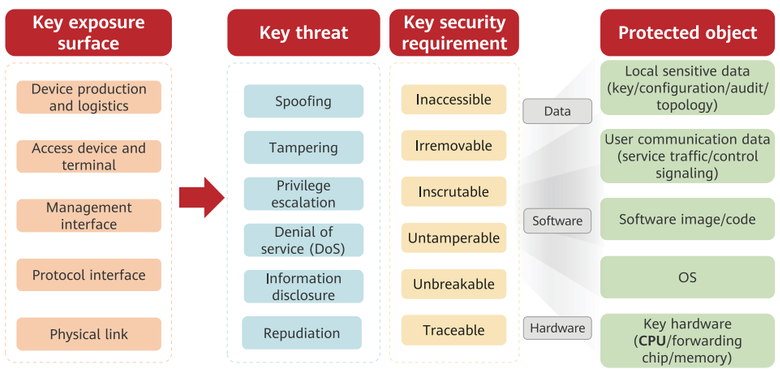


Figure 2-23 Campus network threats

2.7.3 Key Metrics

After the preceding terminal, link, and device security functions are deployed, the network can achieve the following security capabilities.

Table 2-9 Key metrics of zero trust

Category	Metric	Excellent	Good
Wireless security	Data encryption algorithm	WPA3	WPA2
Spatial security	Wi-Fi CSI sensing for spatial security	Intrusion detection, personnel anomaly detection, and scanning of unauthorized devices such as cameras	No spatial security
Privacy security	Unauthorized camera detection	Detecting unauthorized cameras only using the network, without the need to deploy an independent system	Not supported
Connection security	Anti-eavesdropping on air interface signals	Scrambling air interface signals to prevent eavesdropping	Not supported
Connection security	AP + switch link-layer MACsec encryption	Supported for all wireless and wired links; SM series cryptographic algorithms supported by switches	Supported only by switches; SM series cryptographic algorithms not supported
Connection security	Secure service isolation, ensuring service SLA	End-to-end SLA quality assurance (such as slicing) and one-click deployment	QoS-based service assurance
Full visualization of terminals	Terminal identification	Passive traffic analysis and proactive scanning for asset identification AI clustering for unknown asset identification	Passive traffic analysis and proactive scanning for asset identification
Terminal security	Secure and compliant terminal access based on the zero trust concept	Supporting 30 ms fast unauthorized access detection (built in switches) and EDR security posture detection	Not supporting unauthorized access detection (or relying on an off-path device to support the function) or EDR security detection
Microsegmentation	Service-based security isolation for access terminals, preventing the lateral movement of risks	VXLAN tunnels and independent NMS deployment (compatible with third-party NMSs)	Not supported; or supporting only VXLAN tunnels
Network-security collaboration	Near-source threat blocking through network-security collaboration	Near-end threat blocking through collaboration with switches	Supporting threat blocking through collaboration with security devices; not supporting continuous detection
Host security	Unknown advanced threat detection enhanced by graph engine and AI technologies to detect abnormal behaviors such as advanced remote control, phishing, ransomware, zero-day, crypto-mining, information theft, and fileless attacks in a timely manner	Device security capabilities such as secure communication, secure storage of sensitive data, and secure boot	Not supported

03

Typical Applications of High-Quality 10 Gbps AI Campus

3.1 Education Industry

3.1.1 Trends and Requirements

The global education system is accelerating its digital and intelligent transformation, using smart technologies to reinvent experience in all scenarios, including teaching, research, services, and operations.

The proliferation of smart classrooms is reshaping traditional teaching modes. AI-driven personalized learning systems, AR/VR immersive classrooms, and similar innovations are making teaching methods more intelligent, personalized, and interactive, greatly improving the teaching effectiveness and learning experience. At the same time, the expansion of online teaching and virtual classrooms allows high-quality educational resources to be shared anytime, anywhere. This helps to close the education divide between regions and people, promoting education equity. These modern teaching methods require a high-bandwidth, low-latency campus network, as network stability and real-time performance directly impact teaching quality and experience.

In scientific research, AI technologies plays a vital role in areas such as literature data acquisition, experiment prediction, and result analysis. For example, when simulating complex experimental scenarios, AI can predict outcomes in advance, reducing the number of physical trials and improving research efficiency. But to meet the needs of AI model training and complex data processing, campus networks need to provide robust computing power support. In addition, high network transmission speed is essential to enable rapid upload and download of research data, especially during collaboration between teams where efficient data exchange is critical. Moreover, network security is vital for preventing research data leakage and protecting research achievements.

Digital transformation in higher education extends beyond teaching and research, also encompassing the intelligent upgrade of campus services and operations management, which is a critical component of smart campus development. By establishing a one-stop information service platform that integrates teaching and student affairs, as well as the library and logistics systems, the smart campus delivers more convenient and personalized service experience. Beyond that, IoT and intelligent technologies are renovating campus infrastructure management and operating models, transforming operations from manual to automated and intelligent. The large-scale access of mobile devices and IoT terminals poses new requirements on campus network coverage, concurrency, and reliability.

Universities are home to tens of thousands of students and teachers, and provide a wide range of activities such as teaching, research, services, and administration, which require a rapidly growing number of terminals. Traditional O&M — which is carried out manually, relies on experience, and is reactive — is inefficient and results in a long fault handling time. There is a need for an intelligent network O&M platform with global visibility. Such a platform can lower the O&M threshold, enable rapid fault detection, and automatically handle typical faults, thereby supporting campus operations management.

3.1.2 Recommended Networking Architecture

A typical school campus network covers scenarios such as offices, classrooms, and dormitories. The high-quality 10 Gbps campus network offers high bandwidth, deterministic experience, intelligent O&M, and high energy efficiency. These features allow the network to support diverse services and future evolution of schools.

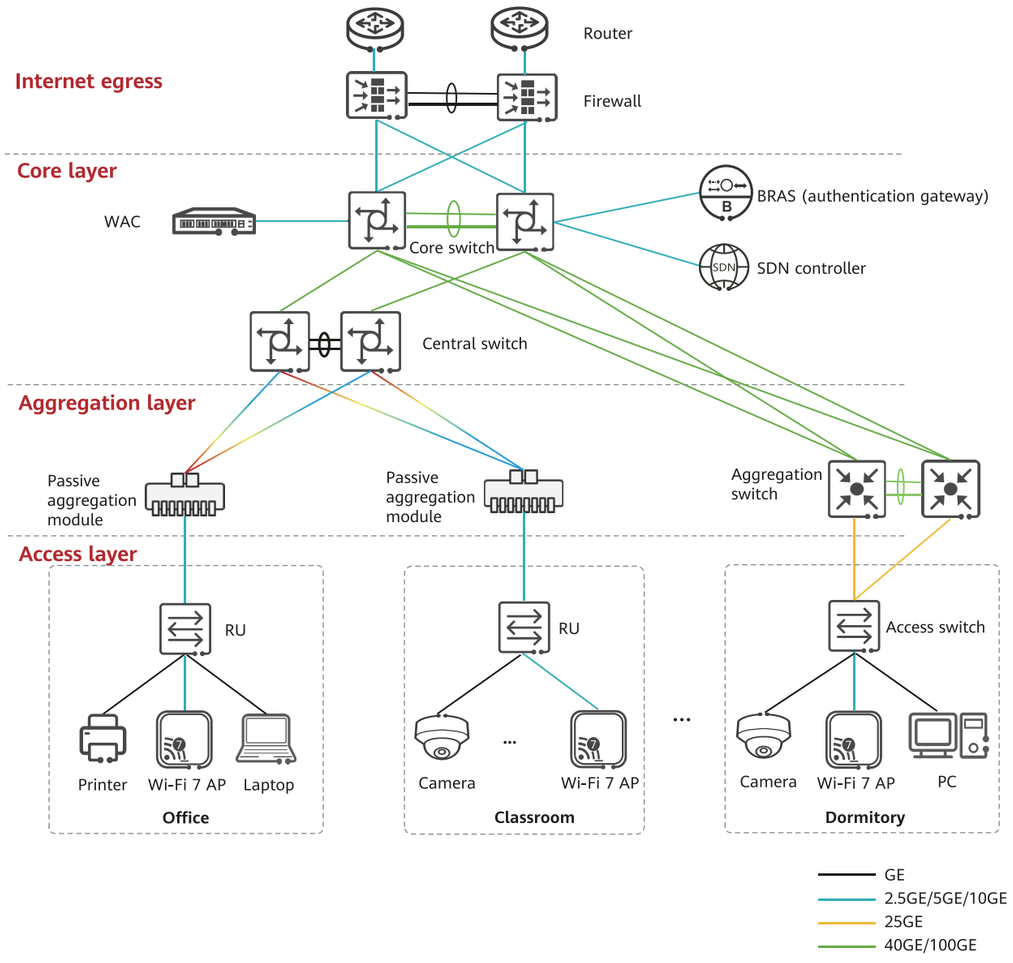


Figure 3-1 Recommended networking architecture

3.1.3 Smart Office

An increasing number of universities are adopting cloud office platforms (such as Microsoft 365 and Google Workspace) to enable remote collaboration, online document editing, task tracking, and data sharing. Moreover, recent years have witnessed the explosive growth in online meetings on applications such as Teams and Zoom. All of these support cross-department and cross-campus collaboration among teachers, improving productivity and reducing O&M costs.

In addition to demanding high network bandwidth, cloud office platforms and HD video conferencing also require lower latency, as shown in the following table.

Table 3-1 Bandwidth and latency requirements of different services

Service	Bandwidth	Latency
4K UHD video streaming	15–30 Mbps	20 ms
8K UHD video streaming	40–100 Mbps	20 ms
HD video conferencing	5–7.2 Mbps	20 ms
Real-time document collaboration	5–10 Mbps	< 100 ms
Cloud desktop	8–20 Mbps	≤ 50 ms
Sources: Huawei, Cisco, Microsoft, Frontier Communications, HealthIT.gov		

Burst traffic, such as uploads and downloads, consumes a large amount of network resources, which may cause poor experience such as freezing in video conferences and collaborative office services. In addition, as these platforms are cloud-based, the quality of carrier networks outside the campus egress is also a key factor affecting user experience. In the current landscape, ensuring optimal experience for key office applications and enabling rapid fault locating are urgent priorities.

Figure 3-2 Cross-region collaboration via video conferencing in universities

The following table lists the recommended indicators for a high-quality 10 Gbps campus office network.

Table 3-2 Recommended indicators for a high-quality 10 Gbps campus office network

Item	Recommended Indicator
Bandwidth of access devices deployed indoors	≥ 10 Gbps
WLAN AP standard	Wi-Fi 7
Total throughput of 18 STAs connected to three APs in 80 MHz networking	≥ 960 Mbps
Concurrent channels of 4K HD video conferencing	≥ 60 channels
Definition and latency of key applications such as video conferencing and cloud desktop	1080p, latency < 100 ms
Service latency of key users	≤ 50 ms

3.1.4 Smart Classroom

Modern education is undergoing unprecedented changes, with traditional classroom models being replaced by advanced teaching methods such as smart classrooms, online teaching, and VR immersive classrooms. By integrating multimedia devices, sensors, and intelligent interaction systems, smart classrooms create a more dynamic and efficient learning environment for students. In addition, the widespread adoption of online and virtual classrooms enables higher education students to learn anytime, anywhere over the Internet. This significantly enhances the flexibility and accessibility of teaching.

The introduction of VR technology has made the higher education experience more immersive than ever. Students can use VR devices to enter simulation labs, remotely operate high-precision research equipment, and even conduct simulated experiments in fields such as medicine and engineering. These modern teaching methods require high-bandwidth, low-latency campus networks.

Figure 3-3 VR smart teaching

Network stability and real-time performance directly impact teaching quality and experience. For example, insufficient bandwidth or high latency can cause lag during class interactions and delayed loading of virtual scenarios, which ultimately affects overall teaching effectiveness. Therefore, the 10 Gbps AI campus network can provide high-speed, stable connectivity to support new teaching modes on smart campuses. This ensures smooth information exchange between teachers and students, making the teaching process more efficient and interactive.

Table 3-3 Bandwidth and latency requirements of services

Service	Bandwidth	Latency
Online class	10–20 Mbps	≤ 100 ms
Standard AR & VR (entertainment)	≥ 30 Mbps	≤ 20 ms
Advanced AR & VR (training)	> 80 Mbps	≤ 15 ms

Schools are big energy consumers. Numerous spaces such as classrooms and laboratories consume a large amount of electricity every day. In particular, network devices, air conditioning, and lighting often continue operating even when not in use, leading to significant energy waste and high OPEX. Traditional energy management methods require manual inspection of each classroom, which is time-consuming, labor-intensive, and prone to oversight. To build a green campus and reduce OPEX, the school urgently needs an intelligent energy-saving system.

Figure 3-4 Intelligent light control in classrooms

The following table lists the recommended indicators for a high-quality 10 Gbps campus classroom network.

Table 3-4 Recommended indicators for a high-quality 10 Gbps campus classroom network

Item	Recommended Indicator
Bandwidth of access devices deployed indoors	≥ 10 Gbps
WLAN AP standard	Wi-Fi 7
Total throughput of 18 STAs connected to three APs in 80 MHz networking	≥ 960 Mbps
Definition and latency of online class applications	1080p, latency ≤ 100 ms
Sensor-free WLAN APs with CSI for human presence detection and interconnection with the building management system to control facilities such as air conditioning and lighting for energy savings	Supported
Colored optical port density	≥ 96 per device
Automatic optimization and resolution of coverage, interference, high channel utilization, air interface congestion, and roaming Wi-Fi issues without manual intervention	Supported
Natural language interaction, fast feedback on network status, faults, and handling suggestions	Supported

3.1.5 Smart Dormitory

To meet the evolving demands of higher education and student life, university dormitories need to support diversified and intelligent network services. Modern university dormitories are no longer merely places for accommodation — they have evolved into integrated environments for studying, entertainment, and social interaction. These dormitories must provide high-speed Internet access to support online learning, remote classes, video conferences, and other academic activities, while also providing a stable network for streaming, gaming, and social applications.

Figure 3-5 Diverse dormitory network services

To meet these demands, university dormitories require high-bandwidth, low-latency network infrastructure, which is essential to ensure smooth performance when multiple devices are online at the same time. In addition, with the advancement of IoT technologies, smart dormitories are becoming a trend. Facilities such as access control, lighting, air conditioning, and temperature control require intelligent management throughout the network, which places higher demands on network reliability and stability. Furthermore, traditional manual O&M models are inadequate for large-scale, high-concurrency networks. Universities need to adopt more intelligent and automated O&M solutions.

The following table lists the recommended indicators for a high-quality 10 Gbps campus dormitory network.

Table 3-5 Recommended indicators for a high-quality 10 Gbps campus dormitory network

Item	Recommended Indicator
Bandwidth of access devices deployed indoors	≥ 10 Gbps
WLAN AP standard	Wi-Fi 7
Per-STA bandwidth when eight STAs access the network concurrently	≥ 50 Mbps
Latency of online classes and real-time games	< 100 ms
Sensor-free WLAN APs with CSI for human presence detection and interconnection with the building management system to control facilities such as air conditioning and lighting for energy savings	Supported
Automatic optimization and resolution of coverage, interference, high channel utilization, air interface congestion, and roaming Wi-Fi issues without manual intervention	Supported
Natural language interaction, fast feedback on network status, faults, and handling suggestions	Supported

3.1.6 Cases

3.1.6.1 A University in Germany

Key Challenges and Requirements

The university is one of Germany's leading universities and also one of the country's oldest technical institutions, renowned for its excellence in engineering and technology. In the student dormitory scenario, more than 10 residential areas cover thousands of students, with over 2,000 concurrent access users on average. Adequate network bandwidth is crucial.

Key Technologies

Broadband access 10 Gbps: The network uses Wi-Fi 7 APs that support the 320 MHz bandwidth on the 6 GHz frequency band, where 160 MHz continuous networking can be implemented on abundant channels. Exclusive dynamic-zoom smart antennas can be freely switched between high-density and omnidirectional coverage modes to increase the coverage by 20%. After this solution is deployed, the Wi-Fi device throughput can reach 18.67 Gbps, effectively ensuring high-concurrency service scenarios.

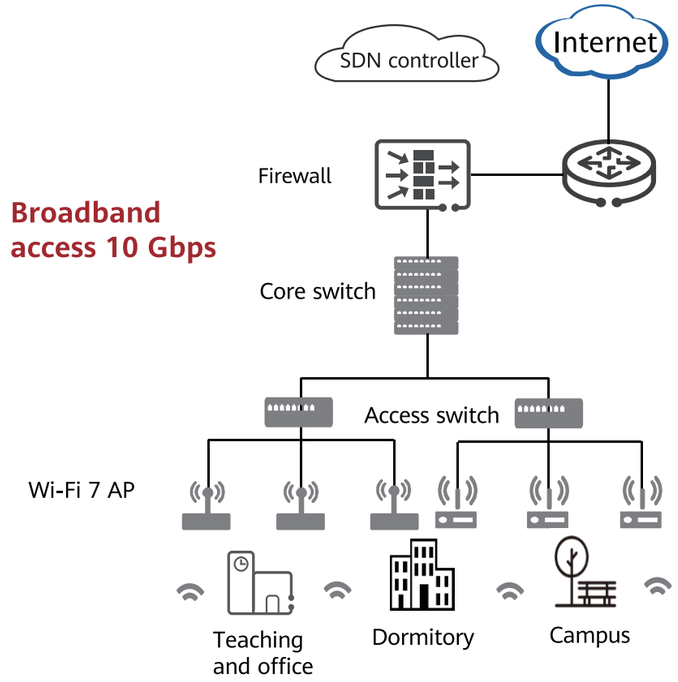


Figure 3-6 Networking diagram

Technology Advantages and Benefits

In most scenarios tested, the speed at least doubled. Impressively, the download speed reached more than 1 Gbps over a distance of more than 10 m.

3.2 Government Industry

3.2.1 Trends and Requirements

According to UN E-Government Survey 2024, 81% of countries worldwide have released digital government strategies to explore how to build a digital government. This facilitates scientific government decision-making, efficient administrative office, convenient public services, and precise social governance.

Governments around the world have accelerated the construction of an integrated government service platform and the creation of one network for all government services. This helps implement cross-region, cross-departmental, and cross-level service collaboration, as well as providing one-stop efficient government services, thereby making government services truly inclusive. According to UN E-Government Survey 2022, 138 countries around the world provide multiple government services online. Among them, 115 countries provide cross-departmental and cross-level integrated government services. The government network needs to provide the public with multiple services featuring wide coverage, and break cross-departmental barriers to enable smooth sharing of data across departments, levels, and regions, so as to provide inclusive one-stop government services.

The annual growth rate of access to mobile government applications worldwide exceeds 30%. After the pandemic, the frequency of video conferencing in policy delivery and cross-departmental collaboration has increased by 3 to 5 times. To support efficient government operations, it is important to improve the quality of mobile access, video assurance capability, and O&M efficiency. Moreover, it is also necessary to build efficient office and video conferencing systems that allow government services to be handled anywhere and conferences to be held anytime. Furthermore, improving document, office, and conference handling efficiency is also a must.

As government services become more mobile and service systems become more complex, security risks increase. In addition, network attack technologies are emerging one after another. This poses more security threats on the critical information infrastructure of different nations. According to the annual report on network security released by the US government, each US government department experiences an average of 32,000 network security events every year. As such, building a security system that integrates network transmission (terminal access, Wi-Fi, and wired links), spatial protection, and privacy protection is an important guarantee for digital government construction.

3.2.2 Recommended Networking Architecture

Typical government campus networks include various scenarios, such as government service hall and mobile office scenarios. The high-quality 10 Gbps government campus network solution provides a 10GE ultra-broadband network that features all-domain security and experience assurance to support digital government transformation.

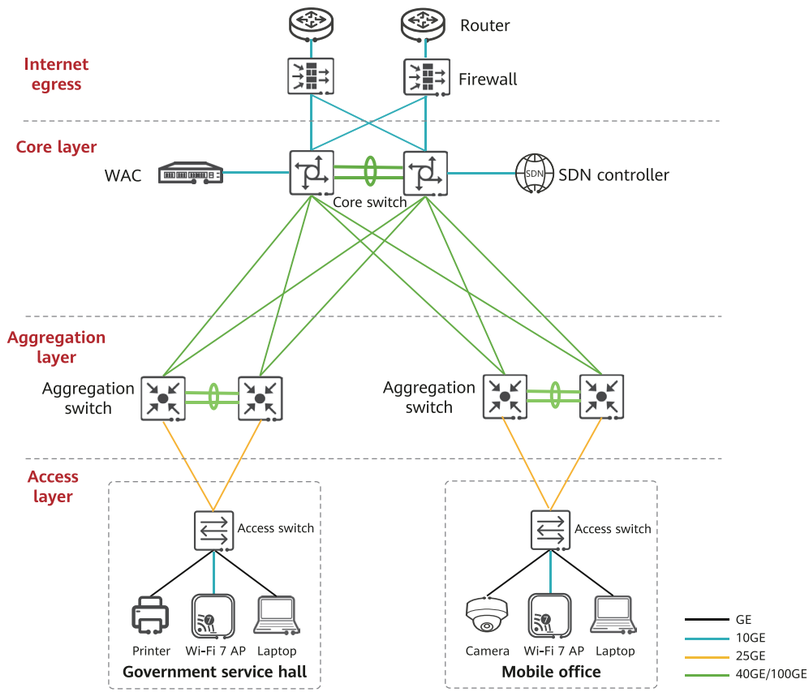


Figure 3-7 Recommended networking architecture

3.2.3 Government Service Hall

As an important window for interaction between the government and the public, government service halls are accelerating their transformation to "online-offline integration", as well as promoting "one network for all services" and "service handling across regions". These facilitate data sharing and intelligent services. Nowadays, government service handling is gradually shifted to online operations. In this way, government service halls can focus on complex services, consultation, and services for people with special needs. In addition, intelligence brings many service upgrades. For example, AI-powered customer services, AI-powered material pre-review, and AI-powered guide robots are rapidly popularized, reducing the pressure on employees at windows. Furthermore, applications such as VR-/AR-based virtual hall navigation and remote video assistance help improve user experience.

Figure 3-8 Smart government service hall

The intelligent upgrade of government service halls also poses new requirements on network infrastructure. First of all, an ultra-high-speed Wi-Fi network with blind-spot-free wide coverage is required to support mobile service handling anytime, anywhere for the public and employees. Next, intelligent applications, such as intelligent customer services and intelligent guide, need to respond in real time to reduce the waiting time of the public. This requires the network to provide high bandwidth, support heavy-traffic data transmission, and have low latency, thereby ensuring smooth service handling and quick system response. In addition, government services involve a large amount of personal privacy and enterprise confidential information. Considering this, the network must offer strong security protection.

The following table lists the recommended indicators for a high-quality 10 Gbps government service hall network.

Table 3-6 Recommended indicators for a high-quality 10 Gbps government service hall network

Item	Recommended Indicator
Bandwidth of access devices deployed indoors	≥ 10 Gbps
WLAN AP standard	Wi-Fi 7
Zero service interruptions upon movement in the government service hall	Supported
Wi-Fi anti-eavesdropping	WPA3 + physical noise–based interference protection
Unauthorized terminal access prevention and anti-spoofing	Supported

3.2.4 Mobile Office

As digital transformation accelerates, government agencies around the world are promoting wireless office to improve administrative efficiency, enhance flexibility, and optimize public services. Currently, mobile devices, such as laptops, tablets, and smartphones, are widely used by government employees for service handling anytime, anywhere. Wi-Fi networks bring convenience but also increase the risk of information leakage. Wi-Fi vulnerabilities (such as the Wi-Fi WPA2 Key Reinstallation Attack in 2017 and FragAttacks in 2021) around the world and Wi-Fi-targeted network attacks in various regions have intensified government customers' concerns about Wi-Fi security. Due to these, some government departments deploy Wi-Fi only in a few areas, hindering the development of wireless office.

The application of video conferencing by governments worldwide has been growing exponentially. According to statistics, 92% of national government agencies around the world have deployed cloud video conferencing systems in 2023, and the number of conferences has increased by 340% compared with that in 2020. By 2026, the market size of government video conferencing is expected to exceed USD8 billion, with a compound annual growth rate (CAGR) of over 18%. However, the ever-growing video conferencing applications pose higher requirements on network bandwidth, latency, and security protection.

The following table lists the recommended indicators for a high-quality 10 Gbps government mobile office network.

Table 3-7 Recommended indicators for a high-quality 10 Gbps government mobile office network

Item	Recommended Indicator
Bandwidth of access devices deployed indoors	≥ 10 Gbps
WLAN AP standard	Wi-Fi 7
Wi-Fi access: zero service interruptions and zero impacts on services when users move in the office area	Supported
Number of concurrent 4K HD video conferences	≥ 60 channels
Wi-Fi anti-eavesdropping	WPA3 + physical noise–based interference protection
Wired security	AP-switch full-link MACsec
Unauthorized terminal access prevention and anti-spoofing	Supported
Service-based security isolation for access terminals, preventing the lateral movement of risks	VXLAN tunnels and independent NMS deployment (compatible with third-party NMSs)
Network-security collaboration for near-source threat blocking	Collaboration with switches for threat blocking

3.2.5 Cases

3.2.5.1 A Municipal Government in South Africa

Key Challenges and Requirements

The city is one of the most urbanized and industrialized economic regions in South Africa. As part of a major metropolitan area, the city is home to leading education and medical resources and a highly skilled workforce. The city is accelerating digital transformation through smart city construction, while network bandwidth, coverage, and data security of electricity payment stations and office campuses serve as the pillar of its transformation.

Key Technologies

Broadband access 10 Gbps: Wi-Fi 7 APs provide high-speed wireless access and expand wireless network coverage. 10GE-capable multi-GE wired access switches provide high bandwidth, ensuring fast file download and higher office efficiency.

Full-scope security: The link-layer anti-eavesdropping technology on wireless air interfaces eliminates wireless security risks. Unauthorized users cannot capture wireless data of office personnel, ensuring secure data transmission over air interfaces.

Autonomous network: Visualized network management, unified management of network-wide devices, and minute-level fault locating improve network O&M efficiency.

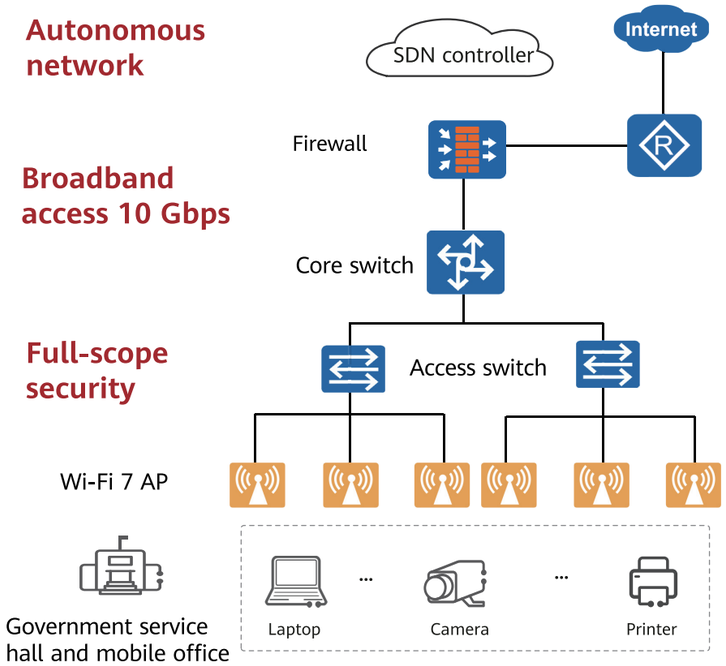


Figure 3-9 Networking diagram

Technology Advantages and Benefits

10 Gbps high bandwidth allows full coverage and network access anytime, anywhere. It also enables zero-lag transmission for large data and file transfers, meeting all daily office demands. The solution also prevents data eavesdropping and unauthorized storage, eliminating risks of capturing or leaking sensitive information such as electricity user information and payment data and safeguarding the office network. Intelligent O&M with automatic locating, inspection, and patrol capabilities provides real-time visibility into network quality, and supports one-click network fault rectification, improving O&M efficiency by 90%.

3.3 Finance Industry

3.3.1 Trends and Requirements

Digital transformation of financial institutions has gone through four eras: Bank 1.0 era where physical branches provide services, Bank 2.0 era where self-services such as ATM services are provided, Bank 3.0 era where services are provided anytime and anywhere through mobile portals such as apps, and Bank 4.0 era where FinTech redefines banking services. Powered by AI, banking services are evolving towards Bank 5.0.

In the Bank 5.0 era, banks are accelerating their intelligent and customer-centric upgrade to achieve efficient communication, intelligent operations, and scenario-based experience. In terms of efficient communication, banks widely deploy video conferencing, intelligent customer service, and enterprise collaboration platforms to implement real-time communication and efficient decision-making between HQs and branches. In terms of intelligent operations, AI, big data, and process automation are used to improve the intelligence level of risk control, operations scheduling, and IT system management, reduce operational costs, and enhance agility. In terms of scenario-based experience, smart terminals, remote tellers, queue-free experience, and online and offline integrated services are becoming standard, providing customers with more convenient, efficient, and personalized service experience.

Bank 5.0 poses higher requirements on the bank network infrastructure, which is expected to ensure stable running of service systems, support high-density access of massive terminals, guarantee low-latency transmission of remote video and data traffic, implement security isolation, and provide intelligent O&M capabilities, to build an agile, secure, and sustainable digital foundation.

3.3.2 Recommended Networking Architecture

Typical financial campus networks include smart office and smart outlet scenarios. The high-quality 10 Gbps financial campus network solution provides a 10GE ultra-broadband network that features all-domain security and deterministic experience to support Bank 5.0 evolution.

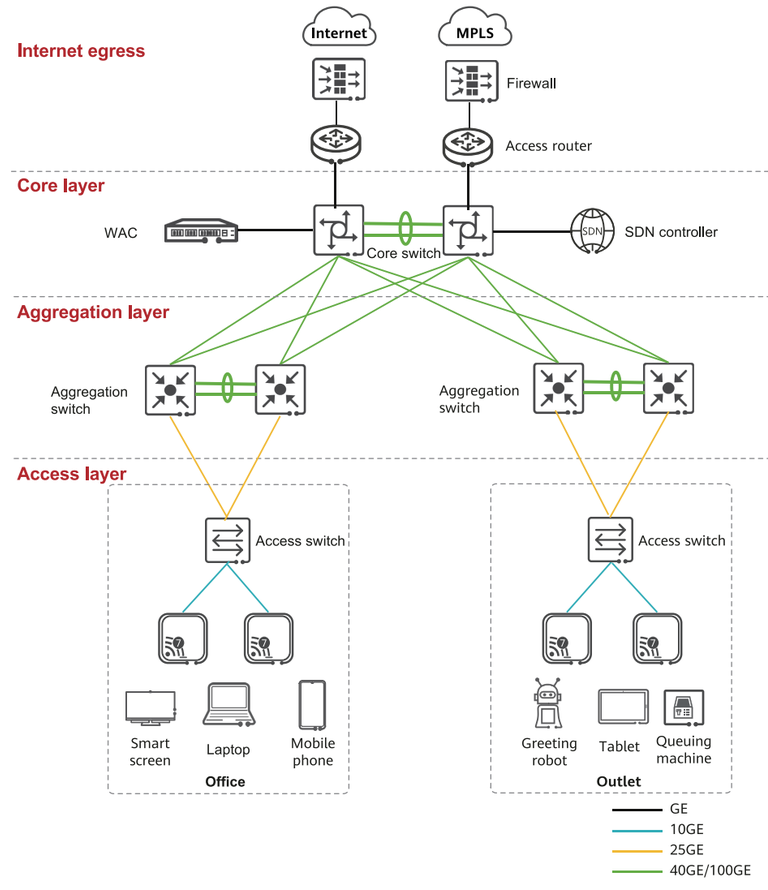


Figure 3-10 Recommended networking architecture

3.3.3 Smart Office

With the wide application of remote office and mobile devices, the number and types of IT terminals in the finance industry are increasing rapidly. These terminals are purchased by different departments through different sources, and are often managed by multiple siloed management platforms. As a result, the network cannot dynamically identify online terminals in real time or detect abnormal terminal behaviors, and unauthorized terminal access and spoofing occur frequently, bringing security risks to banking services. A network that can "see, distinguish, and manage" terminals, as well as provide wired and wireless security is urgently needed.

After the COVID-19 pandemic, hybrid office that becomes commonplace and the development of global operations have made video conferencing a core tool for cross-regional communication in the finance industry. According to Gartner's forecast, video conferencing usage will grow at a CAGR of 15% to 20% in the next three years. In addition, the flexibility of employees' access to the working environment anytime and anywhere, as well as the high requirements of the banking industry on data security and compliance, have also promoted the rapid popularization of cloud desktops in banks. Moreover, with the diversification of banking services and the increasing demand for cross-departmental collaboration, collaborative office applications such as Microsoft 365 have become important tools for improving efficiency, optimizing processes, and promoting digital transformation.

Figure 3-11 Bank employee working remotely on cloud desktop

The experience of core tools such as video conferencing, cloud desktops, and collaborative office applications directly affects employees' work efficiency. The finance industry is in urgent need of a high-quality network that can guarantee deterministic experience of key applications.

The following table lists the recommended indicators for a high-quality smart office network.

Table 3-8 Recommended indicators for a high-quality 10 Gbps smart finance office network

Item	Recommended Indicator
Bandwidth of access devices deployed indoors	≥ 10 Gbps
WLAN AP standard	Wi-Fi 7
Total throughput of 18 STAs connected to three APs in 80 MHz networking	≥ 960 Mbps
Concurrent channels of 4K HD video conferencing	≥ 60 channels
Definition and latency of key applications such as video conferencing and cloud desktop	1080p, latency < 100 ms
Service latency of key users	≤ 50 ms
Wi-Fi anti-eavesdropping	WPA3 + physical noise–based interference protection
Wired security	AP-switch full-link MACsec
Unauthorized terminal access prevention and anti-spoofing	Supported
Service-based security isolation for access terminals, preventing the lateral movement of risks	VXLAN tunnels and independent NMS deployment (compatible with third-party NMSs)
Network-security collaboration for near-source threat blocking	Collaboration with switches for threat blocking

3.3.4 Smart Outlet

Bank outlet is rapidly evolving from traditional service windows to intelligent, digital, and self-service integrated service platforms. The introduction of intelligent customer service, intelligent virtual teller machines (VTMs), and intelligent greeting robots provides efficient self-service options and cuts down customers' waiting time. Virtual financial consultants, metaverse bank experience areas, and AR-based product display have enhanced interactivity and improved customer experience and operations efficiency.

Figure 3-12 Smart bank outlet

Such business upgrades require a high-quality, highly integrated network that features fast deployment, high concurrency, high security, unified LAN/WAN management, and intelligent assurance for high-priority applications.

The following table lists the recommended indicators for a high-quality smart outlet network.

Table 3-9 Recommended indicators for a high-quality 10 Gbps smart finance outlet network

Item	Recommended Indicator
WLAN AP standard	Wi-Fi 7
No service interruption when smart terminals move in the outlet	Supported
Concurrent channels of 4K HD video conferencing	≥ 60 channels
Definition and latency of key applications such as video conferencing and cloud desktop	1080p, latency < 100 ms
Service latency of key users	≤ 50 ms
Service provisioning	Intent-driven deployment through natural language interaction and template-based deployment
O&M and management	Unified management of multiple outlets, and three-dimensional visualization of applications, terminals, and networks
Egress gateway	Hyper-converged gateway, integrating functions such as 5G, WAC, routing, security, and switching
Wi-Fi anti-eavesdropping	WPA3 + physical noise–based interference protection
Wired security	AP-switch full-link MACsec
Unauthorized terminal access prevention and anti-spoofing	Supported
Network-security collaboration for near-source threat blocking	Collaboration with switches for threat blocking

3.3.5 Cases

3.3.5.1 A Bank in Kenya

Key Challenges and Requirements

The bank has significant influence in Kenya's financial services sector. The bank improves its service capabilities through technological innovation and digital transformation, providing real-time financial services to more than 30 million users. Facing the development trend of global fintech, the bank is upgrading its core system to cope with the traffic burst of mobile services, and enhancing the technical adaptability of the system to new services and features to meet the increasing demands of users. This digital transformation not only improves service efficiency and quality, but also helps the bank maintain its leading position in the industry and provide better and more convenient financial services for users in Kenya and beyond.

Key Technologies

Broadband access 10 Gbps: Devices support flexible switching between triple-radio and dual-radio modes and provide a rate of up to 5.95 Gbps. The built-in smart antennas can automatically adjust directions to ensure always-on signals for users. This significantly enhances users' wireless experience and enables the network to respond quickly during peak hours or when a large number of users use services simultaneously.

Autonomous network: The solution provides full-lifecycle campus network automation, intelligent fault auto-solving based on big data and AI, automatic discovery of network devices, fault information collection, and rectification solution recommendation.

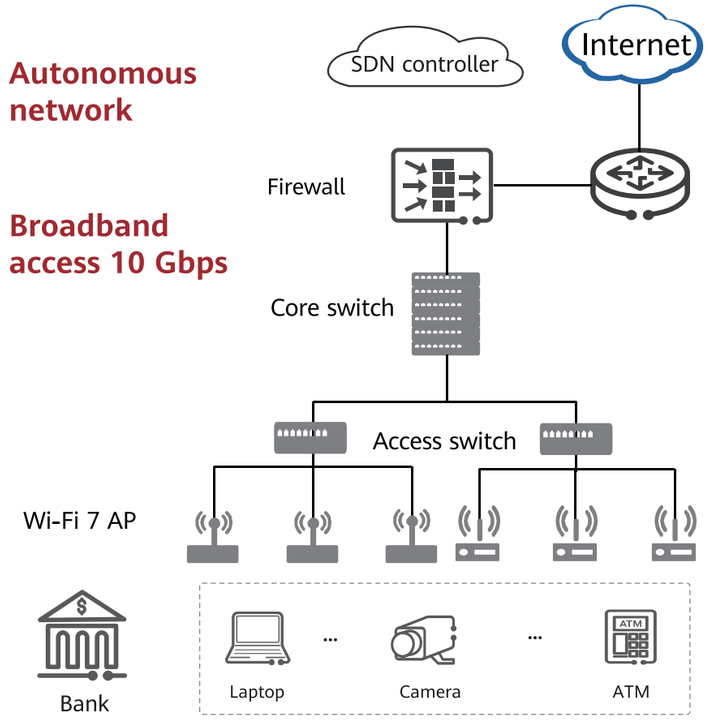


Figure 3-13 Networking diagram

Technology Advantages and Benefits

Full Wi-Fi coverage improves the work efficiency of bank staff and meets the network access requirements of customers, implementing wireless service handling. Files such as banking service materials are uploaded and downloaded at a high speed, improving the service efficiency of bank staff. Video conferences are free from disconnection and freezing, and data transmission experiences zero failures. The financial network is visualized with just one click, and network faults can be located in minutes, significantly improving O&M efficiency and reducing the network fault locating time by 95%.

3.4 Healthcare Industry

3.4.1 Trends and Requirements

Currently, hospitals are in the transition period from full integration to intelligence. In the past, siloed applications and data silos cannot support healthcare services well. How to implement data interconnection and sharing across the hospital and maximize the value of healthcare data in clinical diagnosis and treatment has always been an urgent issue for hospitals. Smart hospital construction implements hospital-wide data integration, strict data security control, and medical data invoking and intelligent warning system that complies with international healthcare standards. This ensures the integrity, validity, and security of patients' healthcare data, effectively optimizes hospital resources, and improves the overall operation efficiency and competitiveness of hospitals.

In 2024, the number of outpatient and emergency visits in Chinese hospitals exceeded 2.38 billion, the number of inpatient visits exceeded 200 million, and the number of surgeries exceeded 80 million. To meet the huge demand for healthcare services, improving outpatient service quality, ward management efficiency, and critically ill patient surgery is an important means to ensure healthcare service quality and accelerate the construction of smart hospitals.

3.4.2 Recommended Networking Architecture

A typical healthcare campus network covers outpatient, inpatient, and operating room scenarios. The high-quality 10 Gbps healthcare campus network provides 10 Gbps ultra-broadband, all-domain security, and ubiquitous connectivity to meet the requirements of smart healthcare construction.

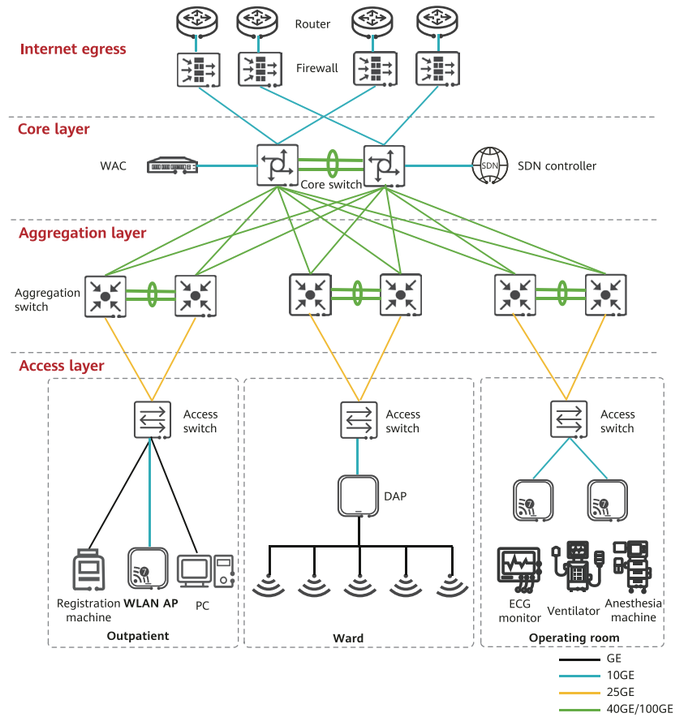


Figure 3-14 Recommended Networking Architecture

3.4.3 Smart Outpatient Service

Outpatient services are the window of hospital services, and the quality of outpatient services directly affects the image of a hospital. In 2024, the number of outpatient and emergency visits in China exceeded 2.38 billion, but the number of doctors and nurses nationwide was less than 10 million. The extremely low doctor-patient ratio results in long registration, payment, and waiting time, as well as short consultation time (less than 10 minutes), which is a long-standing problem. In contrast, the non-consultation time can be as long as 40 to 80 minutes.

Figure 3-15 Patients queuing for medical treatment

Outpatients use the IoT to implement remote device monitoring, intelligent management, and data integration, reducing manual operations and improving diagnosis and treatment precision. However, the IoT is constructed by phase based on requirements, which may lead to conflicts and interference between the wireless network and IoT signals, repeated cabling, long construction period, high costs, multi-protocol incompatibility, and difficult data integration.

The following table lists the recommended indicators for a high-quality smart outpatient network.

Table 3-10 Recommended indicators for a high-quality 10 Gbps smart outpatient network

Item	Recommended Indicator
Bandwidth of access devices deployed indoors	≥ 10 Gbps
WLAN AP standard	Wi-Fi 7
Wi-Fi access of STAs, ensuring uninterrupted services when STAs move in the outpatient department	Supported
IoT construction mode	WLAN APs are integrated with IoT to form a unified network.
GB-level medical image retrieval speed	In seconds
Total throughput of concurrent Wi-Fi access of 30 users	≥ 340 Mbps

3.4.4 Smart Ward

After being consulted and examined by an outpatient doctor, if a patient needs further treatment, the patient needs to be hospitalized. In 2024, the patient-bed ratio in Chinese hospitals with more than 500 beds was 1.2 to 1.5, while that of the Mayo Clinic in the United States was 28.2, a difference of nearly 20 times. The extremely low patient-bed ratio results in heavy workloads for healthcare personnel. 50% of healthcare personnel work overtime for more than 60 hours per month.

Currently, wireless PDAs are mainly used for mobile ward rounds to view patients' medical records, record patients' diagnosis and treatment data, and deliver doctors' medical advice. However, doctors need to shuttle between different wards during ward rounds, and packet loss may occur when PDAs roam between APs. Consequently, doctors need to log in to PDAs repeatedly, severely affecting the ward round efficiency.

Figure 3-16 Mobile ward round with a wireless PDA

The following table lists the recommended indicators for a high-quality smart ward network.

Table 3-11 Recommended indicators for a high-quality 10 Gbps smart outpatient network

Item	Recommended Indicator
Zero roaming of PDAs and zero service interruption during mobile ward rounds	Supported
Bandwidth of access devices deployed indoors	≥ 2.5 Gbps
WLAN AP standard	Wi-Fi 7
Integration of the intranet, extranet, and IoT	Supported
Cuffless heart rate, respiratory frequency, and fall monitoring	Supported

3.4.5 Smart Operating Room

The ICU provides systematic, high-quality, and centralized healthcare monitoring and treatment for patients with severe or critical illnesses. There are dozens of types of bedside devices in ICUs. In addition to basic devices such as the monitor, ventilator, infusion pump, and micro-injection pump, other devices such as the defibrillator, ECG machine, pacemaker, and blood gas analyzer may also be deployed as required. The anesthesiologist in an operating room is also one of the most critical roles in protecting patients. During an operation, the anesthesiologist needs to pay close attention to the patient's vital signs displayed on various medical devices and intervene in a timely manner.

More and more advanced devices are used in ICUs and operating rooms, greatly improving the timeliness and success rate of treatment. However, due to various types of devices, vendors, and standards, different devices work independently and are not interoperable, and a large amount of clinical data generated in ICUs and operating rooms needs to be manually recorded and analyzed by healthcare personnel, which brings a heavy burden to healthcare personnel. In addition, the value of clinical data cannot be maximized due to discontinuous and non-standard data manually recorded.

Figure 3-17 Smart operating room

The following table lists the recommended indicators for a high-quality smart operating room network.

Table 3-12 Recommended indicators for a high-quality 10 Gbps smart operating room network

Item	Recommended Indicator
Bandwidth of access devices deployed indoors	≥ 10 Gbps
WLAN AP standard	Wi-Fi 7
Integration of the intranet, extranet, and IoT	Supported
Core switch upgrade without service interruption	Supported

3.4.6 Cases

3.4.6.1 A Hospital in the UAE

Key Challenges and Requirements

The hospital in the United Arab Emirates (UAE) was established in the 20th century. It develops strategies for the health system, ensuring the delivery of high-quality medical services through continuous assessment of population health. Amidst the digital transformation surge, the hospital upgraded its network with full consideration of advancement and innovation by leveraging cutting-edge emerging technologies, ensuring it became mobile, digital, and intelligent.

Key Technologies

Broadband access 10 Gbps: 10GE-capable access switches provide ultra-high access bandwidth. The core switches support 100GE ports. Wi-Fi 7 APs and smart roaming ensure uninterrupted mobile services of terminals.

Autonomous network: M × N modular deployment can quickly complete device configuration and deliver services in minutes. Centered on user experience, the solution provides refined network O&M. With big data and AI models, network issues can be predicted in advance, making campus network O&M visualized, intelligent, and efficient.

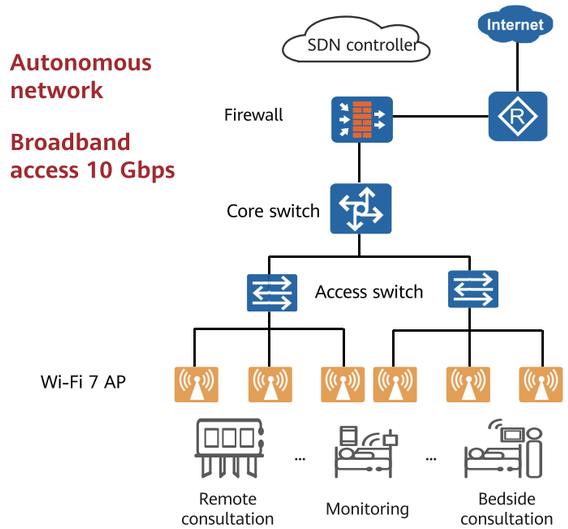


Figure 3-18 Networking diagram

Technology Advantages and Benefits

The solution meets the ultra-high bandwidth requirements of access devices and offers excellent office experience. Full Wi-Fi 7 network coverage with ultra-high bandwidth and ultra-low latency provides strong support for future network service expansion in the next 5 to 10 years. Fast service deployment and simplified network management slash the network OPEX by 63%.

3.5 Manufacturing Industry

3.5.1 Trends and Requirements

Intelligent manufacturing is becoming more digitalized, intelligent, and flexible. With the converged application of technologies such as the industrial Internet of Things (IIoT), artificial intelligence (AI), 5G, and edge computing, manufacturing enterprises are gradually achieving device interconnection, data-driven operations, process collaboration, and autonomous decision-making, and evolving towards predictive maintenance, flexible production lines, tailored customization, and sustainable operations. In the future, intelligent manufacturing will focus on digital twins and industrial foundation models to promote intelligent collaboration and full-lifecycle optimization of industry chains, driving high-quality and sustainable transformation and upgrade of the manufacturing industry.

The network is a foundation for the evolution toward intelligent manufacturing. It connects various factors of production such as people, machines, materials, methods, and environments, and provides support for data generation, collection, transfer, processing, and monetization. To build a network base, various factors of production need to be connected to the network, and the connection requirements of factors of production and upper-layer applications need to be met. Centering on the value chain, manufacturing enterprises demand for stable production, flexible manufacturing, fast R&D, and safe operations during transformation and upgrade towards intelligent manufacturing in terms of R&D, production, and operations.

3.5.2 Recommended Networking Architecture

A typical manufacturing network achieves IT and OT convergence, eliminates data silos, and integrates systems such as the MES, ERP, SCADA, and PLC into a unified network, achieving real-time data collection, analysis, and feedback. The network supports applications such as predictive maintenance, production line optimization, and flexible production, and also enables real-time service collaboration, precise decision-making, and continuous innovation, laying a foundation for intelligent manufacturing.

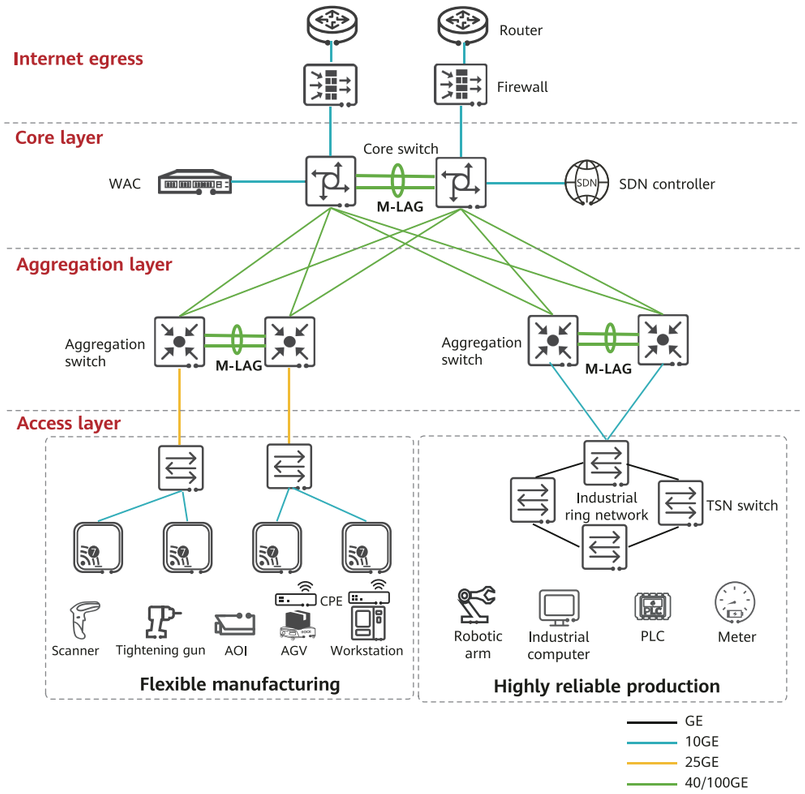


Figure 3-19 Recommended networking architecture

3.5.3 Highly Reliable Converged Production Network

For manufacturing enterprises, each production unit has its own production capacity indicators and production cycle time requirements. For example, for SAIC Motor's factory in Ningde, the production cycle time is 60 jobs per hour (JPH). This means one car is produced every minute. Any service interruptions may affect the production. For instance, 14 factories of a famous Japanese automaker stopped production for 1.5 days due to IT system faults, which directly affected the production and delivery of 14,000 cars. Stable mass production is to ensure the stability and continuity of the production process and execute the production plan, preventing economic losses. To achieve stable mass production, reliability management is required in all aspects such as people, machines, materials, methods, and environment, such as raw materials, energy meters, and production equipment. As the data connection foundation, the network connects the production management and execution systems (such as the ERP, MES, SCADA, PLC, and I/O). It needs to provide all-time online and highly reliable connections to ensure the production continuity of enterprises.

Customized and diversified products are becoming a new normal in the manufacturing industry. In addition, enterprises are actively promoting flexible manufacturing to accelerate delivery, reduce production costs, and improve equipment utilization. According to a market research, the compound annual growth rate (CAGR) of the global flexible manufacturing market in the next five years will reach 20%. Since manufacturing enterprises need to adjust production processes according to orders, the production line adjustment efficiency as well as the flexibility of production equipment and even the entire workshop become a major concern of enterprises. As such, enterprises need to adopt automation, robotics, and smart logistics technologies to build flexible manufacturing systems. The network also needs to adapt to scenario-specific production line adjustment requirements and provide flexible access to related terminals. The traditional wired network access mode involves access point planning and cabling, and cannot meet the flexible manufacturing requirements. Wireless networks enable production equipment to go wireless, and therefore are being gradually deployed at scale in manufacturing enterprises.

Figure 3-20 Smart flexible manufacturing factory

Industrial quality inspection is becoming more intelligent and automated. AI visualization, multi-modal sensors, and edge computing are widely used to implement high-precision and efficient defect identification and real-time quality control. As the number of inspection devices and image data surges, quality inspection imposes higher network requirements. The network is required to provide high bandwidth, low latency, strong isolation, and high reliability to ensure stable backhaul of HD videos, real-time inference and linkage, and closed-loop data analysis.

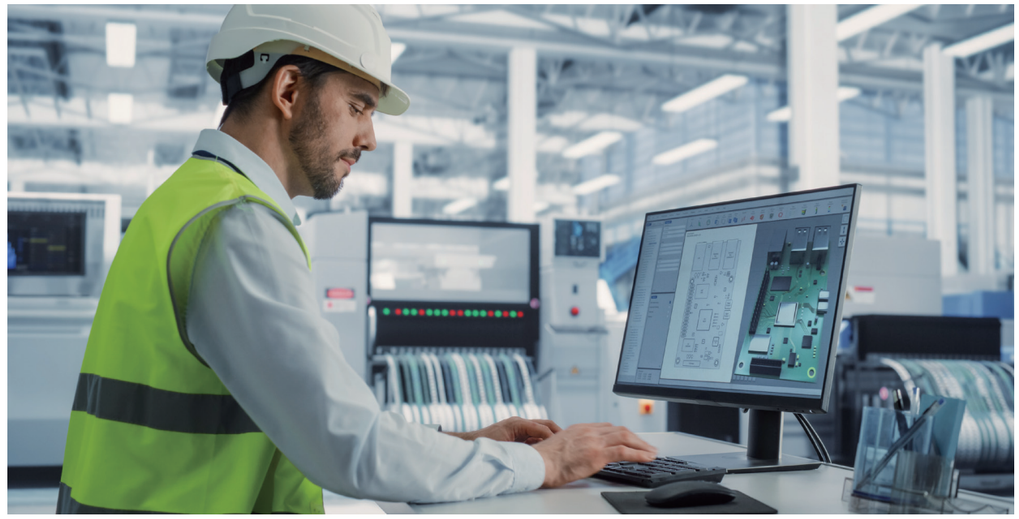


Figure 3-21 AI-based HD quality inspection

Manufacturing enterprises need to protect their fixed assets and information assets from internal and external attacks. As digital transformation continues to sweep across the manufacturing industry, manufacturing enterprises typically have tens of thousands of production devices that are connected to or about to connect to the network in a single factory. The convergence of IT and OT promotes seamless flow of high-value data and blurs the original security boundaries. In this case, ensuring network security is particularly important for secure operations of enterprises.

The following table lists the recommended indicators of a highly reliable converged production network.

Table 3-13 Recommended indicators of a highly reliable converged production network

Item	Recommended Indicator
WLAN AP standard	Wi-Fi 7
Maximum single-user Wi-Fi rate	≥ 3.5 Gbps
Packet loss rate in Wi-Fi roaming	≤ 0.1%
Switchover time upon a link fault	≤ 50 ms, without service interruption
Switchover time upon an industrial ring network fault	≤ 20 ms
Going-wireless of workstations	Dual fed and selective receiving, ensuring service continuity during roaming
1588v2 clock precision @ 64 hops	1 μs
Video definition and latency of key applications such as video conferencing and cloud desktop	1080p: latency < 100 ms
Service latency of key users	≤ 50 ms
Unified O&M for IT/OT networks	Supported

3.5.4 Cases

3.5.4.1 RiaStone Factory (Visabeira Group)

Key Challenges and Requirements

The RiaStone Factory, part of the Visabeira Group, manufactures ceramic tableware. The factory provided a live industrial environment used to assess communication technologies for Industry 4.0 use cases, validating the usage of Wi-Fi 7 and TSN technologies to deploy newly envisioned use cases.

The factory manifested different challenges, highlighted in the following:

- **Quality Control Point (QCP):** This entity required real-time monitoring and fault detection by transferring high-resolution images (over 15 to 120 MB, compressed to 15 to 18.5 MB) to an AI server (YOLOv5) for defect detection. This demands high throughput and high reliability.
- **Security video streaming:** In the factory, there are multiple high-quality video streams from cameras, requiring the network to handle their transport over a fast and reliable wireless medium.
- **Smartwatches:** Due to the large size and high noise levels of the factory, its operators struggled to constantly monitor all equipment. The factory's existing Wi-Fi network provided unreliable connectivity for small smartwatch antennas, making timely alerts ineffective.
- **AGV:** The existence of AGVs at the factory provided a testing opportunity for both improved communications and seamless handover performance.
- **Pressing machines impacted by network traffic:** The factory's pressing machines were halted because their network-enabled latency-sensitive Manufacturing Executing System (MES, which handles, e.g., monitoring and control) features were being disrupted by the underlying network traffic.

Key Technologies

The Wi-Fi 7 network was coupled with Multi-Link Operation (MLO) capabilities, with the tests utilizing frequency bands including 2.4 GHz, 5 GHz, and 6 GHz. Wi-Fi 7 leverages such bands, along with 320 MHz bandwidth, 4096-QAM modulation, Multiple Resource Unit (MRU), and MLO to increase throughput to 23 Gbps. TSN was also deployed by implementing traffic prioritization. Internal press communication was placed in queues 5, 6, and 7 based on criticality, while factory network traffic used queues 0, 1, 2, and 3.

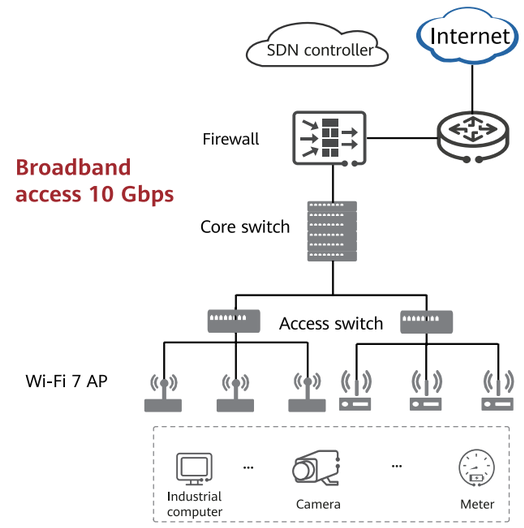


Figure 3-22 Networking diagram

Technology Advantages and Benefits

Wi-Fi 7 demonstrated consistently higher throughput and lower latency compared to Wi-Fi 6. The performance advantage was particularly evident when utilizing wider bandwidths (160 MHz and 320 MHz) and MLO.

The tri-band MLO (2.4 GHz, 5 GHz, and 6 GHz) achieved the highest spectral efficiency at 12.65 Mbps/MHz and supported 228 concurrent streams in downlink tests.

It provided enhanced mobility for mobile devices, achieving lower packet loss and reduced RTTs, compared to Wi-Fi 6 in multi-band configurations. In high-demand media cases, such as the QCP, Wi-Fi 7 significantly improved performance, ensuring the reliable transfer of large, high-resolution images with no losses throughout testing. All factory operational and timing requirements were satisfied using the Wi-Fi 7 network.

The simple upgrade of the existing factory's Wi-Fi to Wi-Fi 7, not only enabled previously unfeasible use cases (e.g., the Smartwatch usage in factory), where Wi-Fi 7's more powerful PoE-enabled hardware was able to significantly improve coverage and communications, despite the end user devices only supporting up to Wi-Fi 5.

Deterministic performance was achieved in the press use case, with TSN guaranteeing real-time communication with low latency, low jitter, and zero packet loss, even under constrained network operations.

TSN solved a critical operational challenge by enabling the integration of isolated press machines into the factory's MES, allowing them to be monitored, controlled, and automated.
Simple configuration is a feature achieved by only having to define the TSN flow on the first switch along the communication path, to ensure prioritization throughout the network. This drastically reduces the complexity of configuration, management, and maintenance in operational environments. This finding supports the potential for adopting an interface-based TSN approach to simplify deployment for industrial IT staff.

3.6 Retail Industry

3.6.1 Trends and Requirements

The retail industry is rapidly integrating digital transformation with omnichannel retail. For example, retailers are using multiple channels, including e-commerce platforms, offline stores, mobile apps, social media, and smart devices, to connect with consumers and deliver seamless shopping experience. Driven by various technologies, such as AI, IoT, cloud computing, and big data analytics, applications like personalized recommendations, automated warehousing and distribution, and intelligent customer service are gradually enhancing customer experience and operational efficiency, thereby accelerating the transition toward smart retail.

Amid growing consumer demand for personalized, convenient, and instant shopping experience, retailers are increasingly investing in smart stores. As the core of digital retail transformation, these stores leverage various innovative technologies, such as IoT, AI, AR/VR, and smart shopping guide, to achieve intelligent upgrades for people, goods, and spaces. These upgrades deliver more convenient and seamless shopping experience.

3.6.2 Recommended Networking Architecture

A typical smart store network integrates IoT, AI, big data analytics, and automation technologies to enable real-time intelligent interconnection of all elements — people, goods, and spaces. This provides customers with personalized, seamless, and convenient shopping experience while enabling efficient and intelligent operations management.

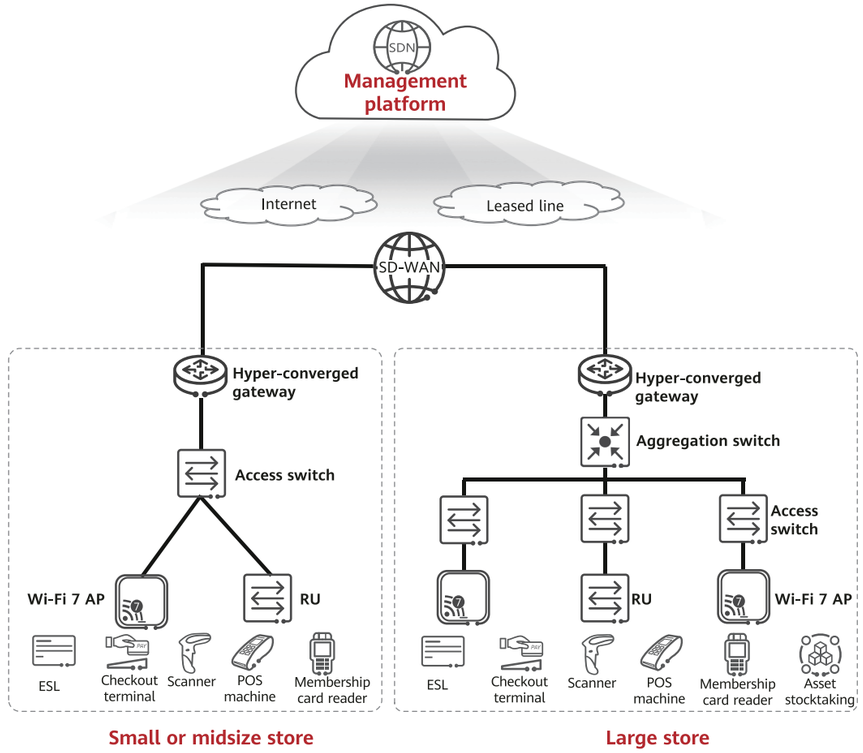


Figure 3-23 Recommended networking architecture

3.6.3 Smart Retail Store

Traditional stores use paper labels to mark product prices, which is inefficient, error-prone, and inflexible. Due to this, an increasing number of stores are now adopting electronic shelf labels (ESLs). ESLs can automatically synchronize prices, promotional details, and inventory status, avoiding errors and delays caused by manual label updates. Additionally, ESLs provide clear displays and dynamic content, enhancing both shopping convenience and interactive experience for customers. They are also environmentally friendly, reducing paper waste while offering retailers a more flexible and precise method of operations and marketing.

Figure 3-24 ESLs

In response to rapidly changing market competition and consumer demands, retailers require standardized, automated, digital, and flexible operations to ensure agile service rollout in stores in a short time. Additionally, centralized management is required to provide multi-dimensional visibility and rapid fault locating across the store network, thereby reducing OPEX and improving operational efficiency.

The following table lists the recommended indicators for a high-quality smart store network.

Table 3-14 Recommended indicators for a high-quality smart store network

Item	Recommended Indicator
WLAN AP standard	Wi-Fi 7
ESL deployment	PCIe cards, containers, and built-in protocols (such as Bluetooth and ZigBee) integrated into WLAN APs
Service provisioning	Intent-driven deployment through natural language interaction and template-based deployment
O&M and management	Unified management of LANs and WANs for multiple stores, and three-dimensional visibility into applications, terminals, and networks
Egress gateway	Hyper-converged gateway, integrating functions such as 5G, WAC, routing, security, and switching

3.6.4 Cases

3.6.4.1 A Chain Retailer in Germany

Key Challenges and Requirements

The large chain retailer in Germany has numerous stores. Driven by continuous business expansion, the retailer opens more than 10 new stores each year, needing to deploy over 300 new network devices. Network configuration before the opening of new stores, commodity price adjustment, and asset stocktaking in stores all require the network to provide high bandwidth and intelligence.

Key Technologies

Autonomous network: After the network administrator selects the service scenario and requirements on the GUI, service planning and configuration generation are automatically completed. Since the network configurations are streamlined within stores of the same scale, M × N template-based configuration can be used for building block–like construction: Deployment tasks can be customized in drag-and-drop mode on the GUI, and differentiated modifications can be made. A single template can be copied to other sites in batches.

Broadband access 10 Gbps: Smart antennas provide full wireless coverage for stores.

Connect everything: The solution innovatively integrates IoT cards that support multiple communication modes, such as Bluetooth, ZigBee, and RFID, helping the enterprise quickly build an IoT network for ESLs and asset stocktaking.

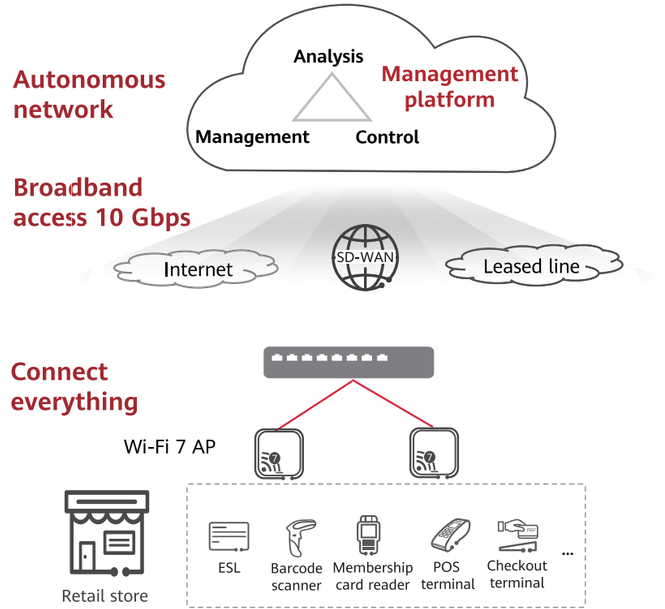


Figure 3-25 Networking diagram

Technology Advantages and Benefits

Wireless coverage without blind spots improves customers' shopping experience. Fast store network configuration and service provisioning shortens the deployment time of a single site to 30 minutes. ESL and automatic asset stocktaking are implemented on one network, improving efficiency by 90%. Local cloud-based deployment of the intelligent O&M system enables visualized management and improves O&M efficiency by 50%.

3.7 Hotel Industry

3.7.1 Trends and Requirements

The hotel industry is transforming towards digitalization, personalization, and sustainable development. As guests increasingly demand personalized services, hotels are using smart devices, mobile apps, AI-driven personalized recommendations, virtual assistants, and many other technologies to improve guest experience. At the same time, the hotel industry is focusing on environmental protection and sustainable development, with green hotels and energy-saving buildings gradually becoming industry standards.

Network infrastructure is the cornerstone of digital hotel transformation. It not only supports the stable running of all smart devices and applications, but also increases operational efficiency, improves guest experience, enhances security, and facilitates data analysis and marketing. With the continuous development of technologies and the change of guest requirements, the reliability, scalability, and security of the hotel network infrastructure determine the competitiveness of hotels in the future market.

3.7.2 Recommended Networking Architecture

A typical hotel network uses various technologies (such as IoT convergence and AI) to ensure high network speed and stability. Also, solutions featuring high security, flexibility, automation, and scalability are available to guests for enjoying smooth and personalized experience when they use various devices and services. This supports the digital transformation of modern hotels, increases operational efficiency, and improves guest satisfaction.

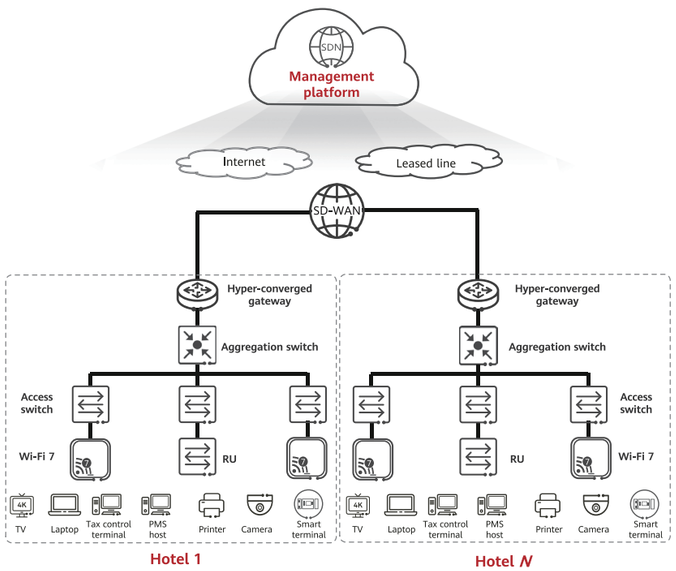


Figure 3-26 Recommended networking architecture

3.7.3 Smart Hotel

Smart hotels require a high-performance, full-coverage, and intelligent wireless network to provide stable and high-speed wireless connections in all areas, such as guest rooms, public areas, conference rooms, and restaurants. Also, the network must provide high bandwidth and low latency to support multiple heavy-traffic applications, such as smart devices, IoT applications, video streams, mobile payment, and smart control systems. Moreover, the network must support high concurrent connections to ensure smooth running during peak hours. This improves guest experience and increases operational efficiency.

Hotel chains around the world bring new opportunities for hotel network deployment. To quickly respond to market changes, shorten the opening time, reduce costs, and improve operational flexibility, hotels hope to complete the opening and operations of new branches in a short time to adapt to rapid market changes and fierce competition.

Hotels have increasing requirements for energy saving. They gradually adopt technologies such as energy-saving building design, renewable energy (such as solar energy and wind energy), dynamic network energy saving, intelligent lighting/air conditioning system optimization, and efficient water resource management to reduce energy consumption and operating costs.

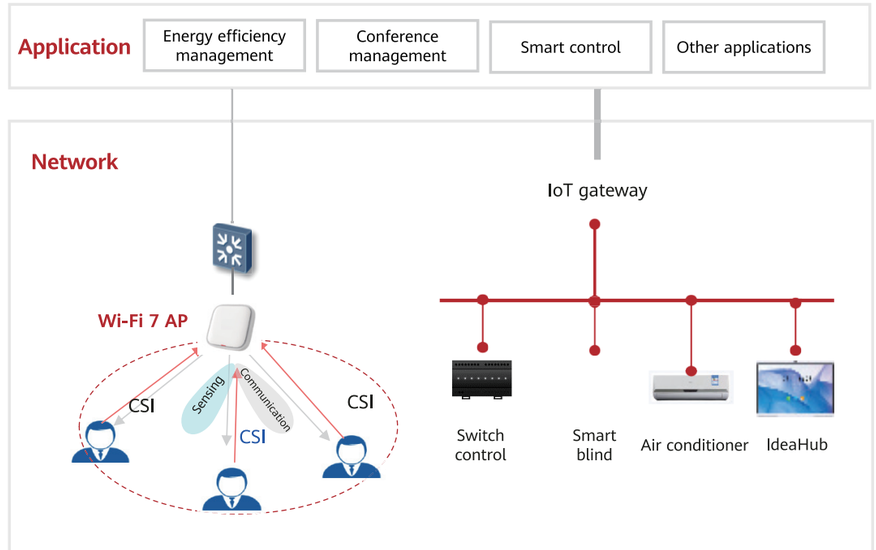


Figure 3-27 Wi-Fi CSI-based precise personnel sensing, linked with building control systems to save energy

In the hotel industry, unauthorized filming tends to be covert, miniaturized, and remote, which severely infringes on guest privacy. Worse yet, it damages the hotel brand image and diminishes guest trust. Therefore, unauthorized filming has become a security risk that the industry urgently needs to address.

Figure 3-28 Pervasive spy cameras

The following table lists the recommended indicators for a high-quality smart hotel network.

Table 3-15 Recommended indicators for a high-quality smart hotel network

Item	Recommended Indicator
WLAN AP standard	Wi-Fi 7
Single-user maximum Wi-Fi rate	≥ 3.5 Gbps
Packet loss rate during Wi-Fi roaming	≤ 0.1%
Energy saving	Dynamic energy saving of APs and energy saving based on Wi-Fi CSI sensing
Service provisioning	Intent-driven deployment through natural language interaction and template-based deployment
O&M and management	Unified management of multiple stores, and three-dimensional visibility into applications, terminals, and networks
Privacy security	Unauthorized camera detection integrated in WLAN APs

3.7.4 Cases

3.7.4.1 A Hotel Chain in Italy

Key Challenges and Requirements

The hotel in Italy has recently renovated its rooms and suites to provide a unique, excellent, and home-like experience for guests from all over the world. High-quality Wi-Fi is now essential for hotel guests, especially in luxury hotels where a high-performance, zero-blind-spot wireless network is a must. On one hand, the network provides unparalleled Wi-Fi experience for hotel guests. They can easily get online for work and entertainment, and stay connected with loved ones. Such seamless connections improve the guests' satisfaction. On the other hand, hotel staff can provide high-quality services for guests through this network, making everything from check-in to room service faster and more efficient. The network also boosts communication efficiency and strengthens overall hotel operations.

Key Technologies

Broadband access 10 Gbps: Smart roaming ensures hotel guests are always online. High-performance APs are applicable to different scenarios and support concurrent access of hundreds of devices.

Full-scope security: End-to-end security protection safeguards data assets of users and carriers.

Autonomous network: The solution supports unified LAN/WAN management, plug-and-play, template-based fast deployment, and unified O&M.

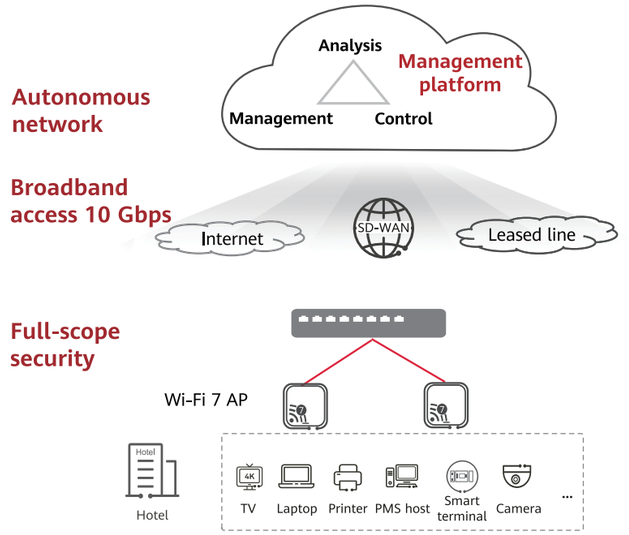


Figure 3-29 Networking diagram

Technology Advantages and Benefits

The NMS manages network-wide devices in a unified manner, ensuring network health. With software-defined networking (SDN), a traditional network can be upgraded to a future-oriented network with just a few clicks. The high-quality 10 Gbps hotel network reshaped the connectivity experience, enabling guests and staff to adapt seamlessly to today's fast-paced, intelligent world. It empowers the hotel to deliver an enhanced stay experience and establish itself as a benchmark for smart hotels in Europe.

3.8 Stadium Scenario

3.8.1 Trends and Requirements

Digital intelligence integration: By deploying IoT devices and sensors to build an omnipresent interconnected network, smart venues are achieving full digitalization through cross-system data collection and fusion. Meanwhile, the synergistic application of large-scale pre-trained models (large models) and customized vertical domain models (small models) drives the transition toward "comprehensive intelligence."

Convergence of physical and virtual realms: Smart stadiums transcend physical boundaries by leveraging augmented reality (AR), virtual reality (VR), and digital twin technologies to create hybrid virtual-physical experiences. For example, AR navigation provides real-time seat information and event updates, while VR enables immersive virtual spectatorship.

Resilience-driven reliability: As a scenario characterized by high-density personnel gathering and high-concurrency service bearing, the network reliability of the stadium serves as the core cornerstone for ensuring event operation, spectator experience, and smart services. Targeting the extreme scenario of 100,000-level concurrent terminal access during large-scale events, the network must be equipped with millisecond-level fault self-healing capability to guarantee zero interruption of core services such as high-definition event broadcasting and IoT device joint control.

Green and low carbon: Based on the highly fluctuating crowd flow in the stadium, the campus network must possess tidal prediction and sensing capabilities. During non-event periods or low-load hours, the system automatically switches to deep sleep or shutdown mode through intelligent algorithms. During high-concurrency event periods, the system supports wake-up within seconds, enabling refined energy consumption control for the stadium network, and building an energy-efficient, environmentally friendly "low-carbon" smart stadium foundation.

3.8.2 Recommended Networking Architecture

Based on the actual service needs of the stadium, the entire network is planned and designed into five separate networks based on service types and functions: public network, office network, competition network, security network, and device network.

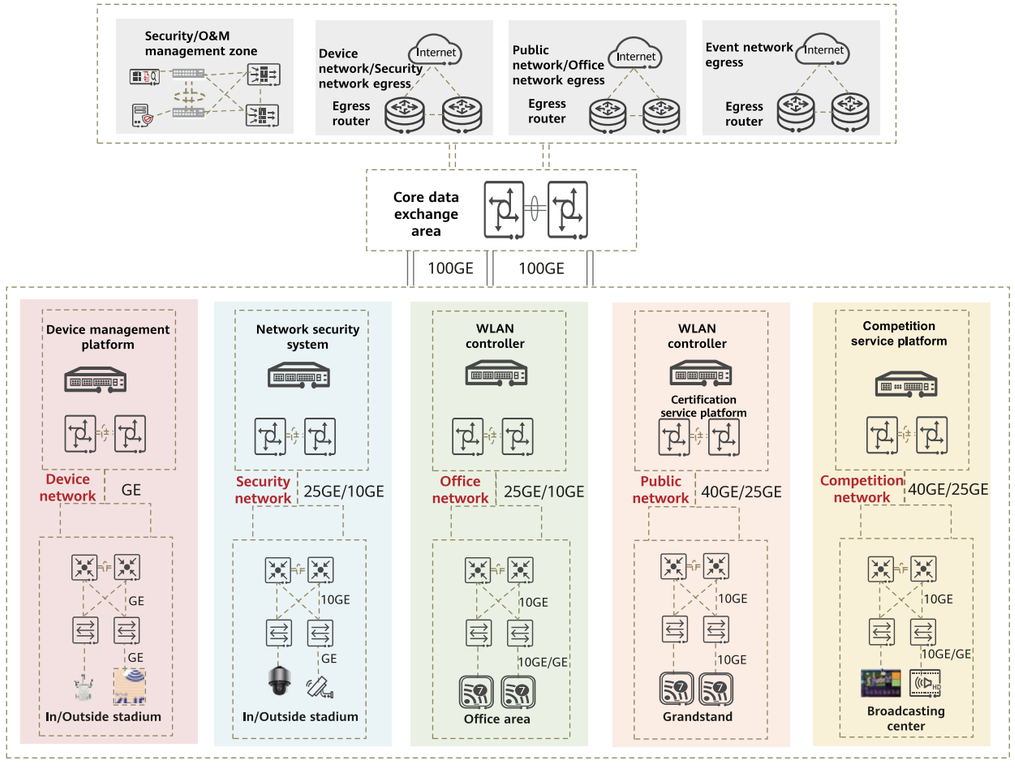


Figure 3-30 Recommended networking architecture

Public network
The public network provides access services for spectators' mobile terminals. It primarily uses Wi-Fi and adopts a three-layer architecture of core, aggregation, and access layers.

Office network
The office network primarily carries the office data for the normal operation of the stadium, as well as unified work orders, stadium scheduling, smart operations, and ordinary office scenarios, providing Internet access and communication functions for the stadium staff, while also offering access services for remote branch offices of the stadium operators.

Competition network
The competition network mainly provides office access services for competition personnel and judges, and provides distribution services for competition videos.

Security network
The security network mainly provides access for cameras of the security management system. Since the system generates large amounts of traffic and requires constant transmission, it is necessary to ensure sufficient bandwidth and reliability for the traffic.

Device network
The device network primarily provides access services for systems such as the access control system, alarm system, patrol system, parking management system, and some IoT devices, such as information display and building equipment monitoring.

3.8.3 Smart Stadium

With the rapid development of technologies such as multimedia live streaming, 4K video, IoT, and AI, there is a significant increase in service volume and data traffic. A high-speed network can handle massive data traffic, thereby enabling the stadium to effectively support these new technologies to ensure the advancement of information systems.

The foundational network of the stadium supports various operations, including live broadcasting of matches, Internet access for spectators, security monitoring, and daily office tasks for stadium staff. Reliability is the cornerstone of sustainable smart stadium operations. The smart stadium network architecture provides a three-level redundancy design to ensure the reliability of daily matches. The first-level network redundancy design ensures network reliability when network devices or links fail. The second-level application experience assurance design ensures experience protection for critical services, real-time monitoring of key application traffic and network quality, and rapid fault detection and isolation. The third-level VIP user experience assurance design ensures that the VIP user experience is guaranteed in high-density access scenarios through preferential access and VIP bandwidth reservation technologies. For critical users, such as executives, celebrities, and high-value fans, the network can be planned to classify these users as VIPs.

As the number of terminal access devices continues to grow and the network carries more operations, managing the network becomes increasingly complex. Manageability is the key requirement for network operations. The smart stadium network solution provides efficient tools and methods, such as network digital map, protocol trace, access analysis, and network health monitoring, to improve network maintenance efficiency and reduce daily maintenance costs for the stadium network.

Meanwhile, as more network devices are deployed, especially APs for wireless coverage, the energy consumption cost accounts for an increasing proportion of the total operating expenditure. The smart stadium network solution provides AI-based tidal prediction and CSI sensing capabilities. By coordinating with systems such as lighting and air conditioning, and AP shutting down or AP sleep mode, the solution achieves energy saving and reduces energy consumption costs for the stadium network.

Figure 3-31 Stadium

Figure 3-32 VIP box

The following table lists the recommended indicators for a high-quality smart stadium network.

Table 3-16 Recommended indicators for a high-quality smart stadium network

Item	Recommended Indicator
Bandwidth of access devices deployed indoors	≥ 10 Gbps
WLAN AP standard	Wi-Fi 7
Concurrent channels of 4K HD video conferencing	≥ 60 channels
Definition and latency of key applications such as video conferencing and cloud desktop	1080p, latency < 100 ms
Service assurance for key users	Latency ≤ 50 ms Bandwidth increase by 30% Fault alarm function
Wired security	AP-switch full-link MACsec
Energy saving	Tidal prediction Wake-up within seconds (WLAN AP) CSI sensing for intelligent control of air conditioner and lighting systems
Wi-Fi anti-eavesdropping (VIP room)	WPA3 + physical noise–based interference protection
O&M and management	Unified management of multiple networks, and three-dimensional visibility into applications, terminals, and networks

3.8.4 Cases

3.8.4.1 A Stadium in a Middle Eastern Country

Key Challenges and Requirements

The Middle Eastern country built a large stadium for hosting major international sports events. The main stadium accommodates over 80,000 spectators, complemented by additional facilities such as training centers for athletes. With service requirements such as CCTV video backhaul, live event broadcasting, and global fan Internet access, the stadium imposes stringent demands on both wired and wireless network coverage. During major events, high-density user access and concurrent Internet usage create significant challenges for network bandwidth, concurrency handling, and overall network O&M. Broadcasting of international sports events requires the network to provide real-time performance, application assurance, and deterministic user experience to ensure reliability for services and access of key customers.

Key Technologies

Broadband access 10 Gbps: On the wireless side, Wi-Fi 7 is used to provide high bandwidth, high concurrency, and seamless roaming capabilities through collaboration among APs. On the wired side, access switches support uplink bandwidth upgrade to 10GE for wired terminals and wireless APs.

Deterministic experience: For core services such as sports event broadcasting that require high reliability, highly reliable end-to-end transmission channels are built based on deterministic application priority, bandwidth, and latency, ensuring ultra-HD video quality and low-latency synchronization for broadcasting world-class international sports events and achieving zero freezing and zero packet loss. For high-value customers in VIP boxes, differentiated services ensure deterministic user priorities and bandwidths to provide stable, smooth dedicated network access experience, meeting communications requirements in premium match watching scenarios.

Autonomous network: A full-dimension traffic and quality monitoring system is built to cover networks, service applications, and terminals. The system supports automatic O&M capable of intelligent fault identification within seconds and precise fault locating within minutes, implementing proactive awareness and fast handling of network exceptions. This provides solid technical support for the continuous and stable broadcasting of large-scale sports events.

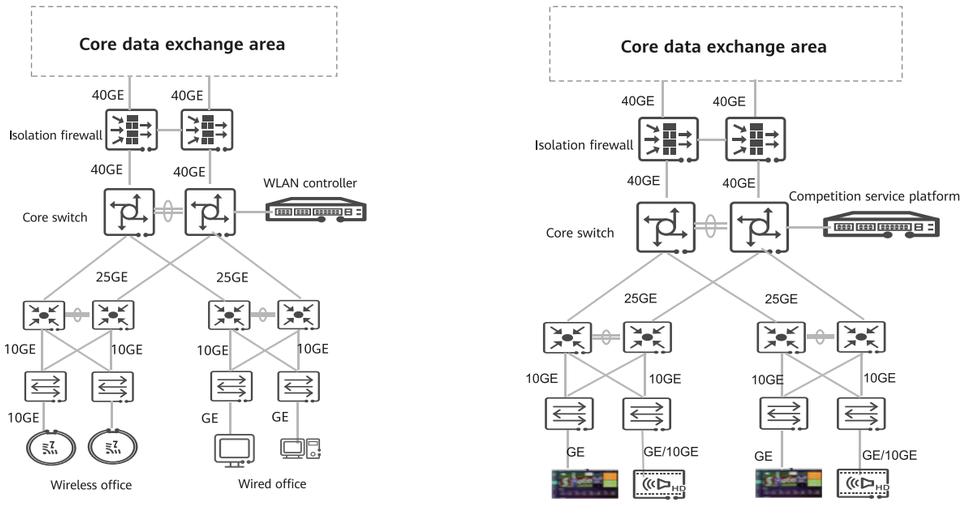


Figure 3-33 Networking diagram

Technology Advantages and Benefits

The 10 Gbps ultra-broadband network architecture with wired-wireless collaboration fully unleashes the potential of high-bandwidth transmission, meeting the requirements of the stadium for high-density concurrent terminal access and ultra-high-speed transmission of services such as ultra-HD sports event broadcasting and VR immersive watching. The deterministic experience assurance system for users and applications ensures zero interruption of core sports event services and delivers dedicated, highly stable services to VIP customers through differentiated assurance. The autonomous network O&M technology provides three-layer full-dimension monitoring, fault detection within seconds, and fault locating within minutes, significantly reducing manual O&M costs and improving network emergency response efficiency. The three approaches together build a high-performance, high-reliability, and high-intelligence technical foundation for the smart stadium, comprehensively supporting the upgrade of event operations and viewing experience.

04

Industry Prospects

4.1 AI Campus Service Prospects

AI is profoundly reshaping the operation modes of key fields such as office, education, healthcare, government, and manufacturing. These changes not only give rise to new application scenarios, but also pose higher requirements on the underlying network infrastructure.

In the enterprise office field, AI applications improve office efficiency. AI-powered document processing automatically identifies the content of documents such as contracts and invoices, enabling digital archiving and data analysis. Automated meeting management automatically schedules meetings, generates agendas and meeting minutes, and reduces manual coordination costs. Cross-language collaboration translates emails and conference content in real time to support cross-country team collaboration.

In the education field, AI promotes personalized and immersive learning. It can dynamically adjust the content difficulty by analyzing learning data and provide customized learning paths for learners. AI can also quickly generate courseware, exercises, and multi-language teaching materials, and create game-based, immersive learning scenarios with VR/AR. Another AI application in the education field is intelligent assessment and learning management, which help assess learning patterns in real time and generate risk profiles.

In the healthcare field, AI empowers precise diagnosis and treatment and resource optimization. In medical imaging diagnosis and genetic analysis, AI identifies tiny lesions in CT/MRI images, accelerates genomic data matching, and tailors cancer treatment solutions. AI-assisted diagnosis and treatment provide clinical decision-making support, and surgical robots implement minimally invasive and precise operations. AI is also used for public health monitoring and resource scheduling, and can analyze the pandemic data in real time to predict the transmission path and optimize the allocation of beds and medicines.

In the government office field, AI reconstructs service and decision-making modes. Intelligent approval and all-in-one network for public services are supported, with AI replacing manual review and cross-departmental data streamlining, improving government office efficiency. In city governance and emergency response, AI analyzes traffic cameras to optimize traffic lights, monitors vehicle congestion points, and automatically performs scheduling. AI also provides policy simulation and precise services, including policy effect prediction based on public services data and personalized service push based on AI profiles.

In the manufacturing industry, AI drives flexible production and full-chain collaboration. AI-based dynamic production scheduling adapts to small-batch customization, and the visual inspection system identifies micron-level defects of products. In terms of predictive maintenance and supply chain optimization, AI uses sensor data to warn of device faults and predicts material requirements to optimize the global supply chain. Digital twins are used to build virtual models of production lines to simulate process parameters, and AR glasses are used to provide remote maintenance guidance.

In the finance, retail, and hotel industries, AI will also be deeply integrated into industry applications to improve efficiency or provide more high-quality and efficient capabilities, promoting the digital and intelligent development. In these fields, AI campuses will pose new technical requirements on the underlying network infrastructure.

4.2 High-Quality 10 Gbps AI Campus Technology Prospects

The future AI campus services will shape the campus network infrastructure with the following key technical focuses and beyond.

4.2.1 Wi-Fi 8 and NearLink: New Era of Wireless Campus with Ultra-High Reliability

With Wi-Fi 7 gradually put into commercial use, the next-generation standard Wi-Fi 8 (IEEE 802.11bn) has entered the early development phase and is expected to be standardized and productized in 2028. The standard shifts its focus from merely improving rates to providing ultra-high reliability (UHR), targeting problems with stability, latency, and spectral efficiency in high-density access environments and laying a technical foundation for future immersive applications. Key technical directions of Wi-Fi 8 include multi-device collaboration, mmWave application, spectrum optimization, low latency, enhanced reliability, and AI-driven intelligent management. Based on Wi-Fi 7/8 mmWave technology and AI channel modeling, centimeter-level positioning and real-time perception of environmental status (temperature, humidity, and crowd density) can be achieved to realize human presence sensing, intelligent security protection, asset management, and spatial management capabilities.

The application of NearLink technology in campus LANs will open up a new paradigm of wireless and intelligent networks. Its ultra-low latency, ultra-high reliability, and multi-node concurrency capabilities can support high-precision scenarios such as real-time control of industrial robotic arms and AGV cluster collaboration, replacing traditional industrial buses to achieve flexible deployment. In office scenarios, NearLink enables millisecond-level synchronous transmission for 8K holographic conference terminals and zero-freezing interconnection of smart terminals such as AR glasses and sensors. In terms of technical features, NearLink provides an anti-interference capability 10 times higher than Wi-Fi, and works with the dynamic resource scheduling algorithm to improve the campus network energy efficiency by more than 30%. Its native security architecture supports E2E encryption and trusted access, providing a basis for wireless reconstruction in high-security scenarios such as finance. With the in-depth integration of NearLink and AI, campus networks will evolve towards touch-free intelligent connections, promoting the digital transformation of industries such as manufacturing and healthcare.

4.2.2 100GE Access and Simplified All-Optical Ethernet Architecture Dealing with Traffic Surges

Campus network bandwidth is continuously upgraded. 2.5GE/10GE access will evolve to 100GE access in the future to meet the requirements of ultra-HD real-time services such as XR and industrial vision.

In the future, all-optical Ethernet will become the norm, and APL/SPE technology will be adopted in process industries such as the chemical industry. The all-optical Ethernet solution "simplifies and greens" the network architecture, saving 90% of device space in ELV rooms and cutting per-bit energy consumption by 70%.

4.2.3 E2E IPv6 Enhanced for Industry Empowerment

In the future, IPv6 Enhanced technology will implement in-depth E2E convergence from LANs, WANs, and to data center networks (DCNs). Based on Segment Routing over IPv6 (SRv6), network slicing, in-band flow measurement and other core protocols and capabilities, IPv6 Enhanced will build a unified cross-domain intelligent IP network architecture to support integrated services of devices, networks, and clouds.

On the LAN side, IPv6 Enhanced identifiers on application endpoints can be used to ensure application experience on campus networks. On the WAN side, carrier's SRv6 and network slicing technologies achieve the combined usage of soft and hard pipes to implement hierarchical service assurance, and in-band flow measurement technology helps locate cross-domain faults in real time, providing E2E slicing services with low latency, high reliability, and data encryption for industries such as finance, government, and healthcare. On the DCN side, IPv6 Enhanced application identifiers can be used to ensure data quality, isolate data, and encrypt data.

In addition, with carrier's specific business model for enterprise private line services, this may foster a win-win scenario for users, carriers, and cloud service providers.

4.2.4 Campus Network Security: From "Passive Defense" to "Proactive Immunity"

Campus network security will evolve towards "intelligent intrinsic security and dynamic immunity". The AI-based digital twin defense system can implement real-time modeling and prediction of network attacks. Quantum key distribution technology will build a physically unbreakable transmission encryption system. The zero trust architecture combined with blockchain technology can dynamically verify device identities and trace behavior. The intelligent sensing network supported by AI and NearLink can identify abnormal traffic in milliseconds.

The proactive security brain shares threat intelligence across the entire network and uses self-healing AI algorithms to improve the defense response speed to nanosecond-level. Privacy-preserving federated learning ensures that data in the campus is available but invisible. Mimic defense technology significantly reduces the risk of unknown vulnerabilities through the dynamic heterogeneous redundancy architecture. The network autonomy system implements automatic policy orchestration and elastic capacity expansion, building a resilient security base with "breath-like elasticity".

A Acronyms and Abbreviations

Table A-1 Acronyms and abbreviations

Acronym or Abbreviation	Full Spelling
GDP	Gross Domestic Product
PC	Personal Computer
SLA	Service Level Agreement
QAM	Quadrature Amplitude Modulation
AP	Access Point
VR	Virtual Reality
AR	Augmented Reality
AI	Artificial Intelligence
VIP	Very Important Person
SDN	Software-Defined Networking
ETH	Extremely High Throughput
PPDU	Physical Layer Protocol Data Unit
RU	Resource Unit
TCO	Total Cost of Operations
PHY	Port Physical Layer
PoE	Power over Ethernet
WLAN	Wireless Local Area Network
HTTP	Hypertext Transfer Protocol
FTP	File Transfer Protocol
QoS	Quality of Service
TSN	Time-Sensitive Networking
RTT	Round Trip Time

Acronym or Abbreviation	Full Spelling
VoIP	Voice over Internet Protocol
SaaS	Software as a Service
POS	Point of Sale
AGV	Automated Guided Vehicle
EDCA	Enhanced Distributed Channel Access
SRv6	Segment Routing over IPv6
VXLAN	Virtual Extensible Local Area Network
VLAN	Virtual Local Area Network
ZTP	Zero Touch Provisioning
DHCP	Dynamic Host Configuration Protocol
LAN	Local Area Network
WAN	Wide Area Network
API	Application Programming Interface
OUI	Organizationally Unique Identifier
LLDP	Link Layer Discovery Protocol
ONVIF	Open Network Video Interface Forum
WPA	Wi-Fi Protected Access
MIMO	Multiple-input Multiple-output
SZTP	Secure Zero Touch Provisioning
CSI	Channel State Information
ALS	Automatic Laser Shutdown
EEE	Energy Efficient Ethernet
RFID	Radio Frequency IDentification
MTTR	Mean Time To Repair
ZTNA	Zero Trust Network Access