Let's continue discussing reliability. This includes two aspects, one is AC reliability, and the other is service reliability. Let's see why we need reliability. Usually, AC has a single point of failure. Here in the topology diagram, it's an AC plus thin AP architecture. Here, N or N+1 APs, each AP establishes a CAPWAP tunnel with the AC. As mentioned before, thin APs cannot operate without AC, which means if the AC goes down, so do the thin APs, and they can no longer provide wireless network access. For such failures, there are actually two solutions. One is solved by AC reliability, the other by service reliability. First, let's look at AC reliability. AC reliability means adding another AC, one primary, one backup, acting as failover for each other. Next, we will introduce several AC reliability solutions. The first one is the VRRP dual-device. AC1 and AC2 use the Virtual Router Redundancy Protocol (VRRP), to virtualize into a single AC. It has a virtual IP address, which we use as an AC source, meaning we use this address to establish CAPWAP tunnels with APs. Although APs establish a CAPWAP tunnel with a virtual AC, there is actually a primary and a backup. For example, AC1 is the primary device, and AC2 is the backup device. APs establish a CAPWAP tunnel with the primary device. So when the primary AC fails, APs will naturally establish a new CAPWAP tunnel with the backup AP. Note that in this network configuration, AP only establishes one CAPWAP tunnel, so for the AP, it only knows about one AC. When the primary AC fails, it switches through VRRP, so the switching speed of VRRP determines the failover speed of the primary and backup AC. This method does not support load sharing, because APs only establish one CAPWAP tunnel with one virtual AC. At the same time, this method, Generally, ACs are deployed in the same geographical location, so their business switch-over speed is quite fast. This is known as VRRP dual-machine hot standby. The second method supports load sharing, called dual-link dual-machine hot standby. In this method, AP establishes a primary CAPWAP tunnel with the main AC1, and also establishes a CAPWAP tunnel with the backup AC2, supporting both failover and load sharing. When the AP disconnects from the main AC1, it will notify AC2 that it can switch to being the main AC. Then the AP continues to communicate with AC2, The primary and backup ACs are determined by priority, if the priorities are the same, it is decided based on load, i.e., the number of APs and STAs compared. And its switch-over speed is also very fast, because it is a hot standby. Here we find, both VRRP and dual-link are hot standbys, then how do they ensure hot standby? Hot standby means that the service is essentially uninterrupted, ensuring no disruption to service. First, AP connects with AC1, at the same time user STA information is also on AC1. When switching to backup AC2, whether backup AC2 has the AP and user information, determines if it can perform hot standby. If AC2 does not have the AP and STA information, it means APs and STAs have to re-register. This re-registration process, This will cause a service interruption, it won't be a hot standby anymore. To ensure it remains a hot standby, we must ensure that the backup AC2 synchronizes AP and user information with the primary AC1. So, how is synchronization achieved? Through the Hot Standby Backup (HSB) between the two ACs, this HSB is used to synchronize the information of APs and STAs. What is this link? It is Huawei's proprietary master-standby mechanism, which can establish and maintain a master-standby channel through master-standby services and backup groups. It uses master-standby services and backup groups to synchronize information of APs and users. Finally, let's discuss cold standby, which does not use

HSB, Cold standby operates on an N+1 model, using one AC as the backup AC, providing backup services for multiple primary ACs, Under normal circumstances, APs only establish CAPWAP tunnels with the primary AC, and only when the primary AC fails, or there is a CAPWAP link failure between the primary AC and AP, will the backup AC take over to manage the AP, and then it establishes a CAPWAP tunnel with the AP, supporting master-standby switchover and failback. This is all about cold standby. Finally, let's summarize AC reliability, focusing on switching speed, geographically distributed master and standby AC deployment, and comparing their applicable scope. and also comparing the applicable range. The difference in switching speed is clear, hot standby is definitely superior to cold standby, VRRP can determine the switching speed, and achieves faster switching compared to other methods, while dual-link requires waiting for the CAPWAP disconnection timeout before switching, so its switching speed is somewhat slower, but with HSB, there is no need to re-login, whereas cold standby waits for the CAPWAP disconnection timeout, the only difference is that cold standby lacks HSB, while hot standby has HSB to synchronize AP and user information, thus, terminals in cold standby need to re-login, and of course, there will be service interruptions. Then, regarding master-standby geographically distributed deployment, since VRRP is a layer 2 protocol, it does not support geographically distributed master-standby AC deployment, whereas these two types, as long as AP and AC can communicate, can be deployed geographically. In terms of applicable scope, both types of hot standby are used in high-reliability scenarios, one does not require geographical deployment, and the other demands it. Dual-link has a broader range of applicability, it can be used without geographical considerations, whereas VRRP cannot be used geographically. Then, N+1 is used in scenarios where reliability requirements are lower. Let's continue looking at service reliability. Service reliability includes two types, one is local forwarding CAPWAP disconnection service maintenance, and the other is wide-area escape. Let's first take a look, at local forwarding CAPWAP disconnection service maintenance, when the CAPWAP tunnel between the AP and the AC hangs, normally, the AP would go offline, But we have a solution here, that is, after the AC fails, the AP will not go offline. Let's take a look, when the CAPWAP tunnel between this AP and AC is interrupted, the business of online users will not be interrupted, and user data can be forwarded normally. But there is a prerequisite, that is, it must not go through the AC. Tunnel forwarding relies on the CAPWAP tunnel, meaning the AC must not fail, while local forwarding does not depend on the CAPWAP tunnel, so only when data forwarding is local, can it support CAPWAP disconnection business continuity, and also support simple user logins. So, what is considered simple? That is, AP wireless security policies include open system authentication, shared key authentication, and WPA/WPA2-PSK, but they do not support complex authentication methods such as 802.11ax, and these three authentication methods can be directly controlled on the AP. This is one of its features, This approach can be considered for small wireless networks without a deployed backup AC, If AC reliability is present, there is no need to consider this method. The second type of service reliability we call wide-area escape. Traditionally, user authentication is done on the AC, but when communication between the AC and AP is interrupted, newly connecting users of course cannot be authenticated, and cannot access the network. But we can create an escape

channel, this is called wide-area escape. When there is a disconnection between the AC and the AP, The AP has local authentication capabilities, it can authenticate newly connecting users. Generally, this escape mechanism is triggered by certain conditions, such as when a user attempts to authenticate, and tries to authenticate multiple times within a few seconds, and finds the authentication fails, then the escape mechanism will be triggered, allowing new users to authenticate directly through the AP, and if authenticated, they can access the internet again, this is called wide-area escape. It also ensures that already online users, through the configuration of the service continuity function, can maintain normal operations, but new users will initiate a wide-area escape mechanism, let's see, before the interruption, users authenticate through the WAN to our AC, then the data is sent to the authentication server for authentication, but after the interruption, the authentication data goes directly to the AP for authentication, this is a wide-area escape. Previously, we discussed the architecture of AC with thin APs, next, the two network architectures we'll discuss are for your understanding, knowing which scenarios they are used in is sufficient. The first one is called cloud management architecture, it involves using a cloud management platform to centrally manage, and configure cloud APs to manage user terminal access uniformly. Compared to the traditional AC plus thin AP architecture, it can be plug-and-play, and allows unified operations, it is suitable for small and medium-sized wireless networks. When deploying networks, traditional network solutions can involve high deployment costs, and challenges in subsequent operations and maintenance, especially for enterprises with numerous branch sites and widespread geographic locations, these issues are particularly pronounced. Cloud management architecture can effectively address this problem, by enabling centralized device management and maintenance from any location through a cloud management platform, significantly reducing the costs of network deployment and operations. Once the cloud APs are deployed, network administrators do not need to be onsite to configure the cloud APs, as the cloud APs automatically connect to the designated cloud management platform upon powering up, and automatically load the specified configuration files, software packages, and patch files among other system files, achieving zero-touch provisioning. Network administrators can also remotely provide configuration to the APs at any time through the cloud management platform, facilitating faster batch configuration of services. The final mode is called Leader AP, This Leader AP mode is designed to address situations with only APs present, where one AP is set to Leader AP mode, and other APs connect to the network in thin AP mode, and communicate at layer 2 with the Leader AP. The functions of the Leader AP are very similar to those of an AC, providing unified access management and configuration operations based on CAPWAP tunnels, offering centralized wireless resource management and roaming management. It provides centralized management of wireless resources and roaming, which is particularly beneficial for small and micro enterprises seeking to establish their own wireless networks, allowing them to set up their wireless networks without requiring extensive infrastructure. managed independently, without adopting a cloud architecture, then if using a fat AP architecture, it's not possible to uniformly manage and maintain APs, nor to provide a good roaming experience for users. If opting for an AC plus thin AP architecture, due to the small number of terminals, not many APs are needed, yet there is a

high cost for AC equipment and licenses. If in the network, some AP could take on the role of managing other APs, providing unified operations and continuous roaming capabilities, it would meet the needs of these small and micro enterprises. Therefore, Huawei's design of the Leader AP architecture, perfectly meets these requirements. Let's compare the different network architecture models, starting with fat APs and thin APs. Fat APs are deployed independently, configuration management and maintenance are more cumbersome, incurring higher labor costs, but the equipment costs are lower, therefore, they are only suitable for small network setups, for SOHO users, and can also be used for wireless geological surveys, to test signal strength. Thin APs, with AC managing and configuring APs, are simpler to configure and deploy, incur lower labor costs, but their equipment costs are higher, suitable for medium to large networks. The third is cloud management, where a cloud management platform uniformly manages and configures APs, deployment and maintenance are relatively simple, suitable for small to medium-sized wireless networks. LeaderAP is a simplified version of the thin AP plus AC architecture, also suitable for small to medium-sized networks. Finally, let's introduce, the cloud management architecture is also based on the Intelligent Simplified Campus, the solution is called the Cloud Campus small campus network solution. Its core is iMasterNCE, upstream generally provides a northbound interface, to create an open application platform, downstream we control some devices through NetConf. Note iMasterNCE, here we focus on cloud management, cloud APs, in fact, our Cloud Campus can also manage many devices, including APs, ACs, routers, switches all can be managed, of course, using these southbound protocols for management. Such a cloud architecture, its feature is simple network planning, simple deployment, it's plug and play, network and management are deployed as needed, at this time iMasterNCE acts as a controller of SDN, these devices, once online with zero configuration, iMasterNCE directly issues service configurations through these southbound protocols, at the same time, it can also perform business data analysis, and the network platform is also open. Here is a highlight of the Cloud Campus solution, firstly, automatic deployment, Then, cloud regulation, simplifying WLAN network design, it provides a cloud regulation software, mobile operations, and a rich product portfolio, supporting switches, firewalls, ARs, APs, and even ACs. All can be managed, and it is a dual-stack platform, though it has implemented cloud management, the underlying devices can continue running traditional networks, without interference. Then value-added services, are a type of value-added application in Cloud Campus. Let's look at what iMasterNCE is, iMasterNCE is an integrated controller, supporting simple zones, virtualized zones, and the interconnection of multi-branch zones. Let’s see what components it has, firstly, the Cloud Campus component, and the authentication component, and Campus Insight for data analysis.