Cisco Universal Small Cell CloudBase Activation Overview

White Paper

August 2014

Contents

1. Scope

This white paper provides an overview of the Cisco Universal Small Cell CloudBase™ (Cisco USC CloudBase™) technology and describes how it is used to install, activate, and recover small cells using Cisco® Universal Small Cell (USC) software in conjunction with the Cisco USC RAN Management System (RMS).

2. Summary

Cost can be of critical concern with small cell deployments: manufacturing costs, deployment costs, and the cost of restoring service if a fault occurs. The main goal of the Cisco Small Cell Solution is to keep these costs low, and to provide a solution that is ready-to-use for the end user. To achieve this goal, the access point must be programmed with key data consisting of the network credentials that allow the access point to connect, authenticate itself, and then start the process of provisioning. The credentials include the address of the operator's secure gateways and small cell management server, the gateway authentication certificates, and the management system login parameters. This information must be securely installed into the access point so that it can't be tampered with. This level of security allows authorized access points to connect and start the provisioning process while rendering unauthorized access points inoperable with an operator's networks.

Configuration of the access points with the network credentials is performed when you install the Cisco Small Cell Solution using the innovative Cisco USC CloudBase software. This software gives you greater flexibility in network design by allowing you to change the credentials at any time, rather than having to define them at manufacture. This software thereby overcomes the logistical problems of having to synchronize network changes with the delivery of small cells through the supply chain. For changes subsequent to first installation, Cisco USC CloudBase software additionally allows you to update the access points in the field. Table 1 summarizes the key functions and benefits provided by Cisco USC CloudBase technology.

Table 1. Cisco USC CloudBase Features and Benefits

Function	Benefits	Section in This Document
Secure boot and zero-touch provisioning	Ready-to-use initialization with no end-user action required	4.1
Operator customization	Flexibility and scalability across high-volume deployments	4.1
Certificate updates	Configurable large-scale changes deployed quickly across fleet or sub-fleet of access points	4.2
Factory recovery	Restoration of failed units to working state without return to base	4.3
Network configuration changes	Rapid re-parenting of units to different network elements across fleets or sub-fleets	4.4

3. Introduction

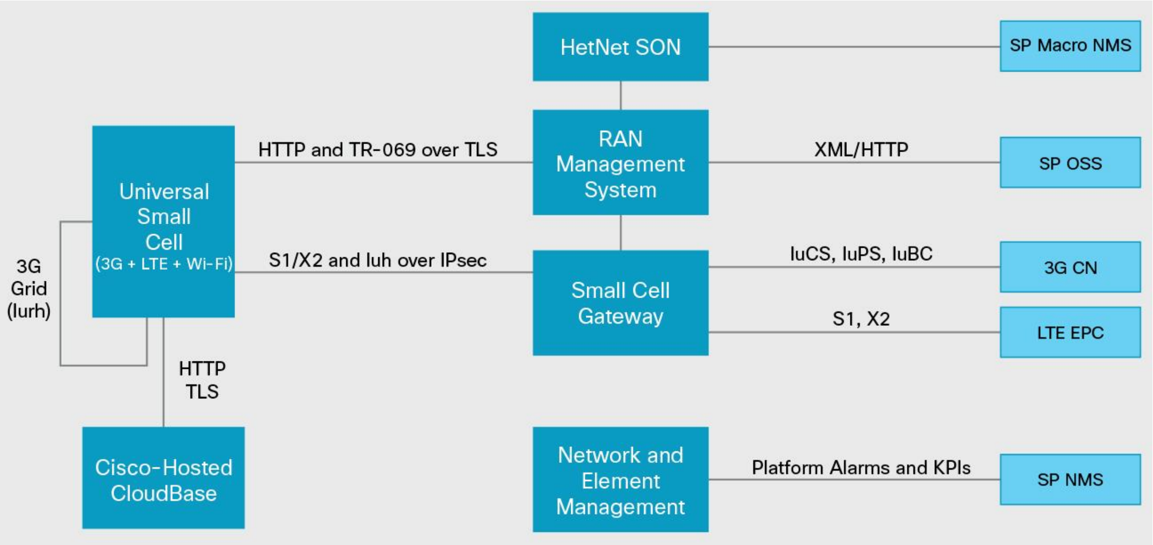
To meet the cost targets of manufacturing a small cell, Cisco Small Cell Solution manufacturing partners create the hardware (excluding any customizable casing) as a generic product and defer the final customization until the device is actually installed by an end user. This approach has two key benefits:

- The manufacturing partner does not need to be involved with the complexities of the small cell installation process, and
- You do not need to include the manufacturing partner in your control process when you want to make network changes, nor does the manufacturer need to be involved in the interoperability testing process to prove that the manufacturing partner has applied the configuration changes correctly.

Cisco USC CloudBase technology is used to activate a small cell with the critical information it needs to connect to an operator's network and provide service. If at any time the small cell loses that data, it can always reconnect to the Cisco USC CloudBase software to restore it to a known state so that your small cell management system can provision it again.

It is important to note that the access point provisioning data (for example, the RF configuration information, subscriber list, etc.) is provided and managed by your TR-069-based Universal Small Cell RAN Management System (USC RMS). In order to connect to the USC RMS, the access point has to be provided with the information it requires to connect with your USC RMS. You cannot configure this information through the USC RMS, because the access point is not delivered from the factory with the connection parameters and public-key-infrastructure (PKI) chain of trust necessary to connect to the RMS. For this reason the access point will connect to the Cisco USC CloudBase software, which is available on the Internet, as shown in Figure 1.

Figure 1. Cisco Small Cell System Overview



The Cisco USC CloudBase software is configured with an activation profile for your network, and all the access points that are associated with your specific network are then configured with this profile. Each operator has to have at least one profile, but you can have more if required (for example, if you have partitioned your network into production and lab deployments with different RMSs).

The cost of recovery and repair of access points should also be considered. Certain access point failures can result from memory or software corruption, and then the access point does not operate correctly. When this situation occurs, your USC RMS customer care systems cannot manage and reinstate the access point into service in the field. You don't have to physically return it, however, because the access point automatically detects such situations and enters into factory recovery mode. This mode allows it to revert back to the state it was in when manufactured. This state allows the access point to restore the network activation profile and connect to your USC RMS, at which point it can be reconfigured. Again, this procedure is fully automatic and does not require any end-user intervention. If the access point cannot detect the fault, you can manually force it into factory recovery mode by initiating a factory reset, typically with a long press on the Reset button.

With the migration of consumer devices from NOR flash-based technology to NAND flash-based technology, it becomes more difficult to directly protect sectors that contain critical parts of the software. The difficulty lies in the fact that NOR flash devices address memory directly, and they protect critical software by locking the sectors within which the critical software is stored. Also, during manufacture, all of the cells in NOR flash devices are tested, and only devices in which all storage cells are 100-percent operational are shipped as working devices.

NAND flash technology is different in that the data in the device is stored in a file system, because not all the sectors in the device are perfect, so some sectors have to be marked as bad and not used by the file system. Normally, the only sector that is guaranteed to work is the first one in the device, where the boot loader is located. To ensure the robustness of a small cell, the manufacturer loads the key elements of the factory recovery system into the boot loader. This placement ensures that if the file system in the remaining sectors of the device is in some way corrupted - for example, by the power being removed at a moment of a critical update to the flash memory - the small cell can be recovered without the need to return the access point under a return materials authorization (RMA). It should be pointed out that the chances of this happening are very small, because the USC software stores two copies of the software. If one of the software images is corrupted, the boot loader can detect the corruption through signature checking of the image and can then revert to using the other software image.

This factory recovery capability is provided through Cisco USC CloudBase software, which is provided as a hosted service by Cisco as part of its USC software support agreement. The Cisco USC CloudBase software is not responsible for any operational management of the access point, but instead acts as an installation and activation aid, as well as a safety net if access point software malfunctions. Under normal circumstances, the access point needs to contact the Cisco USC CloudBase software only once in its lifetime for full activation when you install it, although there may be other events, such as a device certificate or security gateway (SeGW) certificate(s) update, that would require the small cell to contact the Cisco USC CloudBase software.

The access point has the Cisco USC CloudBase software fully qualified domain name (FQDN) loaded in the each small cell flash memory at the time of manufacture. Using this FQDN, the access point can identify the Cisco USC CloudBase software and create a connection. The access point also has a Cisco USC CloudBase public certificate that can authenticate the Cisco USC CloudBase software and create a secure connection (Secure HTTP [HTTPS]) over which it can download and store the public certificates it requires to authenticate any data that it downloads.

When an access point reaches the end of the product line, a record of its details is captured and uploaded to the Cisco USC CloudBase software through the Cisco production servers. These details include the following information:

- Home Node B/Home eNode B ID
- MAC address
- Security authentication data, the device certificate signing request (CSR) containing the device public key of the small cell
- Calibration data
- Model information

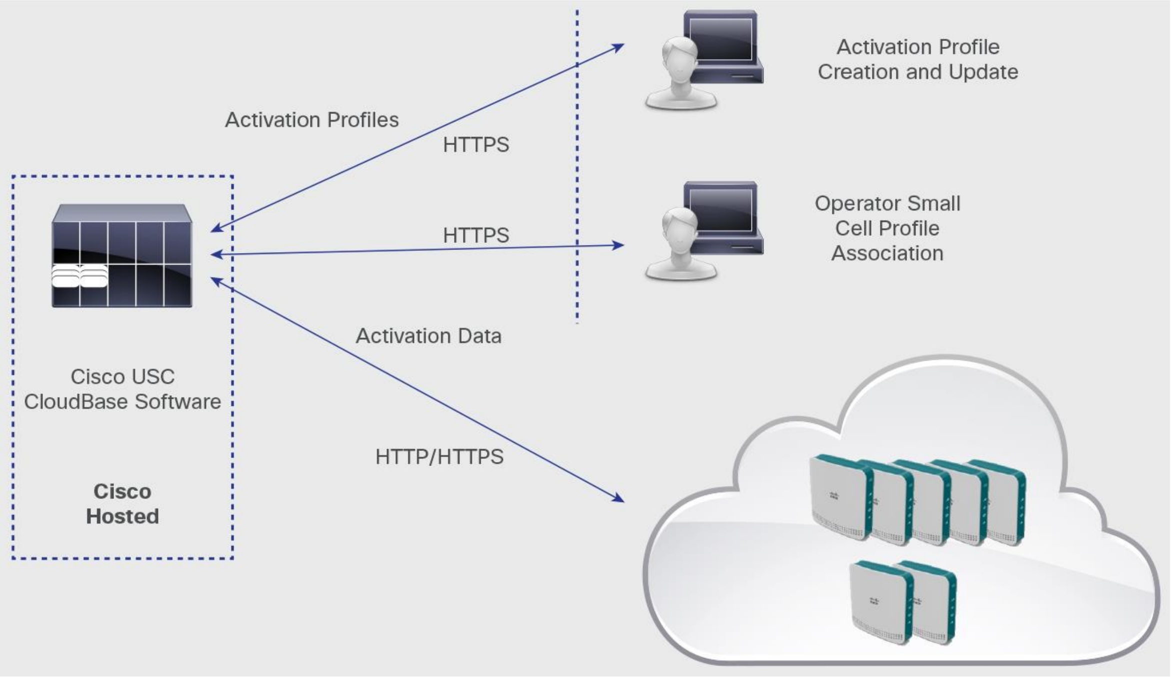
Each access point is then associated with a network activation profile and is configured when it is first installed.

The Cisco USC CloudBase software is hosted in secure data centers, with software images delivered from Akamai’s worldwide edge cache.

Typically systems integrators have full, highly secure access to the Cisco USC CloudBase software for those access points built to operate on their customers' networks and can select which network activation profile each access point is configured with, if different from the product default. Cisco USC CloudBase software has a secure mechanism to help ensure that only legitimate access points are updated, and similarly, each access point has a secure mechanism to help ensure that it will communicate only with legitimate Cisco USC CloudBase software. An overview of this arrangement is shown in Figure 2.

The Cisco USC CloudBase technology is a unique capability provided for Cisco USC software, creating savings for operators and reducing the number of returns. It also provides an additional level of security (preventing access points from being used on other operators' networks), and flexibility (for example, allowing the security gateway certificates to be changed).

Figure 2. Creating and Updating Network Activation Profiles



4. Use Cases

The following use cases describe how and when the Cisco USC CloudBase technology is used.

4.1 Installation Process

When you get a Cisco Universal Small Cell access point, from the software perspective it is a generic product that has the Cisco USC CloudBase FQDN programmed into it at the factory to allow it to connect to the Cisco USC CloudBase software. When you first power it on, it automatically connects to the Cisco USC CloudBase server, from which it downloads your network credentials. This process follows:

- **You define the deployment parameters:** The small cell needs your information to connect to your network and to your USC RMS, including the RMS FQDN and RMS certificate authority (RMS CA) certificates. Only the factory recovery software that the access point downloads from the Cisco USC CloudBase software can configure this information, which is captured in the network activation profile on the software using a web GUI.

When the configuration is complete, the profile is signed as ready for delivery to small cells associated with your network activation profile. Creation of the network activation profile would normally take place during interoperability testing, but may be updated if you make changes in your network, for example, to the RMS FQDN or RMS CA certificates used to sign the USC RMS end entity certificates.

- **The product is manufactured:** When the product is manufactured, the details of all the products released are delivered to the Cisco Production Support system and, upon product shipment, are transferred to the Cisco USC CloudBase software. At this point, the software is set up to either automatically allocate the shipped access points to a network activation profile or be held unassociated with a profile awaiting the association.
- **You receive the access points:** If the delivered access points are not already associated with your network profile, they are assigned to the correct network activation profile. Only when the access points have been associated with a network activation profile can you deploy them in the field. If you do not receive the access points, you are protected because they contain no operator network data and therefore cannot be deployed in any other operator's network.
- **Small cell configuration:** When the access point first initializes, it will determine that it does not have a valid network activation profile and will enter factory recovery mode. The access point will resolve the embedded Cisco USC CloudBase FQDN and connect to the Cisco USC CloudBase software to start the deployment or recovery procedure, which will securely download and install the settings within network activation profile. After the small cell configures these settings, the access point can connect to your network and be provisioned to provide service.
- **Single supply chain:** The activation process also allows you to use a single supply chain to deliver a standard product that can connect to more than one USC RMS. Such a scenario occurs when you have more than one USC RMS installed (for example, one for lab and one for production) and want the option to select which USC RMS the access point is to connect to.

4.2 Certificate Change Process

In some cases you may want to change the CA certificates that are required to authenticate the chain of trust of the USC RMS end entity certificate. These CA certificates may have a limited life span (for example, 5 years), so they may need to be updated. You can change them only by following these steps:

- Update the USC RMS and SeGW CA certificates in Cisco USC CloudBase software: If you generate new CA certificates for signing the USC RMS and SeGW end entity certificates, you must upload these new USC RMS and SeGW CA certificates into the Cisco USC CloudBase network activation profile so they can be downloaded into the access point identities associated with your network activation profile. It should be noted that the USC RMS and SeGW end entity certificates are not uploaded into Cisco USC CloudBase software; the USC RMS and SeGW present their end entity certificates as part of the Transport Layer Security (TLS) and IP Security (IPsec) tunnel initialization authentication process.
- Initiate a factory reset: You should now use the USC RMS to initiate a factory reset on all the access points that use the deployment profile that you have updated. There is usually one network activation profile, and you need to initiate it on the access points deployed. You can schedule the USC RMS-initiated factory recovery on the next initialization or at the least busy hour, or on next power-on reset, and you can manage it across all the access points deployed or in groups (such as access points in different regions).

4.3 Small Cell Factory Recovery

To minimize effects on the customer, the access point initiates factory recovery when there are no active calls. Mechanisms are built into the system to help ensure that different access points recover at different times to control the USC RMS loading, network traffic load, and impact on the customer. When the access point carries out a factory recovery, it connects to the Cisco USC CloudBase software and downloads the new version of the deployment profile. When updated, the access point initializes and reconnects to your network. As part of the factory recovery procedure, the access points clear their provisioning information, so they need to connect to the USC RMS to be configured. The USC RMS has the profile for the access point already, and it provisions the access point. When provisioned, the access point can provide service.

4.3.1 Access Point Recovery

One of the primary purposes of Cisco USC CloudBase software is to allow the access point to recover from a failure and be returned to a known state, referred to as the factory default state. When in the factory default state, the access point can carry out the steps described in the deployment process and configuration, enabling it to connect to your network and provide service.

An access point can fail in many ways, stopping it from providing service and preventing it from connecting to the USC RMS and being brought back into service. In all of these scenarios, the Cisco USC CloudBase software is required to recover the access point.

4.3.2 Corrupted Memory

If the access point flash memory becomes corrupted, it cannot provide service and may not be able to connect to the USC RMS to be reconfigured. In such cases, the access point needs to do a full factory recovery, in which it is restored to the state it was in when it left the factory. The access point software and operator data have their own checksums and signatures, which are validated at every initialization. If they are found to be invalid or missing, the access point automatically connects to the Cisco USC CloudBase software to carry out its factory recovery.

4.3.3 Software Fault

A software problem can cause the access point software to fail to start correctly, so that it cannot connect to the USC RMS to be diagnosed and recovered. The access point has an embedded watchdog timer that, in conjunction with the access point software, detects multiple access point restarts in a short period of time. In such cases, it automatically performs a factory reset and connects to the Cisco USC CloudBase software. This scenario is likely to be an endemic problem across all the access points, implying a faulty software version, in which case the software will have been updated with a new version of software that does not have this fault. When the access point connects to the Cisco USC CloudBase software, it determines whether it has the latest version of software and, if not, downloads the new version from the Cisco USC CloudBase software. The access point can then initialize with the newer software version and connect to your network, to be reprovisioned by the USC RMS.

4.3.4 Configuration Failure

The access point database may be configured by the USC RMS into a state that prevents it from connecting to the USC RMS to be managed. This situation may be due to either an accident or code problems. In either case, if the USC RMS can no longer manager the access point, the situation cannot be corrected automatically. If this occurs, the end user needs to perform a factory reset by pressing on the access point Reset button for several seconds. The access point then resets and clears all the parameter values in its database before connecting to the Cisco USC CloudBase software.

When connected to the software, the access point determines whether it has the latest version of the network activation profile and associated software load. In this scenario the access point has the latest settings, and so it can reconnect to your USC RMS and be correctly reprovisioned.

4.3.5 CA Certificate Expiration

For a small cell access point installed in a consumer's home, the subscriber might power off the access point for an extended period, for example, when they go on vacation. If during this unpowered period the CA certificate needs to be updated because the USC RMS needs to change its certificates (through expiration, etc.), the access point will, when powered up, be unable to connect to the USC RMS and/or SeGW. In such a case, without the Cisco USC CloudBase software, the access point would have to be returned for reconfiguration, because there would be no way to connect to it. However, through the factory recovery process, initiated by pressing the factory Reset button on the access point, the access point can be restored to the factory settings, receive the new USC RMS and SeGW CA certificates, and is then successfully reconnect to the USC RMS and SeGW and go back into service.

4.4 Re-parenting

The re-parenting feature allows small cells to migrate from one USC RMS to another. Re-parenting may be as simple as updating the USC RMS connection settings and credentials, or it may involve a complete change of core network protocol. For example, if you already have GAN or IMS networks and wish to migrate to a new Cisco Iuh network, you can reactivate to update:

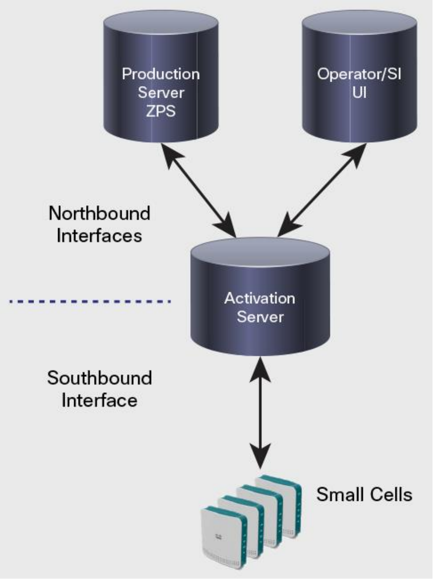
- The core network protocol - GAN, IMS, Iuh, or some future interface protocol
- USC RMS URL/IP addresses and CA certificates

5. Interfaces

5.1 Overview

The Cisco USC CloudBase software has a single southbound interface for connection to the deployed small cells and two northbound interfaces, one for access point data transfers from the production server and the other for the systems integrator to manage the small cell network activation associations. The context is shown in Figure 3.

Figure 3. North- and Southbound Interfaces



5.2 Southbound Interface

The southbound interface is used to communicate with the access points for factory recovery, device certificate deployment, and license file delivery.

5.2.1 Factory Recovery

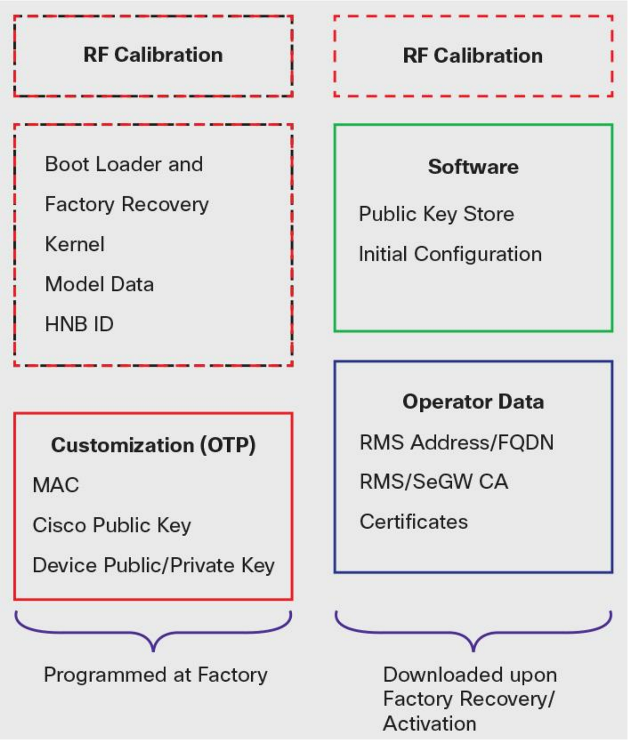
Factory recovery mode is intended to ensure that an access point can be recovered from a critical fault state without having to be returned to the factory. This mode is triggered in the following situations:

- The operator data is missing or corrupt
- Both available versions of the application code fail signature verification
- Request from USC RMS using TR-069
- The internal watchdog detects repeated initializations
- The end user performs a long press on the Reset button
- A factory recovery process failed

The aim of factory recovery mode is to return the Cisco USC Software-enabled access point to the state it was in when shipped from the factory. It should then be able to establish a connection with the USC RMS and download its settings and/or the latest software load as it normally would.

The access point has a nonvolatile memory that it uses to store the data and software it needs to operate. This scenario is illustrated in Figure 4.

Figure 4. File System High-Level Description



The areas in solid red in Figure 4 are programmed in the factory into one-time programmable (OTP) memory within the main processor and cannot be changed. The RF calibration data is loaded at the factory but is not locked into the memory so that the product can be recalibrated at a later date.

As described earlier, the access point requires operator-specific data to operate. This data is not installed at manufacture. This approach allows for operator data changes to occur after manufacture and before installation, without the need for the access points to be returned to the manufacturer.

When the access point enters factory recovery mode, it automatically clears the configuration parameters and the operator data. This action is performed in case the current configuration parameters are causing the access point to fail.

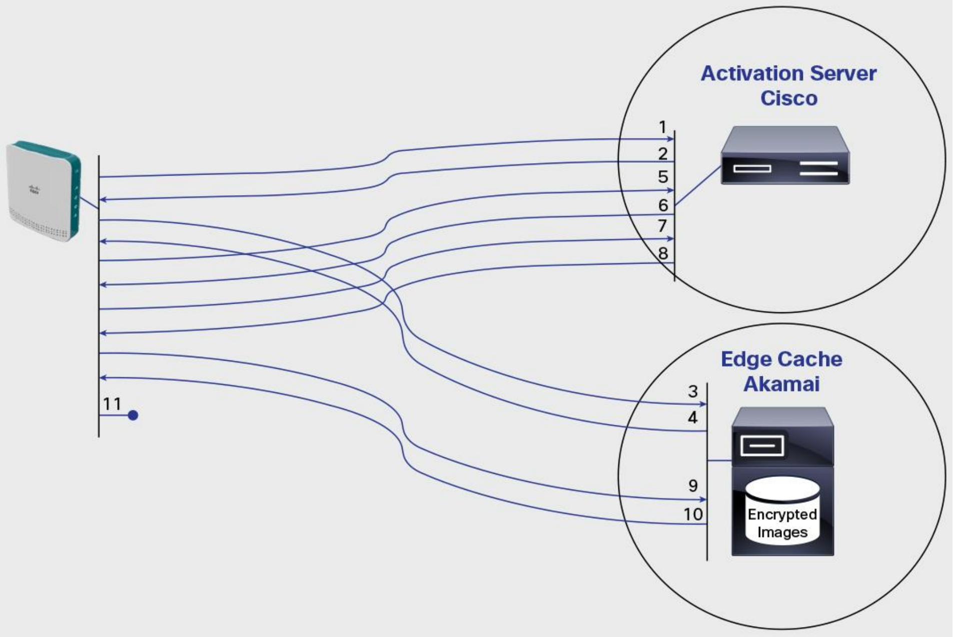
The access point then initializes and senses that it does not have the correct operator data, so it creates a connection with the Cisco USC CloudBase software and downloads the relevant operator data.

If, as part of the factory recovery, the access point determines that it does not have a valid version of its application code, it downloads a new version of the application software image. If it does have a valid version, the factory recovery software is started.

5.2.2 Factory Recovery Communications

When the access point is triggered into factory recovery, it attempts to get an IP address through Dynamic Host Configuration Protocol (DHCP). The access point keeps retrying until it obtains an IP address. It then follows the sequence shown in Figure 5.

Figure 5. Network Communications During Factory Recovery



1. The access point starts by making an HTTP request to the Cisco USC CloudBase URL. The access point passes its MAC address, software version, and hardware information in the request so that the Cisco USC CloudBase server can select the appropriate image to pass to the access point.

2. The Activation server responds with a web redirect to a downloadable archive containing the factory recovery file system image and associated signature.
3. The access point requests the encrypted and signed factory recovery file system image from the Akamai edge cache server using a HTTP request.
4. The edge cache returns the encrypted and signed factory recovery file system image. The access point authenticates the image using its local software signing root of trust public key stored in OTP. If the signature check passes, the file system starts. If the signature check fails, the access point retries indefinitely, with an increasing random back-off delay (the maximum back-off delay is approximately 1000 seconds).
5. When the factory recovery file system image is running, the access point makes a mutually authenticated HTTPS request to authenticate that it is entitled to download its device end entity certificate. The transfer uses the MAC address and hardware information in the request, so that the Activation server can select the associated device certificate to return to the access point. The Activation server uses a challenge and response within this HTTPS session to authenticate that the access point has the private key corresponding to the public key within the device end entity certificate.
6. After the Activation server authenticates the request of the access point in step 5, the website responds with the end entity certificate of the access point signed by the Cisco USC CloudBase CA certificates. To allow the SeGW and USC RMS to authenticate the Cisco USC end entity certificates of the access point, you must install the Cisco USC CloudBase root and intermediate CA certificates on your USC RMS and SeGW.
7. The access point opens an HTTPS connection to the Activation server using the device certificate obtained in step 6. The access point passes the same information as in the HTTP request in step 1, the versions of software that it has detected and requests to download an ini file, decryption keys, and a software compatibility file.
8. The Activation server creates and returns to the access point through the HTTPS connection an ini file containing calibration data, any certificates, license files, and links to download the operator data and appropriate software release of the access point. The configuration file also includes the associated decryption keys and signatures for each file that the access point may need to download. The configuration file contains:

   - Operator data information:
     - Download URL
     - Blowfish decryption key

     Note: The operator data image has the signature embedded within it.

   - Software release information:
     - Kernel
       - Download URL
       - Blowfish decryption key
       - Signature, checked against the operator software key contained in the key store
     - Root file system
       - Download URL
       - Blowfish decryption key
       - Signature, checked against the operator software key contained in the key store
     - Cisco file system

        - Download URL
        - Blowfish decryption key
        - Signature, checked against the operator software key contained in the key store
    - Public key, key store
        - Download URL
        - Signature

    If the calibration data on the access point does not match the related SHA1 digest downloaded in the previous step, the access point updates its calibration data.

9. The access point checks the kernel, root file system, and Cisco file systems against the signatures returned in step 8. If valid, the signatures in the environment are updated. If any are invalid, the access point requests the appropriate images from the edge cache.
10. The edge cache returns the requested images. The access point decrypts them with the keys provided in step 8 and verifies the signatures provided in that step. If valid, the software images are updated. If they are invalid, the factory upgrade restarts.
11. The access point wipes the configuration file system and then reboots; the access point can now connect to your USC RMS and then be provisioned into service.

6. Cisco USC CloudBase Activation Server

6.1 Server Hosting

The Cisco USC CloudBase software is hosted in two secure data centers located in London and Amsterdam, Amsterdam being the disaster recovery site.

The sites are configured as an active-passive architecture, with each site having:

- Dual active-passive load-balanced front-end web servers
- Replicated database servers
- Replicated file stores
- Dual firewalls
- Denial-of-service (DoS) attack protection

All of the common software images are delivered from Akamai’s edge cache, consisting of more than 100,000 servers worldwide. All of the common software elements are stored as encrypted images on the Akamai edge cache.

7. Cisco USC CloudBase Device Certificate Authority

To help ensure device certificate security integrity and to make it easier to bring in hardware production partners, the device certificates are not signed within the production facilities or installed onto the small cells on the production sites. This architecture is possible because of the activation process, which delivers the device certificate upon activation and thus can eliminate the real-time dependency between the secure generation of the small cell CSR at the production site and the signing of the small cell device CSRs by the certificate authority.

Breaking this real-time dependency enables the certificate authority to be located in Cisco's hosting partner's secure data centers in London and Amsterdam. This scenario prevents any regulatory problems occurring when the certificate authority is located on the production sites, which may be in parts of the world where there are restrictions on the deployment of secure hardware-security-module (HSM) technology critical to the security of the certificate authority. It also helps ensure that the certificate authority is located in a secure location that Cisco can reliably audit.

Within the secure data centers, the certificate authority keys are protected by using Thales secure HSMs, which are FIPS 140 level 3 compliant.

8. Definitions and Abbreviations

8.1 Abbreviations

For the purposes of this document, the following abbreviations apply:

- **CA:** Certificate Signing Authority
- **CSR:** Certificate Signing Request
- **RMS:** RAN Management System
- **OTP:** One-Time Programmable
- **SeGW:** Security Gateway
- **SHA-1:** Secure Hash Algorithm
- **UI:** User Interface
- **USC:** Universal Small Cell

8.2 Notes

Note: As of June 2014, these features form part of Server releases SR3.15 and SR3.16.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Printed in USA C11-730079-01 08/14