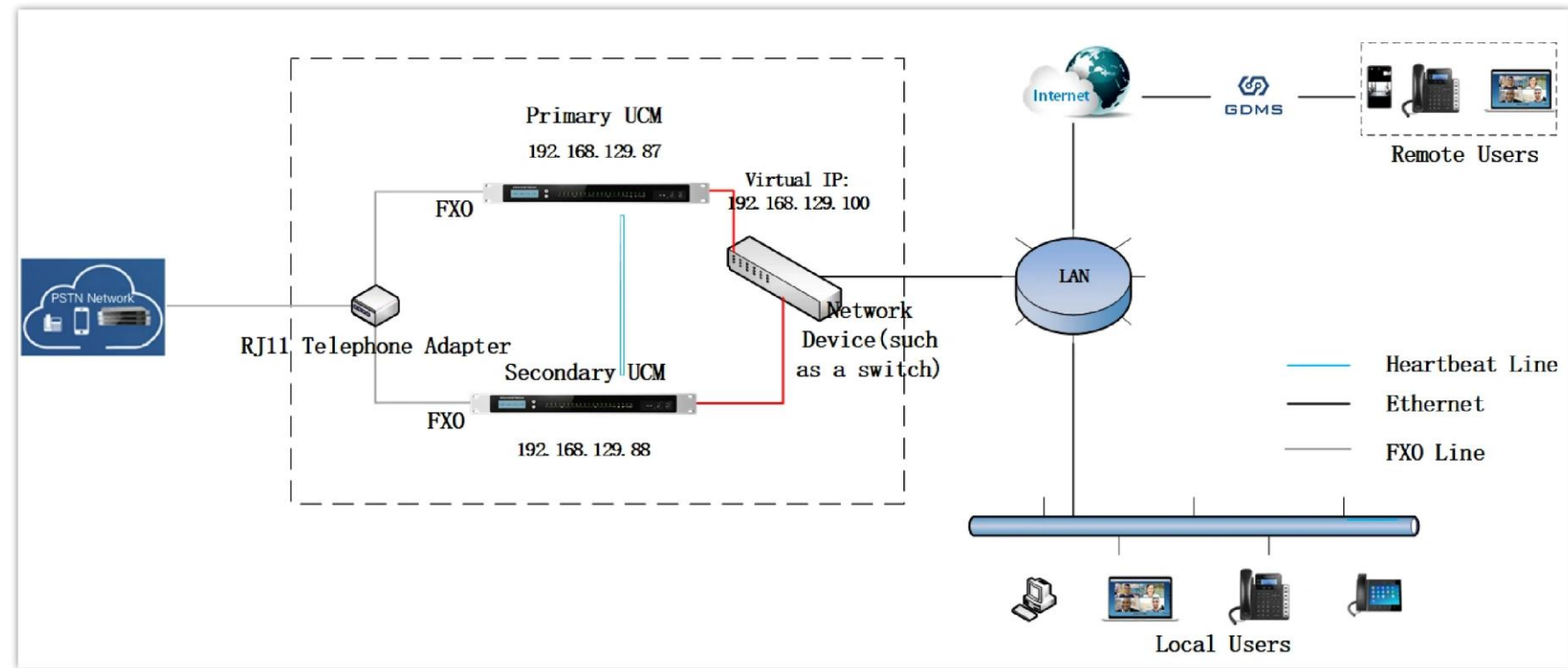


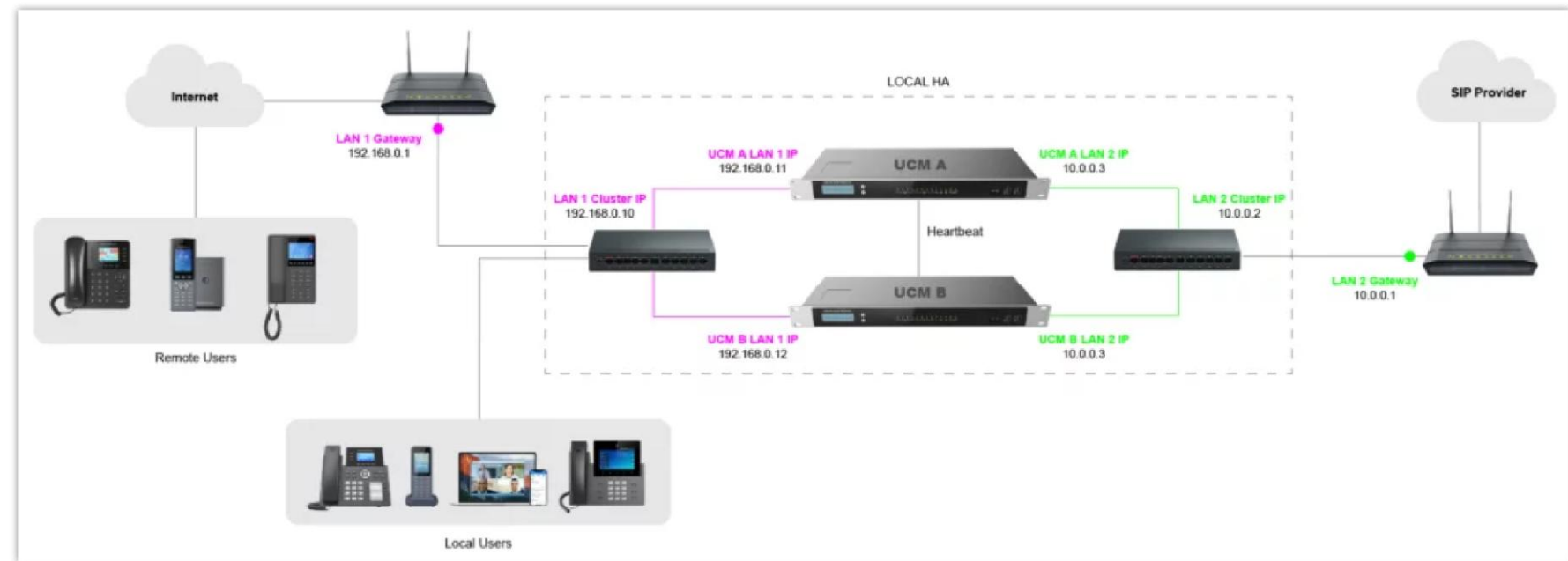
UCM630x/A – High Availability User Guide: Local HA

The High Availability feature on the Grandstream UCM6300 series/UCM6300 Audio series provides enterprises with a reliable solution for PBX redundancy and failover support. In HA setup, there are two UCM with one UCM in the “active” role and the other in the “standby” role. The two UCMs must be the same model and use the same firmware version. The data on the active UCM will be synchronized to the standby UCM in a real-time manner, and the standby UCM monitors the active UCM’s running status regularly. When the active UCM runs into hardware or critical software issues, the standby UCM will take over immediately and become the active server. HA feature supports automatic call recovery for UDP point-to-point calls and conference calls, allowing enterprises to communicate and collaborate without the hassle of service interruption.

TYPICAL NETWORK TOPOLOGY



Typical Local HA Topology Single LAN



Typical Local HA Topology Dual LAN

The two UCMs in the High Availability setup must be deployed in the same location and connected directly to each other via the heartbeat port on each UCM. The primary UCM and secondary UCM can be connected via a straight-through Ethernet cable on the heartbeat port. For each UCM, connect its WAN or LAN port to the uplink network device. For the FXO port, an RJ11 telephone adapter is required to split the PSTN line connection into two ports for each UCM’s FXO port to connect to.

HA PREREQUISITES

Prerequisites

The two UCMs used for High Availability deployment must be the same model and use the same firmware version to ensure proper sync-up on the configuration and data.

Connecting UCM for HA Setup

The two UCMs in the High Availability setup must be deployed in the same location and connected directly to each other via the heartbeat port on each UCM.

- Connect a straight-through Ethernet cable between the heartbeat port on the primary UCM and secondary UCM.
- For each UCM, connect its WAN or LAN port to the uplink network device (such as a switch or router).
- For the FXO port, an RJ11 telephone adapter is required to split the PSTN line connection into two ports for each UCM's FXO port to connect to. The same FXO port must be used on each UCM when connecting to the adapter.

 **Note:**

Please be aware that the UCM heartbeat relies on Ethernet cables (RJ45) with a theoretical maximum length of 100 meters before potential performance degradation may occur.

Network Configuration

Before enabling the High Availability feature, each UCM must be configured with the appropriate network settings.

- The network method can be set to Switch, Route, or Dual Mode.
- All LAN interfaces used by HA must be assigned static IPv4 addresses. These addresses can be configured from **UCM Web UI→Network Settings→Basic Settings**.

Static addressing is required so that the HA cluster IP addresses can be bound consistently to the active node during operation.

Network Settings

Basic Settings

802.1X Settings

Static Routes

Port Forwarding

Port Management

ARP Settings

Method

Switch

MTU

1492

IPv4 Address

IPv6 Address

Network Port Traffic Control

Preferred DNS Server

IP Method

Static

* IP Address

192.168.0.160

* Subnet Mask

255.255.0.0

* Gateway IP

0.0.0.0

* DNS Server 1

DNS Server 2

Enable VLAN

☐

Enable VoIP VLAN

☐

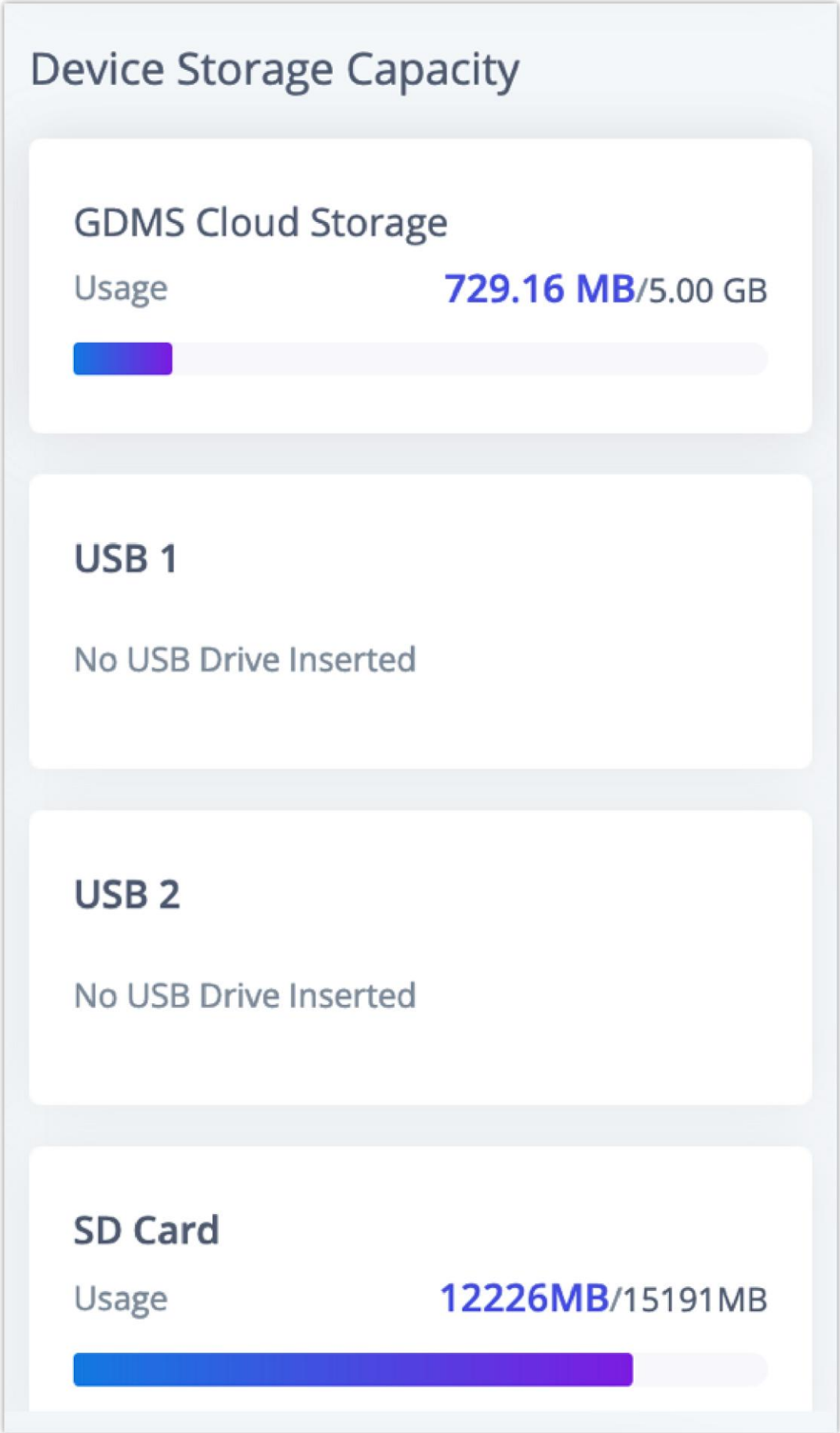
UCM Network Settings

Storage Device

Before enabling the High Availability feature on the two UCMs, the system admin must check to ensure both UCM devices have the same storage devices connected and the same storage configuration in place. This is to ensure that the standby UCM device can store the data normally.

For example, if UCM A has one SD card and one USB storage device connected, UCM B must have a SD card and a USB storage device with the same capacity connected as well. If UCM A has configured to use GDMS cloud storage, UCM B must support and use GDMS cloud storage as well. Please note the UCM admin doesn’t necessarily need to configure the storage path to be the same at this point because the active UCM’s configuration will be applied to the standby UCM after HA is enabled.

The UCM storage configuration and status can be found under UCM webUI → System Status → Dashboard:



Storage Status Under Dashboard

HA Configurations

For UCM without UCM RemoteConnect Plan

HA Configuration Using “Switch” Mode

For two new UCMs on the factory default setting, the system admin can choose to configure any of them for HA first. However, if one of the UCMs is already configured, up and running for PBX service, the system admin should configure this UCM as an HA Primary server and complete all HA settings on it first so it can act as an active role. Assuming no UCMRC (RemoteConnect) service is used on any UCM, please refer to the steps below to configure HA on UCM:

- 1. Ensure both UCMs have the same model and the same firmware version. They have been connected properly at the same location and configured with a static IP. The UCM admin also needs to ensure that the same type and amount of storage is connected to each UCM.
- 2. Select one UCM to be the active device (UCM A). If both UCMs are new on factory default settings, select any of them as the active UCM. If one of the UCMs is already configured and running, then select this UCM as the active device.
- 3. If Cloud IM service is needed, please enable Cloud IM on UCM A (active UCM) and ensure Cloud IM is disabled on the other UCM (UCM B).

Before enabling the High Availability feature on the two UCMs, the system admin must configure each UCM with proper network settings.

The IPv4 address configured on the UCM must be a static IP. It can be configured under **Network Settings > Basic Settings**.

Network Settings

Basic Settings

802.1X Settings

Static Routes

Port Forwarding

ARP Settings

Method :

Switch

MTU :

1492

IPv4 Address

IPv6 Address

Preferred DNS Server :

LAN

IP Method :

Static

* IP Address :

192.168.129.57

* Subnet Mask :

255.255.255.0

* Gateway IP :

192.168.129.1

* DNS Server 1 :

8.8.8.8

DNS Server 2 :

Layer 2 QoS 802.1Q/VLAN Tag :

0

Layer 2 QoS 802.1p Priority Value :

0

Network Settings Switch Mode

- 4. Log in to the active UCM (UCM A) web UI and go to the System Settings→HA page. Enable HA and configure UCM A as the primary station type.

Note:

Please refer to HA-related parameters in the [HA CONFIGURATION PARAMETERS] section below to complete other HA-related settings.

- 4. Save the HA settings on UCM A and reboot UCM A. Ensure UCM A boots up normally.

HA

HA Settings

HA Log

ⓘ When setting up an HA dual-system, please ensure that the the models and firmware versions of the two devices used for HA are the same. Otherwise database compatibility issues may occur.
 When connecting external USB devices, it is recommended to use USB3.0 for both machines. Please ensure that the specifications for both USB devices are the same. Otherwise, you may experience abnormal behavior.
 When enabling HA IPv6 support, it is highly recommended to reboot both UCMs at the same time after completing the HA configuration.

High Available Enable ⓘ

☒

HA Mode ⓘ

☒ Local Hot Standby ⓘ
 ☐ Remote Disaster Recovery ⓘ

Force Switch ⓘ

Switch

* Hot Standby Station Type ⓘ

* Hot Standby Cluster IP ⓘ

* Hot Standby Peer IP ⓘ

* Hot Standby Peer MAC Address ⓘ

* Heartbeat Port ⓘ

* Heartbeat Timeout Period (s) ⓘ

Network Detection ⓘ

☐

Software Fault Switch

☐

Hardware Fault Switch ⓘ

☐ FXO1
 ☐ FXO2

Enable IPv6 ⓘ

☐

Cancel

Save

HA Settings on Primary UCM

- After UCM A restarts with HA parameters configured, verify the HA dual-node status. Log in to UCM A's web UI using its static IP and administrator credentials. Navigate to **System Settings** → **HA**, confirm that the HA function is enabled, then click **HA Status**. UCM A should display as "Active" and operate as a single node.
- Once UCM A is confirmed active, configure UCM B as the secondary node. Log in to UCM B's web UI, go to **System Settings** → **HA** → **HA Settings**, enable the HA function, and set the station type to "Secondary". Complete the other HA-related parameter configurations as per the HA parameter descriptions below. Save the settings and restart UCM B.

HA

HA Settings

HA Log

ⓘ When setting up an HA dual-system, please ensure that the the models and firmware versions of the two devices used for HA are the same. Otherwise database compatibility issues may occur.
 When connecting external USB devices, it is recommended to use USB3.0 for both machines. Please ensure that the specifications for both USB devices are the same. Otherwise, you may experience abnormal behavior.
 When enabling HA IPv6 support, it is highly recommended to reboot both UCMs at the same time after completing the HA configuration.

High Available Enable ⓘ

☒

HA Mode ⓘ

☒ Local Hot Standby ⓘ
 ☐ Remote Disaster Recovery ⓘ

Force Switch ⓘ

Switch

* Hot Standby Station Type ⓘ

* Hot Standby Cluster IP ⓘ

* Hot Standby Peer IP ⓘ

* Hot Standby Peer MAC Address ⓘ

* Heartbeat Port ⓘ

* Heartbeat Timeout Period (s) ⓘ

Network Detection ⓘ

☐

Software Fault Switch

☐

Hardware Fault Switch ⓘ

☐ FXO1
 ☐ FXO2

Enable IPv6 ⓘ

☐

Cancel

Save

HA Settings on Secondary UCM

7. After UCM B restarts with HA parameters configured, log in to UCM B's web UI using **its static IP address and UCM A's administrator credentials**. Navigate to **System Settings** → **HA** and confirm that the HA function is enabled, the "Switch" toggle button is grayed out, and only the HA Peer IP and HA Peer MAC Address options are available for configuration. Click **HA Status** to verify that UCM B's role is displayed as "Standby".

HA	
HA Settings	HA Status
HA Mode	Local Hot Standby
Hot Standby Status	Dual
Hot Standby Full Backup Status	Idle
MAC Address of Current UCM	C0:74:AD:45:3E:40
Role of Current UCM	Standby

HA Status on Secondary UCM

HA Configuration Using "Route" Mode

When UCM's network method is "Route", UCM supports HA local hot standby mode to use IP cluster deployment in the LAN network while using UCM's WAN access for SIP service. Please refer to the configuration below.

Firstly, configure the LAN IP for each UCM in HA (UCM A and UCM B) under UCM web UI->System Settings->Network Settings. Here we configure UCM A LAN IP address as 192.168.2.2, UCM B LAN IP address as 192.168.2.3.

When the DHCP service is running, the DHCP configuration must be the same on both UCMs. If UCM is used as a gateway, please configure the default gateway as the HA Hot Standby Cluster IP address.

The screenshot displays the 'Network Settings' page in the UCM web UI. The left sidebar shows a navigation menu with 'System Settings' expanded, and 'Network Settings' selected. The main content area is titled 'Network Settings' and has tabs for 'Basic Settings', '802.1X Settings', 'Static Routes', and 'Port Forwarding'. The 'Basic Settings' tab is active, showing the 'LAN' configuration section. The 'IP Address' field is set to '192.168.2.2' and is highlighted with a red box. The 'Subnet Mask' is '255.255.255.0'. The 'DHCP Server Enable' checkbox is checked. The 'DNS Server 1' is '8.8.8.8' and 'DNS Server 2' is '208.67.222.222'. The 'Allow IP Address From' field is '192.168.2.100' and 'Allow IP Address To' is '192.168.2.254'. The 'Default Gateway' field is '192.168.2.1' and is also highlighted with a red box. The 'Default IP Lease Time (s)' is '43200'. At the bottom, there are 'Cancel' and 'Save' buttons.

HA UCM A Network Configuration When Network Method is Route

HA UCM B Network Configuration When Network Method is Route

Then, go to UCM web UI > **System Settings** > **HA** > **HA Settings**, configure Hot Standby Cluster IP as an address different from UCM A LAN IP or UCM B LAN IP. As mentioned, if UCM is used as a gateway, the HA cluster IP address is the same as the gateway IP.

For Hot Standby Peer IP, configure the LAN IP of the peer UCM.

UCM A HA Settings

HA

HA Settings

HA Log

ⓘ When setting up an HA dual-system, please ensure that the the models and firmware versions of the two devices used for HA are the same. Otherwise database compatibility issues may occur.
 When connecting external USB devices, it is recommended to use USB3.0 for both machines. Please ensure that the specifications for both USB devices are the same. Otherwise, you may experience abnormal behavior.
 When enabling HA IPv6 support, it is highly recommended to reboot both UCMs at the same time after completing the HA configuration.

High Available Enable ⓘ

☒

HA Mode ⓘ

☒ Local Hot Standby ⓘ
 ☐ Remote Disaster Recovery ⓘ

Force Switch ⓘ

Switch

* Hot Standby Station Type ⓘ

Secondary

* Hot Standby Cluster IP ⓘ

192.168.2.1

* Hot Standby Peer IP ⓘ

192.168.2.2

* Hot Standby Peer MAC Address ⓘ

C0:74:AD:00:00:01

* Heartbeat Port ⓘ

9527

* Heartbeat Timeout Period (s) ⓘ

7

Network Detection ⓘ

☐

Software Fault Switch

☐

Hardware Fault Switch

☐ FXO1 ☐ FXO2

Cancel

Save

UCM B HA Settings

Lastly, go to **PBX Settings > SIP Settings > NAT** to make the following changes:

System Status

Extension/Trunk

Call Features

Messaging

PBX Settings

General Settings

SIP Settings

IAX Settings

RTP Settings

Music On Hold

Voice Prompt

Call Prompt Tones

SIP Settings

General

Session Timer

TCP/TLS

NAT

ToS

STIR/SHAKEN

Misc

External Host

192.168.129.86

Use IP address in SDP

☒

Get External IP via STUN

☐

* External UDP Port

5060

* External TCP Port

5060

* External TLS Port

5061

Local Network Address

IP Address

/

24

Add

Learn more about NAT Settings with the [Remote Work Environment - Setup Guide](#)

LOCAL NETWORK ADDRESS

192.168.2.0

SUBNET MASK

24

UCM A SIP NAT Settings

SIP Settings

General Session Timer TCP/TLS **NAT** ToS STIR/SHAKEN

External Host 192.168.129.81

Use IP address in SDP ☒

Get External IP via STUN ☐

* External UDP Port 5060

* External TCP Port 5060

* External TLS Port 5061

Local Network Address IP Address / 24 **Add**

Learn more about NAT Settings with the [Remote Work Environment - Setup Guide](#)

LOCAL NETWORK ADDRESS	SUBNET MASK
192.168.2.0	24

UCM B SIP NAT Settings

- **“External Host”**: configure as the UCM’s WAN IP.
- **“Local Network Address”**: configure as the UCM LAN subnet. In addition to the UCM LAN subnet, also add the network segment(s) where the phone terminals reside.

Please configure the above separately on each UCM. This configuration enables SIP service access via the WAN IP interface.

HA Configuration Using “Dual” Mode

When the UCM network method is configured as Dual Mode, the system supports Local Hot Standby HA with two independent LAN networks. In this deployment, each UCM uses both LAN1 and LAN2 interfaces, and HA operates using two cluster IP addresses that migrate with the active node.

Before enabling High Availability, ensure the following:

- Both UCM devices use the same model and firmware version.
- LAN1 and LAN2 on both UCMs are configured with static IP addresses.
- The heartbeat connection is properly connected between the two devices.
- The same storage devices and configuration exist on both systems.

To configure the network settings, start by setting LAN IP addresses for both UCMs under **System Settings > Network Settings**.

In this example, the configuration is:

- LAN1 IP: 192.168.0.11
- LAN2 IP: 10.0.0.3

LAN 1

IP Method ⓘ

Static

* IP Address ⓘ

192.168.0.11

* Subnet Mask ⓘ

255.255.255.0

* Gateway IP ⓘ

192.168.0.1

* DNS Server 1 ⓘ

8.8.8.8

DNS Server 2 ⓘ

Enable VLAN

☐

LAN 2

IP Method ⓘ

Static

* IP Address ⓘ

10.0.0.3

* Subnet Mask ⓘ

255.255.255.0

* DNS Server 1 ⓘ

8.8.8.8

DNS Server 2 ⓘ

- LAN1 IP: 192.168.0.12
- LAN2 IP: 10.0.0.4

LAN 1

IP Method ⓘ

Static

* IP Address ⓘ

192.168.0.12

* Subnet Mask ⓘ

255.255.255.0

* Gateway IP ⓘ

192.168.0.1

* DNS Server 1 ⓘ

8.8.8.8

DNS Server 2 ⓘ

Enable VLAN

☐

LAN 2

IP Method ⓘ

Static

* IP Address ⓘ

10.0.0.4

* Subnet Mask ⓘ

255.255.255.0

* DNS Server 1 ⓘ

8.8.8.8

DNS Server 2 ⓘ

To configure HA in dual mode, please follow the steps below:

1. Go to **System Settings**→**HA**→**HA Settings** and check the “**High Availability Enable**” box.
2. Select “**Local Hot Standby**” HA Mode, and configure each UCM separately using the values below.

- **Station Type:** Primary
- **Hot Standby Peer IP:** LAN1 or LAN2 IP address of the Secondary UCM (UCM B)
- **Hot Standby Peer MAC Address:** MAC address of the Secondary UCM (UCM B)

The screenshot shows the 'HA Settings' configuration page. At the top, 'High Available Enable' is a toggle switch that is turned on. Below it, 'HA Mode' has two radio buttons: 'Local Hot Standby' (selected) and 'Remote Disaster Recovery'. A 'Force Switch' button is also present. The 'Hot Standby Station Type' is set to 'Primary' in a dropdown menu. The 'Hot Standby Cluster IP1' and 'Hot Standby Cluster IP2' fields are empty. The 'Hot Standby Peer IP' is set to '192.168.0.12' and the 'Hot Standby Peer MAC Address' is set to 'C0:74:AD:BB:BB:BB'. All the input fields for Peer IP and MAC Address, as well as the Station Type dropdown, are highlighted with red rectangular boxes.

- **Station Type:** Secondary
- **Hot Standby Peer IP:** LAN1 or LAN2 IP address of the Primary UCM (UCM A)
- **Hot Standby Peer MAC Address:** MAC address of the Primary UCM (UCM A)

The screenshot shows the 'HA Settings' configuration page for a secondary station. The settings are identical to the primary station's page, except for the 'Hot Standby Station Type' which is set to 'Secondary'. The 'Hot Standby Peer IP' is set to '192.168.0.11' and the 'Hot Standby Peer MAC Address' is set to 'C0:74:AD:AA:AA:AA'. The input fields for Peer IP and MAC Address, as well as the Station Type dropdown, are highlighted with red rectangular boxes.

Note:

- It is recommended to use the **LAN1 IP addresses** in the *Hot Standby Peer IP* field to ensure a reliable control path.

◦ Both LAN1 and LAN2 are required network paths. If the active UCM loses physical link on either LAN interface, the system treats this as a hardware fault.

3. In Dual Mode, the HA configuration requires two cluster IP addresses that are identical on both UCMs (A & B):
- **Hot Standby Cluster IP1:** Cluster IP in the LAN1 subnet.
 - **Hot Standby Cluster IP2:** Cluster IP in the LAN2 subnet.

* Hot Standby Cluster IP1 ⓘ	192.168.0.10
* Hot Standby Cluster IP2 ⓘ	10.0.0.2

⚠ Notes:

- The cluster addresses must not be the same as the LAN IP addresses configured on either UCMs.
- Cluster IP1 and Cluster IP2 must not be the same.
- Cluster IP1 and Cluster IP2 follow the active node, but they are only reachable within their respective networks.
- If certain destinations must traverse LAN2, configure static routes to direct only those networks through LAN2.

4. On both UCMs, set the same *Heartbeat Port and Timeout*. The default heartbeat port is 9527. When the timeout is reached and the peer is not detected, failover will be triggered.

* Heartbeat Port ⓘ	9527
* Heartbeat Timeout Period (s) ⓘ	7
Network Detection ⓘ	☒
Software Fault Switch	☐

Heartbeat Configuration

5. (Optional) Enable Software Fault Switch and/or Hardware Fault Switch. When enabled, the system will trigger failover when critical software or hardware faults are detected.
6. Click Save, then reboot both UCMs to apply the HA configuration.

Reboot Device

HA settings updated successfully. Reboot the device now to apply changes?

Cancel

Reboot

After both systems reboot, log in to the UCM interface and navigate to **System Settings→HA→HA Status**. Confirm that each UCM displays the following:

- **HA Mode:** Local Hot Standby
- **Hot Standby Status:** Dual
- **MAC Address of Current UCM:** UCM A MAC address
- **Role of Current UCM:** Active

HA	
HA Settings	HA Status
HA Log	
HA Mode	Local Hot Standby
Hot Standby Status	Dual
Hot Standby Full Backup Status	Idle
MAC Address of Current UCM	C0:74:AD:AA:AA:AA
Role of Current UCM	Active

- **HA Mode:** Local Hot Standby
- **Hot Standby Status:** Dual
- **MAC Address of Current UCM:** UCM B MAC address
- **Role of Current UCM:** Standby

HA	
HA Settings	HA Status
HA Log	
HA Mode	Local Hot Standby
Hot Standby Status	Dual
Hot Standby Full Backup Status	Idle
MAC Address of Current UCM	C0:74:AD:BB:BB:BB
Role of Current UCM	Standby

After configuration is complete, both cluster IP addresses (*Cluster IP1 and Cluster IP2*) follow the active node (*UCM A*). During fail over, they automatically migrate to the standby UCM (*UCM B*), ensuring continuous service on both networks.

For UCM with the UCM RemoteConnect Plan

Scenario 1: Two new UCMs on factory default settings, and both UCMs use the UCM RemoteConnect service.

1. Ensure both UCMs have the same model and the same firmware version. They have been connected properly at the same location and configured with a static IP. The UCM admin also needs to ensure that the same type and amount of storage devices are connected to each UCM.
2. Since both UCMs are on factory settings, select any of the UCMs to be the active UCM (UCM A).
3. If Cloud IM service is needed, please enable Cloud IM on UCM A (active UCM) and ensure Cloud IM is disabled on the other UCM (UCM B). When UCM uses Cloud IM servers from GDMS, please ensure that both UCMs have a UCM RemoteConnect plan with Cloud IM support.

4. Log in to the active UCM (UCM A) web UI and go to the System Settings→HA page. Enable HA and configure UCM A as the primary station type. Please refer to HA related parameters in Table 2 below and complete the other HA-related settings. Save the HA settings on UCM A and reboot UCM A. Ensure UCM A boots up normally.
5. Verify HA status on UCM A. Log in to UCM A using its static IP and admin login information. On the web UI→System Settings→HA page, ensure HA function is enabled. HA status should display as “Active”.
6. After ensuring UCM A’s HA status is active, configure UCM B as a secondary UCM and complete its HA settings. Log in to UCM B’s web UI and go to System Settings→HA page, enable HA, and set the station type as “Secondary”. Please refer to HA related parameters in Table 2 below to complete other HA-related settings. Save the settings and reboot UCM B.
7. Verify UCM B’s HA status. UCM B boots up normally, log in to UCM B’s web UI via the static IP address and admin login information. Go to the System Settings→HA page, ensure the HA function is enabled, the “Switch” button is grey, and only HA Peer IP / Peer MAC address options are available for configuration.
8. Purchase the UCM RemoteConnect plan for both UCM. Log in UCM web UI and go to the WebUI→RemoteConnect→Plan page, click on “Learn More”. Then follow the page to add the 2 UCM to GDMS and assign the UCM RemoteConnect plan for them. It doesn’t matter which UCM is assigned the UCM RemoteConnect plan first.
9. For UCM A, which has a station type of “Primary”, configure a custom domain name. Please refer to the “Custom Domain Configuration” section below.

 Note:

For UCMRC-related settings, please refer to section “UCMRC Configurations”.

Scenario 2: 1 UCM is configured and running, and the 2nd UCM needs to be added for HA setup. Both UCMs use the UCM RemoteConnect service.

1. Ensure both UCMs have the same model and the same firmware version. They have been connected properly at the same location and configured with a static IP. The UCM admin also needs to ensure that the same type and amount of storage devices are connected to each UCM.
2. Since UCM A is already configured and running, choose this UCM as the active UCM.
3. If Cloud IM service is needed, please enable Cloud IM on UCM A (active UCM) and ensure Cloud IM is disabled on the other UCM (UCM B). When UCM uses Cloud IM servers from GDMS, please ensure that both UCMs have a UCM RemoteConnect plan with Cloud IM support.
4. Log in to the active UCM (UCM A) web UI and go to the **System Settings > HA page**. Enable HA and configure UCM A as the primary station type. Please refer to HA related parameters in Table 2 below and complete the other HA-related settings. Save the HA settings on UCM A and reboot UCM A. Ensure UCM A boots up normally.
5. Verify HA status on UCM A. Log in to UCM A using its static IP and admin login information. On the web **UI > System Settings > HA** page, ensure HA function is enabled. HA status should display “Active”.
6. After ensuring UCM A’s HA status as active, now configure UCM B as a secondary UCM and complete its HA settings. Log in to UCM B’s web UI and go to **System Settings > HA** page, enable HA, and set the station type as “Secondary”. Please refer to HA related parameters in Table 2 below to complete other HA-related settings. Save the settings and reboot UCM B.
7. Verify UCM B’s HA status. UCM B boots up normally, log in to UCM B’s web UI via the static IP address and admin login information. Go to **System Settings > HA** page, ensure the HA function is enabled, the “Switch” button is grey, and only HA peer IP/HA MAC address buttons are available for configuration.
8. Purchase the UCM RemoteConnect plan for each UCM and ensure the purchased plan for each UCM has the same specification and supports HA. It doesn’t matter which UCM is assigned the UCM RemoteConnect plan first.
9. For UCM A, which has a station type of “Primary”, configure a custom domain name. Please refer to the custom domain name configuration section below. If UCM A already has a custom domain name, this step can be skipped.

 Note:

For UCM RemoteConnect related settings, please refer to section “UCMRC Configurations”.

HA CONFIGURATION PARAMETERS

Settings	Description	Value Range	Default Value	Notes
High Available Enable	Enable or disable HA.	Toggle On/Off	No	–
HA Mode	Configure HA mode. “Local Hot Standby”: Deploy HA in the same location which provides redundancy and recovery in case the primary UCM has hardware issues. “Remote Disaster Recovery”: Deploy two UCMs in different locations to prevent service interruption in case of large-scale disaster at the primary UCM site.	Local Hot Standby Or Remote Disaster Recovery	Local Hot Standby	For “Local Hot Standby”, must use network mode “Switch” or “Router” and use static IP address. For “Remote Disaster Recovery” UCM must be configured static IP. Grandstream endpoints are fully supported. UCM HA remote disaster recovery feature for failover.
Force Switch	Force to switch the roles of active UCM and standby UCM.	NA	NA	Caution: Please do not use this function unless necessary (it can be used during firmware upgrading).
Hot Standby Station Type	Configure the HA station type for the UCM.	Primary Secondary	NA	In HA setup, one UCM must be primary and the other one must be secondary.
Hot Standby Cluster IP	This is the IP address for the active UCM in service.	NA	NA	This IP address is shared by the primary and secondary UCM. The UCM in active status providing PBX service will always be using this IP address regardless it’s the primary or secondary UCM. This IP address can only be used by the active UCM.
Hot Standby Peer IP	This is the IP address of the peer UCM in HA setup.	NA	NA	This is the static IP address of the peer UCM in HA setup connected via heartbeat.
Hot Standby Peer MAC Address	This is the MAC address of the peer UCM in HA setup.	NA	NA	This is the MAC address of the peer UCM in HA setup connected via heartbeat.
Heartbeat Port	This is the port used for communication between the two UCM via the heartbeat port.	0 – 65535	9527	It is recommended to use the default port.
Heartbeat Timeout Period (s)	This is the heartbeat timeout period that active and standby UCM will check with each other for the status (in seconds).	3 – 10	7	If the standby UCM detects the active UCM disconnected and it reaches the timeout, failover will be triggered and the standby UCM will start taking over as active UCM.
Network Detection	Enable/Disable Network Detection feature. When enabled, the active device continuously checks reachability to the configured detection node(s).	Toggle On/Off	Off	–

	If the active device loses connectivity to any configured detection node a switchover is triggered and the standby device assumes the active role. Note: HA settings on both the active and standby UCM must be consistent. In case of inconsistency, the settings on the active device will be prioritized.			
Network Detection Node (Appears when the UCM networking mode is set to Route or Switch)	Displayed in Switch and Route mode. If connectivity to this node is lost on the active device, a switchover is triggered. Notes: • The standby device does not initiate switchover on its own. • Only IP addresses are supported. • For correct operation, this setting must be configured identically on active and standby devices.	IPv4 IP Address	N/A	–
Network Detection Node 1 (Appears when the UCM networking mode is set to Dual)	Displayed in Dual mode. This detection node associated with Cluster IP1 / LAN1. If connectivity to this node is lost on the active device, a switchover is triggered. Notes: • The standby device does not initiate switchover on its own. • Only IP addresses are supported. • For correct operation, this setting must be configured identically on both devices.	IPv4 IP Address	N/A	–
Network Detection Node 2 (Appears when the UCM networking mode is set to Dual)	Displayed in Dual mode. Detection node associated with Cluster IP2 / LAN2. If configured, loss of connectivity to this node on the active device will also trigger a switchover. Notes: • The standby device does not initiate switchover on its own. • Only IP addresses are supported. • For correct operation, this setting must be configured identically on both devices.	IPv4 IP Address	N/A	–

Software Fault Switch	Enable failover upon software failure	On/Off	Off	If enabled, when there is software failure such as deadlock or system crash detected, it will trigger failover from active UCM to standby UCM. Otherwise, failover will not happen.
Hardware Fault Switch	Enable failover upon hardware failure	On/Off	Off	If enabled, when there is hardware failure such as port no longer working, it will trigger failover from active UCM to standby UCM. Otherwise, failover will not happen.
Enable IPv6	If enabled, HA will support IPv6 while compatible with IPv4.	On/Off	Off	Please enable this option if required for HA deployment. Otherwise, please keep it disabled. Before enabling this option, please configure both UCMs with static IPv6 address.
Sync External Storage Files	Syncs externally stored files (USB, SD Card, etc.) on the Active UCM to the Standby UCM's external storage. External storage must be of the same type and capacity. It is recommended to manually sync existing external storage files after setting up HA for the first time. Files created after HA has been set up will be automatically synced. Currently configured storage paths can be viewed on the File Manager page.	N/A	N/A	–

HA Related Parameters

After the above configurations, click on Save and follow the reboot prompt to reboot the device.

 **Critical Note**

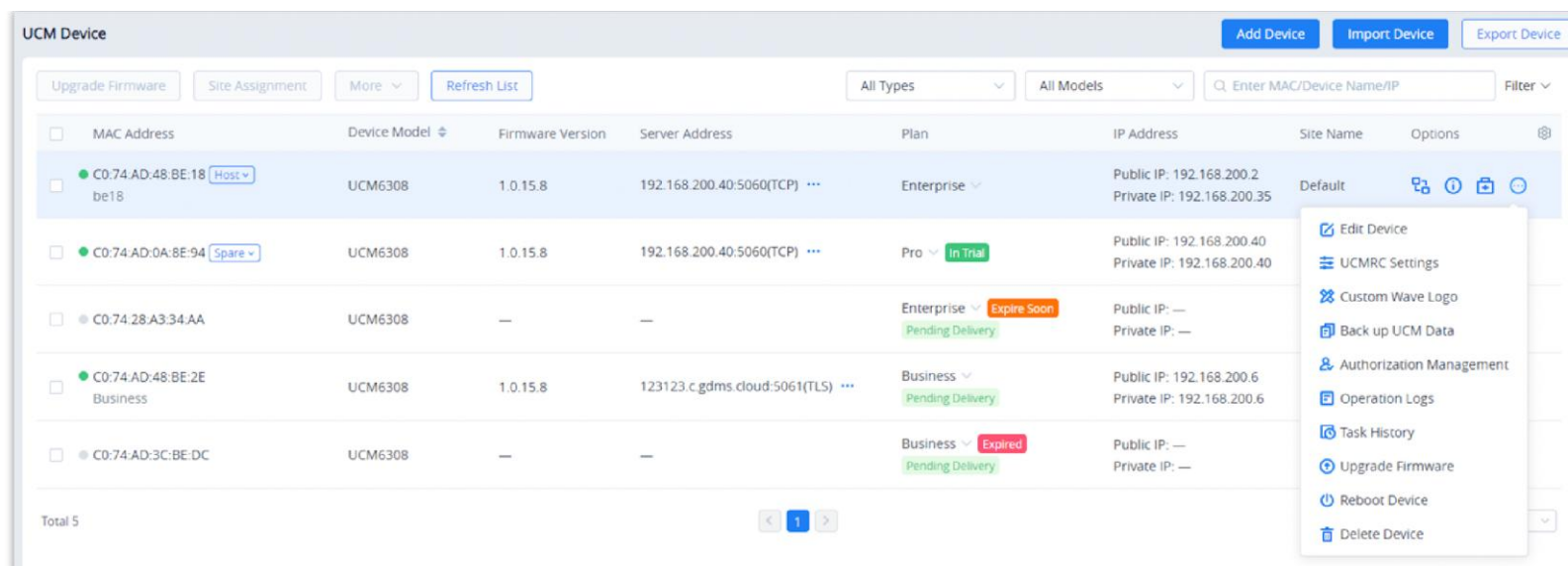
HA configuration requires the UCM to reboot. Please reboot the UCM during non-service hours to avoid service interruption.

UCM RemoteConnect Configurations

UCM RemoteConnect Plan

To ensure that the UCM RemoteConnect plan can be used normally on HA setup, the UCM RemoteConnect plan must be purchased and assigned to both UCM on GDMS. If only one UCM has a UCM RemoteConnect plan, the GDMS operation may fail due to HA backup. If only one UCM has the UCM RemoteConnect plan with HA support, HA-related functions will not work in HA deployment.

Log into GDMS web UI and go to UCMRC→UCM Devices. Click to add a new device and enter the UCM information.



Add UCM to GDMS

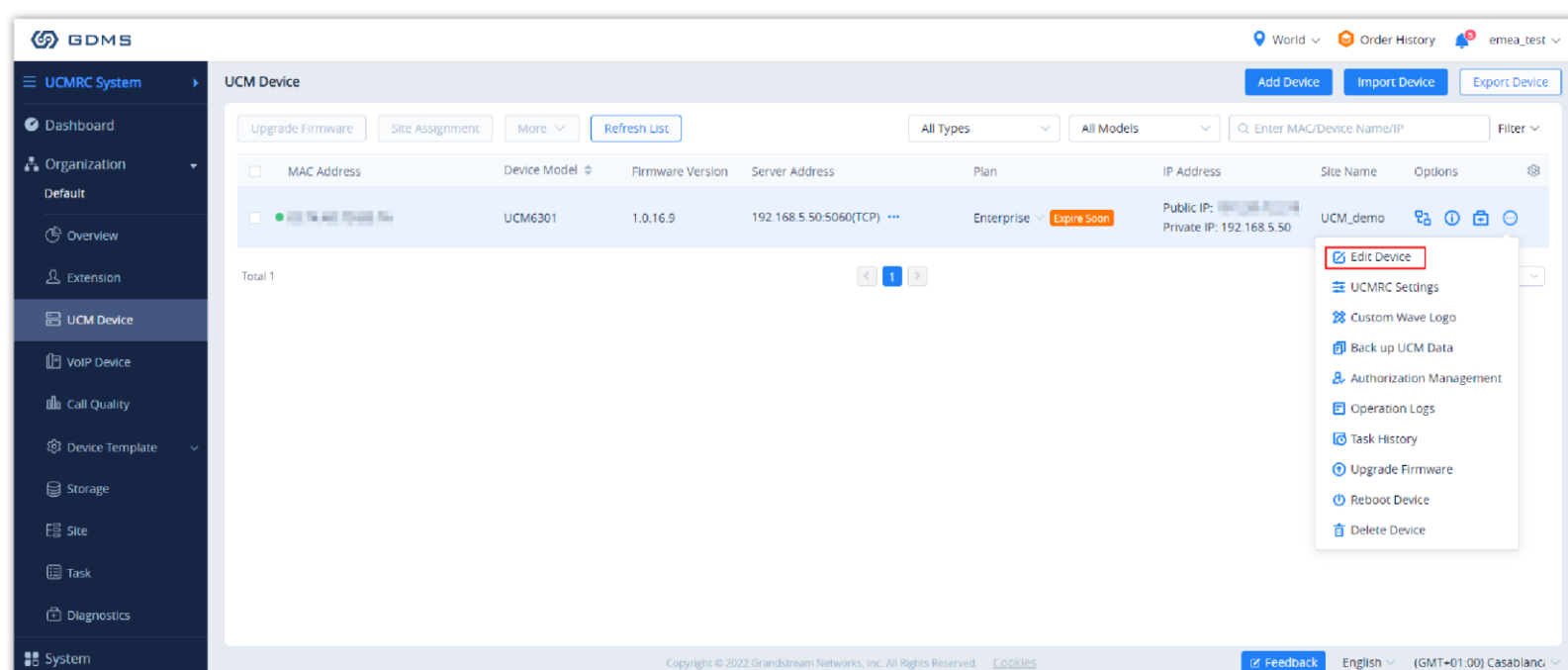
Custom Domain Configuration

Info

If you need to purchase the UCM RemoteConnect plan with a custom domain, please use the following link to refer to more details and to purchase the corresponding plan. <https://ucmrc.gdms.cloud/plans>

For two UCM devices that have purchased the UCMRC package with HA service, you must configure a custom server address or domain name for the **UCM set as Primary**.

Custom Domain Name must be set via GDMS. Log in to GDMS and go to UCMRC System→UCM Devices, select the UCM, and click on “Edit Device” to configure it.



Edit Device

Edit Device

MAC Address

C0:74:AD:53:73:72

Device Name

89-57

*

Site

Default

Zone

e.gdms.cloud (Miami)

Access Server

c074ad537372-16781.e.gdms.cloud

Switch to Custom Domain

*

Custom Server Address

.e.gdms.cloud

Cancel

Save

Configure Custom Domain

Click on “Switch to Custom Domain” to edit device custom server access, private secret key, etc. Save the configuration. After changing the custom domain name, please notify UCM users of the new public address for UCM. For more information about configuring a custom domain name on GDMS, please refer to the GDMS user manual.

!

Note:

If you need to purchase a UCMRC plan with HA service rights, please contact the corresponding equipment agent for more details.

Verify HA Settings

- After configuring HA settings on both UCMs, log in to the UCM web UI from each UCM’s static IP using the active UCM’s login information and check HA status. Under the HA status page, both UCMs should show HA Status as “Dual”. One of the UCMs should show its role as “Active” and the other one should show “Standby”. For “HA Full Backup Status”, it will show backup in progress during backup and show as idle during the rest of the time.

HA	
HA Settings	HA Status
HA Status:	Dual
HA Full Backup Status:	Idle
MAC Address of Current UCM:	C0:74:AD:53:73:72
Role of Current UCM:	Active

HA Status for Active UCM

HA

HA Settings

HA Status

HA Log

HA Status :

Dual

HA Full Backup Status :

Idle

MAC Address of Current UCM :

C0:74:AD:53:73:6C

Role of Current UCM :

Standby

HA Status for Standby UCM

2. Log in to the active UCM’s web UI and create new SIP extensions. Then log in to the standby UCM’s web UI to check whether the same extensions created on the active UCM are synchronized here. If there are already endpoints registered to UCM, both UCMs should show the same extensions and registration status. This indicates that the active UCM’s data has been synchronized to the standby UCM.

Verify HA Status via GDMS

GDMS allows the user to verify which UCM is primary and which one is secondary. On the GDMS interface, go to the **UCM Device** tab.

UCM Device

Add Device

Import Device

Export Device

Upgrade Firmware

Site Assignment

More

Refresh List

All Models

Q. Enter MAC/Device Name/IP

Filter

☐	MAC Address	Device Model	Firmware Version	Server Address	Plan	IP Address	Site Name	Options
☐	ucm Host	UCM6302	1.0.13.5	192.168.5.92:5061(TLS)	Open Beta	Public IP: Private IP: 192.168.5.92	ucm	
☐	UCM6302_LAB Spare	UCM6302	1.0.13.5	192.168.5.92:5061(TLS)	Open Beta	Public IP: Private IP: 192.168.5.58	Default	

Total 2

<

1

>

10/page

UCM Devices

- **Host:** indicates the primary UCM.
- **Spare:** indicates the secondary UCM.

If you want to check which UCM is performing high availability with which UCM, click on “spare” or “host” to verify, as indicated in the screenshots below.

UCM Device

Upgrade Firmware

Site Assignment

More

Refresh List

☐	MAC Address	Device Model	Firmware Version
☐	ucm Host	UCM6302	1.0.13.5
☐	UCM6302_LAB Spare	UCM6302	1.0.13.5

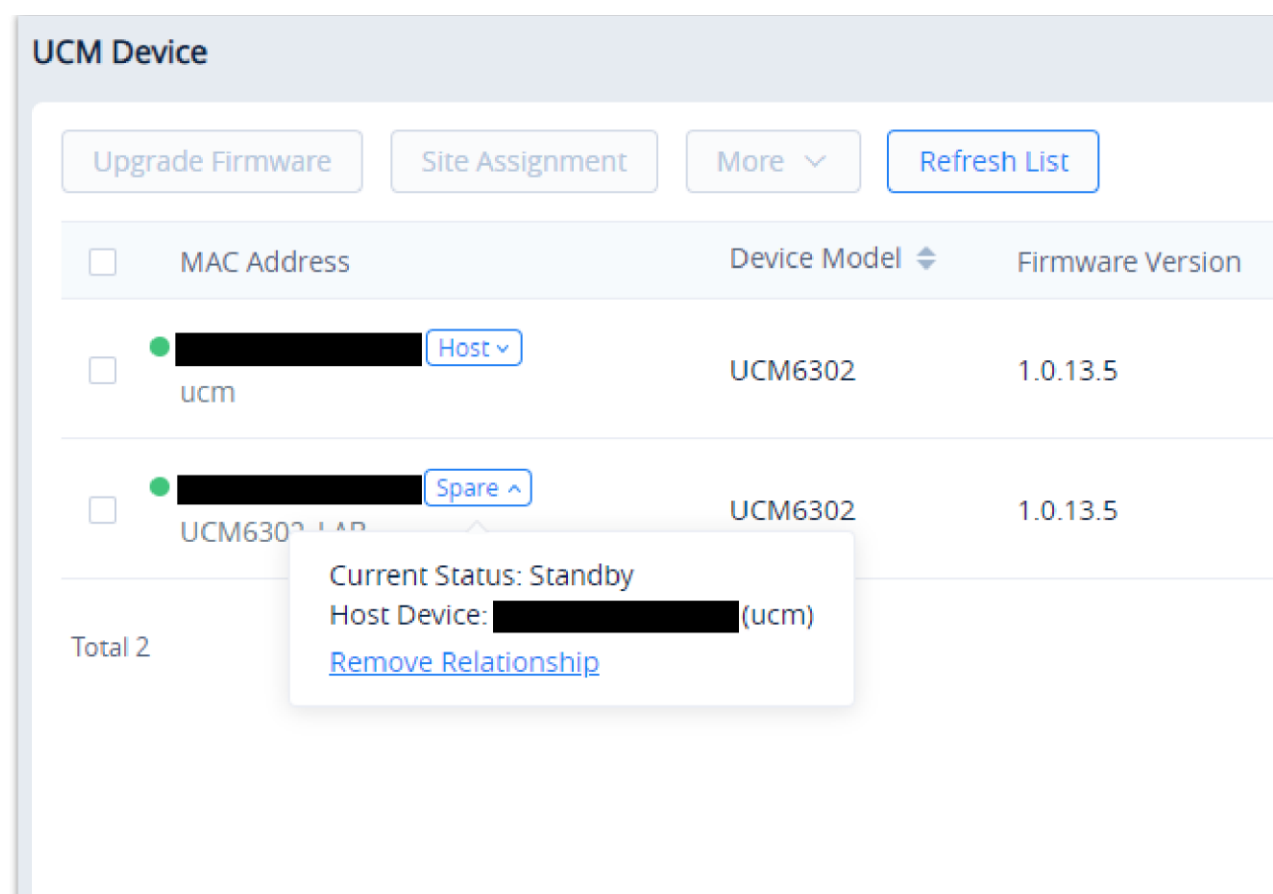
Total 2

Current Status: Active

Spare Device: (UCM6302_LAB)

[Remove Relationship](#)

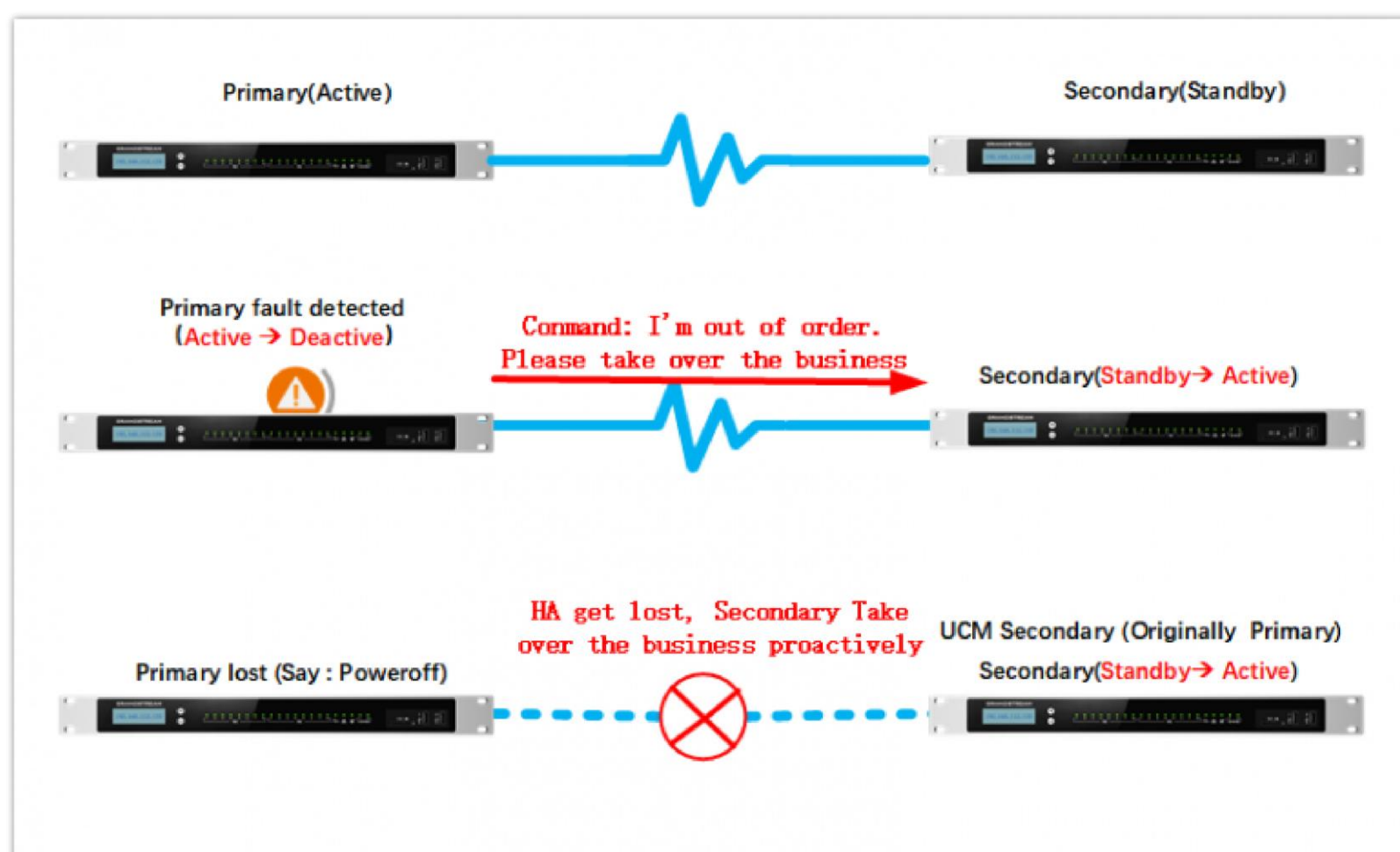
Active UCM



Idle UCM

Active/Standby Role in HA

Automatic Failure Detection



Active and Standby UCM Failover

Important Note

In case of a failure, the user needs to manually unplug the LAN cable from the formerly Active UCM and plug it into the newly Active UCM to fully restore connection with the SIP endpoints.

Active UCM: Self-Failure Detection

The active UCM monitors and regularly checks whether there is any failure on itself. When there is a failure detected on itself, it will notify the standby UCM to take over as an active server. Then the original active UCM will reboot automatically and become the standby server. This scenario applies to an active UCM that has part of the function or specific service in a faulty status, and it can still work partially without shutting down the service completely.

For example, if the active server has a core dump generated for the core service, FXO port failure, or WAN/LAN port disconnection, with this detection and notification mechanism, the standby UCM can take over immediately without noticeable delay or service interruption.

Standby UCM: Periodic Heartbeat

On HA mode, the standby UCM will check the active UCM’s status periodically by sending a heartbeat message to the active UCM. The heartbeat message is sent via the heartbeat port. If the active UCM is under normal working conditions, it will respond to the standby UCM after it receives a heartbeat request from the standby UCM. If the active UCM runs into a faulty situation, such as the network chip becomes abnormal or the power adapter no longer works, it will stop responding to heartbeat requests. After the heartbeat period times out, the standby UCM will consider the active UCM as faulty and start taking over as the active server.

The heartbeat timeout period determines how soon the standby UCM can detect an active server’s failure and switch over. By default, the heartbeat timeout period is 7 seconds. Users could modify the heartbeat timeout period as preferred, and this will affect the detection/switchover sensitivity.

Force Switch

For a UCM currently in the Active role, you can click the Switch button to change between Active and Standby roles. This operation is generally avoided unless performing a firmware upgrade or if the current Active UCM encounters a problem that requires manual switching.

HA

HA Settings

HA Log

High Available Enable ⓘ

HA Mode ⓘ

Local Hot Standby ⓘ

Remote Disaster Recovery ⓘ

Force Switch ⓘ

Switch

* Hot Standby Station Type ⓘ

Primary

* Hot Standby Cluster IP ⓘ

192.168.5.222

* Hot Standby Peer IP ⓘ

192.168.5.92

* Hot Standby Peer MAC Address ⓘ

C0:74:AD:45:3E:40

* Heartbeat Port ⓘ

9527

* Heartbeat Timeout Period (s) ⓘ

7

Network Detection ⓘ

Software Fault Switch

Hardware Fault Switch ⓘ

FXO1

FXO2

Enable IPv6 ⓘ

Sync External Storage Files ⓘ

Sync

Learn more about HA Settings with the [HA Local Standby User Guide](#) | [HA Remote Disaster Recovery User Guide](#)

Cancel

Save

Force Switch

Firmware Upgrade

To ensure that there is no service interruption in HA setup, upgrading UCM requires the user to follow the steps below strictly:

- **Step 1:** Log in to the web UI of the standby UCM (A), upload firmware via web UI, and the standby UCM will reboot. Wait for it to boot up.
- **Step 2:** After the standby UCM (A) boots up, log in to the web UI of the active UCM (B) and check the HA web page. The “Force Switch” button on the UCM B’s HA web page will be available. Press it to manually trigger a switchover. After switchover, UCM A will become active, and UCM B will become standby.
- **Step 3:** After switchover, log in to UCM B and upload firmware to its web UI. UCM B will reboot and request data from UCM A for a full backup.

In short, when upgrading UCM in an HA setup, the standby UCM needs to be upgraded first and becomes the active UCM. Then we can upgrade the standby UCM. This will ensure the active UCM is always working and providing PBX functions, so there is no service interruption during upgrading or switchover.

Replacing UCM in HA

HA Setup with UCM RemoteConnect

Assuming 2 UCM (A and B) with UCMRC plan on GDMS have been set up for HA, and UCM B becomes defective, which requires replacement, please follow the steps below to replace the defective UCM B with UCM C.

Scenario 1: UCM A’s station type is “Primary” and it’s the active UCM. UCM B’s station type is “Secondary” and it’s in standby status.

1. Add UCM C to GDMS first. Then assign the UCM RemoteConnect plan to UCM C. The UCMRC plan can be a new plan for UCM C or transferred from UCM B.
2. Turn off the power for UCM B.
3. Modify UCM A’s HA settings by changing the HA Peer MAC address from UCM B to UCM C’s MAC address. Save and reboot UCM A.
4. After UCM A boots up, log in UCM A web UI and confirm the HA status to be Active. Connect UCM C to the HA setup using appropriate cables for the WAN port, heartbeat port, FXO port, etc.
5. After powering on UCM C, log in to UCM C’s web UI and configure the basic network settings to match those of UCM B. Ensure that UCM C is set with the same site type and the same static IP address as UCM B.
6. Check if Cloud IM is enabled on UCM C. If it is enabled, disable Cloud IM to ensure that UCM C can replace UCM B without the Cloud IM service active.
7. Log in to UCM C’s web UI, enable HA, configure HA station type and other HA settings to be the same as UCM B. Save and reboot UCM C.
8. After UCM C boots up, check and verify the HA status. UCM A should be active, and UCM C should be standby.

Scenario 2: UCM A’s station type is “Secondary” and it’s the active UCM. UCM B’s station type is “Primary” and it’s in standby status.

1. On GDMS, delete the custom domain name for UCM B.
2. Add UCM C to GDMS and assign the UCMRC plan to UCM C. The UCMRC plan can be a new plan for UCM C or transferred from UCM B. On GDMS, configure the custom domain name for UCM C to be the same as the one for UCM B. Please note that UCM C must have a custom domain name configured on GDMS.
3. Turn off the power for UCM B.
4. Modify UCM A’s HA settings by changing the HA Peer MAC address from UCM B to UCM C’s MAC address. Save and reboot UCM A.

5. After UCM A boots up, log in UCM A web UI and confirm the HA status to be Active. Connect UCM C to the HA setup using appropriate cables for the WAN port, heartbeat port, FXO port, etc.
6. After powering on UCM C, log in to UCM C's web UI and configure the basic network settings to match those of UCM B. Make sure UCM C is set with the same site type and static IP address as UCM B.
7. Check whether Cloud IM is enabled on UCM C. If it is enabled, disable Cloud IM to ensure UCM C can replace UCM B without the Cloud IM service active.
8. Log in to UCM C's web UI, enable HA, configure HA station type and other HA settings to be the same as UCM B. Save and reboot UCM C.
9. After UCM C boots up, check and verify the HA status. UCM A should be active, and UCM C should be on standby.

HA Setup without UCM RemoteConnect

Assuming 2 UCM (A and B) in the HA setup have no UCMRC plan on GDMS, UCM A is in active status, and UCM B is in standby status. UCM B becomes defective and requires replacement. Please follow the steps below to replace the defective UCM B with UCM C:

1. Turn off the power for UCM B.
2. Modify UCM A's HA settings by changing the HA Peer MAC address from UCM B to UCM C's MAC address. Save and reboot UCM A.
3. After UCM A boots up, log in UCM A web UI and confirm the HA status to be Active. Connect UCM C to the HA setup using appropriate cables for the WAN port, heartbeat port, FXO port, etc.
4. After powering on UCM C, log in to UCM C's web UI and configure the basic network settings to be the same as UCM B. Ensure that UCM C is configured with the same site type and static IP address as UCM B.
5. Check whether Cloud IM is enabled on UCM C. If it is enabled, disable Cloud IM to ensure UCM C can replace UCM B without the Cloud IM service active.
6. Log in to UCM C's web UI, enable HA, configure HA station type and other HA settings to be the same as UCM B. Save and reboot UCM C.
7. After UCM C boots up, check and verify the HA status. UCM A should be active, and UCM C should be on standby.

Critical Note:

HA configuration requires the UCM to reboot. Please reboot the UCM during non-service hours to avoid service interruption.

Disabling HA Setup

If the HA setup is no longer required for the UCM, log in to the web UI using the active UCM's IP or the cluster's IP and go to the system settings→HA page to disable HA. Save and reboot the UCM. After both UCM boot up, check the HA status, and it should show HA as off.

Cloud IM in HA Setup

Please ensure only one UCM in the HA setup has Cloud IM enabled. If using a domain name assigned from GDMS, please ensure both UCM devices have the UCM RemoteConnect plan, which supports Cloud IM.

After the active UCM A in HA setup enables Cloud IM, the standby UCM B will synchronize from UCM A and obtain Cloud IM service as well. Cloud IM service is always available on the active UCM, and the associated MAC address will change if the active/standby UCM changes. Therefore, failover in the HA setup does not affect the Cloud IM service.

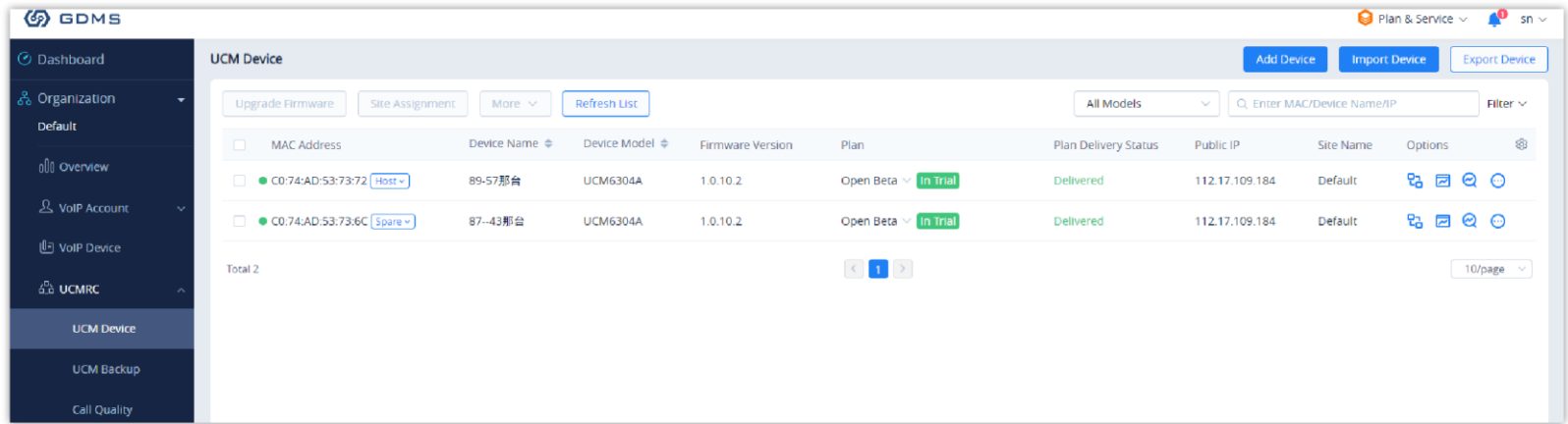
If UCM B fails and a replacement UCM C with Cloud IM disabled takes its place to form a dual-node HA system with UCM A, Cloud IM will continue to provide HA services for both nodes without any additional configuration. However, if Cloud IM was previously enabled on UCM C, it must be disabled before swapping to ensure Cloud IM is not active when UCM C replaces UCM B.

Using UCM RemoteConnect with HA

If the user has purchased a UCM RemoteConnect plan with HA, the GDMS web page can show the UCM with HA status “Host” or “Spare”.

Note

For more information about UCMRC plans, please refer to the following link: <https://ucmrc.gdms.cloud/plans>



GDMS Display for UCM HA Status

Switching UCM RemoteConnect Role in HA

Prerequisites:

- Both UCMs must have the UCM RemoteConnect plan with the HA feature purchased on GDMS.
- UCMRC service has been successfully delivered to both UCM.

Implementations:

- The call service is provided by GDMS and the active UCM.
- When the active UCM A is faulty condition and has triggered a switchover, the standby UCM B will take over and become active. UCM B will send the switchover command to GDMS and notify GDMS that call service will be provided by UCM B and GDMS afterwards.

Note

1. With UCMRC, after the UCM is configured with HA, UCM will notify its HA role to GDMS. System admin does not need to designate the HA role for UCM on GDMS.

2. On GDMS, the system admin can still remotely access and operate each UCM in HA. However, the configuration on the standby UCM is limited because it synchronizes data from the active UCM regularly in the HA backup process.

3. The PBX providing service is the active UCM. However, GDMS will always assign the domain name for the Remote Connect service based on the primary UCM as configured initially.

Service Status

Active/Standby Status

After the HA setup is completed, the PBX will provide service using the HA cluster IP. During the initial stage, the standby UCM will request and synchronize all data from the active UCM.

The standby UCM monitors and prepares to become active at any time when needed. Manual configuration on standby UCM is restricted because it always synchronizes up data from active UCM. When the active UCM has any hardware or critical software failure, the standby UCM will immediately take over and become the active UCM. The previous active UCM will reboot and become the standby UCM. Calls during the role switchover will be recovered after the failover process completes.

Web UI Access for UCM

After the HA setup is completed, the cluster IP becomes a floating IP for providing external services. To log in to the UCM web UI, the system admin only needs to enter the cluster IP address. Regardless of any role switch, the floating IP remains unchanged and is always bound to the UCM currently in the Active role, providing services. For example, assuming the HTTP/HTTPS port is 8089, the system admin can access the active UCM using the URL `https://cluster_IP:8089`.

- System admin can log into the current active UCM using `https://cluster_IP:8089` or `https://activeUCM_IP:8089`.
- If the system admin logs into the standby UCM's web UI by using the standby UCM IP `https://standbyUCM_IP:8089` and attempts to modify configurations, it will not be allowed. The system will prompt that configuration is restricted on the standby UCM.

Important Note

After HA setup, the administrator identity and account information from the active UCM are synchronized to and overwrite those on the standby UCM. Therefore, when logging in through the floating cluster IP or either UCM device's IP address, the system admin must always use the administrator credentials of the current active UCM.

Log in Wave

After HA configuration, the login URL for Wave may be changed. Users can log in to Wave using the following addresses:

1. Log in via IP.

Since the UCM providing the RemoteConnect service can be the primary or secondary UCM, the user should always use the cluster IP to log in to Wave. For example, `https://cluster_IP:8089/gswave#`.

2. Log in via domain name.

No matter whether a failover happens, users can always use the domain name assigned from the GDMS Remote Connect service, which is determined by the initially configured primary UCM.

Failover during Call

When the active server encounters a failure, if there is an ongoing call on the active server, the switchover process will only cause a few seconds of audio cut off, and then it will be recovered automatically.

Notes

- Currently, if the call is using UDP as a transport method, the call can be recovered after switchover. However, if the call is using TCP as a transport method, the call cannot be recovered after switchover.
- Point-to-point calls, such as audio calls or audio meeting can be recovered after switchover. However, for calls using ring group, call queue and other call features and services, the call will not be automatically recovered.

Data Sync

HA setup provides a data sync mechanism:

1. After UCM boots up, the standby UCM will send requests for all the data on the active UCM and perform data sync. Every time the active UCM has a configuration change, it will also synchronize the data to the standby UCM automatically and immediately.
2. Data sync is triggered in a real-time manner. It not only synchronizes configuration data, but also extensions, voicemail, CDR, etc.
3. Every day at midnight, a full backup will be performed to ensure active and standby UCM always have the same data daily.

Backup and Restore

For backup restore, the admin needs to log in to the active UCM and restore the backup file on the active UCM first. UCM devices will reboot automatically. Once the UCM finishes booting up, the standby UCM will start synchronizing data from the active UCM to restore the backup as well.

Maintenance

In the HA setup, the system admin can check HA-related alerts under the UCM web UI’s system events page to learn if there is any abnormal event related to HA. According to the alerts, the admin can further diagnose by checking the event time and logs with more details.

System Events			
Alert LogAlert Events ListAlert Contact Delete Search Result(s)ClearDisplay Filter			
TIME	EVENT NAME	TYPE	CONTENT
2021-08-27 14:48:37	HA failure warning	Restore to normal	MAC : c074ad537372 -- HEARTBEAT 2021-08-27 14:48:37 has recovered from failure
2021-08-27 14:48:33	HA failure warning	Generate Alert	MAC : c074ad537372 -- HEARTBEAT 2021-08-27 14:48:33 loose connection
2021-08-25 10:31:00	HA failure warning	Restore to normal	MAC : c074ad537372 -- HEARTBEAT 2021-08-25 10:31:00 has recovered from failure
2021-08-25 10:30:55	HA failure warning	Generate Alert	MAC : c074ad537372 -- HEARTBEAT 2021-08-25 10:30:55 loose connection
2021-08-25 10:30:49	HA failure warning	Restore to normal	MAC : c074ad537372 -- HEARTBEAT 2021-08-25 10:30:49 has recovered from failure
2021-08-25 10:30:48	HA failure warning	Generate Alert	MAC : c074ad537372 -- HEARTBEAT 2021-08-25 10:30:48 loose connection
2021-08-25 10:29:01	HA failure warning	Restore to normal	MAC : c074ad537372 -- HEARTBEAT 2021-08-25 10:29:01 has recovered from failure
2021-08-25 10:28:56	HA failure warning	Generate Alert	MAC : c074ad537372 -- HEARTBEAT 2021-08-25 10:28:56 loose connection
2021-08-25 10:24:00	HA failure warning	Restore to normal	MAC : c074ad537372 -- HEARTBEAT 2021-08-25 10:24:00 has recovered from failure
2021-08-25 10:23:55	HA failure warning	Generate Alert	MAC : c074ad537372 -- HEARTBEAT 2021-08-25 10:23:55 loose connection

System Alert Events

HA log also shows all HA backup and failover logs.

HA	
HA Settings	HA Status
HA Log	
HA Backup LogHA Failover Log Clean [2021-06-15 03:00:35 AM] HA backup success!! [2021-06-14 03:00:34 AM] HA backup success!! [2021-06-13 03:00:32 AM] HA backup success!! [2021-06-12 03:00:33 AM] HA backup success!! [2021-06-11 02:23:05 PM] HA backup success!! [2021-06-11 11:13:01 AM] HA backup success!! [2021-06-11 11:07:23 AM] HA backup failed!! [2021-06-11 03:00:38 AM] HA backup success!! [2021-06-10 09:57:06 PM] HA backup success!! [2021-06-10 09:45:43 PM] HA backup success!! [2021-06-10 08:47:21 PM] HA backup success!! [2021-06-10 03:46:17 PM] HA backup success!! [2021-06-10 02:55:03 PM] HA backup success!! [2021-06-10 01:57:09 PM] HA backup success!! [2021-06-10 02:36:23 AM] HA backup success!! [2021-06-10 10:21:12 AM] HA backup failed!! [2021-06-10 09:52:39 AM] HA backup success!!	

HA Logs