

UCM630x/A – High Availability User Guide: Remote Disaster Recovery

OVERVIEW

A remote disaster recovery site refers to a separate location from the main site where the primary server is, and the secondary server in the remote disaster recovery site is used for backing up data and recovering the service when the main location with primary server has any unexpected events such as natural disaster causing service interruption. High availability remote disaster recovery feature on UCM6300/UCM6300A series provides reliability and redundancy for deployment when the primary server has hardware failure, power outage, network outage or other disaster events.

To use remote disaster recovery feature, the primary UCM and secondary UCM must be the same model using the same firmware version. The UCM providing service is in “active” role while the other UCM is in “standby” role. The data on active UCM is synced to the standby UCM in real-time manner. The standby UCM always monitors active UCM. If the active UCM has failure, the standby UCM will take over and become active to ensure the service is not interrupted.

 Notes

- 1. The UCM63xx remote disaster recovery feature requires using Grandstream endpoints in the deployment. 3rd party end points may not be fully supported in UCM’s HA remote disaster recovery scenario.
- 2. If Grandstream Wave application is used with UCMRC plan of UCM63xx, only Wave clients registered from external network can be supported in UCM’s HA remote disaster recovery scenario. Wave clients registered to UCM from the same LAN is not supported for recovery.

DEFINITIONS

Primary/Secondary:

The high availability remote disaster recovery sites have two types of UCM: primary and secondary. The UCM HA type doesn’t change while the roles of the UCM can change between “active” and “standby”.

In HA scenario, the primary UCM has higher chance to be in “active” role. Therefore, if enabling remote disaster recovery on UCMs, please make sure to configure the current UCM providing PBX service at the main site as type “Primary” and configure the backup failover UCM at the recovery site to be “Secondary”.

Active/Standby:

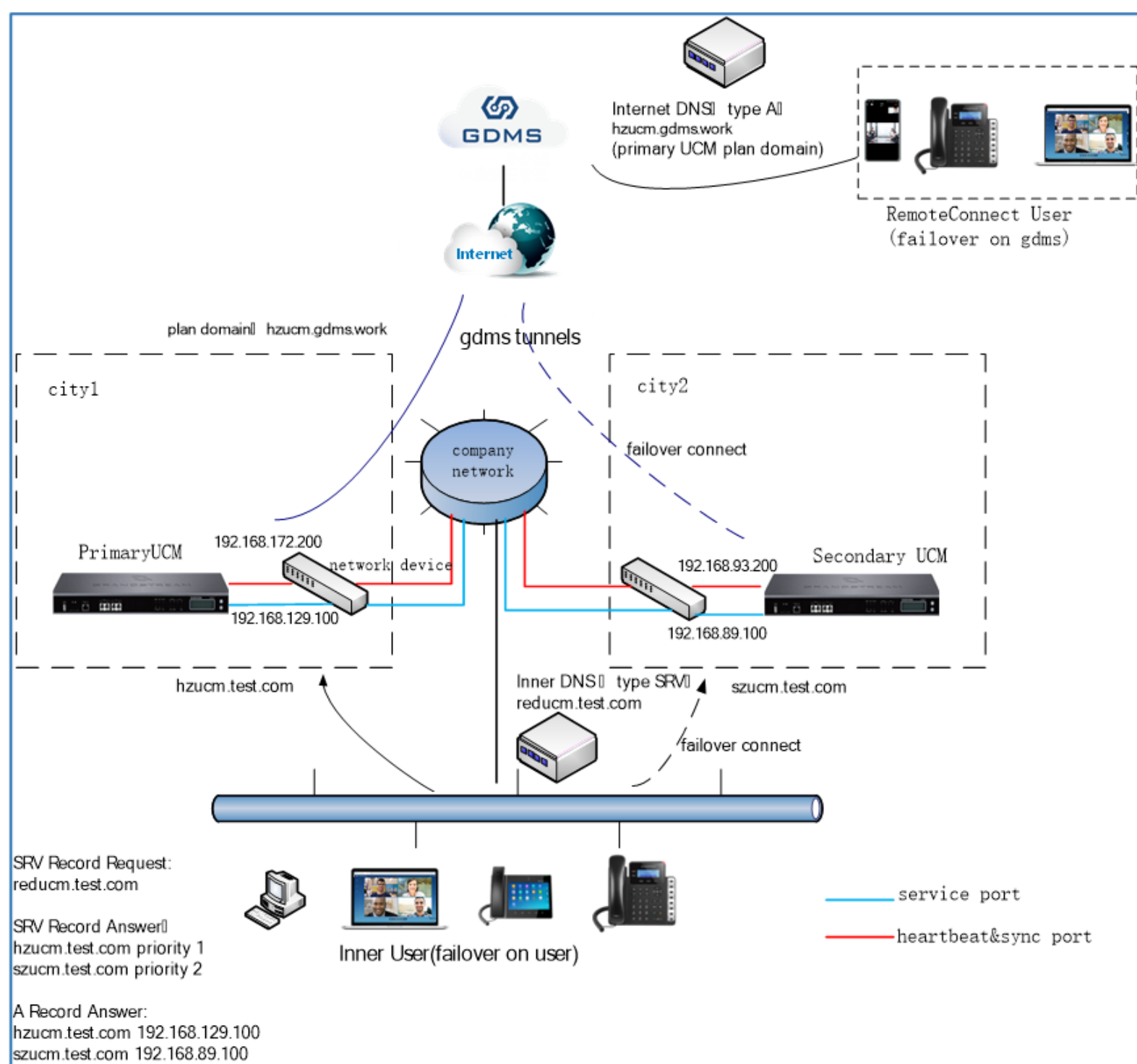
The HA remote disaster recovery involves two roles for the UCMs:

Active: this is for the UCM currently providing all PBX service.

Standby: this is for the backup UCM.

Please note “primary” UCM can be different from “active” UCM, “secondary” UCM can be different from “standby” UCM. The UCM can switch between active role and standby role. However, the UCM always has the same type (primary or secondary) as configured on the UCM webUI.

REMOTE DISASTER RECOVERY DEPLOYMENT TOPOLOGY



Typical Topology for Remote Disaster Recovery Scenario

The primary UCM and secondary UCM are deployed in server rooms in two separate locations. The two locations have network connecting all the devices between them.

The end devices in the company LAN network register to the UCM using domain name via DNS SRV. The DNS server in the LAN network returns two servers with priority assigned. The primary UCM is the one with high priority to provide PBX service and end devices will send service request to the primary UCM first. If the primary UCM has failure or the main site where the primary UCM is located encounters unexpected disasters causing service unavailable, the end devices in the LAN network will switch sending request to the secondary UCM within a few minutes for failover and service recovery.

For users in external network, the users can register to the domain name provided by the UCMRC (UCM RemoteConnect) plan which is the custom server address configured for the primary UCM's RemoteConnect plan. When the primary UCM or the main site has failure, the secondary UCM will notify GDMS to switch all activities to the secondary UCM so the secondary UCM can take over and provide RemoteConnect service to the users.

During deployment, the UCM's network ports for service and heartbeat are separate. This ensure PBX service and heartbeat for backup/recovery are independent from each other.

REMOTE DISASTER RECOVERY CONFIGURATION

Prerequisites

UCM Requirements

The two UCMs used for remote disaster recovery deployment must meet below requirements:

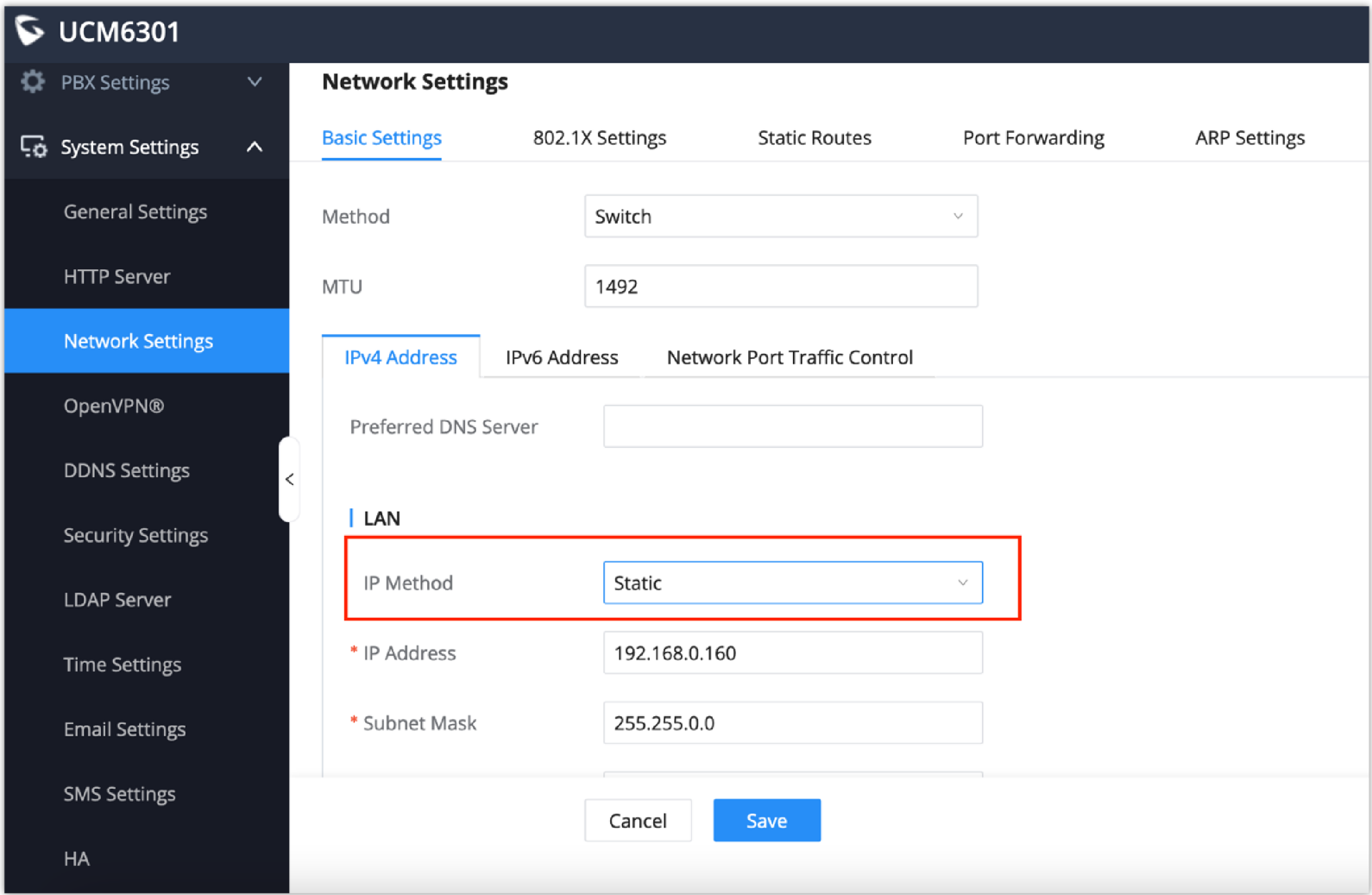
- 1. Both UCMs must be the same model.
- 2. Both UCMs must use the same firmware version.

Hardware Requirements

For end devices registered to the UCMs in remote disaster recovery deployment, only Grandstream end devices are fully supported for service recovery. 3rd party end devices used with UCM may not be supported.

Network Requirements

- 1. Before configuring the UCM for HA remote disaster recovery feature, each UCM must complete individual network configuration first.
- The UCM must be configured with static IP before enabling remote disaster recovery feature. Please log in UCM webUI as admin and go to System Settings->Network Settings->Basic Settings->IPv4 Address to configure static IP for the UCM.



Network Settings (on UCM6301)

- 2. In the LAN network, deploy a DNS server and use SRV. The DNS server should return the IP addresses of the 2 UCMs as primary and secondary UCM. Please note the primary UCM’s IP address should have higher priority in SRV response.
- 3. The network port on UCM used for HA heartbeat must be in a different subnet from the one used for PBX service on the UCM. The network admin should plan ahead to assign the IP addresses in different subnet. For example, in the local network, assign two subnets, one for the UCM’s service port, one for the UCM’s heartbeat port.
- 4. Additionally, if the two locations have firewall or routers between their network, i.e., the UCMs in the two locations do not have direct Internet connection, the network admin will need to configure firewall rules or forwarding rules such as port forwarding so that the communications for heartbeat ad traffic between the two UCMs can go through. Different networks may have different configurations depending on the network devices and infrastructures. Please refer to an example in section [Deployment example].

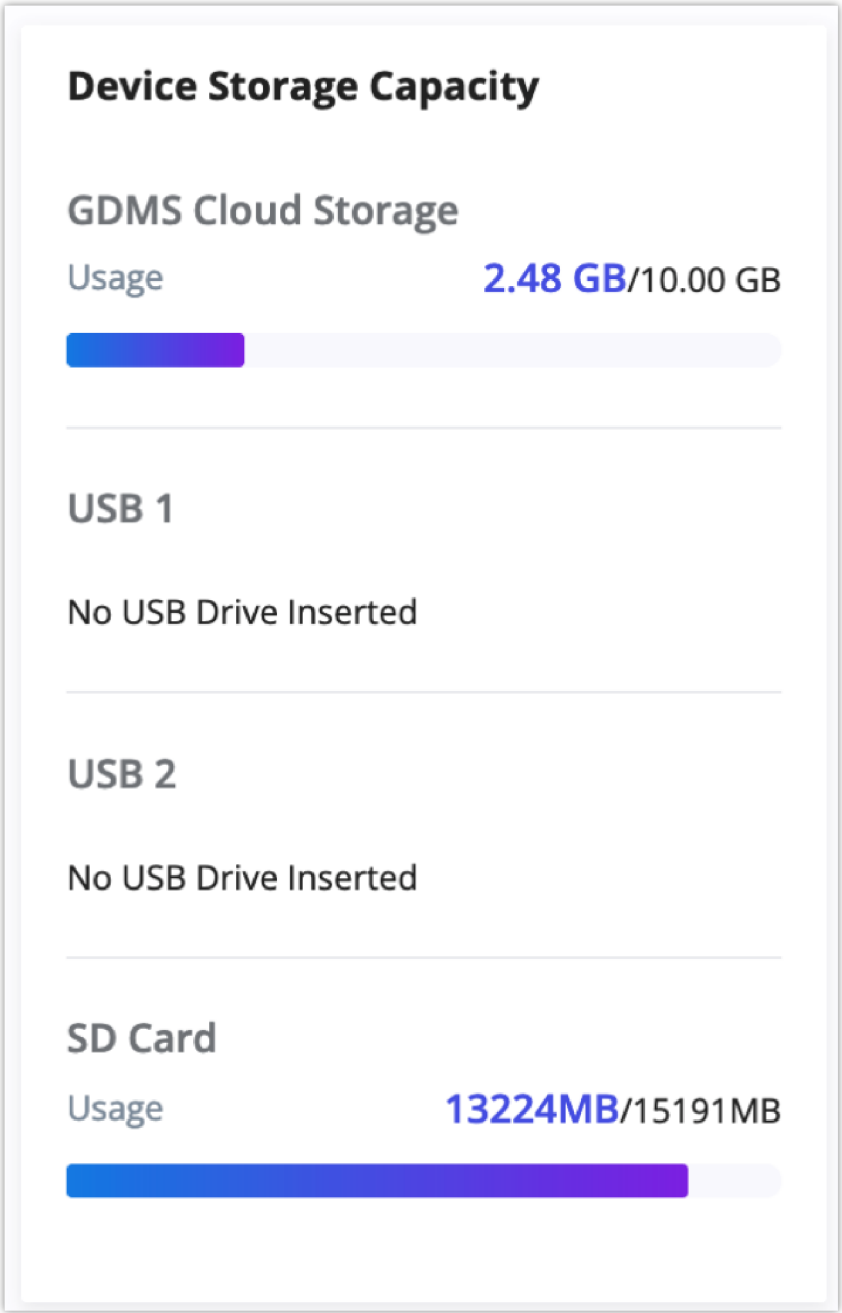
Below are the ports which need to be forwarded/opened in both routers/firewalls, in the case where the UCMs are behind the routers.

Port Number	Protocol	Description
9527	UDP	Heartbeat port
3510	TCP	Data sync port

8989	TCP	Data sync port
873	TCP	File sync port
9292	TCP	Data sync port
8796	TCP	Data sync port

Storage Device Requirements

Before enabling HA remote disaster recovery, please check and ensure the two UCMs have the same type of external storage devices plugged in. For example, if UCM A has a SD card and a USB flash drive plugged in, UCM B must have a SD card and a USB flash drive with the exact same type and storage size. This is mandatory so that the standby UCM can always store the data properly in the same way as active UCM. If UCM A uses GDMS cloud for storage, UCM B must use the same. However, the storage path related settings can be different on each UCM at initial settings because the active UCM will sync its configuration to the standby UCM after HA is enabled.



Dashboard->Device Storage Capacity

Step-by-step Configuration

Scenario 1: For two new UCMs, or for two UCMs currently providing service, here are the configuration steps:

- 1. Check your UCMs and network to make sure they meet the prerequisites requirements and ready.
 - UCMs are using the same model and same firmware version.
 - Grandstream end devices are registered to UCM.
 - Network configurations: ensure both UCMs are using static IP.
 - Both UCMs are using the exact same storage device(s)

- 1. Choose one of the UCM to be the primary UCM (UCM A) and the initial role for this UCM is “active”.
 - 1. If both UCMs are new devices, any one of them can be used as UCM A.

2. If one of the UCM is already deployed and providing PBX service, please use this UCM as UCM A.
2. If Cloud IM service is used, please enable Cloud IM on UCM A and ensure Cloud IM is turned off on UCM B.
3. On UCM A, configure HA related settings under UCM web UI->System Settings->HA->HA Settings.
- o High Available Enable: Yes

o HA Mode: Remote Disaster Recovery

o Remote Disaster Station Type: Primary

o Please refer to table [HA CONFIGURATION PARAMETERS FOR REMOTE DISASTER RECOVERY] for all configuration parameters information.

o Save and apply the settings. Reboot is required for the changes to take effect.

System Settings

General Settings

HTTP Server

Network Settings

OpenVPN®

DDNS Settings

Security Settings

LDAP Server

Time Settings

Email Settings

SMS Settings

HA

SNMP

RADIUS

TR-069

Contacts

Device Management

HA

HA Settings

HA Status

HA Log

High Available Enable

☒

HA Mode

☐ Local Hot Standby

☒ Remote Disaster Recovery

* Network Port Domain Name

LAN

test.a.gdms.cloud

Force Switch

Switch

* Remote Disaster Recovery Station Type

Primary

* Remote Disaster Recovery Peer MAC Address

C0:74:AD:00:00:01

* Heartbeat Port

9527

* Heartbeat Timeout Period (s)

30

* Local Heartbeat IP

10.210.0.10

* Local Heartbeat Gateway IP

10.210.0.1

* Local Heartbeat Address Subnet Mask

255.255.0.0

* Peer Heartbeat IP

10.212.0.10

Scan External Storage Files

Sync

Cancel

Save

HA Configuration on UCM A

1. After configuration is completed on UCM A and UCM A reboots, please verify the HA status by logging in UCM A’s web UI via its IP address with admin’s credentials. Go to UCM web UI->System Settings->HA->HA Status, it should show HA enabled and HA status should show as “Active”.
2. After verifying UCM A’s configuration and status, now you can configure HA for UCM B. Log in UCM B’s web UI and go to System Settings->HA->HA Settings. On UCM B:
- o High Available Enable: Yes

o HA mode: Remote Disaster Recovery

o Remote Disaster Station Type: Secondary

o Please refer to table [HA CONFIGURATION PARAMETERS FOR REMOTE DISASTER RECOVERY] for the configurations for all configurations.

o Save and apply the settings. Reboot is required for the changes to take effect. Please note it will take longer for UCM B to fully boot up because UCM B will automatically perform a full backup during bootup process.

System Settings

General Settings

HTTP Server

Network Settings

OpenVPN®

DDNS Settings

Security Settings

LDAP Server

Time Settings

Email Settings

SMS Settings

HA

SNMP

RADIUS

TR-069

Contacts

Device Management

HA

HA Settings

HA Status

HA Log

High Available Enable

HA Mode

Network Port Domain Name

Force Switch

Remote Disaster Recovery Station Type

Remote Disaster Recovery Peer MAC Address

Heartbeat Port

Heartbeat Timeout Period (s)

Local Heartbeat IP

Local Heartbeat Gateway IP

Local Heartbeat Address Subnet Mask

Peer Heartbeat IP

Scan External Storage Files

Cancel

Save

HA Settings on UCM B

After UCM B boots up, please verify the HA status on UCM B by logging in UCM B’s web UI via its IP address with UCM A’s admin credentials. Go to UCM web UI->System Settings->HA->HA Settings, it should show HA enabled with the Force Switch “Switch” button in grey (unavailable). Only HA heartbeat related settings, peer heartbeat IP and MAC address configurations are available for configuration. Click on HA status tab, it shows UCM B’s role as “Standby”, and HA status should show as “Active”.

HA

HA Settings

HA Status

HA Log

HA Mode

Remote Disaster Recovery

Remote Disaster Recovery Status

Dual

Remote Disaster Recovery Full Backup Status

Idle

MAC Address of Current UCM

C0:74:AD:00:00:01

Role of Current UCM

Standby

HA Status on UCM B

HA Configuration Parameters For Remote Disaster Recovery

Please configure HA parameters and deploy HA when the UCM is not in service period to avoid service interruption.

Table 1: HA Parameters

Parameter	Description	Value Range	Default Value	Note
High Available Enable	Enable or disable HA function	Yes/No	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”, UCM must use network mode “Switch” or “Router” and use static IP address. For “Remote Disaster Recovery”, UCM must be configured with static IP. Grandstream end devices are fully supported with UCM HA remote disaster recovery feature for failover.
Network Port Domain	Configure the domain name according to the network mode on the UCM. This is for local end devices to register to the UCM via local network.	A valid domain name		This domain name is used for remote disaster recovery scenario only. Note: if the network method is “Route” or “Dual”, please ensure the domain name is mapped to the correct network method. For network method “Dual”, if both network interfaces provide PBX service, please specify domain names for both of them.
Force Switch	Force switch HA roles between “Active” and “Standby”.	N/A	N/A	This should be only used in special circumstances. It can be used during firmware upgrade. Please refer to section [Firmware upgrade] for details. Also, after failover happens, if the admin decides to manually switch back to the original primary UCM at admin’s preferred time, this can be used.
Remote Disaster Recovery Station Type	This configures the UCM’s station type. In HA deployment, one UCM should be primary type and the other UCM should be secondary. The station type is always fixed for the UCM and does not change when the UCM’s role changes between active and standby. In HA deployment, primary UCM is more likely to be the active role. Therefore, in the initial HA configuration, please configure the UCM currently providing PBX service to be the primary station, and configure the backup UCM to be secondary.	Primary/ Secondary	N/A	The purpose to define station type is to ensure there is always only one active UCM providing service and avoiding having two active UCMs at the same time. The active/standby roles are negotiated between the two UCMs during heartbeat. Please note, active UCM is the UCM providing PBX service at the moment, standby UCM is the backup UCM. Station type “primary” doesn’t mean the UCM’s role is active , “secondary” doesn’t mean the UCM’s role is standby. The “active” and “standby” roles can be changed between the two UCMs. But station type is always fixed for each UCM, no matter which role it is.
Remote Disaster	Peer UCM’s MAC address	N/A	N/S	This is the MAC address for the UCM in the remote location to pair with the current

Recovery Peer MAC Address				UCM for HA remote disaster recovery deployment.
Heartbeat Port	The port used for heartbeat communications between the active and standby UCM.	0 to 65535	9527	The heartbeat port is configurable but it's suggested to keep the default value to avoid misconfiguration issues. Please note both UCMs must use the exact same value.
Heartbeat Timeout (s)	This is the timeout for heartbeat connection (in seconds)	7 to 45	7	When the standby UCM detects heartbeat timeout from the active UCM, failover will happen and the standby UCM will become the primary UCM. If the network condition is not ideal (jitter, packet loss, etc), it's suggested to adjust the heartbeat timeout to a larger value such as 15 seconds or longer.
Local Heartbeat IP	Enter the heartbeat IP address for the local UCM (the UCM itself) in the format of xxx.xxx.xxx.xxx. This is the address used for the remote peer UCM to detect local UCM's status and heartbeat, as well as communications for data sync.	A valid IP address	N/A	The LAN network of the heartbeat IP must be a different network segment from the one for service IP address.
Local Heartbeat Gateway IP	Enter the gateway of the local UCM's heartbeat IP for remote disaster recovery. Format: xxx.xxx.xxx.xxx.	A valid IP address	N/A	
Local Heartbeat Address Subnet Mask	Enter the subnet mask of the local UCM's heartbeat IP for remote disaster recovery. Format: xxx.xxx.xxx.xxx. Example: 255.255.255.0	A valid subnet mask address	N/A	
Peer Heartbeat IP	Enter the IP address for the remote UCM's heartbeat port. Format: xxx.xxx.xxx.xxx. This is used for detecting peer status and heartbeat negotiation. This is also the address used for data sync-up communications.	A valid IP address	N/A	
Scan External Storage Files	If the local UCM's file storage path is configured as SD card, USB flash drive or NAS, you can press the "Sync" button here to sync up all files and data from these external storage devices.	NA	NA	If the UCM currently providing PBX service already has data, it's suggested to sync external storage files during initial HA deployment. Files and data generated after HA deployment can be automatically synced up without manual operations.

After above HA settings, click on "save" button and it will prompt users to reboot the UCM. Follow the instruction to reboot the device.



Important Note

HA settings require UCM reboot to take effect. It's recommended to configure HA when the UCM is not in service hour to prevent service interruption.

HA Configuration With UCMRC

Scenario 2: For UCM A and B which are using UCMRC, besides the above configurations, additional plan configurations are required. Please see steps below:

1. If Cloud IM service used, please enable Cloud IM for UCM A and please ensure Cloud IM is disabled for UCM B. When using Cloud IM (service provided by GDMS), please ensure that both UCMs have the UCMRC plan with Cloud IM.

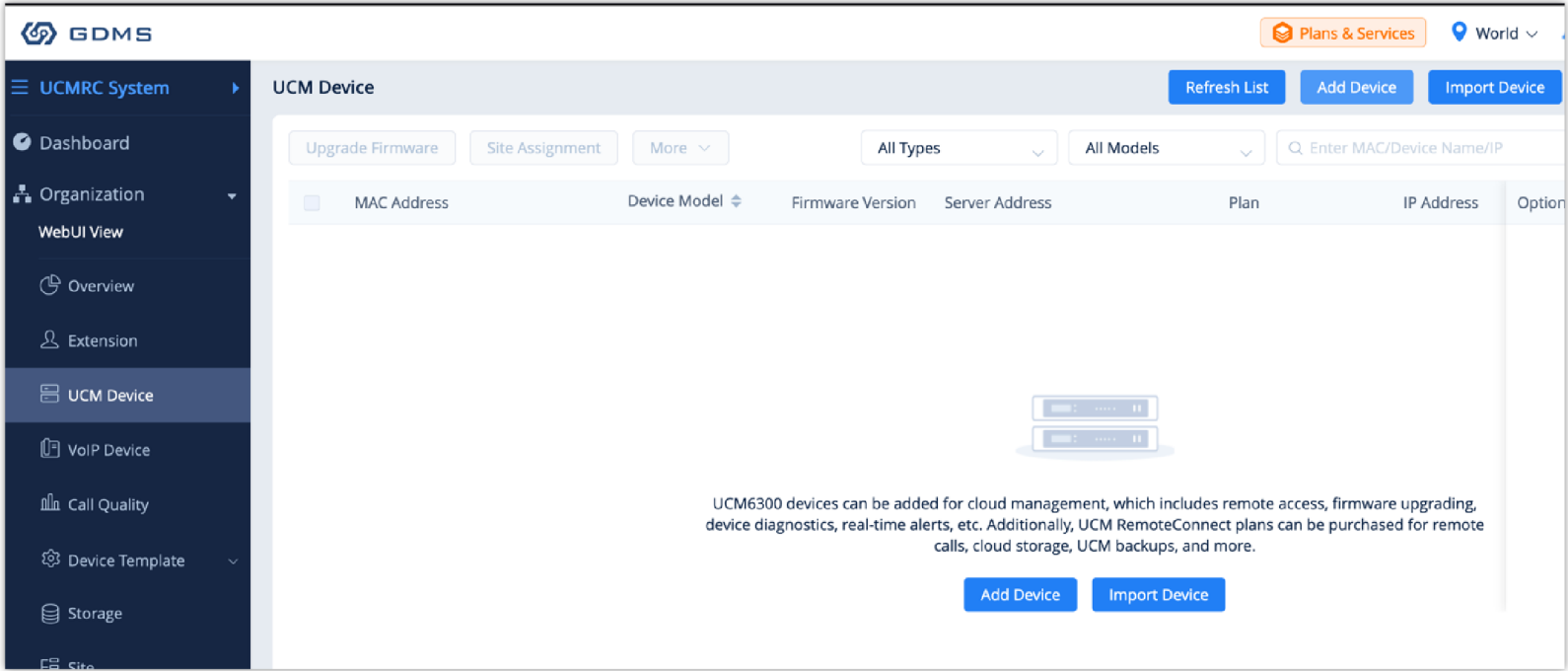
2. Make sure both UCMs have the same UCMRC plan with HA supported. If UCM A already has the UCMRC plan, then you just need to purchase UCMRC plan for UCM B. It’s OK if one of the UCM has the UCMRC plan purchased later than the other one.
3. Configure custom server address for UCM A which has station type “Primary” and use the custom server address. See section below for details. If UCM A already has custom server address, then this step can be skipped.

UCMRC Plan For HA

For the UCMRC plan to work normally when the UCMs use HA, it’s required to purchase the same UCMRC plan with HA ability via GDMS. Each UCM needs its own plan purchased and delivered.

Here are the steps:

1. Log in GDMS and make sure you are on “UCMRC System” view. Go to page “UCMRC Device”, click “Add Device” and enter the device information.



Add UCM on GDMS Device List

✔

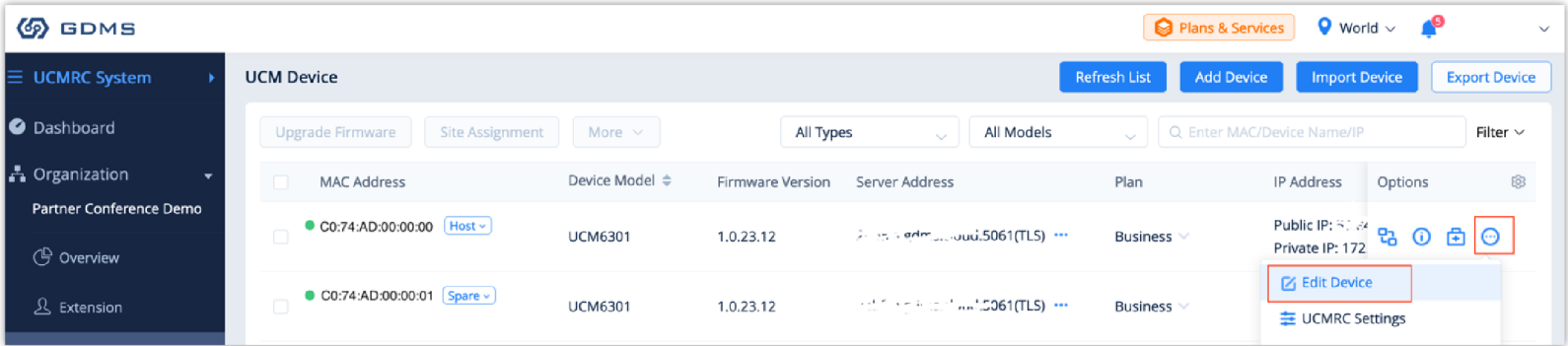
Note

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

Custom Server Address Configuration

For the two UCMs already having UCMRC plan with HA supported, please configure custom server address for the primary UCM and ensure this UCM uses this custom address.

The custom server address must be configured on GDMS. Please log in GDMS first. On UCMRC System view, go to UCM Device page->select options for the UCM->select “Edit Device”.



Custom Server Address Example

Edit Device

MAC Address

C0:74:AD:D5:2E:B8

Device Name

LAOFFICEUCM

*

Site

Default

Remarks

Access Server

Zone

Miami

Default Server Address

c074ad000000.a.gdms.cloud

Switch to Custom Domain

*

Custom Server Address

laofficeucm.a.gdms.cloud

Cancel

Save

Edit Device->Custom Server Address Example

Please notify UCM users with the new server address so they can use it.

For more details on how to configure custom server address, please refer to the GDMS user guide.

Verify HA Status

1. After configuring HA on both UCMs, please use each UCM’s IP address to open UCM’s webUI and log in using the active UCM’s login credentials. Check the HA status under WebUI->System Settings->HA->HA Status page. Normally, it shows the Remote Disaster Recovery status as HA, and the roles as Active or Standby.

For the Remote Disaster Recovery Full Backup Status, it shows backup if the device is currently performing backup. Otherwise it shows “No backup”.

HA	
HA Settings	HA Status
HA Mode	Remote Disaster Recovery
Remote Disaster Recovery Status	Dual
Remote Disaster Recovery Full Backup Status	Idle
MAC Address of Current UCM	C0:74:AD:00:00:00
Role of Current UCM	Active

HA Status for an Active UCM

HA	
HA Settings	HA Status
HA Mode	Remote Disaster Recovery
Remote Disaster Recovery Status	Dual
Remote Disaster Recovery Full Backup Status	Idle
MAC Address of Current UCM	C0:74:AD:00:00:01
Role of Current UCM	Standby

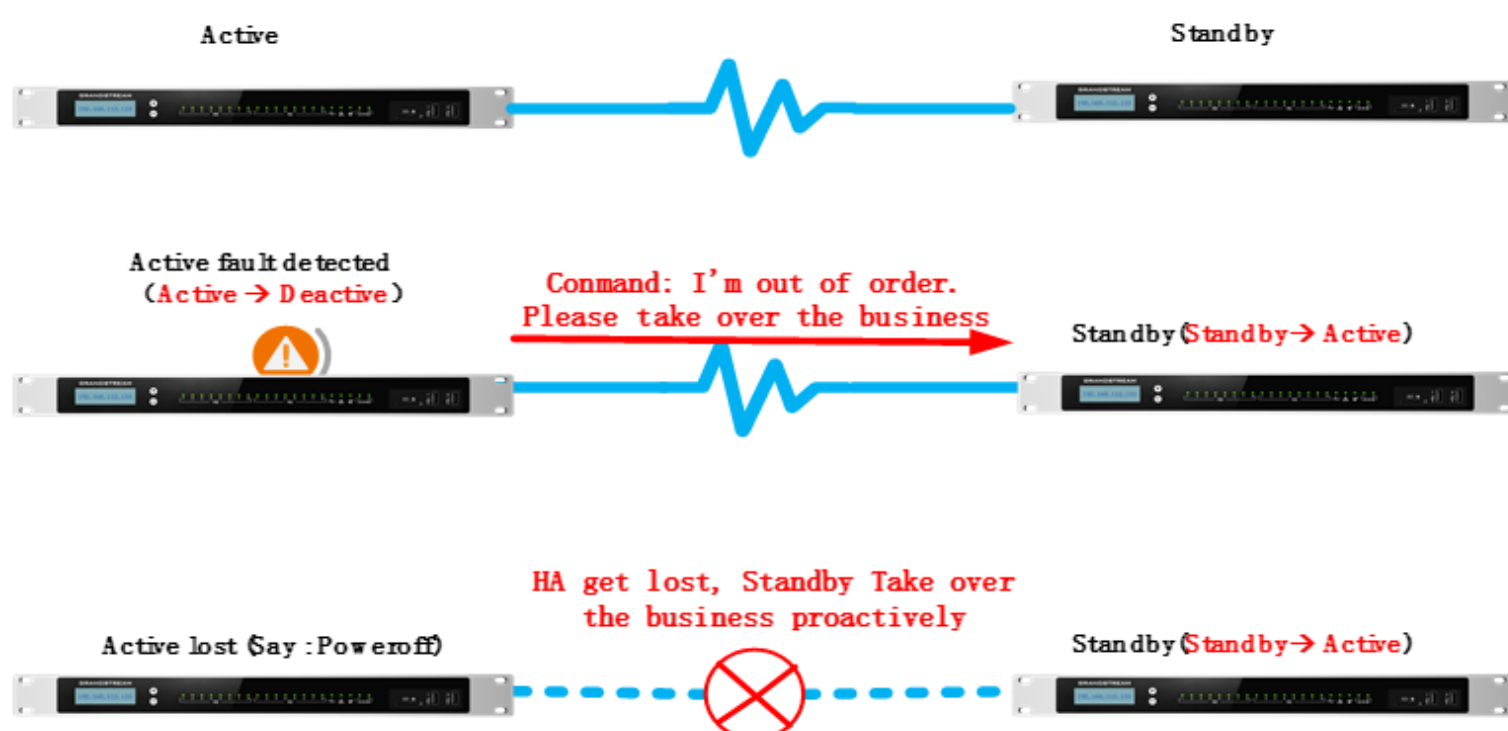
HA Status for a Standby UCM

2. Log in the web UI of the active UCM and create an extension. Then log in the web UI of the standby UCM to check extension page. You should be able to see the same extension created on the standby UCM automatically. This indicates the standby UCM has synced up from the active UCM and the HA configuration is successful.

ROLE CHANGE BETWEEN ACTIVE UCM AND STANDBY UCM

The remote disaster recovery feature supports automatic role change upon failover and service will be taken over. Once the primary UCM recovers, the admin must manually switch the service back to the primary UCM when the UCM is idle. Unless the secondary UCM experiences failure, there is no automatic fallback to primary UCM after the primary UCM is recovered. The admin can find a time when service is not required to perform switchover so that it doesn't affect normal operation and service.

Automatic Failure Detection and Switchover



Switchover between Active UCM and Standby UCM

Active UCM Auto Detection

With HA enabled and configured, if the active UCM detects disconnection on the network port for PBX service, it will trigger switchover and the peer UCM will take over PBX service.

Standby UCM Heartbeat Detection

In HA deployment, the standby UCM will check the active UCM’s status periodically. Standby UCM sends heartbeat message to active UCM and communicate the status via the heartbeat message. Normally, the active UCM will respond to the standby UCM via heartbeat port. Once the active UCM has failure or if the site encounters unexpected events causing power or network outage, the active UCM is unable to respond heartbeat message to the standby UCM. After the heartbeat timeout, the standby UCM will consider the active UCM in faulty state and start taking over.

The length of period for the standby UCM to detect and take over the service depends on the configuration of heartbeat timeout on the UCM. By default it’s set to 7 seconds. Admin can adjust it as needed for different sensitivity. If there is network jitter, delay, packet loss between UCM A and UCM B, the heartbeat timeout can be configured to a larger value such as 30 seconds.

Manual Switchover

The admin can log in the active UCM’s web UI and click on “Switch” button on the HA page to manually switch the active role to the other UCM. Here are a few scenarios that manual switchover can be used:

 **Note**

Please note that manual switchover should be used with caution.

Scenario 1:

Firmware upgrade. Please refer to section [[Firmware upgrade](#)] for more details.

Scenario 2:

Active UCM has problem switching over automatically.

Scenario 3:

After failover, the primary UCM recovers and the admin can manually switch over the active role back to the primary UCM again. After switching back the roles, the users can check CDR, recording files, scheduled meetings and chat history incurred on the primary UCM during the period that the secondary UCM provides PBX service.

HA

HA Settings

HA Status

HA Log

High Available Enable

☒

HA Mode

☐ Local Hot Standby ?

☒ Remote Disaster Recovery ?

* Network Port Domain Name

LAN

test.a.gdms.cloud

Force Switch

Switch

* Remote Disaster Recovery Station Type

Primary

* Remote Disaster Recovery Peer MAC Address

C0:74:AD:00:00:01

* Heartbeat Port

9527

* Heartbeat Timeout Period (s)

30

* Local Heartbeat IP

10.210.0.10

* Local Heartbeat Gateway IP

10.210.0.1

* Local Heartbeat Address Subnet Mask

255.255.0.0

* Peer Heartbeat IP

10.212.0.10

Scan External Storage Files

Sync

Switch Roles Manually

FIRMWARE UPGRADE

- To avoid service interruption, please follow below instructions to upgrade firmware for both UCMs in the HA deployment.
1. Log in the standby UCM’s web UI (UCM A). Upload firmware to UCM web UI and complete upgrade on the standby UCM first.
 2. After the standby UCM boots up from firmware upgrade, log in the web UI of the current active UCM which is the primary UCM (UCM B). On UCM B’s web UI HA page, the switch button for “Force Switch” will be available. Click to force switch the roles manually. This will make UCM A become the active role and make UCM B become the standby role.
 3. On UCM B, log in web UI to upload firmware and perform firmware upgrade. Once UCM B boots up from firmware upgrade, it will request full backup by syncing up from UCM A. Wait for the full backup to complete.
 4. After full backup is completed and while both UCMs are on HA mode, log in the secondary UCM (UCM A)’s web UI and click on switch button for “Force Switch”. This will make UCM A (secondary) change back to the standby role, and UCM B (primary) will become the active UCM again as initial state. The secondary UCM (UCM B) will reboot. After bootup, both UCMs are back to the initial role.
- This upgrading process ensures the primary UCM remains the active role after upgrading, and the secondary UCM remains the standby role.

REPLACE DEFECTIVE UCM

UCM With HA And UCMRC Plan

This scenario assumes UCM A and UCM B in the HA deployment already have their individual UCMRC plan that supports HA. If UCM B is defective and needs replacement by UCM C, please follow the steps below.

Scenario 1:

UCM A is the primary UCM and active role. UCM B is the secondary UCM with standby role. UCM B becomes defective and needs to be replaced by UCM C.

1. Add UCM C to GDMS. Purchase UCMRC plan with has HA ability. The UCMRC plan should be the same specifications as UCM A and UCM B.
2. Power off UCM B.
3. Modify the UCM A's HA parameters. Change the peer MAC address from UCM B's MAC address to UCM C's MAC address. Save and reboot device.
4. After UCM A boots up, verify on web UI that UCM A is the active role. On UCM C, ensure necessary hardware connections such as WAN port, heartbeat port and FXO port have cable plugged in and ready to use.
5. Boot up UCM C and configure network settings. The network settings should be exactly the same as UCM B. UCM C must have the same station type and static IP address as UCM B.
6. Check the external storage devices connected to UCM C. Ensure it has the exact same type external storage devices as UCM A (and UCM B).
7. Check if UCM C has Cloud IM enabled. If enabled, please turn it off. Please ensure there is no Cloud IM service on UCM C when replacing UCM B.
8. On UCM C, enable HA and configure HA parameters. The configuration should be exactly the same as UCM B. Save and reboot.
9. After UCM C reboots, check the HA status on both UCMs. UCM A should be active role and UCM C should be standby role.

Scenario 2:

UCM A is the secondary UCM and active role. UCM B is the primary UCM with standby role. UCM B becomes defective and needs to be replaced by UCM C.

1. On GDMS, delete UCM B's custom address.
2. On GDMS, add UCM C. Purchase UCMRC plan with HA for UCM C. The UCMRC plan specification should be exactly the same as the plan for UCM A and UCM B. On GDMS, configure custom server for UCM C and the custom server should be exactly the same as the one previously configured for UCM B. Make sure UCM C is switched to use custom address on GDMS.
3. Power off UCM B.
4. On UCM A's web UI, modify UCM A's HA settings. Modify the peer MAC address from UCM B's MAC address to UCM C's MAC address.
5. After UCM A reboots, check UCM A's web UI HA status to ensure UCM A is active role. On UCM C, ensure necessary hardware connections such as WAN port, heartbeat port and FXO port have cable plugged in and ready to use.
6. Boot up UCM C and configure network settings. The network settings should be exactly the same as UCM B. UCM C must have the same station type and static IP address as UCM B.
7. Check the external storage devices connected to UCM C. Ensure it has the exact same type external storage devices as UCM A (and UCM B).
8. Check if UCM C has Cloud IM enabled. If enabled, please turn it off. Please ensure there is no Cloud IM service on UCM C when replacing UCM B.
9. On UCM C, enable HA and configure HA parameters. The configuration should be exactly the same as UCM B. The station type on UCM C should be primary. Save and reboot.
10. After UCM C reboots, check the HA status on both UCMs. UCM A should be active role and UCM C should be standby role.
11. After step (10), it's confirmed that UCM A is active role and UCM C is standby role, wait for the full backup to finish between UCM A and UCM C. At this moment, UCM A is the active UCM and the station type is still secondary. Log in UCM A's web UI and go to HA settings page. Find option "Force Switch" and click the "Switch" button so the primary UCM (UCM C) can be changed to active role. UCM A (the secondary UCM) will then be changed back to standby role.

UCM With HA And No UCMRC Plan

For the two UCMs (UCM A and UCM B) without UCMRC plan in HA deployment, if one of the UCM (UCM B) becomes defective such as hardware failure, please follow the steps below to replace the defective UCM B with a new UCM C.

Assuming UCM A is the active role and UCM B is the standby role, regardless the station type on each UCM, the steps to replace UCM B with UCM C is the same as following:

- (1) Power off UCM B.
 - (2) Modify the UCM A’s HA parameters. Change the peer MAC address from UCM B’s MAC address to UCM C’s MAC address. Save and reboot device.
 - (3) After UCM A boots up, verify on web UI that UCM A is the active role. On UCM C, ensure necessary hardware connections such as WAN port, heartbeat port and FXO port have cable plugged in and ready to use.
 - (4) Boot up UCM C and configure network settings. The network settings should be exactly the same as UCM B. UCM C must have the same station type and static IP address as UCM B.
 - (5) Check the external storage devices connected to UCM C. Ensure it has the exact same type external storage devices as UCM A (and UCM B).
 - (6) Check if UCM C has Cloud IM enabled. If enabled, please turn it off. Please ensure there is no Cloud IM service on UCM C when replacing UCM B.
 - (7) On UCM C, enable HA and configure HA parameters. The configuration should be exactly the same as UCM B. Save and reboot.
 - (8) After UCM C reboots, check the HA status on both UCMs. UCM A should be active role and UCM C should be standby role.
 - (9) After step (8), it’s confirmed that UCM A is active role and UCM C is standby role, wait for the full backup to finish between UCM A and UCM C.
- If UCM A is the active UCM and the station type is secondary, log in UCM A’s web UI and go to HA settings page. Find option “Force Switch” and click the “Switch” button so the primary UCM (UCM C) can be changed to active role. UCM A (the secondary UCM) will then be changed back to standby role.
- If UCM A’s station type is already primary, then no action is needed.

DISABLE HA FROM UCM

To disable HA from the UCM, please log in the web UI of the active UCM’s IP. Go to System Settings->HA->HA settings, uncheck the option “High Available Enable”. Save and apply the change, then reboot the UCM. After bootup, check the HA status from each UCM.

After disabling HA, since the server address may be changed, the end devices registering to the UCM needs to update to the new address.

 Important

HA related settings require reboot to take effect. Please make configuration changes when the UCM is idle to avoid service interruption.

HA FOR UCM WITH CLOUD IM

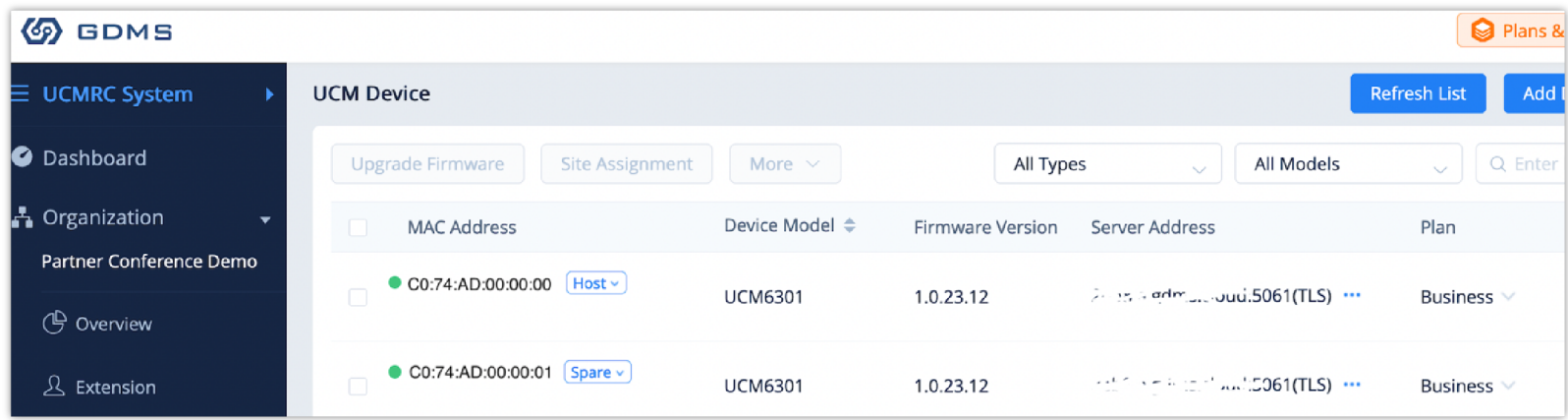
Please ensure only one Cloud IM service plan is used for the two UCMs in the HA deployment. When using the server address from GDMS, please ensure both UCMs have the UCMRC plan with Cloud IM.

When the active UCM A enables Cloud IM, the standby UCM B will obtain the Cloud IM service from the data sync in HA. Cloud IM always provides service with the active UCM and the associated MAC address with Cloud IM can change if the active UCM device changes between the two UCMs.

When UCM B becomes defective and requires replacement by a new UCM C which does not have Cloud IM enabled, once UCM C is set up in HA, Cloud IM automatically works without additional configurations. If UCM C has Cloud IM enabled before HA configurations, please ensure to disable it before replacing UCM B.

HA DEPLOYMENT WITH UCMRC PLAN

After purchasing UCMRC plan with HA supported and setting up HA, on GDMS, the UCM device will be displayed as Primary (Host) and Secondary (Spare).



GDMS Device List Example

ROLE CHANGE PROCESS

Prerequisite:

- 1. Both UCM must have UCMRC plan with HA ability and the plans for each UCM must have the same specifications.
- 2. The UCMRC plan is delivered to the UCM successfully for each UCM.

The call service is provided by the active UCM with GDMS. If the active UCM A has failure which triggers the failover switch, the standby UCM B will take over and becomes the active UCM. UCM B sends the switchover command to GDMS notifying that it will take over the call service with GDMS from now on.

ROLE STATUS WITH UCMRC

If both UCMs have UCMRC plan with HA ability, the role status on each UCM is reported to GDMS by the UCM automatically. Admin does not need to manually assign role for the UCMs on GDMS.

On GDMS, admin can remotely access each UCM and operate on them. However, certain configurations on the standby UCM can be overridden due to HA backup. Active UCM will be the one always providing PBX service, but GDMS always provides Wave login address based on the primary UCM.

SERVICE STATUS AND LOGIN

Active/Standby Status

After HA configurations on both UCMs, upon system bootup, the standby UCM will request a full backup from the active UCM.

The standby UCM is always prepared to take over from active UCM. The configuration changes allowed on the standby UCM is limited because the standby UCM syncs up the data from the active UCM in real-time. The standby UCM monitors the active UCM’s status so that it can take over quickly when the active UCM fails. This provides uninterrupted call service while the admin can work on recovering the faulty UCM.

Admin Login

Admin can use the UCM’s local IP address to log in UCM web UI. After HA is set up, the active UCM’s admin login information is synced up to the standby UCM and overrides the standby UCM’s own admin login. Therefore, the active UCM’s admin login is always used for both UCMs in HA.

Wave Login

HA setup affects Wave login methods.

- 1. Wave login from local network:

https://UCM IP/gswave/#

UCM IP is the primary or secondary UCM's IP. (Currently Wave doesn't support automatic switchover after HA failover).

2. Wave login from remote network:

On Wave, use the custom domain address for the primary UCM provided by GDMS.

Currently, only Wave clients registered from remote network can switch over automatically after HA failover. For Wave clients in the local network, users must manually change the server address to register to the active UCM after HA switchover.

End Device Registration

1. Register on phones in local network:

1. Method 1: register using the local domain name which is configured on the UCM HA settings->Network port domain name.
2. Method 2: if phones support Secondary SIP Sever, you can configure Secondary SIP Sever with the Secondary UCM IP.
3. For both methods, it's recommended to enable keep-alive so the phones can detect UCM status via OPTIONS and trigger new registration if needed.

2. Register on phones from remote network:

On the phone, enter the custom domain address for the primary UCM provided by GDMS as the SIP server for registration.

DATA SYNC

HA deployment provides data sync mechanism with the following features:

1. Full backup and data sync is performed during system bootup. The standby UCM requests full backup from the active UCM when it boots up. Also, whenever the active UCM has configuration changes, it will sync up the configuration change to the standby UCM to ensure both UCM always have the same configurations. Besides configuration changes, data sync is also triggered by adding extensions, changes in voicemail, CDR, recordings stored locally and on external storage devices.
2. At 3am every day, a full backup is performed automatically to sync up data. UCM web UI HA status page can display "Remote Disaster Recovery Full Backup Status" in real time.

RESTORE BACKUP

To restore a backup file to UCM, admin just needs to import it to the active UCM. After importing and restoring it to the active UCM, both UCMs will reboot automatically. After reboot, the active UCM will provide its full backup to the standby UCM so the standby UCM will sync up the data from the backup file.

MAINTENANCE INTERFACE ON UCM WEBUI

After HA deployment, admin can check HA related alerts under UCM web UI->Maintenance->System Events. According to the time of alert events, admin can further check logs to find out the cause of failure and failover.

Device Management

Maintenance

User Management

Login Settings

Operation Log

Syslog

System Events

Upgrade

Backup

System Cleanup/Reset

Network Troublesho...

Signaling Troublesho...

Service Check

System Events

Alert LogAlert Events ListAlert Contact

Delete Search Result(s)

Clear

Display Filter

TIME	EVENT NAME	TYPE	CONTENT
2023-08-26 00:36:15	HA Switch	Generate Alert	Remote Disaster Recovery HA switchover completed. MAC : C074ADD52EB8 has assumed operations.
2023-08-26 00:23:28	HA Switch	Generate Alert	Remote Disaster Recovery HA switchover completed. MAC : C074AD9FD036 has assumed operations.
2023-08-25 22:29:42	HA Switch	Generate Alert	Remote Disaster Recovery HA switchover completed. MAC : C074ADD52EB8 has assumed operations.
2023-08-25 20:48:26	HA Switch	Generate Alert	Remote Disaster Recovery HA switchover completed. MAC : C074AD9FD036 has assumed operations.
2023-08-23 13:46:41	HA Switch	Generate Alert	Remote Disaster Recovery HA switchover completed. MAC : C074ADD52EB8 has assumed operations.

Total: 9110 / pageGoto

System Alert Events

Admin can also go to UCM web UI->System Settings->HA->HA Settings->HA Log to view HA backup log, HA failover log and external data sync log.

PBX Settings

System Settings

General Settings

HTTP Server

Network Settings

OpenVPN®

DDNS Settings

Security Settings

LDAP Server

Time Settings

Email Settings

SMS Settings

HA

SNMP

HA

HA SettingsHA StatusHA Log

HA Backup Log

HA Failover Log

External Data Sync Log

Clean

Remote Disaster Recovery

[2023-08-27 03:01:31] HA backup success!!

Remote Disaster Recovery

[2023-08-26 03:01:32] HA backup success!!

Remote Disaster Recovery

[2023-08-26 00:39:34] HA backup success!!

Remote Disaster Recovery

[2023-08-26 00:26:34] HA backup success!!

Remote Disaster Recovery

[2023-08-25 22:32:50] HA backup success!!

Remote Disaster Recovery

[2023-08-25 20:52:04] HA backup success!!

Remote Disaster Recovery

[2023-08-25 18:33:45] HA backup success!!

Remote Disaster Recovery

[2023-08-23 21:29:01] HA backup success!!

Remote Disaster Recovery

[2023-08-23 20:28:31] HA backup success!!

Remote Disaster Recovery

[2023-08-23 20:15:13] HA backup success!!

Remote Disaster Recovery

[2023-08-23 19:32:28] HA backup success!!

Remote Disaster Recovery

[2023-08-23 18:53:25] HA backup success!!

Remote Disaster Recovery

[2023-08-23 17:56:35] HA backup success!!

Remote Disaster Recovery

[2023-08-23 17:10:15] HA backup success!!

HA Backup Log

⚙️ PBX Settings

⚙️ System Settings

General Settings

HTTP Server

Network Settings

OpenVPN®

DDNS Settings

Security Settings

LDAP Server

Time Settings

Email Settings

SMS Settings

HA

HA

HA SettingsHA StatusHA Log

HA Backup LogHA Failover LogExternal Data Sync Log

Clean

Remote Disaster Recovery [2023-08-26 00:36:15] [HA Rearrange] UCM(C0:74:AD:D5:2E:B8) promotes to master, Reason: force switch

Remote Disaster Recovery [2023-08-26 00:23:28] [HA Rearrange] UCM(C0:74:AD:9F:D0:36) promotes to master, Reason: force switch

Remote Disaster Recovery [2023-08-25 22:29:41] [HA Rearrange] UCM(C0:74:AD:D5:2E:B8) promotes to master, Reason: force switch

Remote Disaster Recovery [2023-08-25 20:48:26] [HA Rearrange] UCM(C0:74:AD:9F:D0:36) promotes to master, Reason: force switch

Remote Disaster Recovery [2023-08-23 13:44:33] [HA Rearrange] UCM(C0:74:AD:D5:2E:B8) promotes to master, Reason: heart beat lost

Remote Disaster Recovery [2023-08-23 13:40:13] [HA Rearrange] UCM(C0:74:AD:D5:2E:B2) promotes to master, Reason: force switch

Remote Disaster Recovery [2023-08-23 12:41:11] [HA Rearrange] UCM(C0:74:AD:D5:2E:B8) promotes to master, Reason: force switch

Remote Disaster Recovery [2023-08-23 12:35:39] [HA Rearrange] UCM(C0:74:AD:D5:2E:B2) promotes to master, Reason: force switch

HA Failover Log

HA

HA SettingsHA StatusHA Log

HA Backup LogHA Failover LogExternal Data Sync Log

Clean

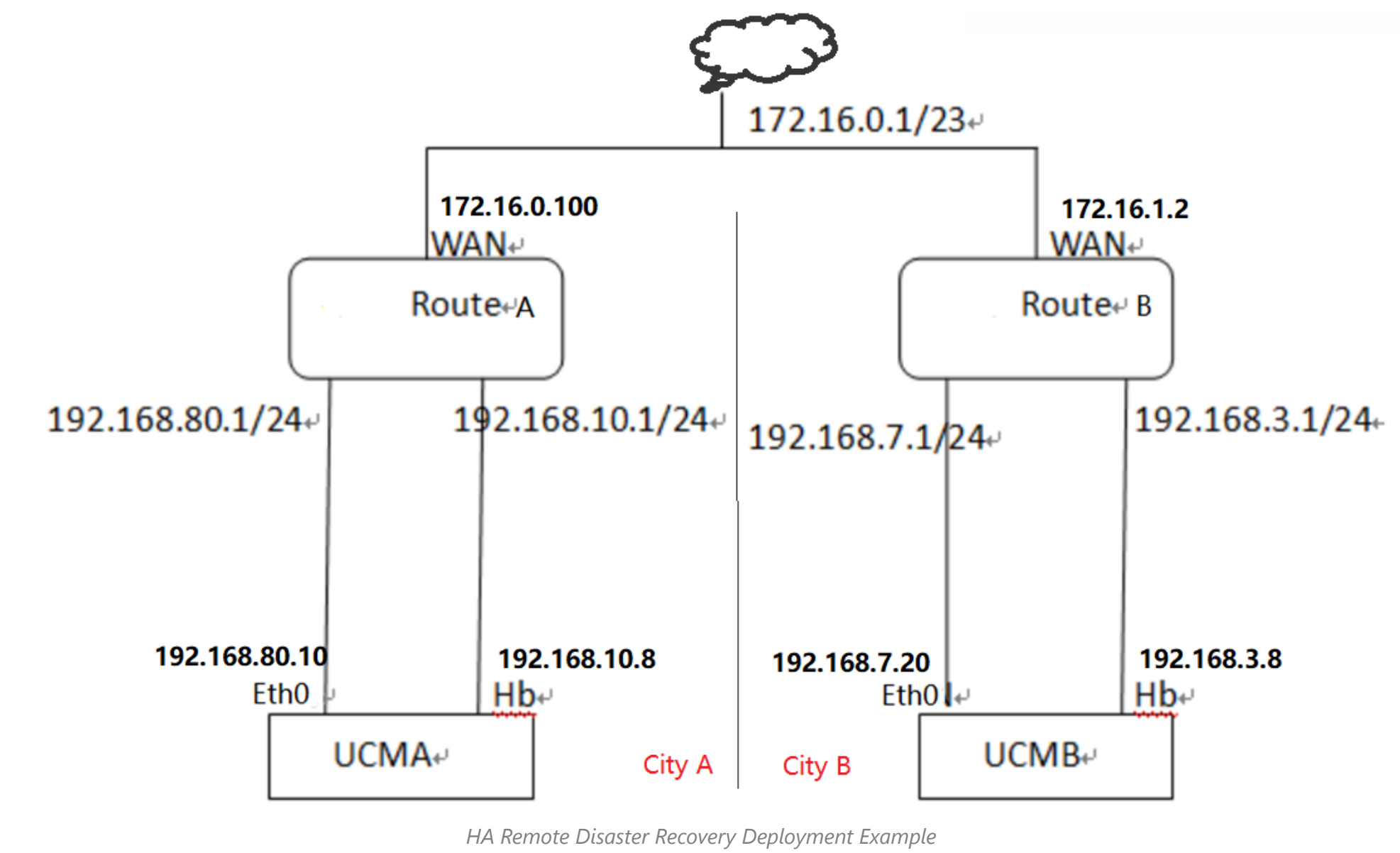
Remote Disaster Recovery [2023-07-07 17:08:32] HA external data synchronization success!!

Remote Disaster Recovery [2023-06-07 16:20:19] HA external data synchronization success!!

Remote Disaster Recovery [2023-06-07 14:26:25] HA external data synchronization success!!

HA External Data Sync Log

DEPLOYMENT EXAMPLE



- 172.16.0.1/23 is the enterprise network
- Two locations A and B have their own main router A and B. Router A and B can communication with each other via 172.16.0.1/23 network.
- UCM A is set up under router A in location A. UCM B is set up under router B in location B. UCM A and UCM B are configured with their own LAN network IP under their router with different network segment and they cannot directly communicate with each other.
- On router A (or firewall A) and router B (or firewall B), configure port forwarding to allow traffic to reach the UCM under each router. See forwarding rules below for both routers:

Router A:

Port Description	Source IP Address	Protocol Type	Source Port	Destination IP Address	Destination Port
Heartbeat Port	172.16.1.2	UDP	9527	192.168.10.8	9527
Data Sync Port 1	172.16.1.2	TCP	3510	192.168.80.10	3510
Data Sync Port 2	172.16.1.2	TCP	8989	192.168.80.10	8989
File Sync Port	172.16.1.2	TCP	873	192.168.80.10	873
Data Sync Port 3	172.16.1.2	TCP	9292	192.168.80.10	9292
Data Sync Port 4	172.16.1.2	TCP	8796	192.168.80.10	8796

Router B:

Port Description	Source IP Address	Protocol Type	Source Port	Destination IP Address	Destination Port
------------------	-------------------	---------------	-------------	------------------------	------------------

Heartbeat Port	172.16.0.100	UDP	9527	192.168.3.8	9527
Data Sync Port 1	172.16.0.100	TCP	3510	192.168.7.20	3510
Data Sync Port 2	172.16.0.100	TCP	8989	192.168.7.20	8989
File Sync Port	172.16.0.100	TCP	873	192.168.7.20	873
Data Sync Port 3	172.16.0.100	TCP	9292	192.168.7.20	9292
Data Sync Port 4	172.16.0.100	TCP	8796	192.168.7.20	8796

In the above table, only port 9527 for heartbeat port is configurable on UCM. All other ports are fixed and cannot be changed. Please note when assigning peer heartbeat IP, the IP address is the router’s IP in the remote network. For example, on UCM A, please configure peer heartbeat IP with router B’s IP address 172.16.1.2.

For DNS deployment, it’s suggested to configure a DNS server on each location.

- For DNS server A, DNS SRV should return 192.168.80.10 (UCM A’s IP) and router B’s IP 172.16.1.2.
- For DNS server B, DNS SRV should return router A’s IP 172.16.0.100 and 192.168.7.20 (UCM B’s IP).

Additionally, on router A and router B, admin needs to configure port forwarding for SIP signaling port such as 5060 and RTP port range such as 20000-30000.

- On UCM A:

For SIP:

Router A 172.16.0.100:5060 <—> UCM A’s service address 192.168.80.10:5060. Protocol: TCP/UDP.

For RTP:

Router A 172.16.0.100:20000-30000 <—> UCM A’s service address 192.168.80.10:20000-30000. Protocol: TCP/UDP.

- On UCM B, configure similar way as UCM A.

On UCM A web UI->PBX Settings->SIP Settings->SIP NAT, configure external host as 172.16.0.100 (router A’s IP). On UCM B, configure the external host as 172.16.1.2 (router B’s IP).

UCM6301

RC Services

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

If Local Network Address is not configured, External Host will not take effect.

External Host

172.16.0.100

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

Get more information about NAT Settings at Remote Work Environment – Setup Guide

LOCAL NETWORK ADDRESS

SUBNET MASK

192.168.80.1

24

Cancel

Save

HA Remote Disaster Recovery Example – NAT Configuration

 Note

The configuration varies depending on the network topology.

