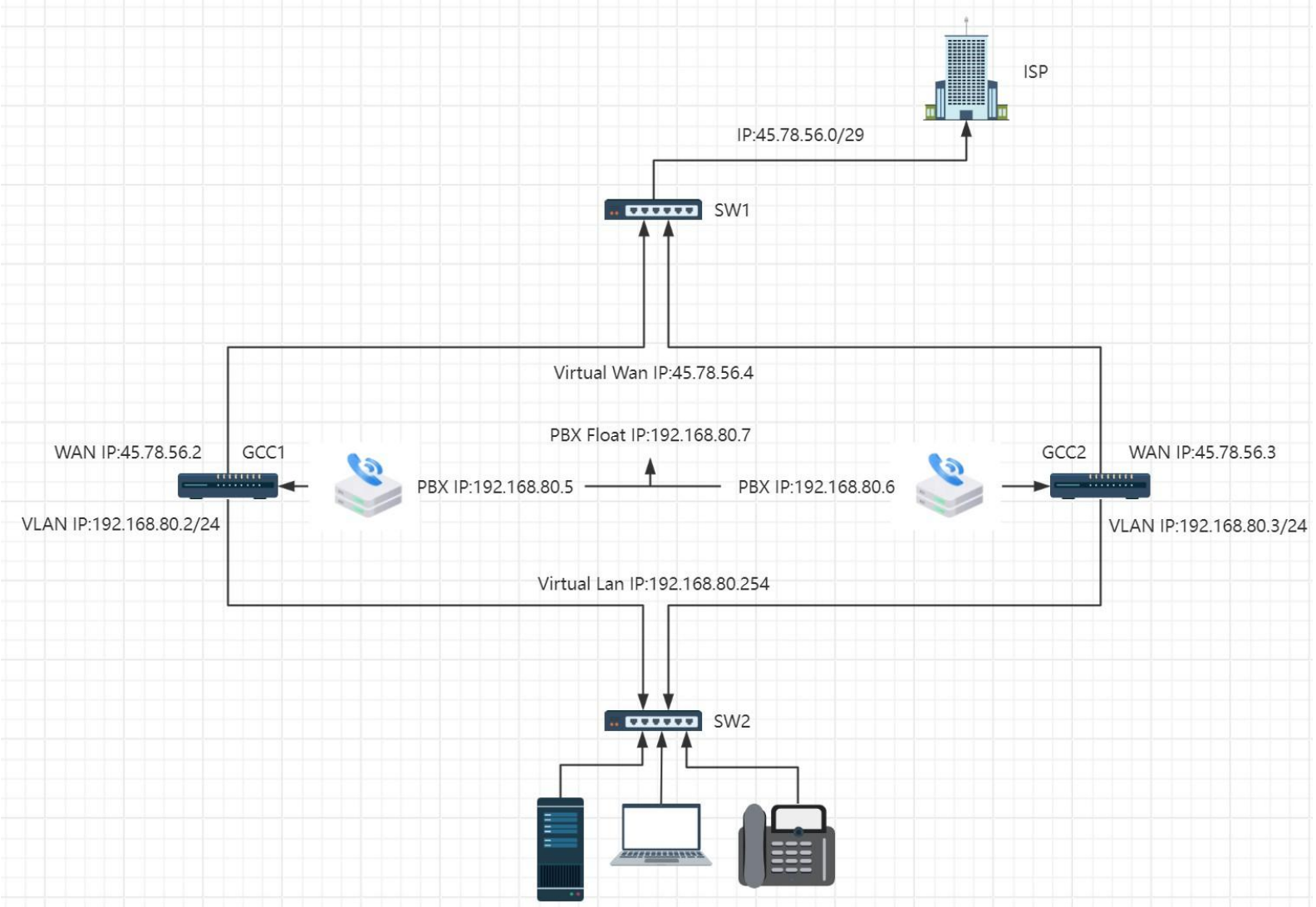
GCC6000 Series IPPBX High Availability – User Guide

HA INTRODUCTION

The High Availability feature on the Grandstream GCC series provides enterprises with a reliable solution for PBX redundancy and failover support. In the HA setup, there are two GCC PBXs with one PBX in the “active” role and the other in the “standby” role. The two GCCs must have the same model and the same firmware version. The data on the active GCC PBX will be synchronized to the standby GCC PBX in a real-time manner and the standby GCC PBX monitors the active GCC PBX’s running status regularly. When the active GCC PBX runs into hardware or critical software issues, the standby GCC PBX 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.

TOPOLOGY

Take the following topology as an example (for more scenarios and configurations, please refer to the GCC6000 Series VRRP User Guide):



> **Note**
>
> Before performing the following configuration, please refer to the topology diagram to connect to the network.

Configuration instructions:

- If two new GCCs form HA, users can select any one device as GCC1 in the example of this configuration manual.
- If one is an old GCC and the other is a new GCC to form HA, and the existing user data needs to be retained, the old GCC needs to be selected as GCC1. It is also recommended to back up the old GCC data before setting up HA.

HOT STANDBY CONFIGURATION PROCESS

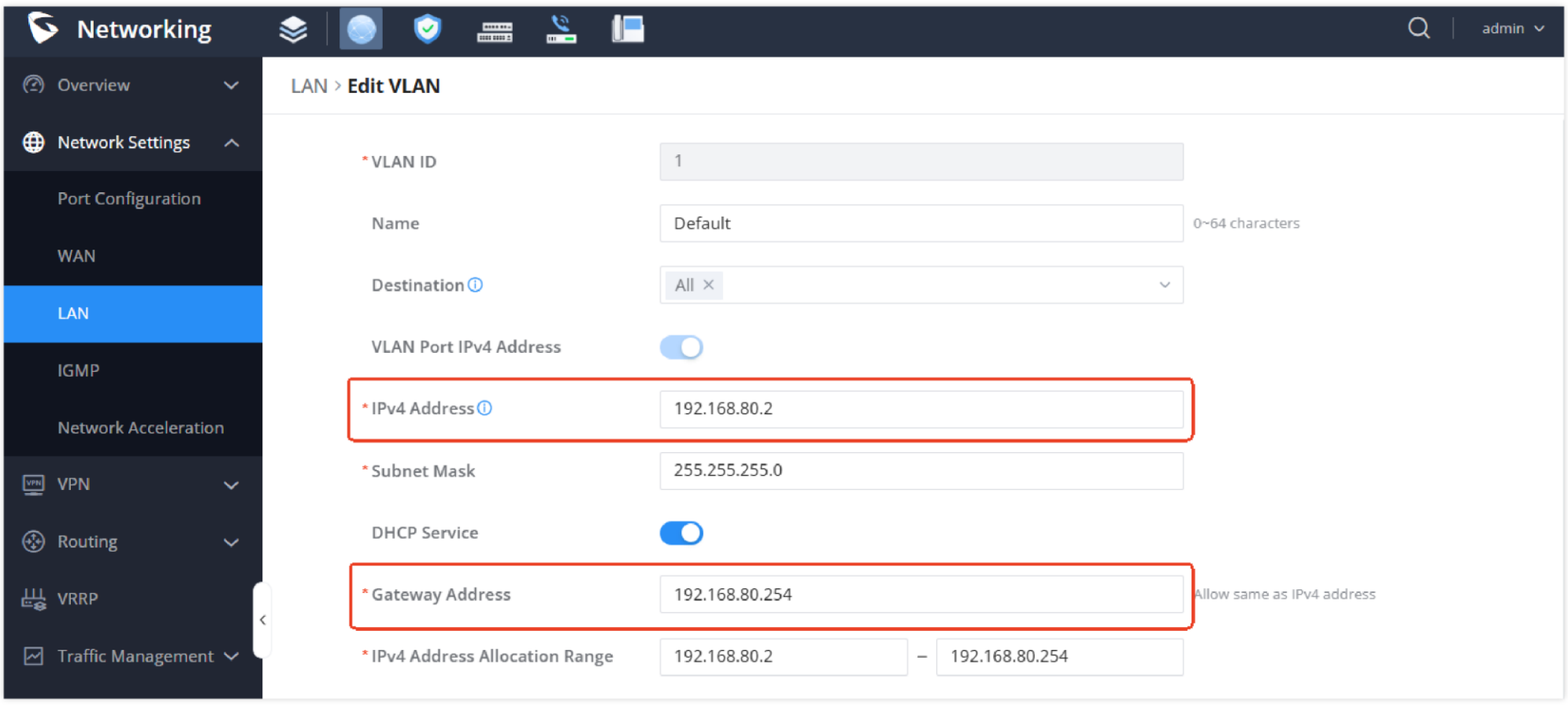
Configuring VRRP

PBX HA follows the VRRP role, and the IP of PBX is in the same network segment as the default VLAN, so the VRRP of the default VLAN interface must be configured.

GCC1 VRRP environment configuration

Configure the default VLAN interface

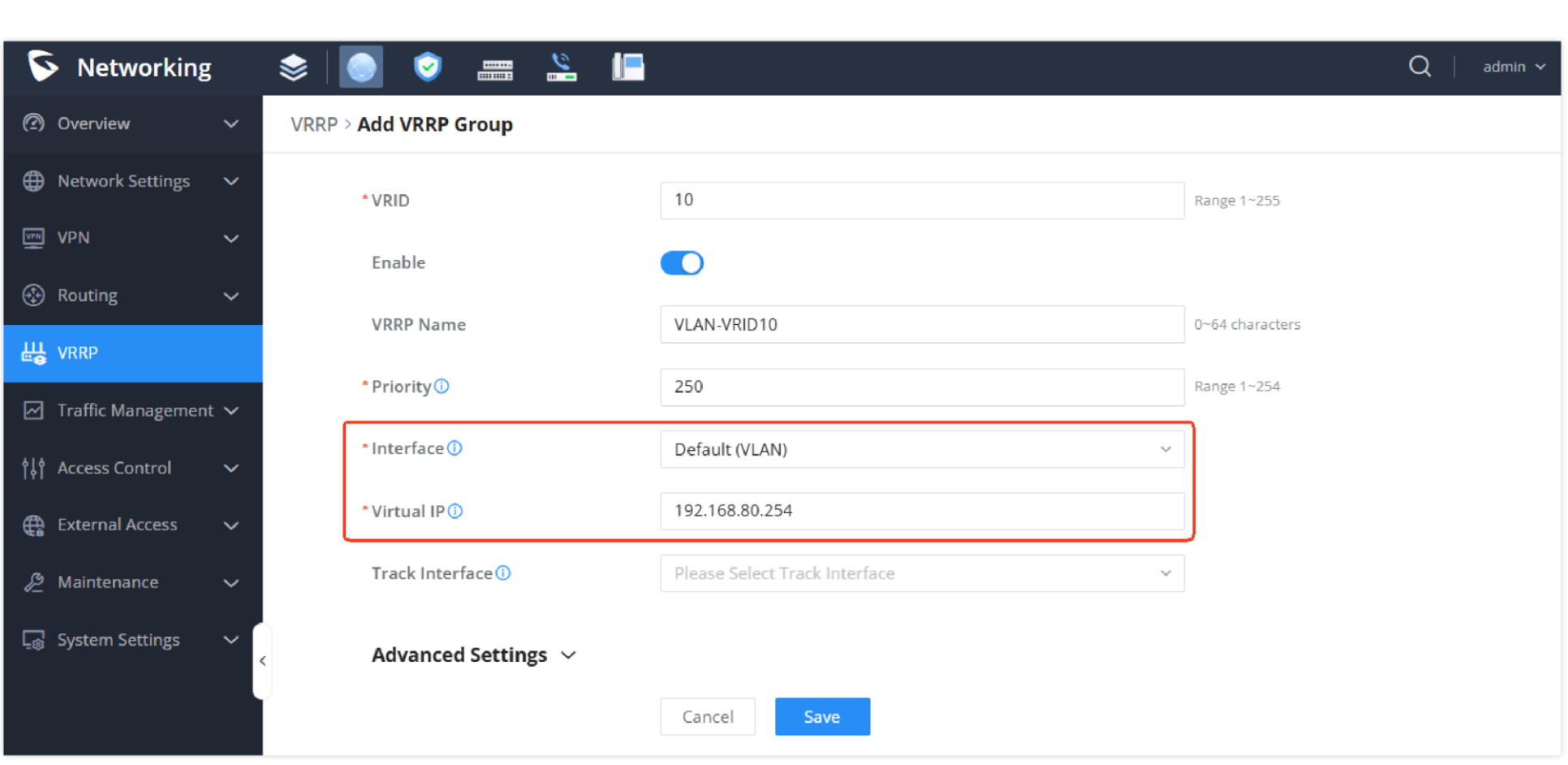
Enter the **Networking module → Network Settings → LAN**, and configure the Default VLAN.



GCC Networking LAN Settings

Configure VRRP for the default VLAN interface

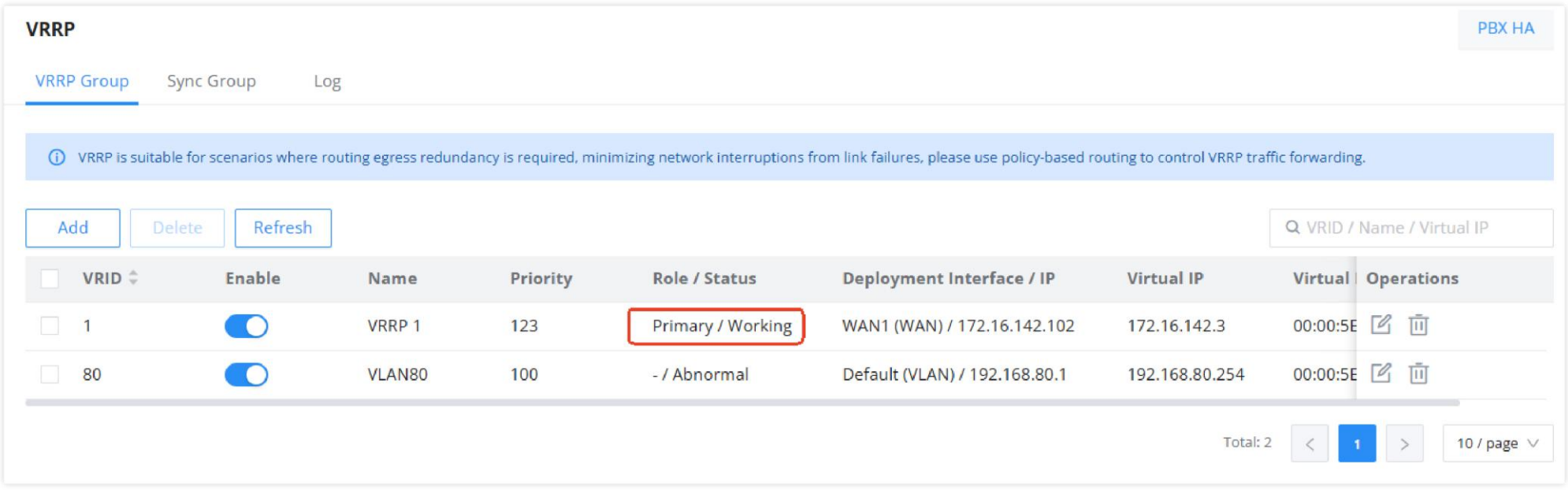
Enter the **Networking module → VRRP** page and add a VRRP group.



GCC Networking VRRP Settings

> **Note**
>
> Because network fluctuations may cause changes in VRRP roles or working status, affecting the establishment of HA, it is not recommended to configure Track Interface before forming HA dual machines.

After configuration, check the VRRP group role/status and wait for it to become Primary/Working:

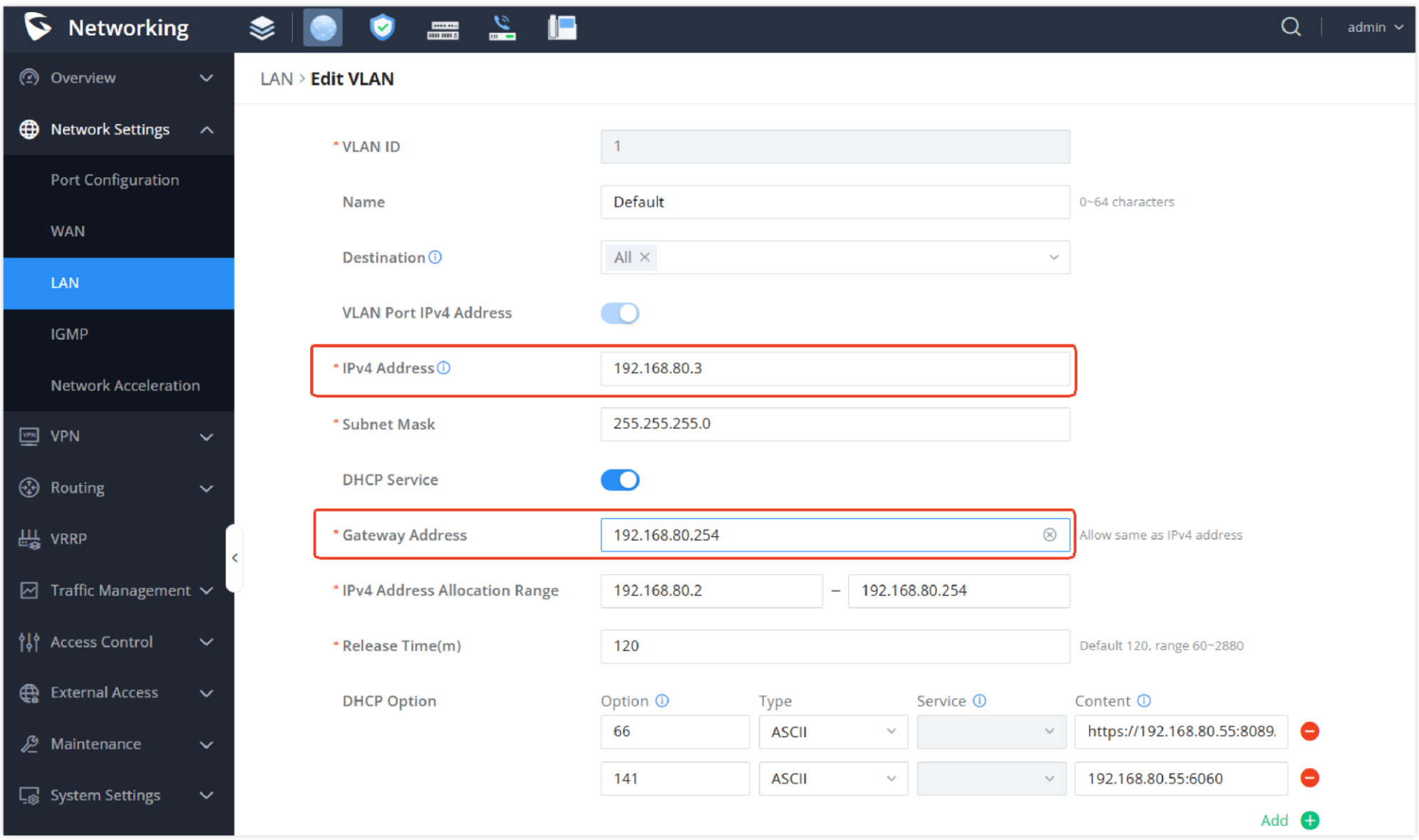


GCC VRRP Group

GCC2 VRRP environment configuration

Configure the default VLAN interface

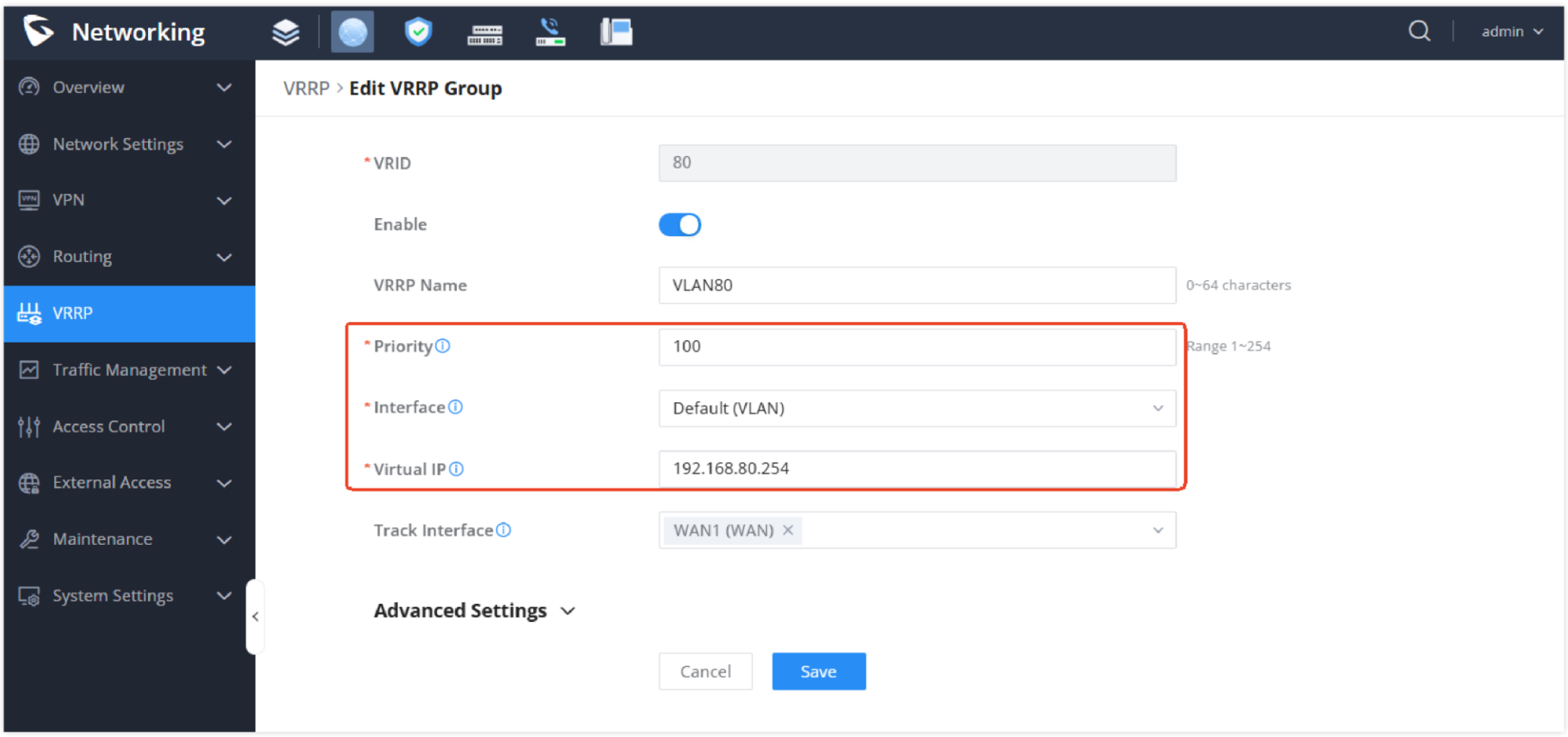
Enter the **Networking module → Network Settings → LAN**, and configure the Default VLAN:



GCC Networking LAN Settings

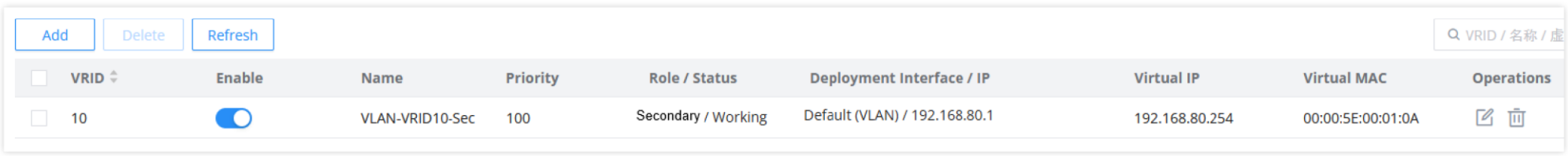
Configure VRRP for the default VLAN interface

Enter the **Networking module → VRRP** page, add a VRRP group, and note that the configuration **priority should be lower than GCC1**:



GCC Networking VRRP Group Settings

After configuration, check the VRRP group role/status and wait for it to become standby/working:



GCC Networking VRRP

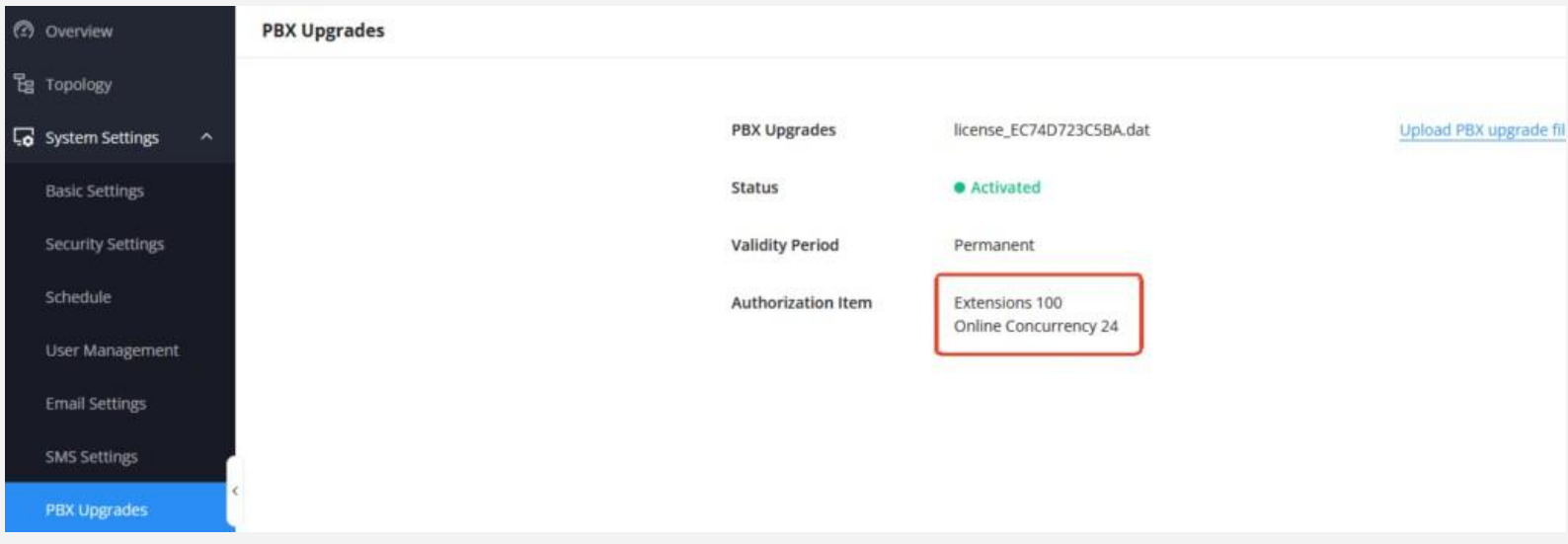
Enable HA

Before Enabling HA, you need to ensure that:

1. The PBX version of GCC1 and GCC2 is the same. Users can check the version information on the Home Component Overview page.
2. The PBX License specifications of GCC1 and GCC2 are the same. On the Upgrades page, check the number of extensions and concurrent users.
3. If you need to connect and use external storage devices, you need to ensure that the storage devices are consistent before setting up HA (including device type, device storage size, and quantity).

To view the PBX version information, go to the Home component and click the Overview page:

PBX License specifications, enter the Home component, **System Settings → PBX Upgrades** page to view:

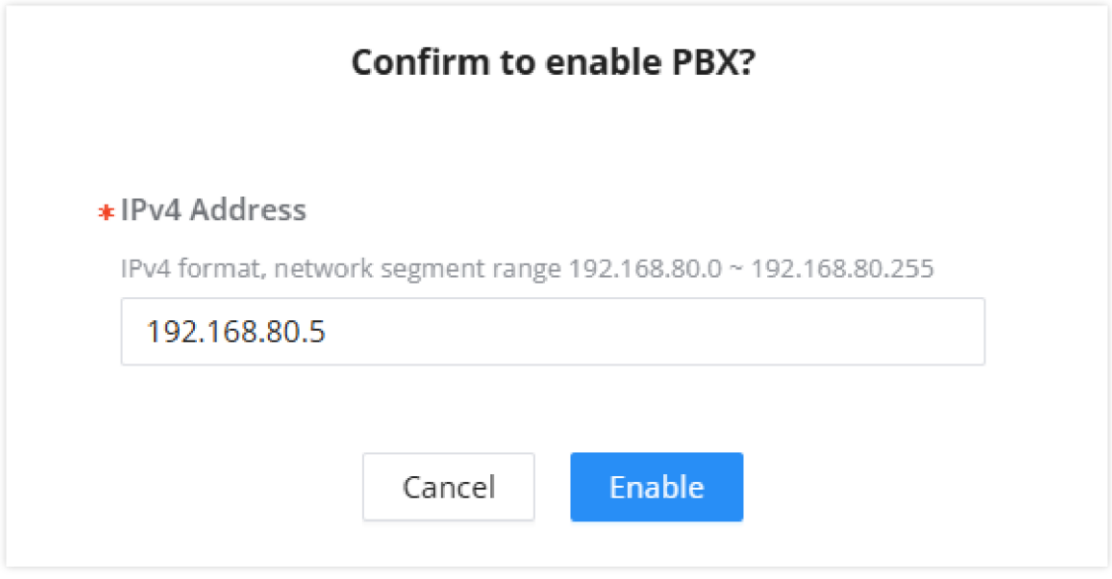


Note:

If you upload a license, you need to activate it before configuring HA. If it is not activated, even if the number of extensions and the number of online concurrent connections on both devices are the same, HA dual machines cannot be formed

- First, configure GCC1, turn on PBX on GCC1, and configure the PBX IP address:

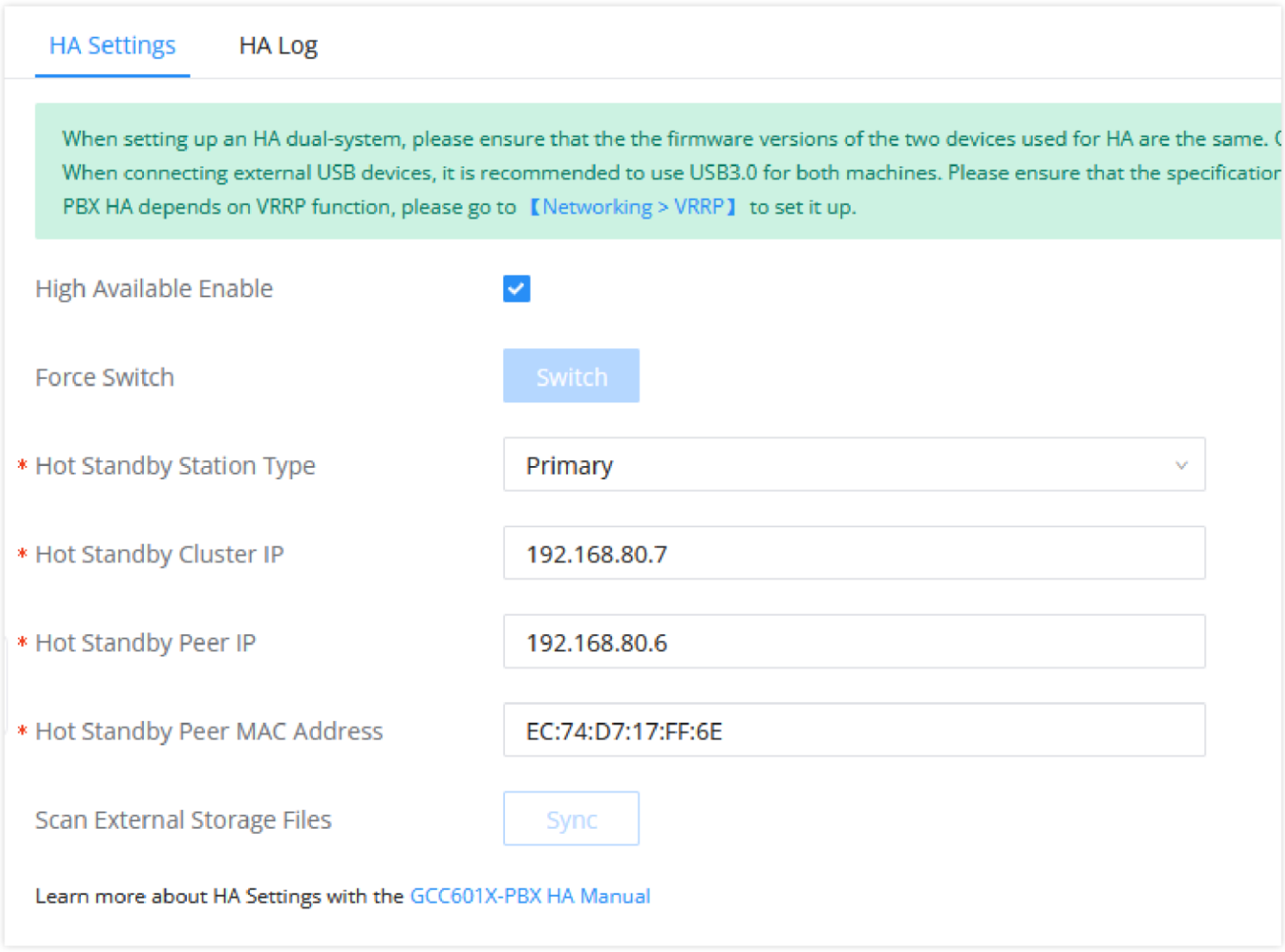
Enter Home and enable the PBX component:



Enable PBX

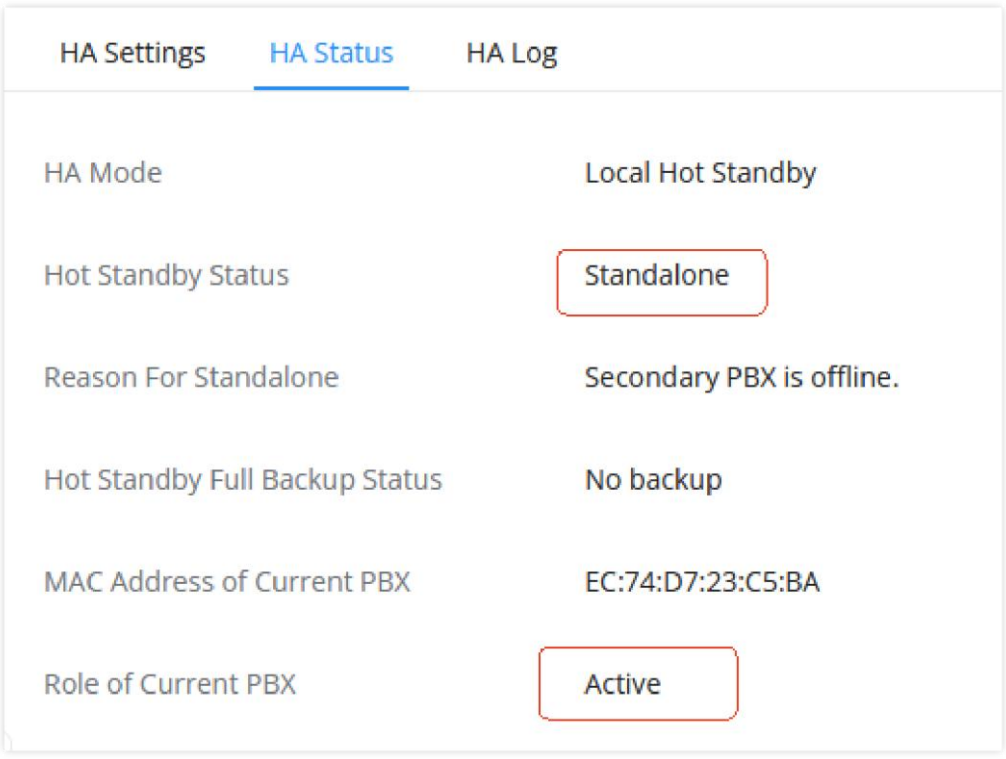
- After the PBX is started successfully, enable HA.

Go to **Networking → VRRP**, confirm that the VRRP role is active/working; then go to the PBX component, **System Settings → HA** page, and enable HA:



GCC PBX HA Settings

After enabling and restarting successfully, enter the PBX component and check the HA status on the **System Settings → HA → HA Status** page:



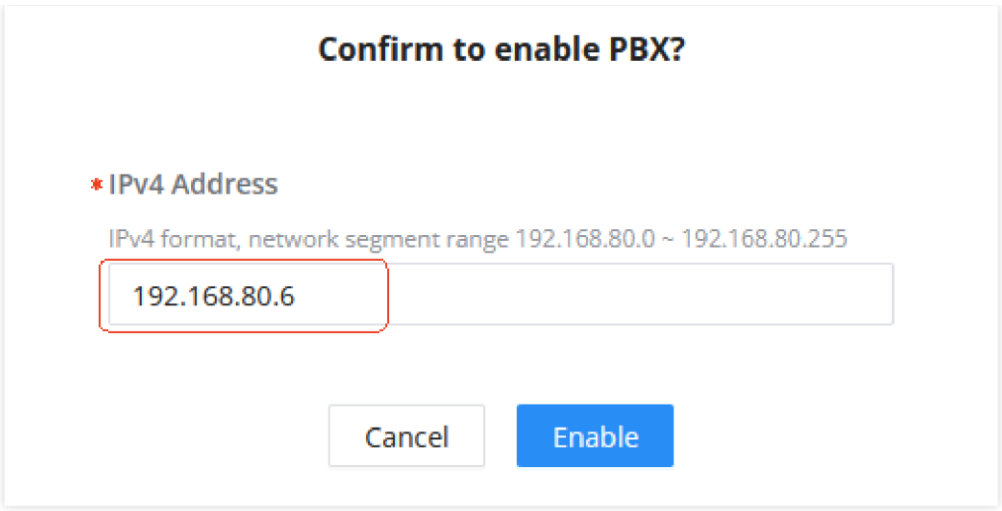
GCC PBX HA Status

Ensure that the HA status is currently displayed as Single-node Active.

> If it is displayed as a single-machine Standby, you need to confirm the VRRP role. If the VRRP role is active, disable and then enable the PBX component and recheck the HA status. If the VRRP role is on standby, you need to switch VRRP to active, and then disable and enable the PBX component.

- Then configure GCC2, GCC2 starts PBX and configures the PBX IP address:

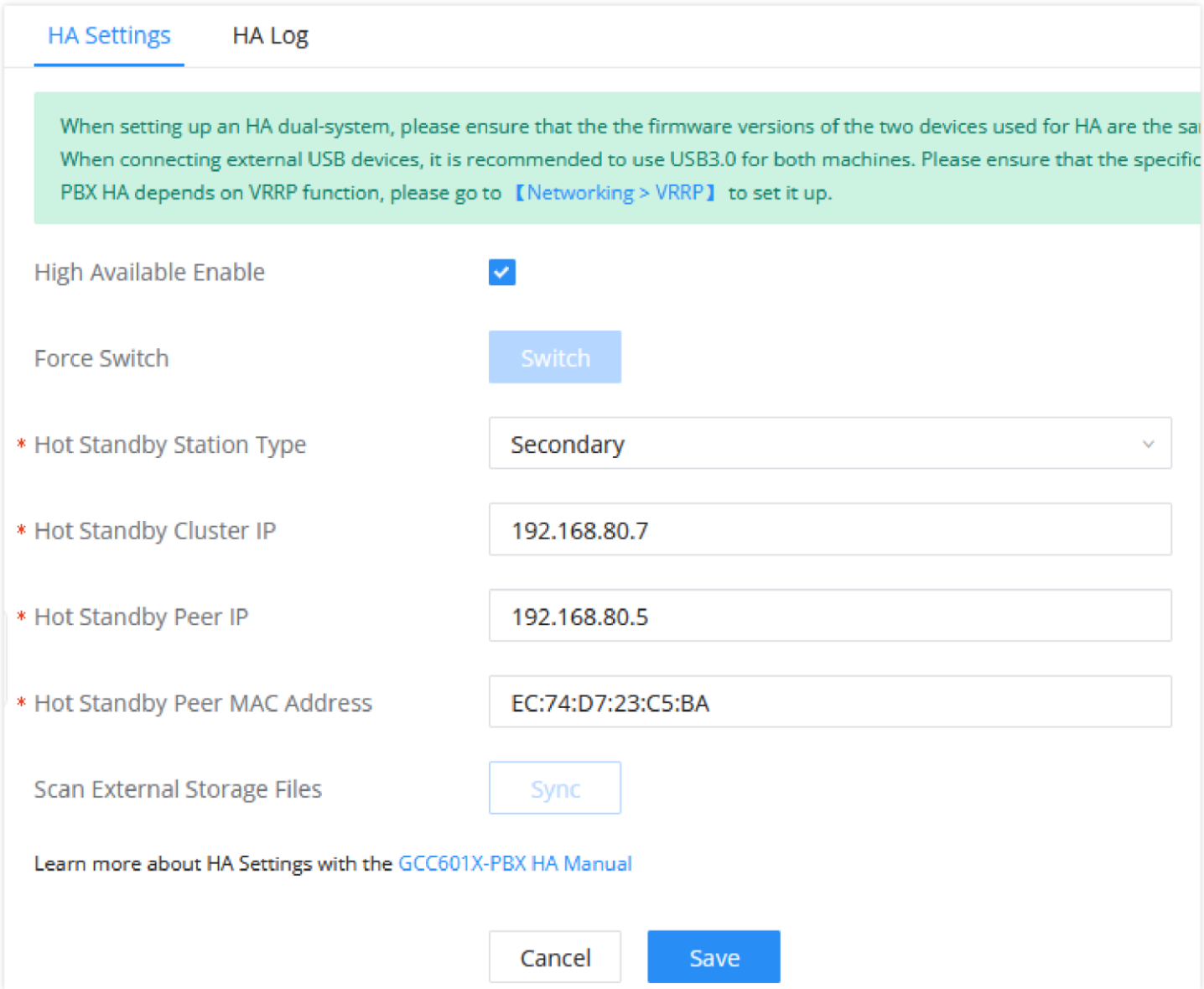
Enter Home and enable the PBX component:



Enable GCC PBX

- After the PBX is started successfully, enable the HA.

After entering the Networking module and confirming that VRRP is in the backup role, enter the PBX component, **System Settings → HA** page, and enable HA:

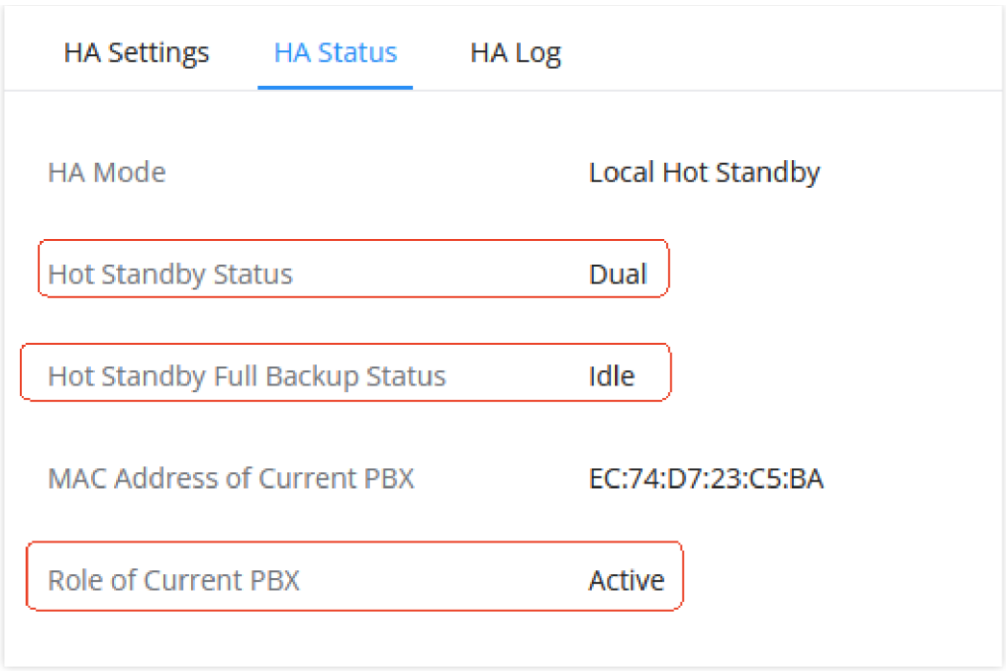


GCC PBX HA Settings

- After enabling and restarting successfully, verify the dual-machine status.

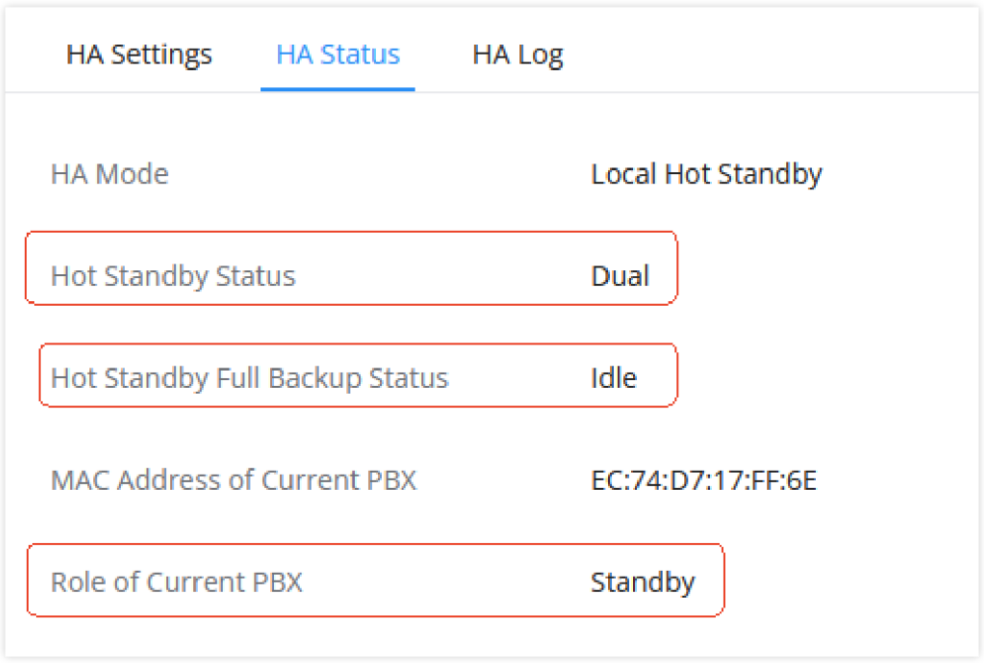
Enter the PBX component, **System Settings → HA → HA Status** page to check the HA status:

GCC1 is the active node of the dual-machine system:



HA Status – Active PBX

GCC2 is a dual-machine standby:



HA Status – On-standby PBX

HA configuration parameter description:

UCMRC PACKAGE RELATED CONFIGURATION

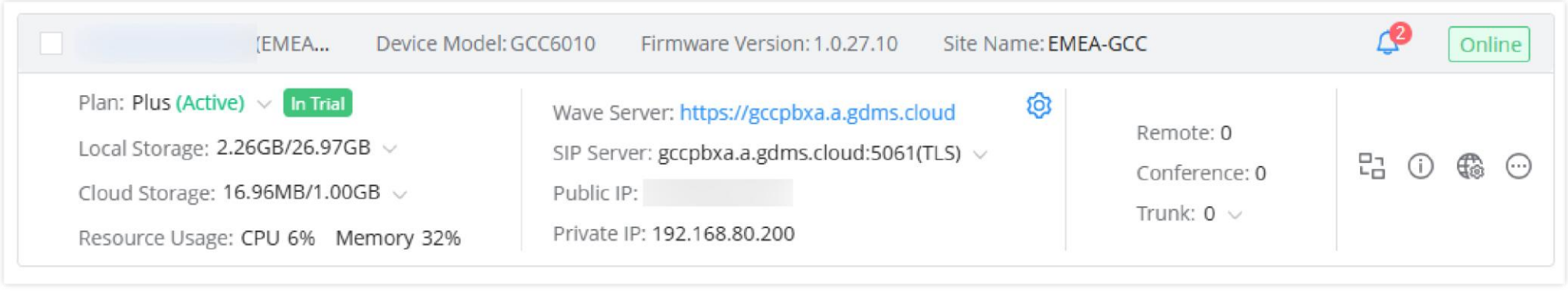
For two new GCC601X devices A and B, if the devices require UCMRC, in addition to completing the basic configuration process, the following package-related configuration is required:

1. If Cloud IM service is needed, please enable Cloud IM on device A (if it is enabled before HA is established, make sure Cloud IM is disabled on device B). When using the Cloud IM server issued by GDMS, make sure that both devices use the UCMRC package with Cloud IM permission.
2. Purchase the same UCMRC package with HA permissions for both devices. The order does not matter. (If A has already used the UCMRC package, you only need to purchase the package for B)
3. Configure a custom server address or domain name for device A with a primary site type and use it. For specific operations, refer to the following custom server address/domain name configuration. (If device A has already been configured with a custom server address or domain name, this step can be omitted)

UCMRC Permission Package

If you want to ensure the normal use of the UCMRC package in the HA situation, you need to purchase two UCMRC packages of the same specifications with HA service rights for the GCC device through GDMS and issue them to ensure the normal operation of the HA device on GDMS. If you only purchase a single package, GDMS operation may fail due to HA backup. If you only purchase a single UCMRC package with HA service rights, HA-related functions will not work properly.

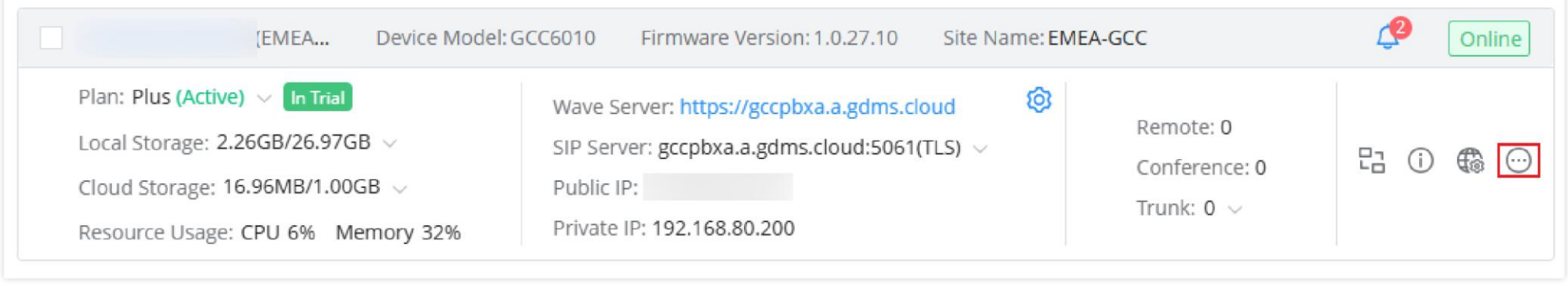
Specific steps: After logging in to the GDMS WEB page, in the GDMS Unified Communications → **UCMRC** → **PBX Device List** interface, click “Add Device” and enter the device information.



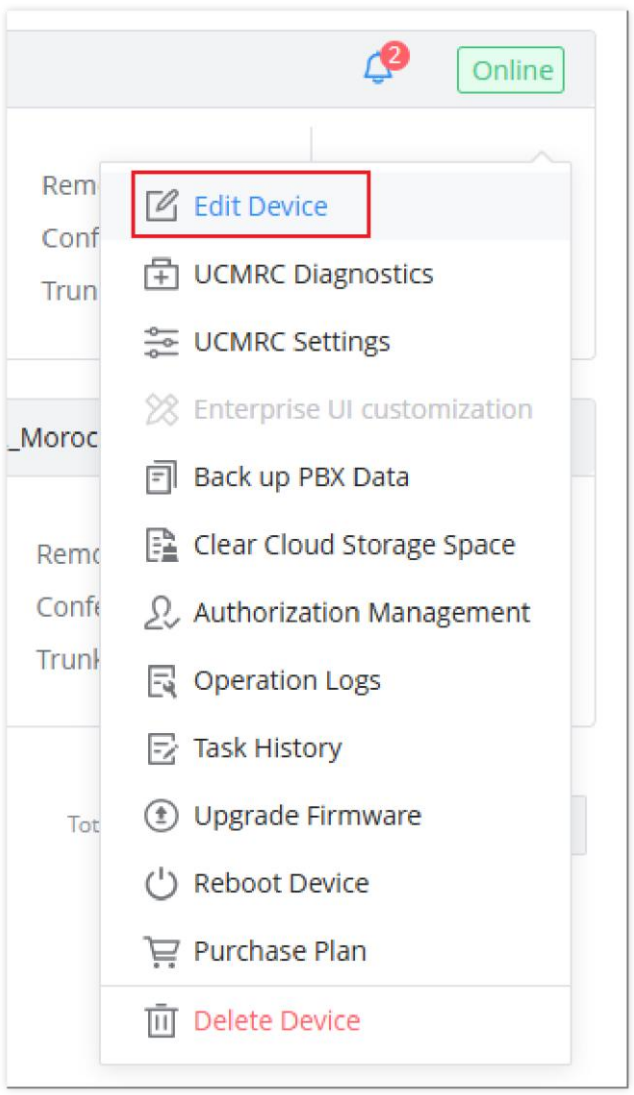
Custom Server/Domain Name Configuration

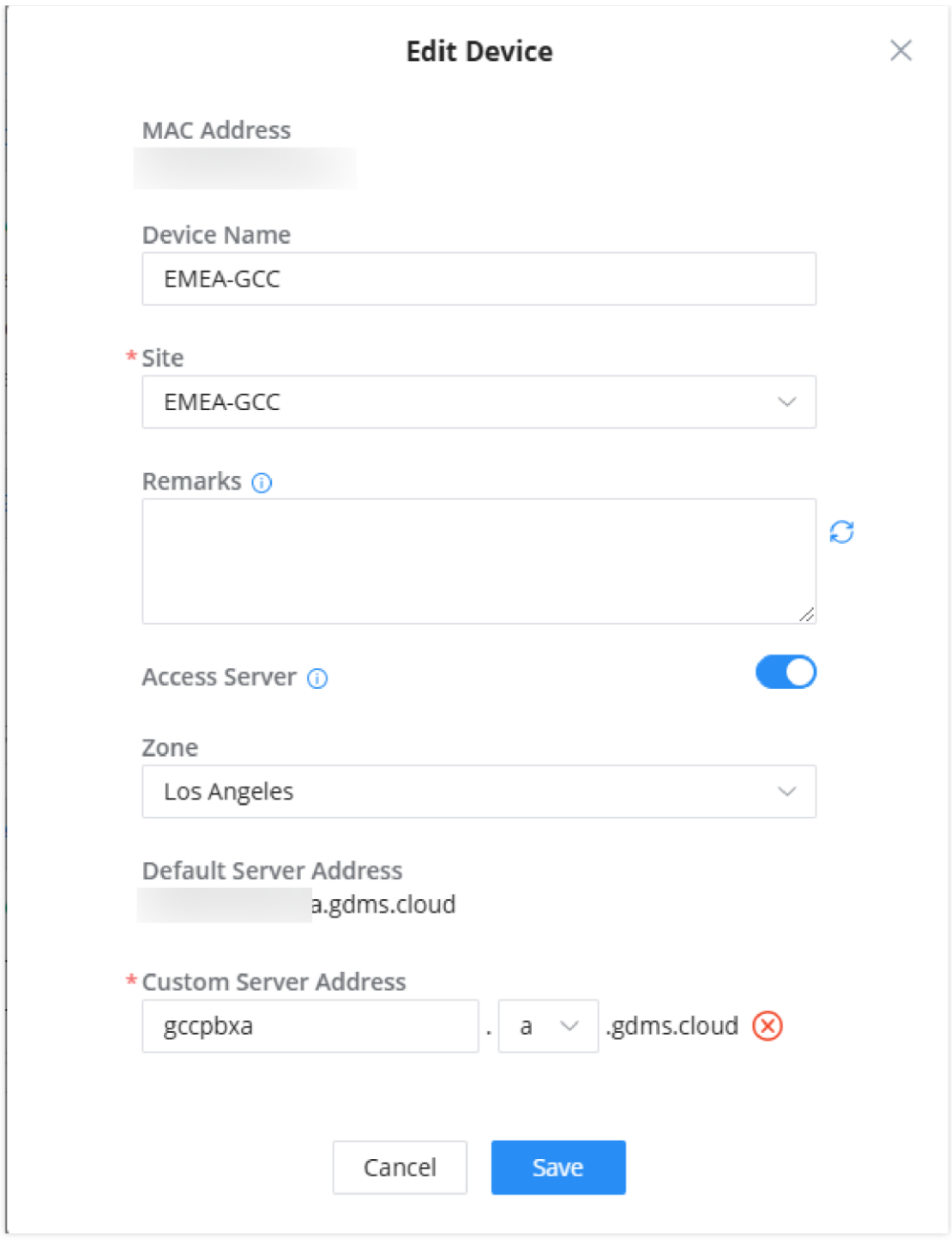
For two GCC devices that have purchased the UCMRC package with HA service, you need to configure a custom server address or domain name for the A device of the Primary site type.

The custom server address or domain name needs to be set through GDMS, which can be configured through **UCMRC** → **On-Premise PBX**, then click on ⋯.



Click on “Edit Device”





Users can configure the server address on this page. After saving, the custom domain name will be used.

After modifying the custom server address or domain name, please inform the user PBX of the new public network address.

For detailed configuration methods and questions about the custom server address or domain name, please refer to the GDMS UC User Guide.

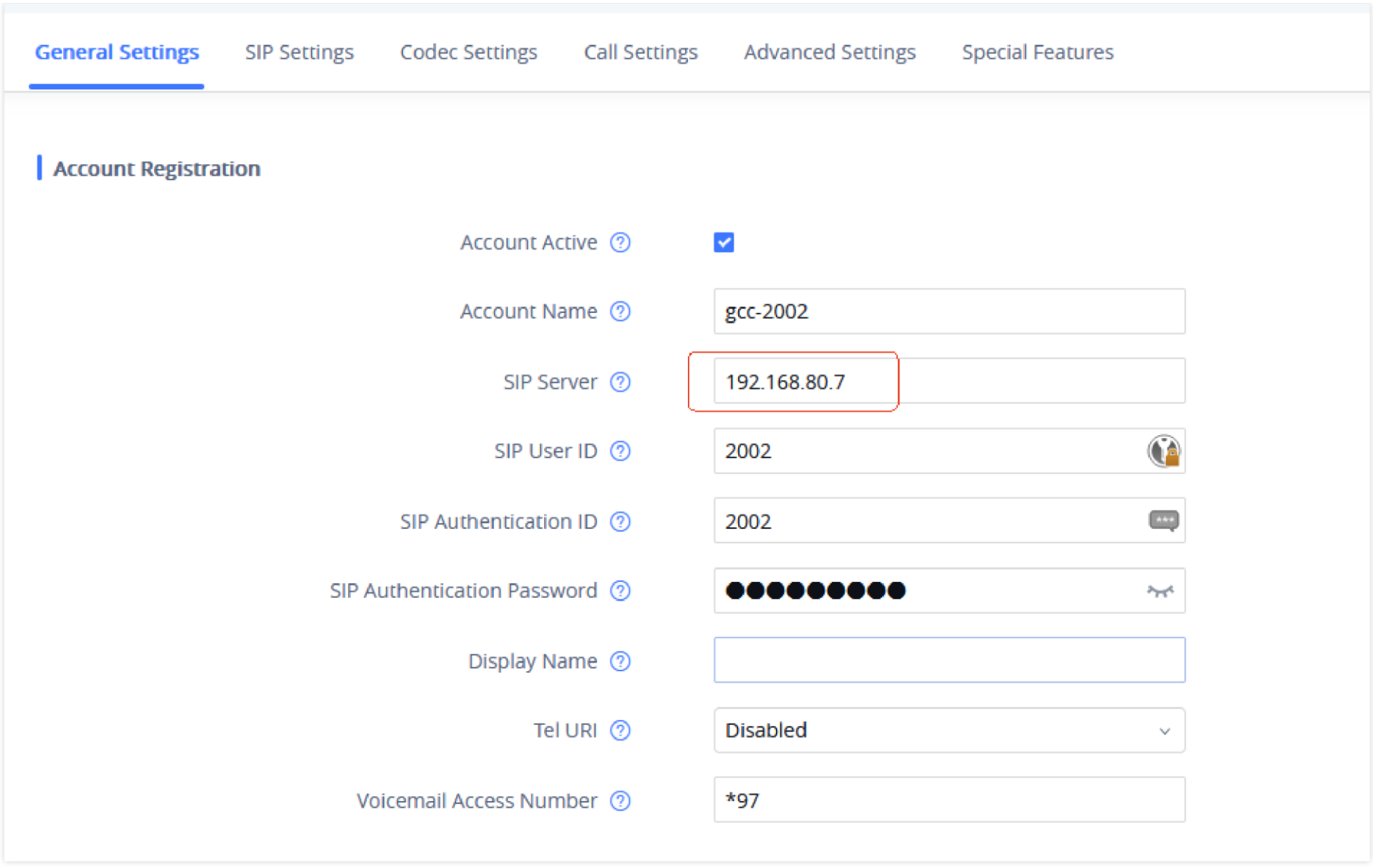
Note

If you need to purchase a UCMRC package with HA service rights, users can contact the corresponding equipment agent for package details.

REGISTRATION / CALL RELATED CONFIGURATION

Terminals in LAN Registration via HA Cluster IP

1. Taking the GXV3370 phone as an example, the phone registration configuration is:



192.168.80.7 is the cluster IP of the HA dual-machine in our example.

2. Wave login:

Intranet PCs can log in to Wave via **https://cluster IP/gswave/#/**.

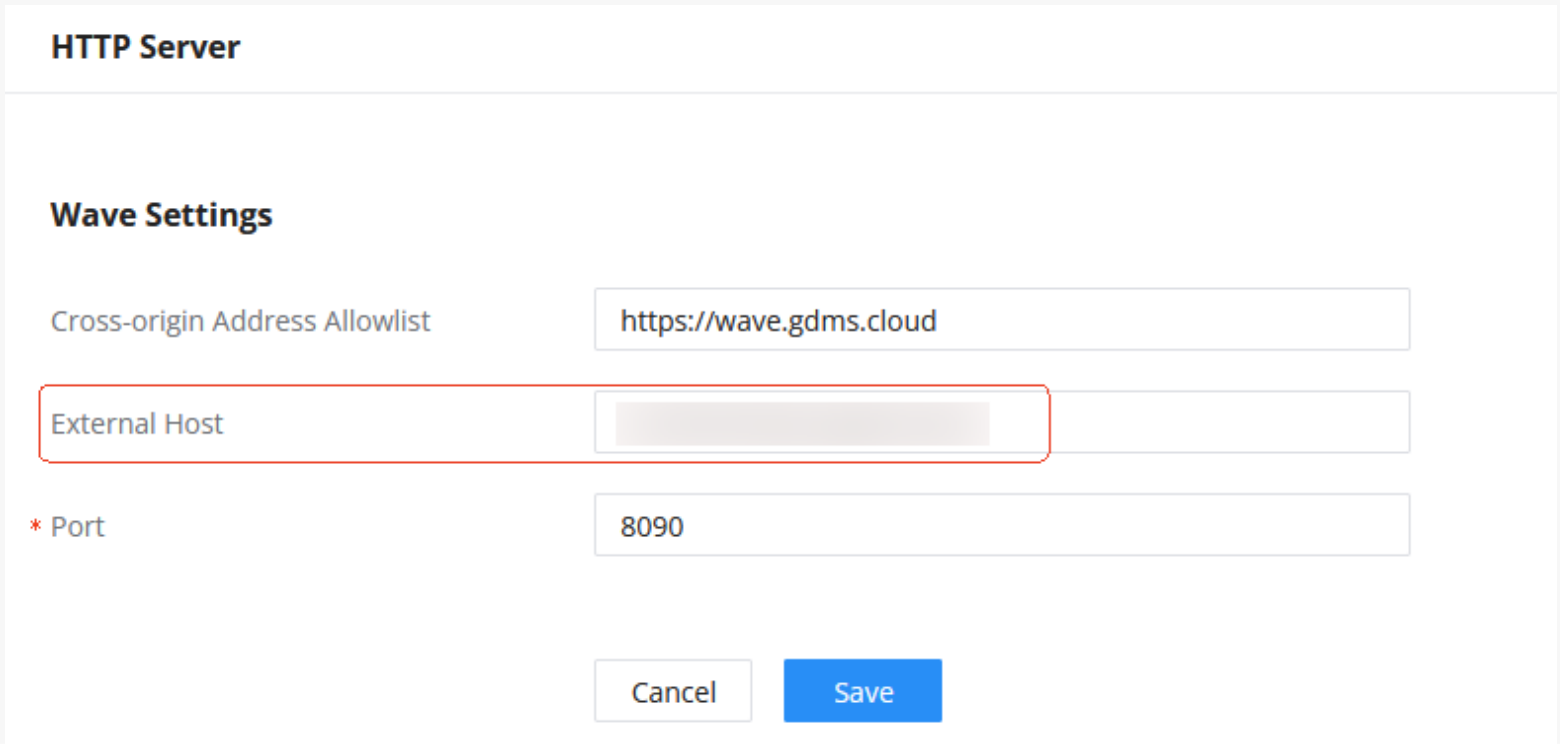
For example, https://192.168.80.7:8089/gswave/#/ (where 192.168.80.7 is the cluster IP of the HA dual-machine).

Terminal Registration Through the GDMS Domain Name

After obtaining the UCMRC package, both WAN-side devices and LAN-side devices can be registered directly through the GDMS domain name.

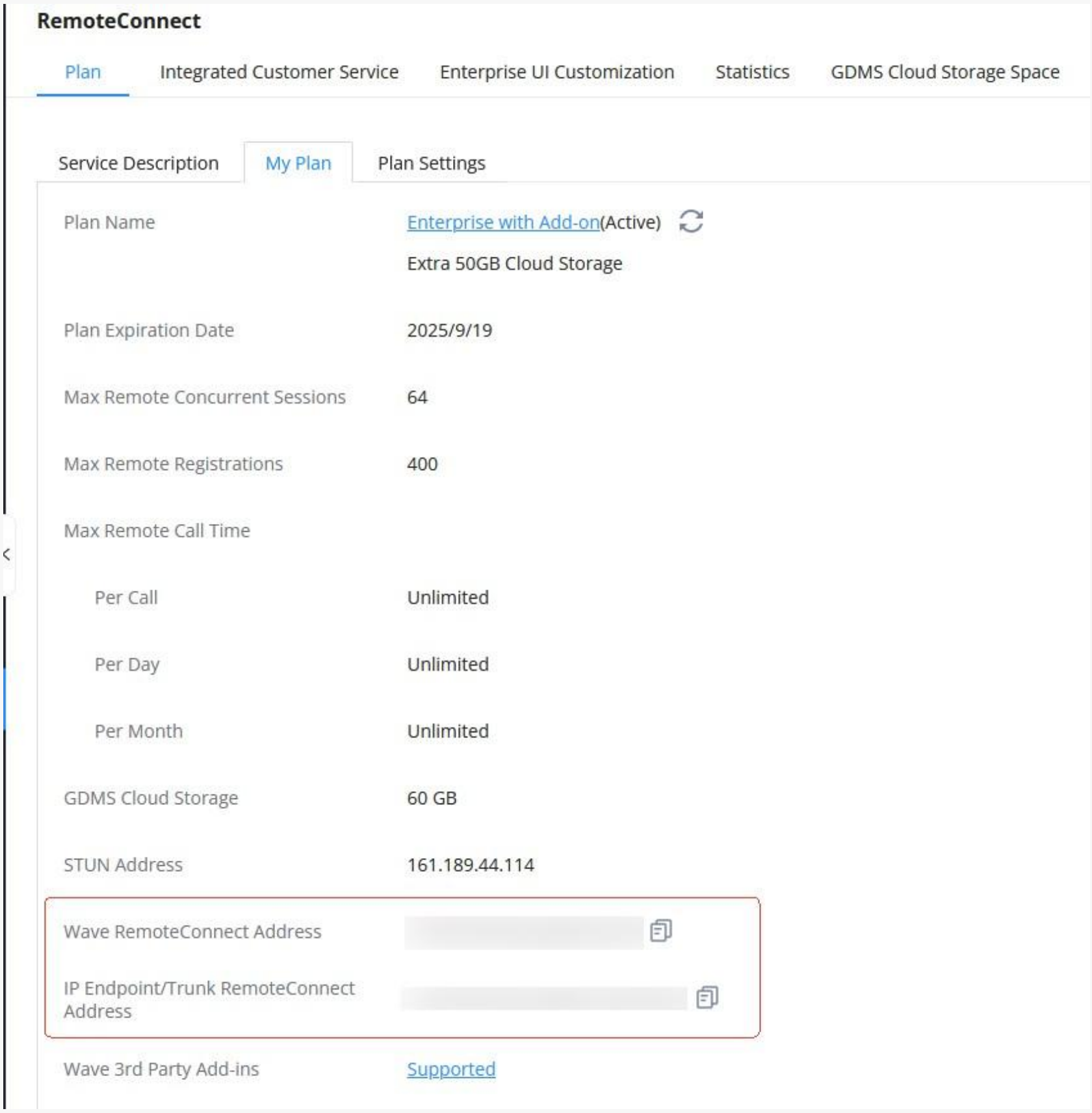
Regardless of how the roles are switched, the domain name is based on the one issued by GDMS, and GDMS issues it based on the device initially set as Primary.

The GDMS domain name can be checked in the PBX component, **System Settings → HTTP Server** page:



HTTP Server

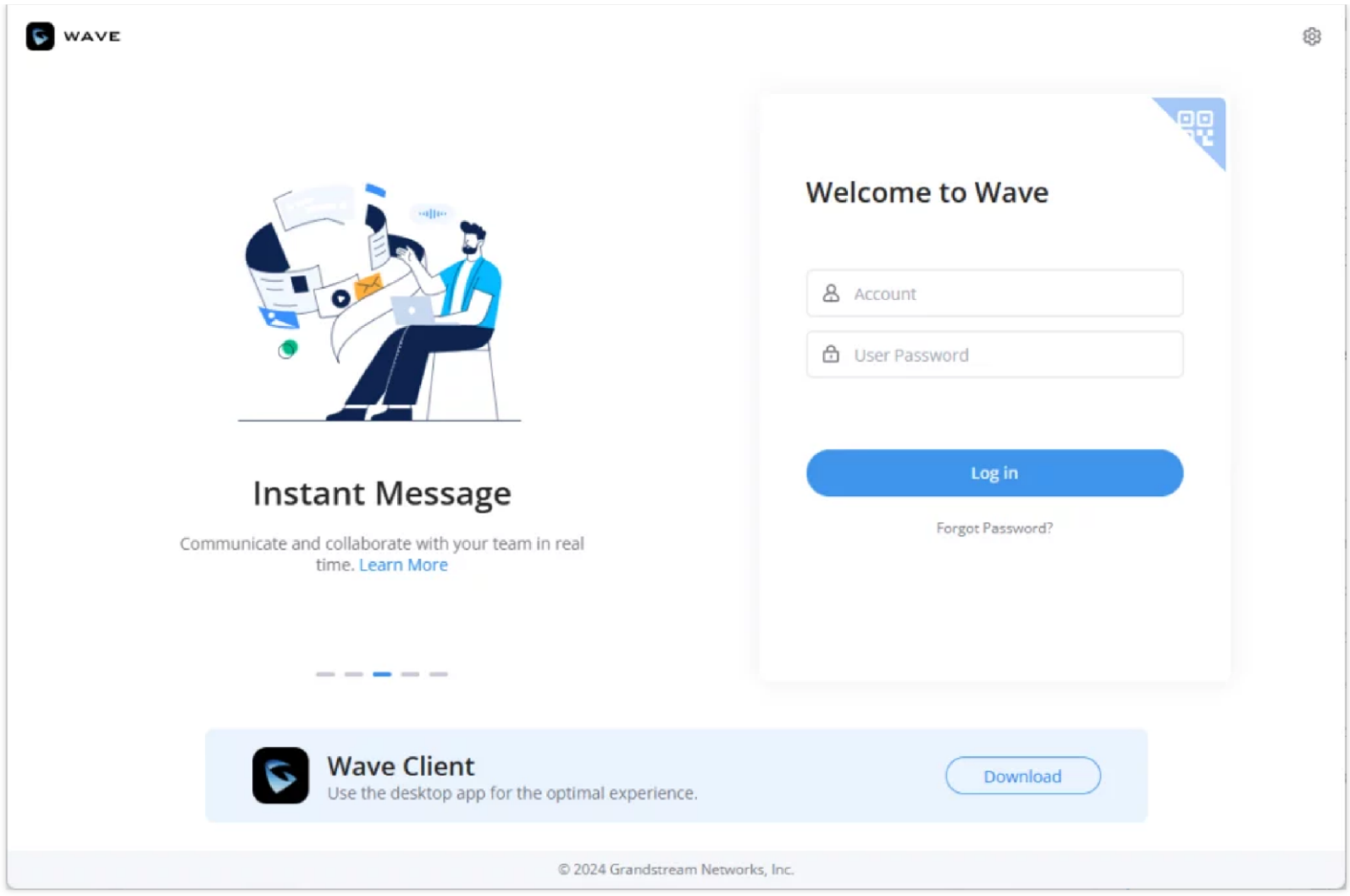
Or it can be checked on the RemoteConnect page:



RemoteConnect Plan

After obtaining the domain name, users can:

1. Directly access it through the browser (using Wave Web) to log in and register:

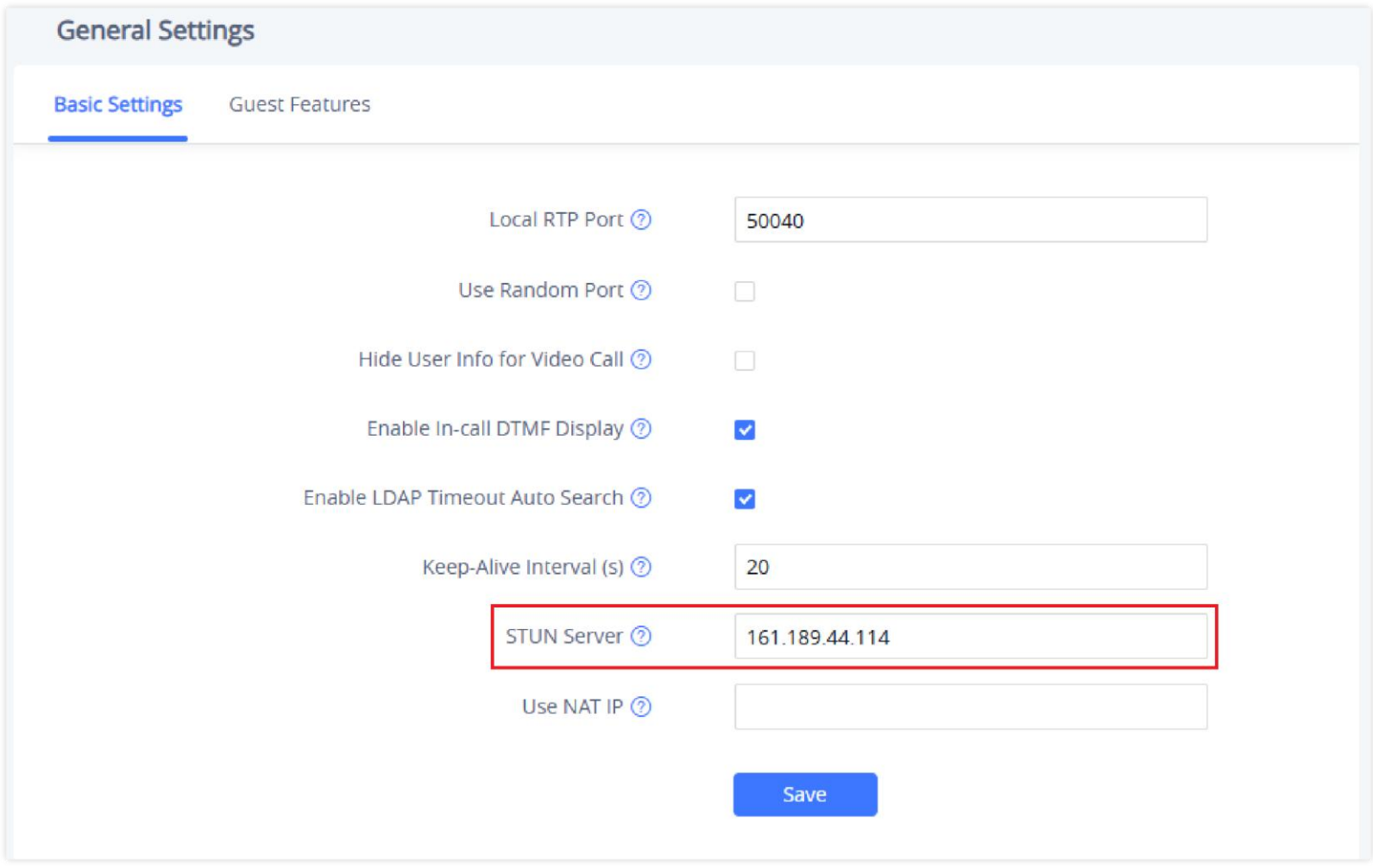


Wave Web

The same goes for Wave Desktop and Wave Mobile APP. Users can directly use the domain name to log in and register.

2. Register the phone through the domain name:

Take GXV3370 as an example. Log in to the phone web, go to **Phone Settings → General Settings → Basic Settings** page, and configure the STUN server (the address can be obtained on the RemoteConnect page):



GXV3370 – General Settings – Basic Settings

Enter the phone account page, configure the registration information, and use TLS to register. The configuration is as follows:

General Settings | SIP Settings | Codec Settings | Call Settings | Advanced Settings | Special Features

Account Active
Account Name: gcc-2002
SIP Server:
SIP User ID: 2002
SIP Authentication ID: 2002
SIP Authentication Password: ●●●●●●●●
Display Name:
Tel URI: Disabled
Voicemail Access Number: *97

Network Settings

Outbound Proxy:
Secondary Outbound Proxy:
DNS Mode: A Record
NAT Traversal: Keep-Alive

GXV3370 – Account Page – General Settings

Account 1 | Account 2 | Account 3 | Account 4 | Account 5 | Account 6

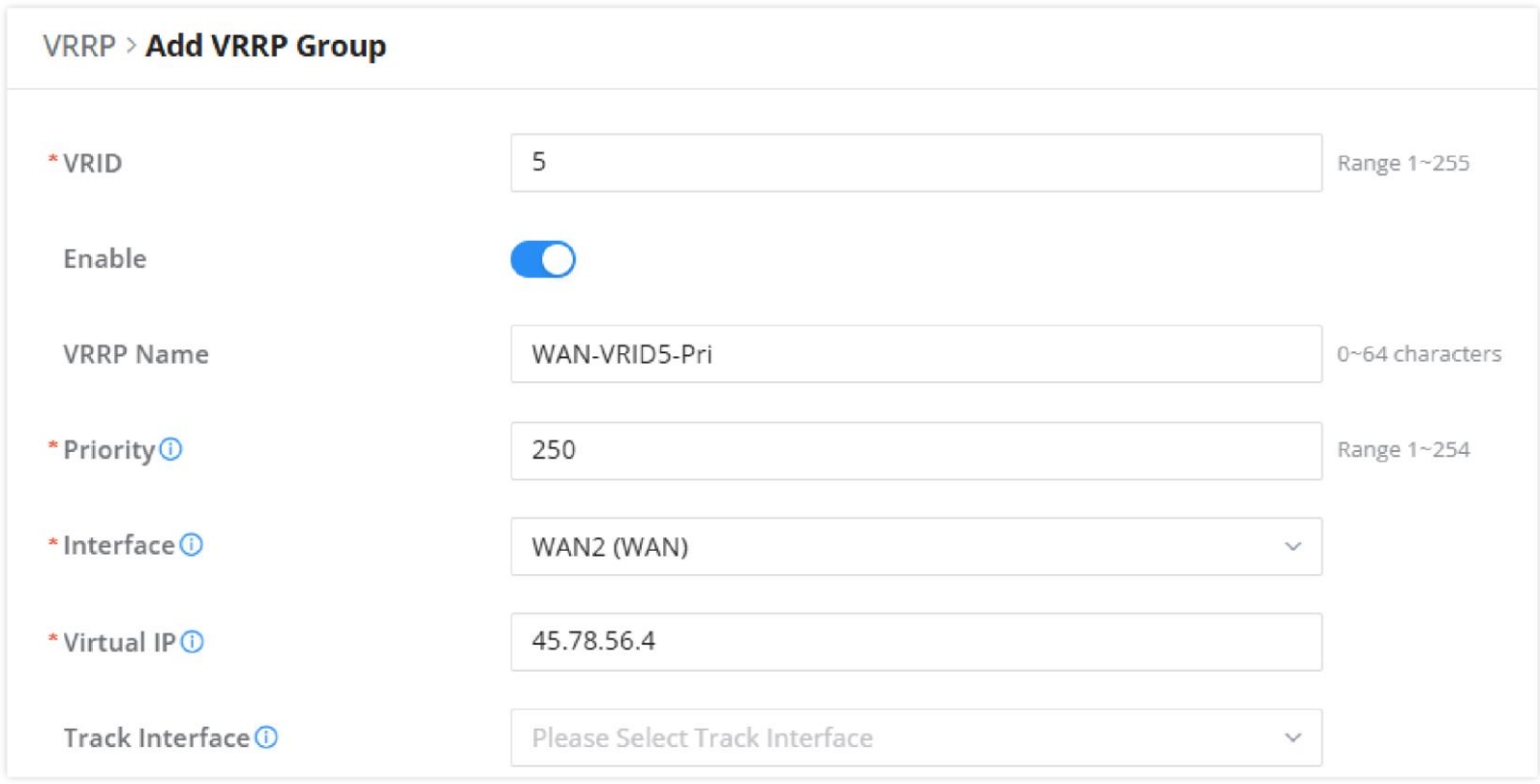
General Settings | SIP Settings | Codec Settings | Call Settings | Advanced Settings | Dial Plan | Hidden Number Pl

Use P-Emergency-Info Header
Use P-Asserted-Identity Header
Use P-Early-Media Header
Use Zoom E911 X-switch-info SIP Header
Use MAC Header: No
Add MAC in User-Agent: No
SIP Transport: TLS/TCP
Enable TCP Keep-alive
SIP Listening Mode: Transport Only
Local SIP Port: 5060
SIP URI Scheme When Using TLS: sips
Use Actual Ephemeral Port in Contact with TCP/TLS
Support SIP Instance ID
SIP T1 Timeout: 0.5 sec
SIP T2 Timeout: 4 sec

Save | Save and Apply | Reset

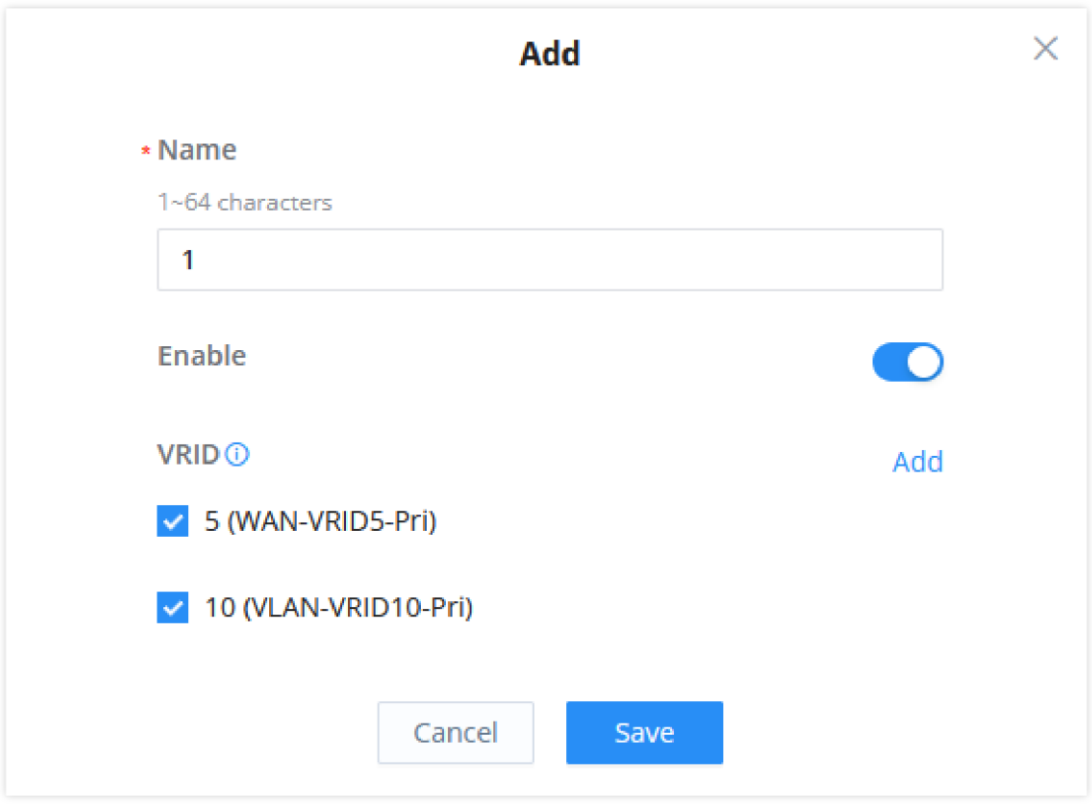
WAN Side Terminal Registration via WAN IP

1. First, configure WAN VRRP and add the WAN VRRP group to GCC1:



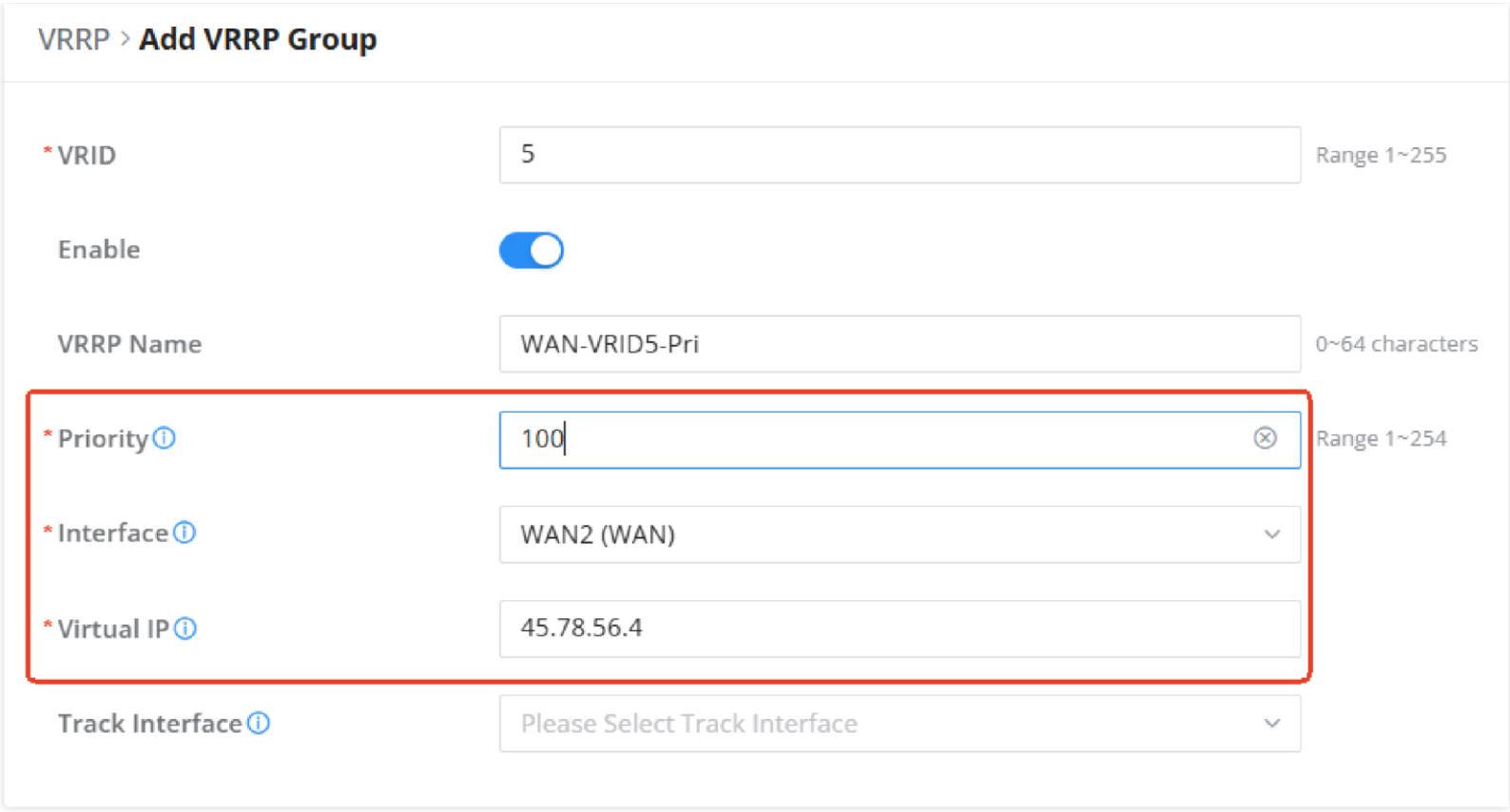
GCC 1 – Add VRRP Group

After WAN VRRP becomes the master, add WAN VRRP and LAN VRRP to the same synchronization group:



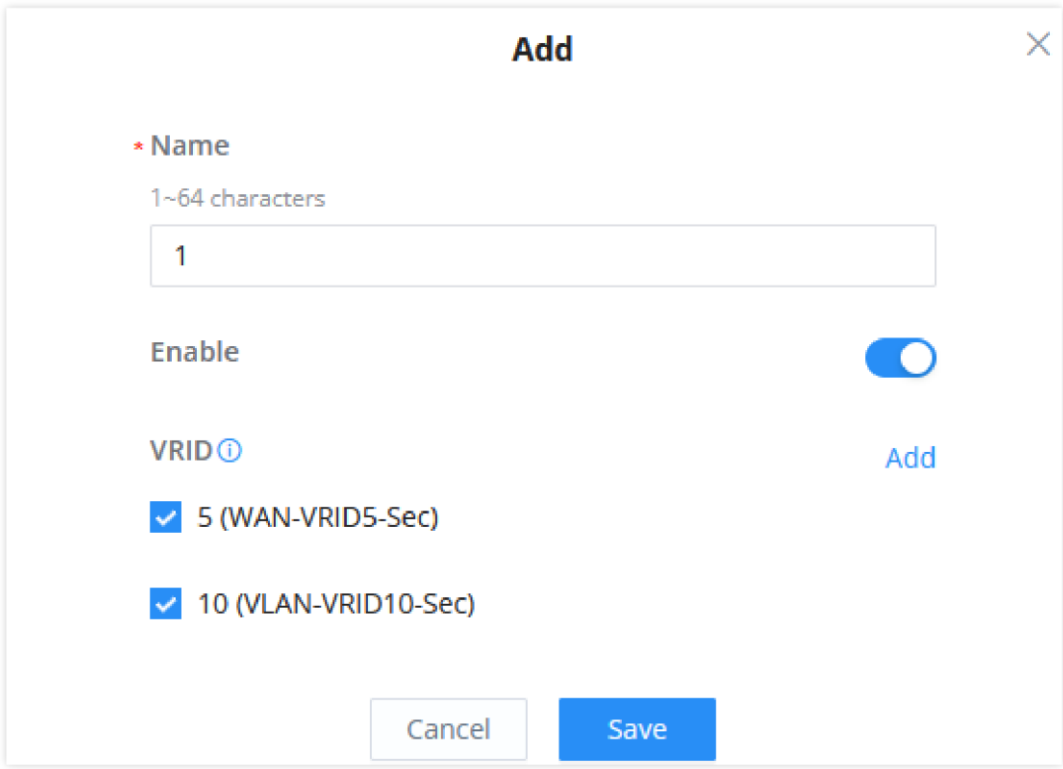
GCC 1 – VRRP – Add Synchronization Group

GCC2 adds WAN VRRP group:



GCC 2 – Add VRRP Group

After WAN VRRP becomes the standby role, add WAN VRRP and LAN VRRP to the same synchronization group:



GCC 1 – VRRP – Add Synchronization Group

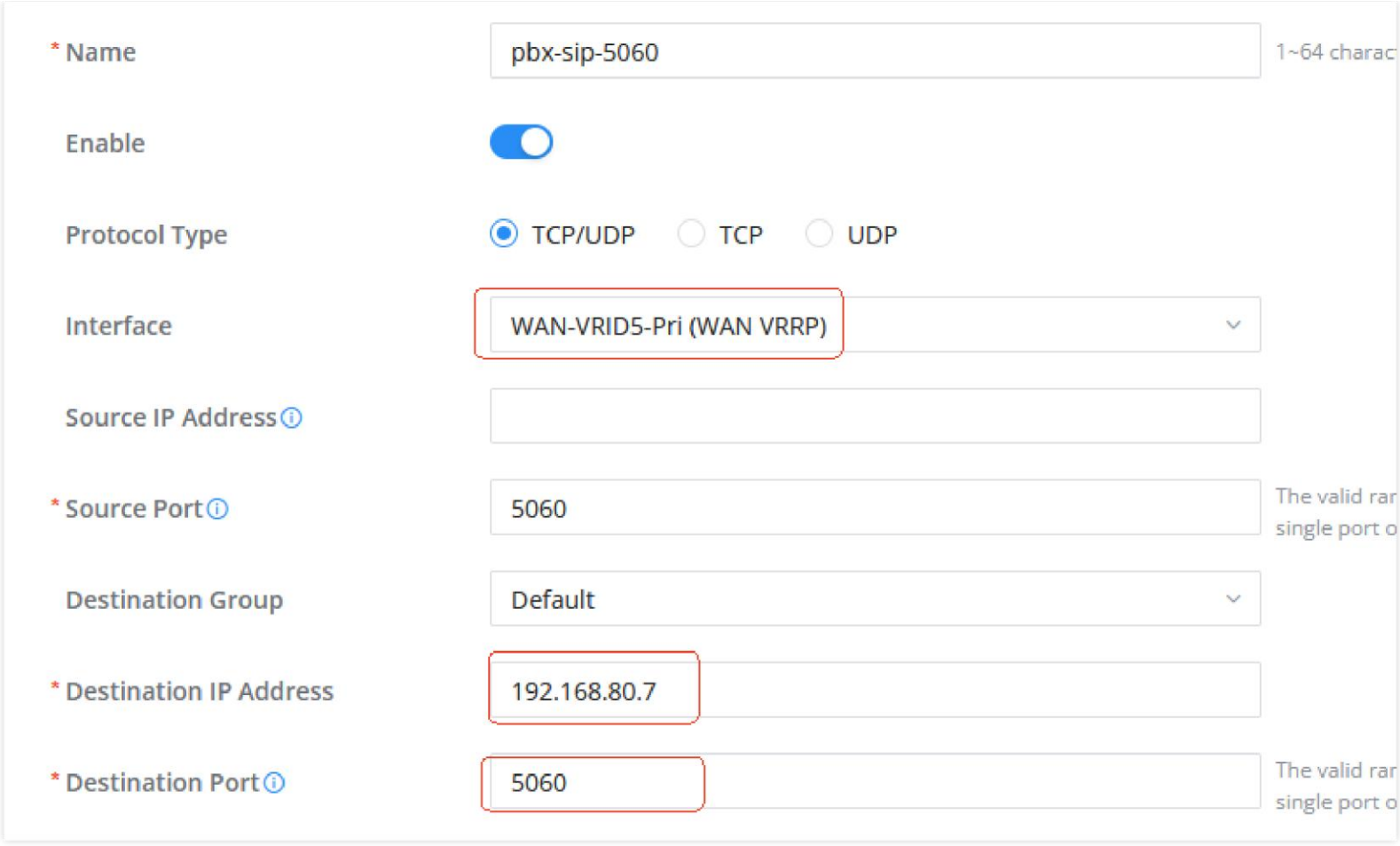
Reference:

For more details, refer to [Configuring VRRP] section.

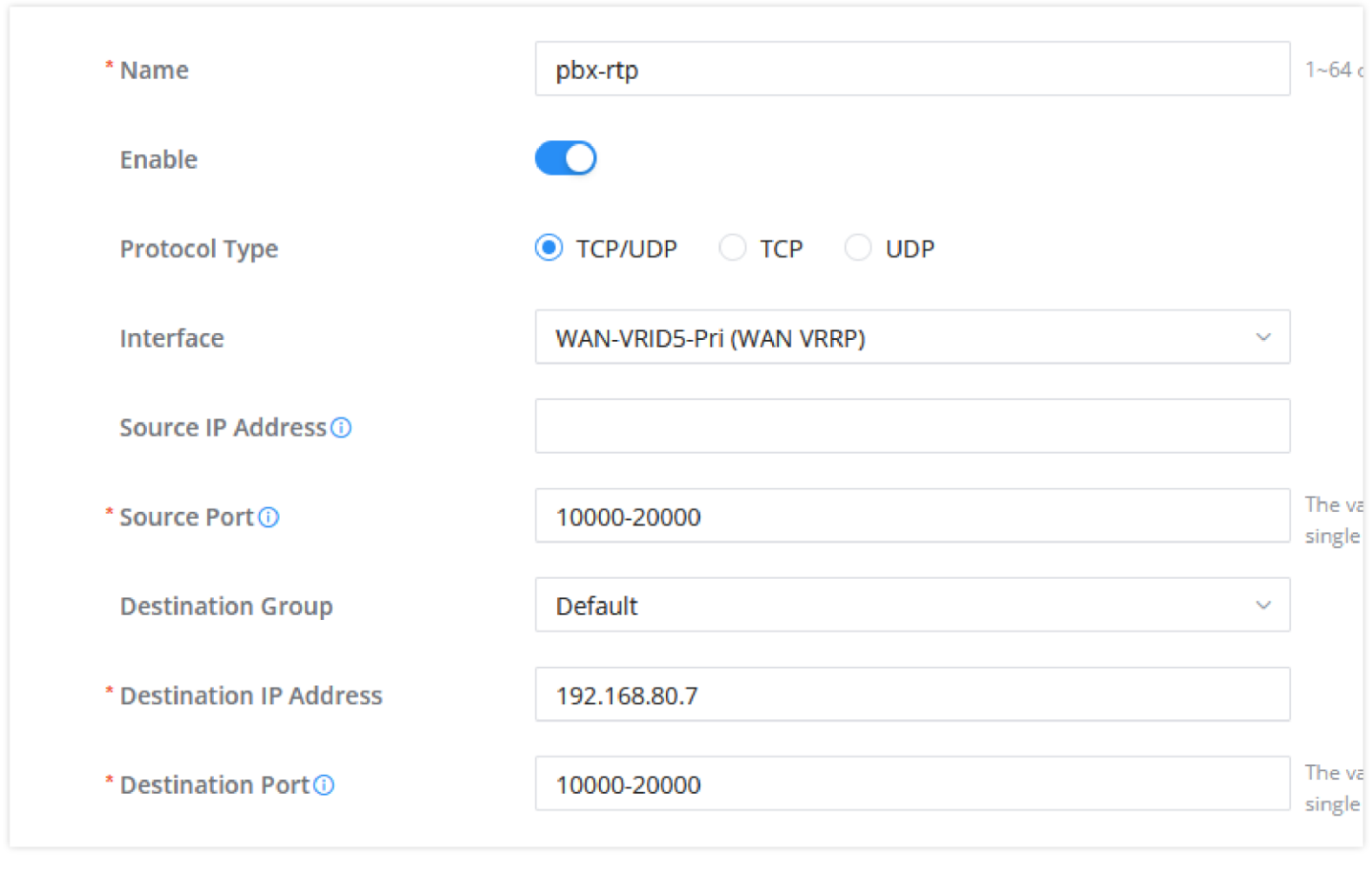
2. Then configure the port forwarding rules:

    1. GCC1 configures port forwarding rules:

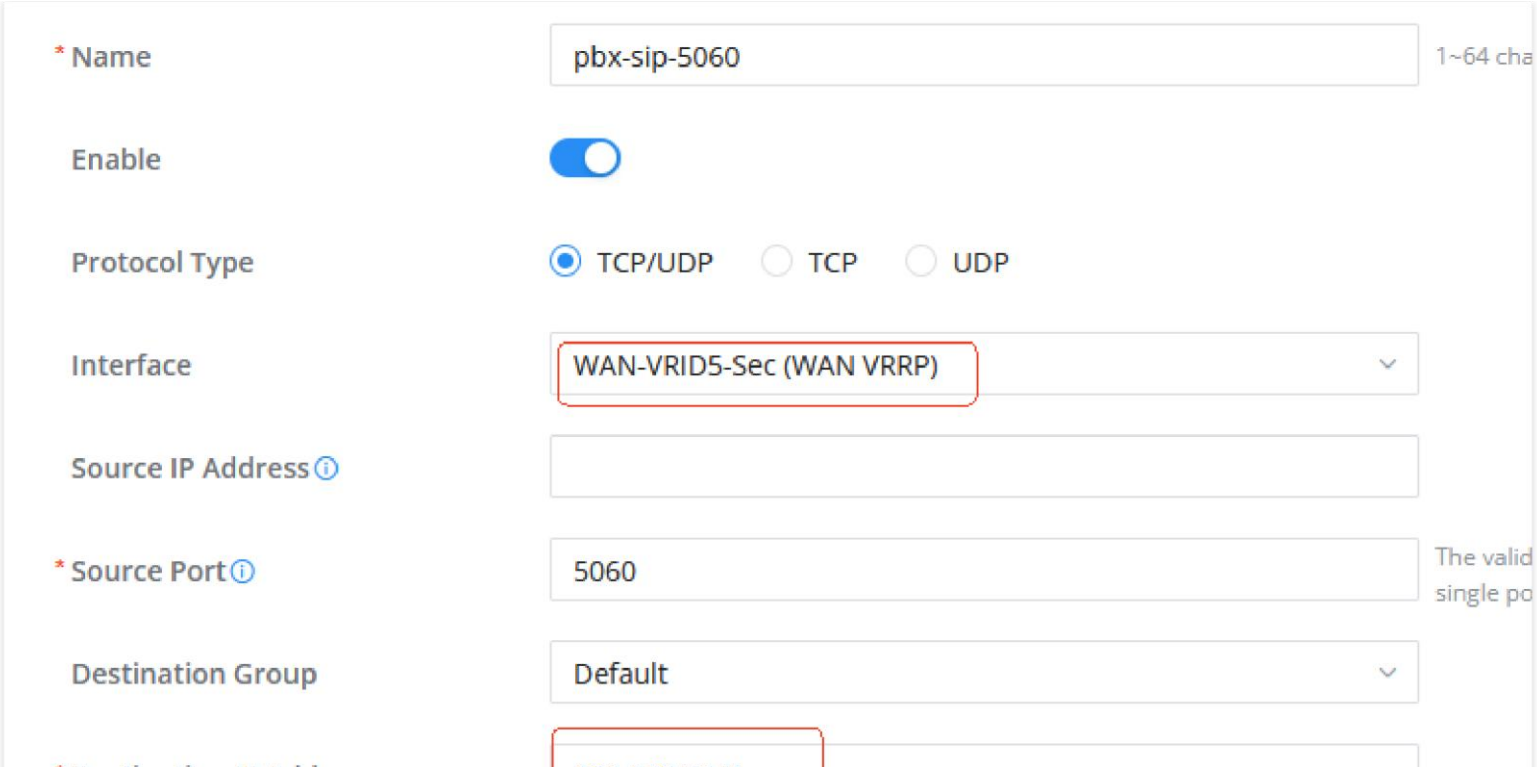
Go to the **Networking module → External Access → Port Forwarding** page, and add a forwarding rule from the WAN VRRP interface source port 5060 to the PBX cluster IP address destination port 5060:



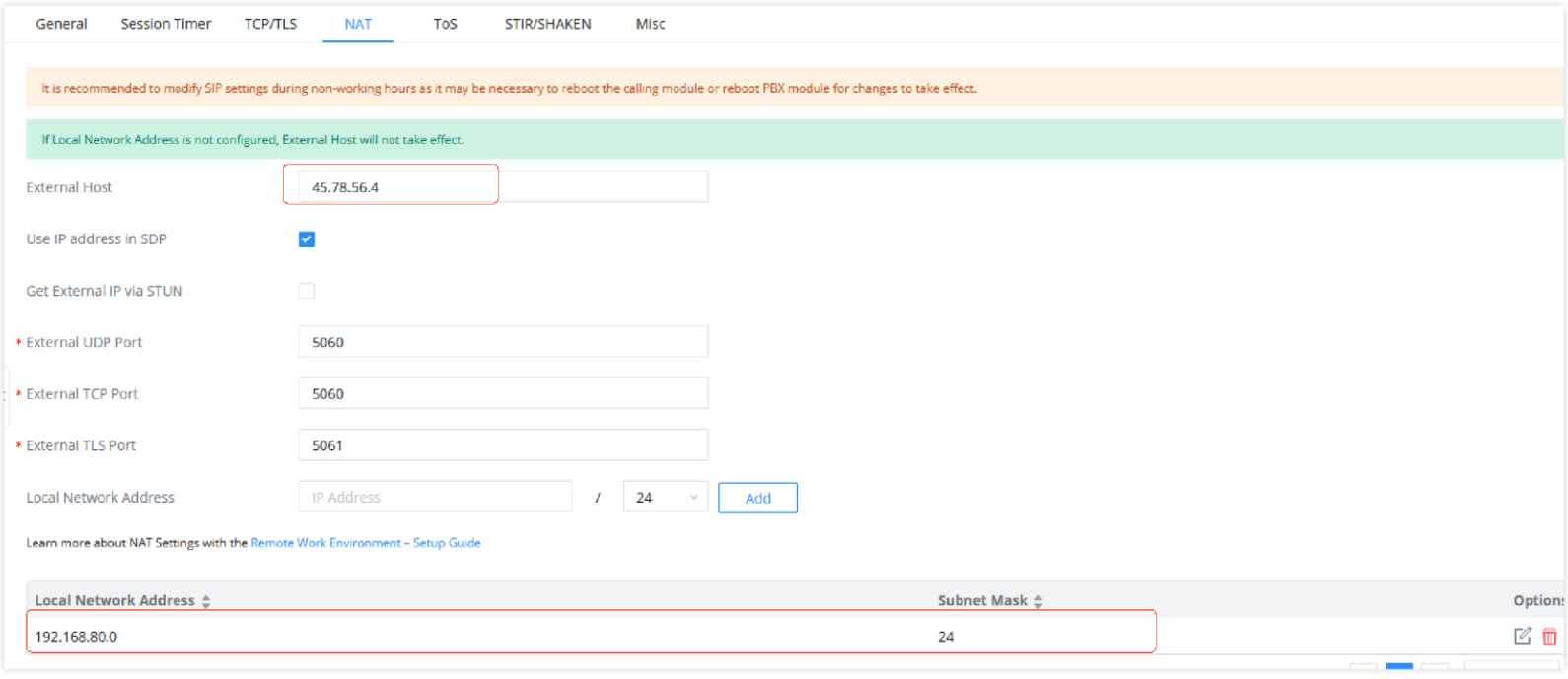
2. Add port forwarding rules for RTP:



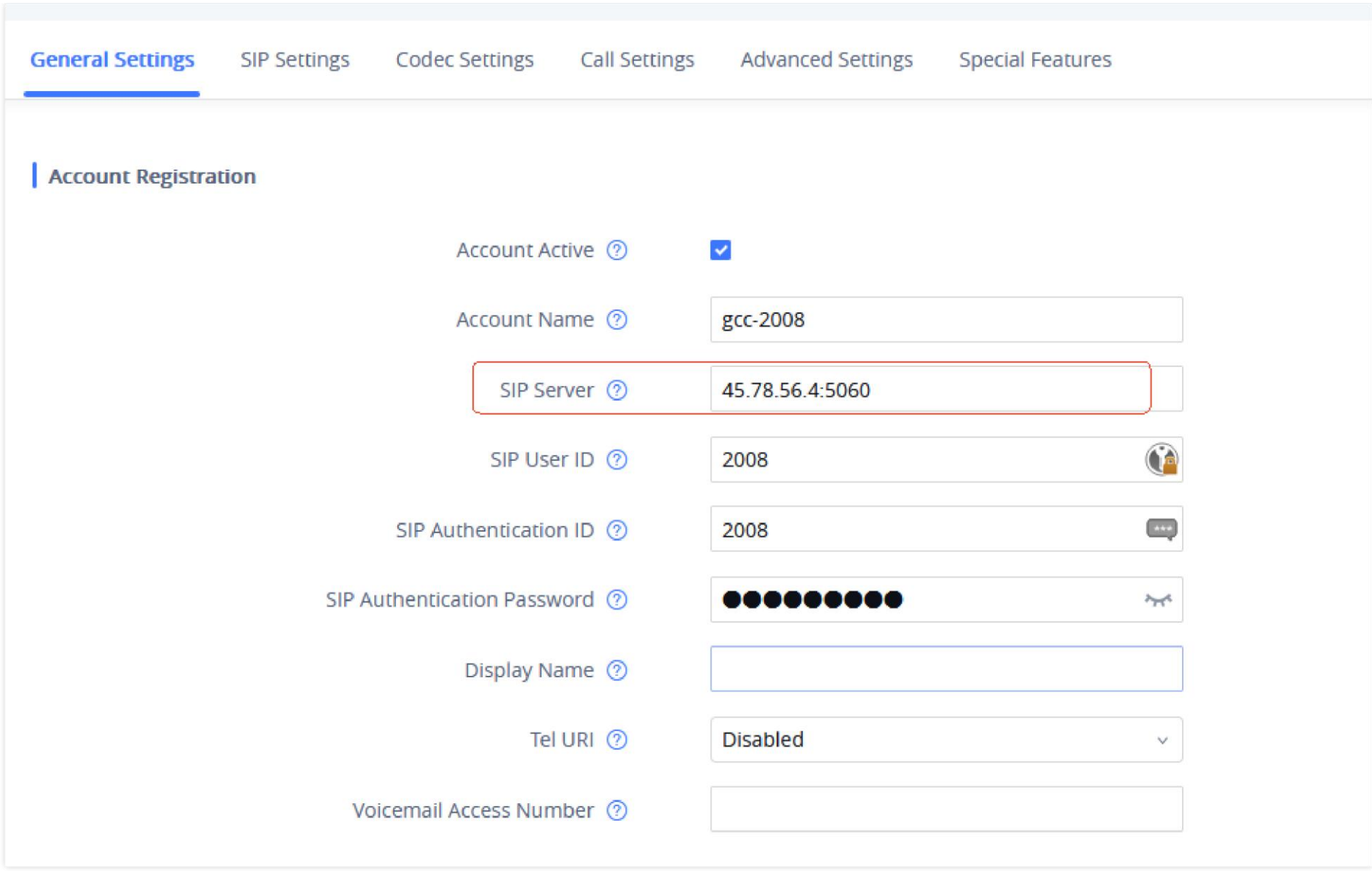
3. GCC2 configures port forwarding rules, similar to GCC1 configuration:



Enter the GCC1 (VRRP master, HA role Active) PBX component, **PBX Settings → SIP Settings → NAT** page, and configure the external address and local network address:



The phones on the same network segment as the WAN port can register and call through the GCC WAN VRRP virtual IP address. The following is the configuration of registration information using the GXV3370 phone as an example:

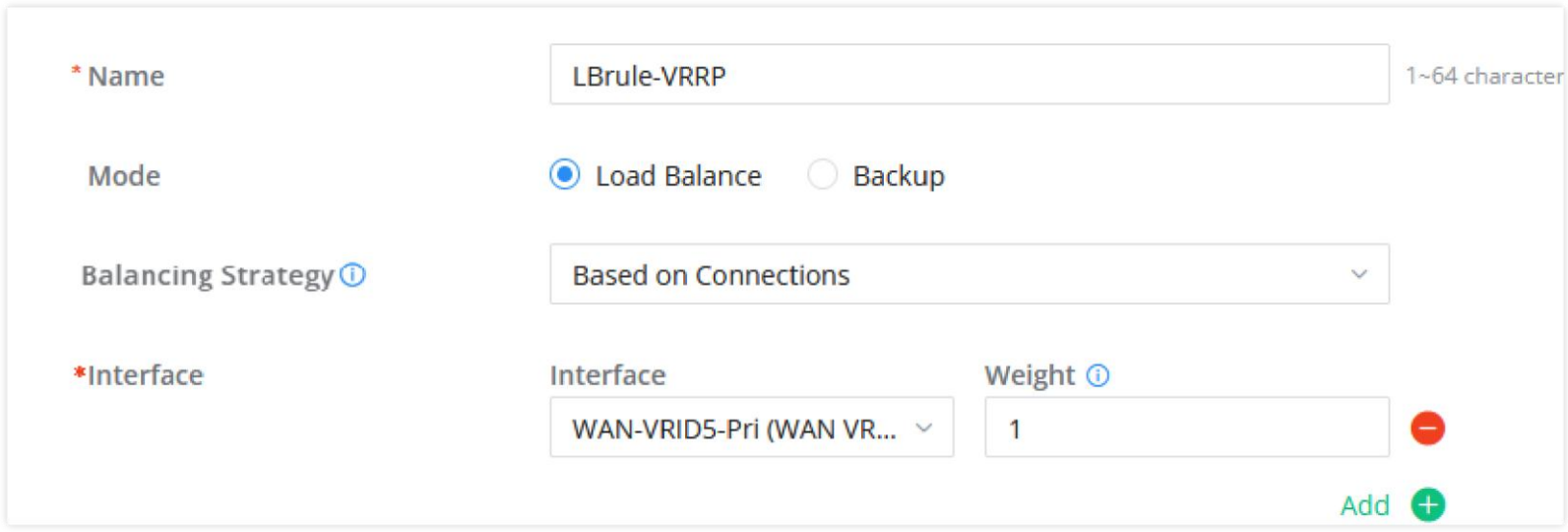


WAN Side Terminal Registration (GXV3370 as an example)

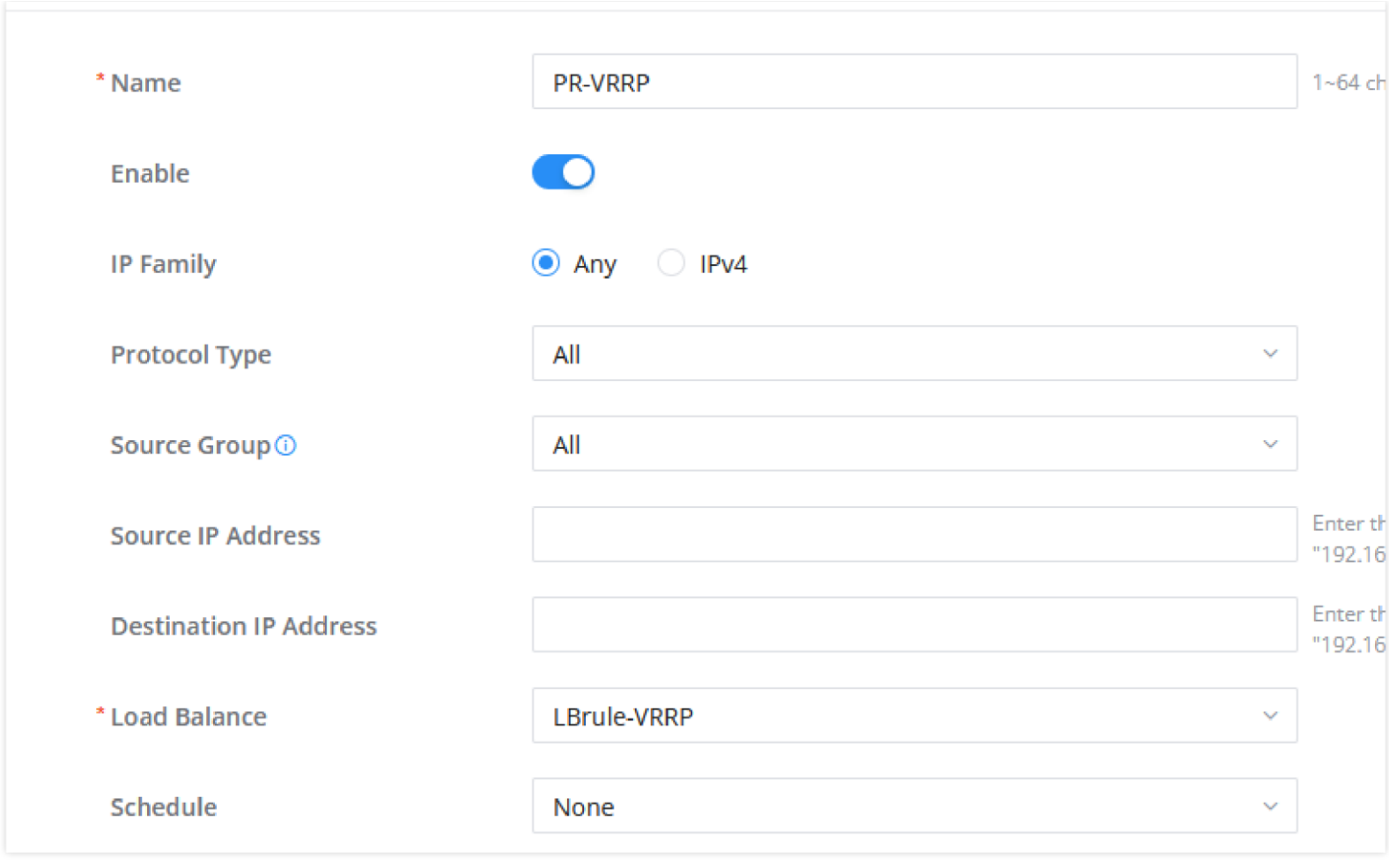
After registration is complete, users can make calls.

If the cross-segment terminal registers/calls through the WAN VRRP virtual IP address, policy routing configuration is also required.

GCC1 configures policy routing, and all packets sent by PBX go out from WAN VRRP:



GCC – Policy Routing – Load Balance Rule



GCC – Policy Routing – Add Policy Route

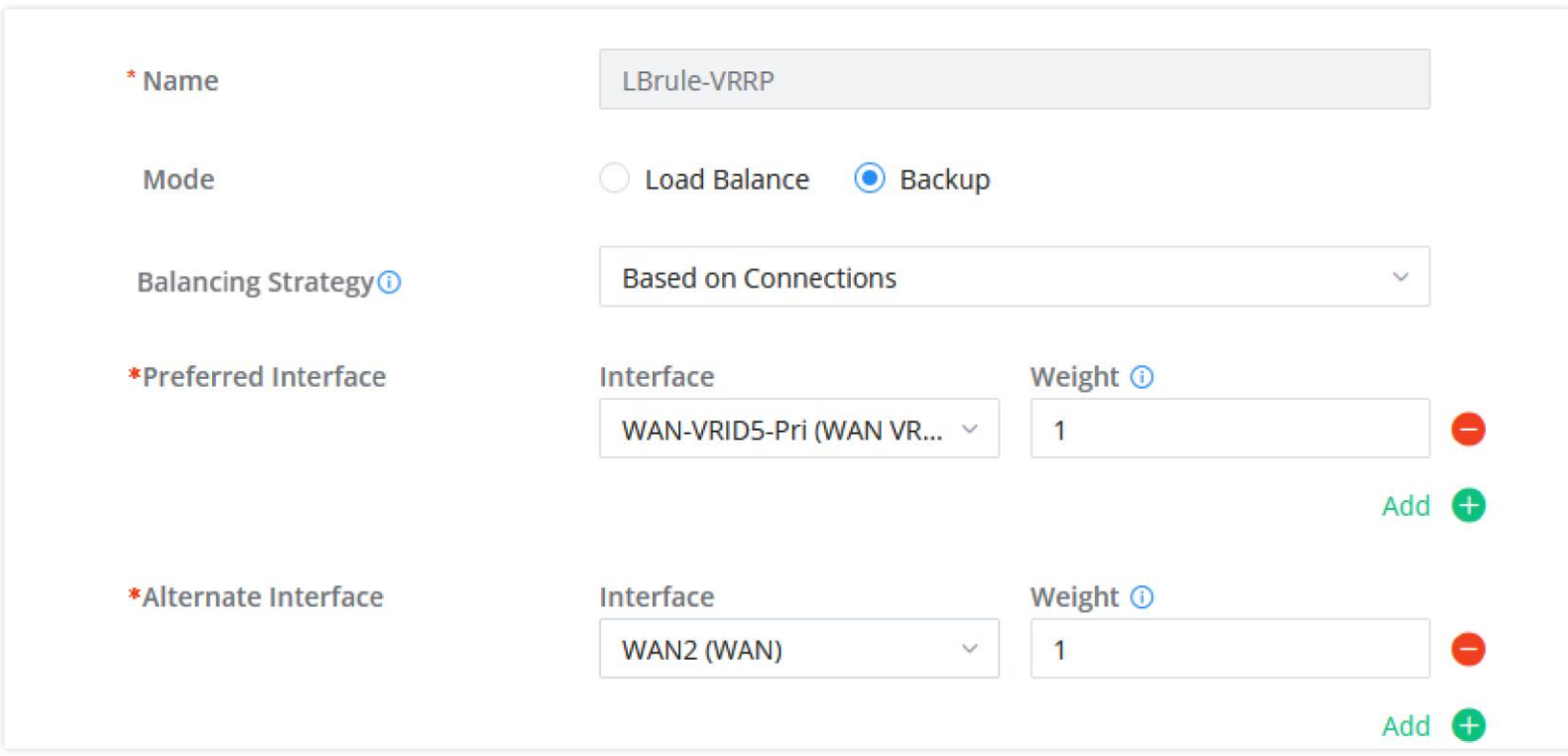
GCC2 configuration is similar.

For more details, refer to the GCC6000 – VRRP User Guide.

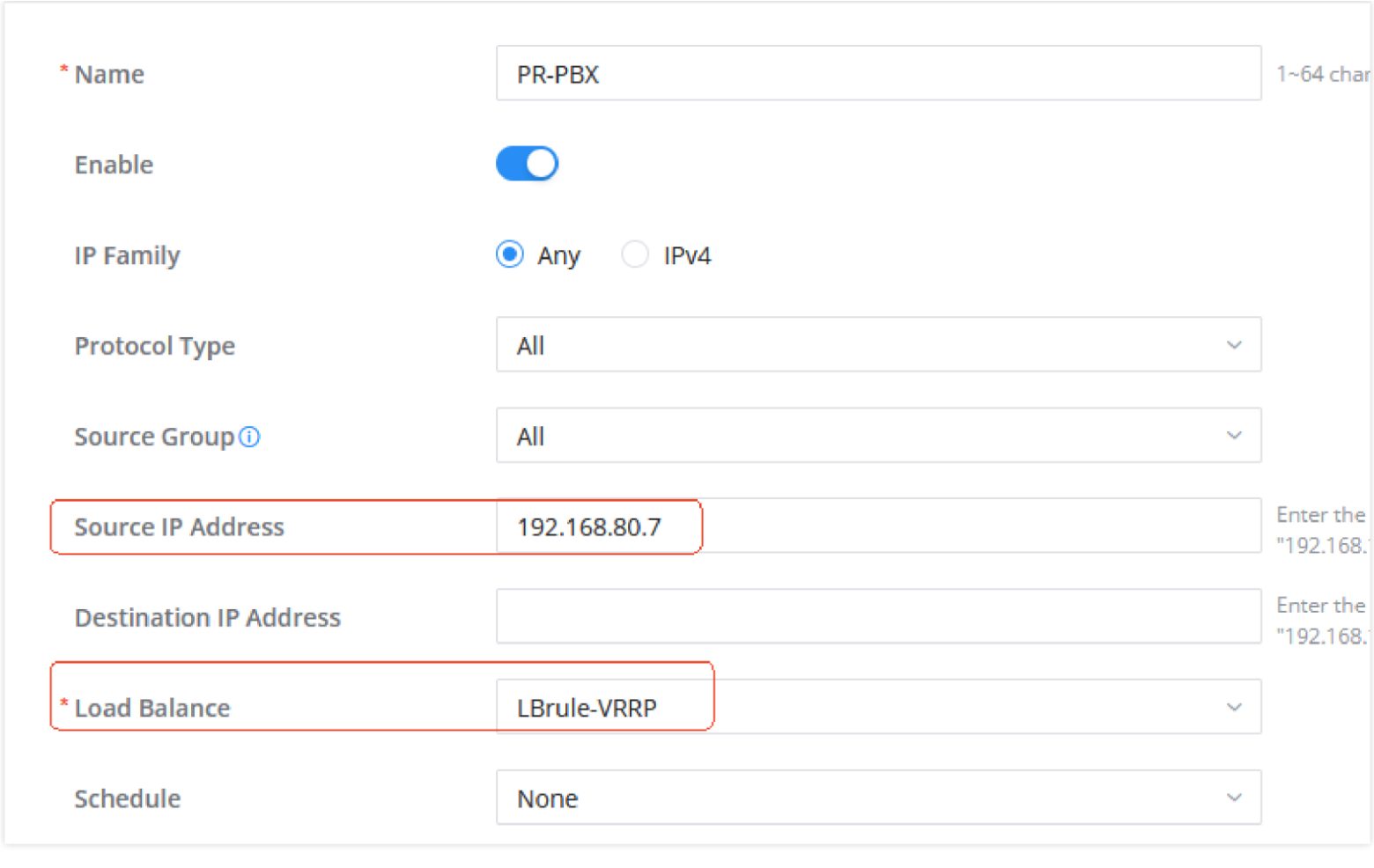
Notice:

When GCC WAN VRRP is in the backup role, WAN VRRP does not work. Therefore, when configuring policy routing, you need to pay attention to the fact that when **all traffic is configured to go through WAN VRRP**, you need to configure a **backup interface WAN port** to ensure that when WAN VRRP is in the backup role, traffic can go out through the WAN port. Note that **both GCCs** need to be configured.

Configuration example:



GCC – Policy Routing – Load Balance Rule (Example)



GCC – Policy Routing – Add Policy Route (Example)

HA ROLE SWITCHING

Depends on the VRRP role of the deployed interface in the same network segment as the PBX. When the VRRP role switches, the HA role switches accordingly.

HA DEVICE FAILURE, NEW DEVICE REPLACEMENT PROCESS

After a single machine has been used for a period of time, users can set up a dual machine. To avoid PBX data loss caused by the active machine being snatched away, you need to increase the priority of the currently working device before setting up the dual machine.

Here below are the steps to follow to replace a failed device in HA Dual-Node scenario, with or without UCMRC package:

HA Dual-Node without UCMRC Package Scenario

When two GCC devices that do not use UCMRC form HA dual machines, if a device fails and needs to be replaced, the example steps are as follows:

A and B have formed a HA dual-machine environment. When B fails (such as hardware failure), C needs to replace B. Before the replacement, it is ensured that the PBX version and license of C are consistent with those of A.

Device A is in Active state, and device B is in Standby state, regardless of the site types of the two:

1. Disconnect the power supply of device B.
2. Modify the VRRP priority of device A and set it to the highest priority.
3. Modify the HA parameters of device A, change the peer MAC address from B to the MAC address of device C, save the settings, and restart.
4. After A restarts, confirm that A is in an Active state and connect the physical lines to device C, including the WAN port cable and LAN port cable.
5. After C is powered on, perform basic network settings. The parameters of the network settings are the same as those of B, including the WAN port IP and VLAN port IP/gateway address/DHCP service configuration; configure VRRP, and note that its priority should be lower than that of device A. After the configuration is completed, confirm that the VRRP of device A is the active role and device C is the standby role.
6. Check the storage devices connected to device C to ensure that the type and number of storage devices connected to the two devices are consistent.

7. Check whether Cloud IM is turned on on C’s device. If it is turned on, turn off Cloud IM on C to ensure that C replaces B without the Cloud IM service.
8. Enable C and configure HA parameters. The configuration is the same as B. After the configuration is completed, save and restart. Note that C must be configured with the same site type as B.
9. After C restarts, check the HA status. The display shows that both devices are in HA dual-machine status, with A as the Active role and C as the Standby role.

HA Dual-Node with UCMRC Package Scenario

When two devices purchase the UCMRC package with HA service on GDMS and form HA dual machines, if a device fails and needs to be replaced, the sample steps are as follows:

A and B have formed a HA dual-machine environment. When B fails (such as hardware failure), C needs to replace B:

Scenario 1: Site A is Primary and in Active state. Site B is Secondary and in Standby state.

1. Add device C to GDMS and purchase a UCMRC package with HA permissions for device C that has the same specifications as those of devices A and B.
2. Disconnect the power supply of device B.
3. Modify the VRRP priority of device A and set it to the highest priority.
4. Modify the HA parameters of device A, change the peer MAC address from B to the MAC address of device C, save the settings, and restart.
5. After A restarts, confirm that A is in an Active state and connect physical lines to device C, including the WAN port cable and LAN port cable.
6. After C is powered on, perform basic network settings. The parameters of the network settings are the same as those of B, including the WAN port IP and VLAN port IP/gateway address/DHCP service configuration; configure VRRP, and note that its priority should be lower than that of device A. After the configuration is completed, confirm that the VRRP of device A is the active role and device C is the standby role.
7. Check the storage devices connected to device C to ensure that the type and number of storage devices connected to the two devices are consistent.
8. Check whether Cloud IM is turned on on C’s device. If it is turned on, turn off Cloud IM on C to ensure that C replaces B without the Cloud IM service.
9. Enable and configure HA parameters on C. The configuration parameters are the same as those on B. After configuration is complete, save and restart. Note that C must be configured with the same site type as B.
10. After C restarts, check the HA status. The display shows that both devices are in HA dual-machine status, A is the Active role and C is the Standby role.

Scenario 2: Site A type is Secondary and in Active state. Site B type is Primary and in Standby state.

1. Delete the custom server address or domain name of device B through GDMS.
2. Add device C in GDMS and purchase a UCMRC package with HA permissions for device C with the same specifications as A and B. Configure C’s custom server address or domain name through GDMS. It must be the same as B’s previous custom server address or domain name and must be used by C.
3. Disconnect the power supply of device B.
4. Modify the VRRP priority of device A and set it to the highest priority.
5. Modify the HA parameters of device A, change the peer MAC address from B to the MAC address of device C, save the settings, and restart.
6. After A restarts, confirm that A is in an Active state and connect physical lines to device C, including the WAN port network cable and LAN port network cable.
7. After C is powered on, perform basic network settings. The parameters of the network settings are the same as those of B, including the WAN port IP and VLAN port IP/gateway address/DHCP service configuration; configure VRRP, and note that its priority should be lower than that of device A. After the configuration is completed, confirm that the VRRP of device A is the active role and device B is the standby role.

8. Check the storage devices connected to device C to ensure that the type and number of storage devices connected to the two devices are consistent.
9. Check whether Cloud IM is turned on on C's device. If it is turned on, turn off Cloud IM on C to ensure that C replaces B without the Cloud IM service.
10. C Enable and configure HA parameters. The configuration is the same as B. The site type device is Primary. After the configuration is completed, save and restart.
11. After C restarts, check the HA status. The display shows that both devices are in HA dual-machine status, A is the Active role and C is the Standby role.

REMOVING HA DUAL MACHINES

When the devices that make up the HA dual-machine need to release HA, directly log in to the HA Active device IP or PBX cluster IP, in **System Settings → HA → HA Settings**, uncheck the " HA Function Enable" button, turn off the HA function, save the configuration, restart the device, and verify the HA status after restarting to confirm that both PBX devices have turned off HA.

DUAL-MACHINE CLOUD IM SCENARIO

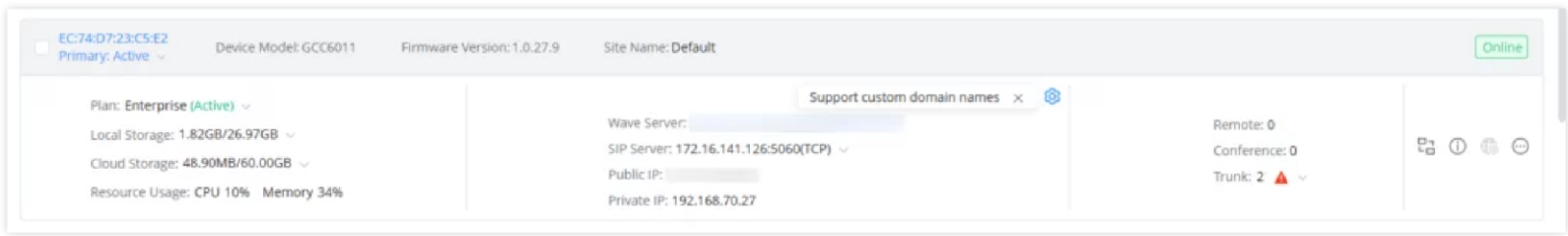
Please ensure that only one Cloud IM service is enabled on the two GCCs (PBXs) that form the HA dual-machine. When using the server address or domain name issued by GDMS, please ensure that both use the package with Cloud IM permissions.

When Cloud IM is enabled on the Active device A that forms the HA dual machine, the Standby device B will obtain the Cloud IM service along with the HA data backup. Cloud IM will provide services along with the Active device, and the MAC address of the bound device will change with the role switch, so when the active-standby switchover occurs, Cloud IM will not be affected.

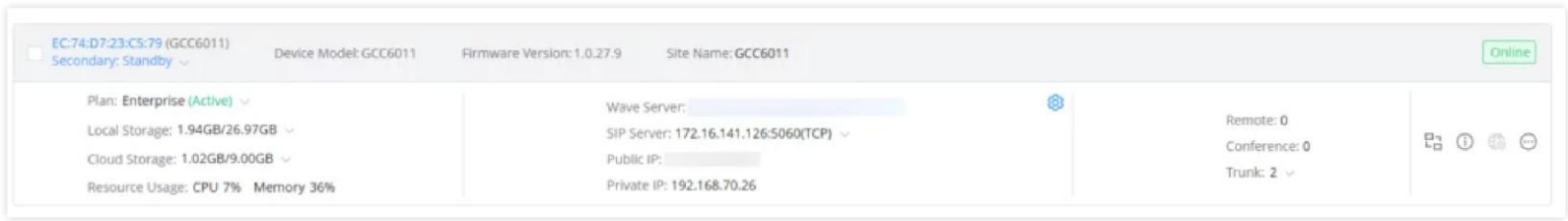
When device B fails, when device C without Cloud IM enabled replaces device B to form a dual-machine system with A, Cloud IM will still provide HA services for B and C, and no other configuration is required. If device C has Cloud IM enabled, you need to disable the original Cloud IM first to ensure that C replaces B without Cloud IM service. For more details about device replacement, refer to [HA DEVICE FAILURE, NEW DEVICE REPLACEMENT PROCESS].

DUAL-MACHINE UCMRC REMOTE ACCESS SCENARIO

Purchase a UCMRC package with HA permissions. After the HA package binding is successful, the GDMS page will display Primary (Host) type devices and Secondary (Spare) type devices:



Primary Active GCC



Secondary On-standby GCC

UCMRC Role Switching Process

Prerequisites:

1. HA permissions on GDMS.

2. The primary and backup packages are successfully sent and bound.

Business implementation:

1. The call service is completed by the interaction between GDMS and Active working state devices.
2. When the Active working state device A fails and causes a master-slave switchover, the Standby working state device B takes over the service and enters the Active working state. Device B sends a master-slave switch command to GDMS, informing it that subsequent service interactions will be completed by device B and GDMS.

UCMRC Role Status

It should be noted that when the two machines purchase the UCMRC package with HA permissions, the role status will be actively reported to GDMS by GCC (PBX), and there is no need to manually specify it on GDMS.

At the same time, for GDMS, different remote operations can still be performed on the two PBXs, but some operations on the standby machine will fail and be reset due to HA backup. The service is provided by the Active role PBX, but GDMS always sends the Wave login domain name according to the Primary device.

SERVICE STATUS

Active/Standby Working Status

The GCC (PBX) device completes the HA configuration, the IP for providing services to the outside world is the cluster IP. Full backup data synchronization will be performed during the initial system startup phase, that is, the Standby role PBX requests full data from the current Active role PBX. The Standby role PBX is ready to take over the Active role PBX business at any time, and changes to the Standby role PBX business data will also be restricted. Daily data on the Active role PBX will be synchronized to the Standby role PBX in real-time. When the Active role device fails, including hardware failure and network failure, the standby VRRP is promoted to the master, and the PBX Standby role is upgraded to the Active role. The new Active device immediately takes over the business to ensure that the business is not interrupted, and the original Active role PBX will restart and become the Standby role. At the same time, some calls will be automatically restored.

PBX Administrator Login Method

- Access the PBX component by logging into the GCC page.

It is relatively simple to access the PBX component by logging in to GCC. This is the recommended way to access the PBX.

- Log in using the PBX independent page

The cluster IP becomes a floating IP for providing external services. To perform regular service configuration on the PBX page, you only need to log in and access it according to the cluster IP address format. Regardless of how the roles are switched, the floating IP remains unchanged and is always bound to the PBX with the Active role that currently provides services.

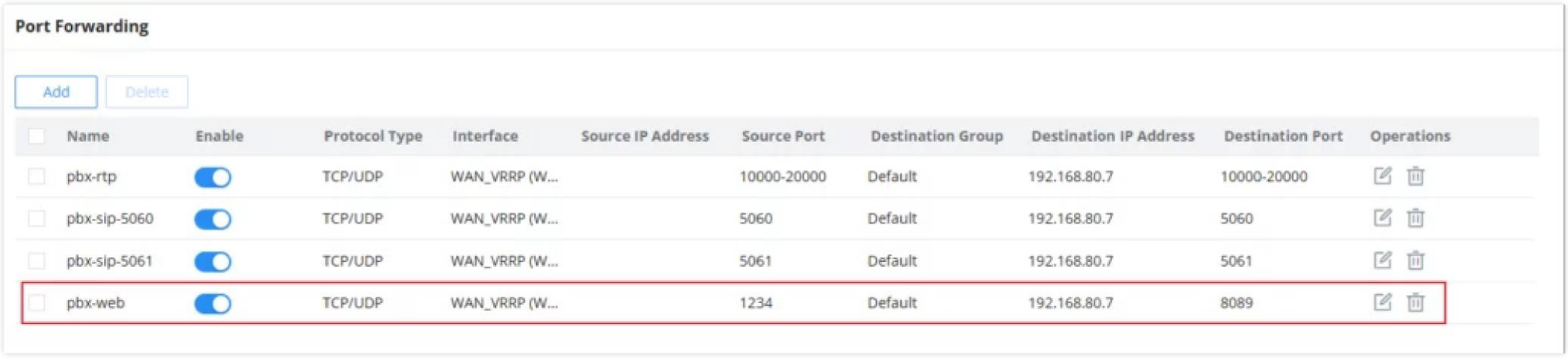
Intranet PCs can log in to the current Active PBX via ***https://cluster IP:8089*** or ***https://current Active PBX IP:8089***. In particular, after logging in to the Standby PBX via ***https://current Standby PBX IP:8089***, the business data configuration will also be restricted.

It should be noted that after forming HA, the administrator identity of the Active device will also be synchronized to the Standby device and overwrite the administrator information of the Standby device. Therefore, whether logging in through the floating IP or logging in to the IP addresses of the two PBX devices, use the administrator identity and account of the Active role to log in.

Since the top-level configuration of GCC is not synchronized between the master and the slave, it is recommended that the same user and password be configured on the master and slave GCCs before setting up HA.

The external PC can log in by configuring port forwarding rules:

For example, configure port forwarding rules for the WAN VRRP interface on both the active and standby devices to enable the WAN-side PC to log in to the Active PBX by accessing the WAN VRRP IP+port regardless of how the VRRP & HA roles are switched:



Port Forwarding

CALL HOT STANDBY

When a device in the Active role fails (the VRRP role switches and the HA role switches accordingly), if there is an ongoing call in the system, the call voice will only be briefly paused during the Standby and Active role switching process, and the call can be restored within a few seconds.

Note

1. Currently, call resumption based on UDP protocol is supported, but call resumption based on TCP protocol is not supported.
2. Currently, the service types that support call hot standby are point-to-point audio calls and audio conferences. Call recovery under various PBX supplementary services, such as Ring Group, Call Queue, and other call services, is not supported.

DATA SYNCHRONIZATION

The HA dual-node scenario provides a complete data synchronization mechanism, including the following points:

1. Full backup data synchronization at the initial startup of the system, that is, the full data requested by the Standby PBX to the current Active PBX. The Active PBX will also synchronize the configuration actions to the Standby PBX in real-time during each service configuration to achieve consistency between the two sides. The data that is triggered to be synchronized to the Standby PBX in real time is not limited to configuration data but also includes adding extensions, voice messages, CDRs, local recording files, etc.
2. Perform full backup synchronization at 3:00 a.m. to ensure that the data between the two machines is always consistent. During full backup, the HA full backup status will display “backup in progress” in real-time, and “idle” will be displayed at other times.

BACKUP PACKAGE EXPORT AND RESTORATION

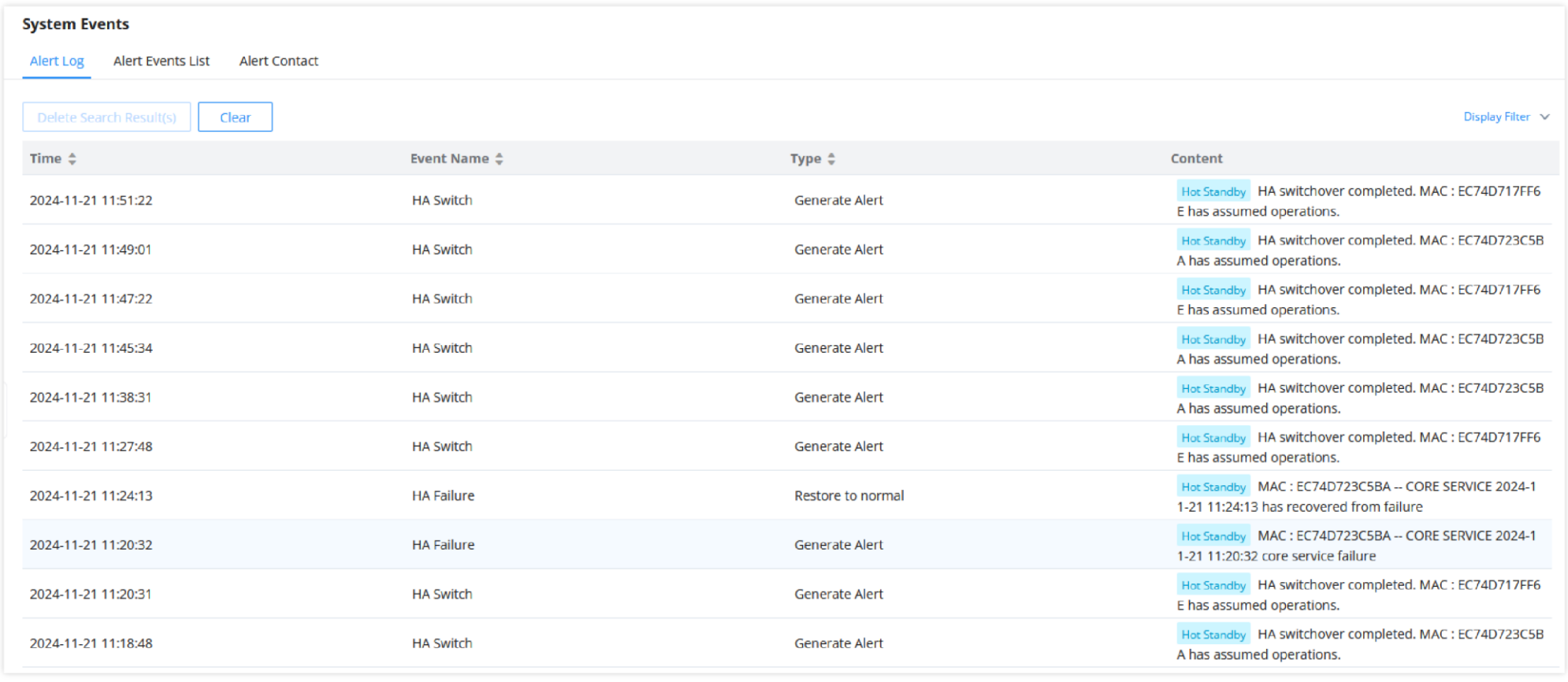
The backup package of PBX components can be backed up to GDMS or restored from GDMS cloud storage on the PBX component **Maintenance → Backup** page. Backup and restoration can also be performed on the top-level **Maintenance → Backup&Restore** page.

The running HA dual machine:

1. If you want to restore the backup package of a device with HA enabled, you only need to restore the backup package on the Active device. After the restoration, both PBXs will automatically restart. After the Active restart is complete, the configuration and data will be fully backed up and synchronized to the Standby device.
2. If you restore the backup package of a device that does not have HA enabled, you need to first disable HA on the Active and then perform the restore. After the restore is complete, re-establish the HA dual machine.

MAINTENANCE INTERFACE

HA dual-machine applications, we can check whether there are any HA-related alarm events from **System Management → System Events**, to directly know whether there are any system abnormalities:



View the relevant backup logs and switchover logs through **System Settings → HA → HA Log**. The HA log effectively records the execution results of the past full backup actions and the historical records of triggering the active/standby switchover:

HA.

HA Settings | HA Status | HA Log

HA Backup Log | HA Failover Log | External Data Sync Log

Clean

Hot Standby [2024-11-22 09:42:41] HA backup success!!

Hot Standby [2024-11-22 03:00:56] HA backup success!!

Hot Standby [2024-11-21 2.0:21:11] HA backup success!!

Hot Standby [2024-11-21 2.0:17:49] HA backup success!!

Hot Standby [2024-11-2118:07:33] HA backup success!!

Hot Standby [2024-11-21 17:47:29] HA backup success!!

Hot Standby [2024-11-21 17:30:37] HA backup success!!

Hot Standby [2024-11-21 17:13:07] HA backup success!!

Hot Standby [2024-11-21 17:03:51] HA backup success!!

Hot Standby [2024-11-21 17:01:SB] HA backup success!!

Hot Standby [2024-11-21 16:53:42] HA backup success!!

Hot Standby [2024-11-21 16:49:09] HA backup success!!

Hot Standby [2024-11-2116:46:16] HA backup success!!

Hot Standby [2024-11-21 16:26:56] HA backup success!!

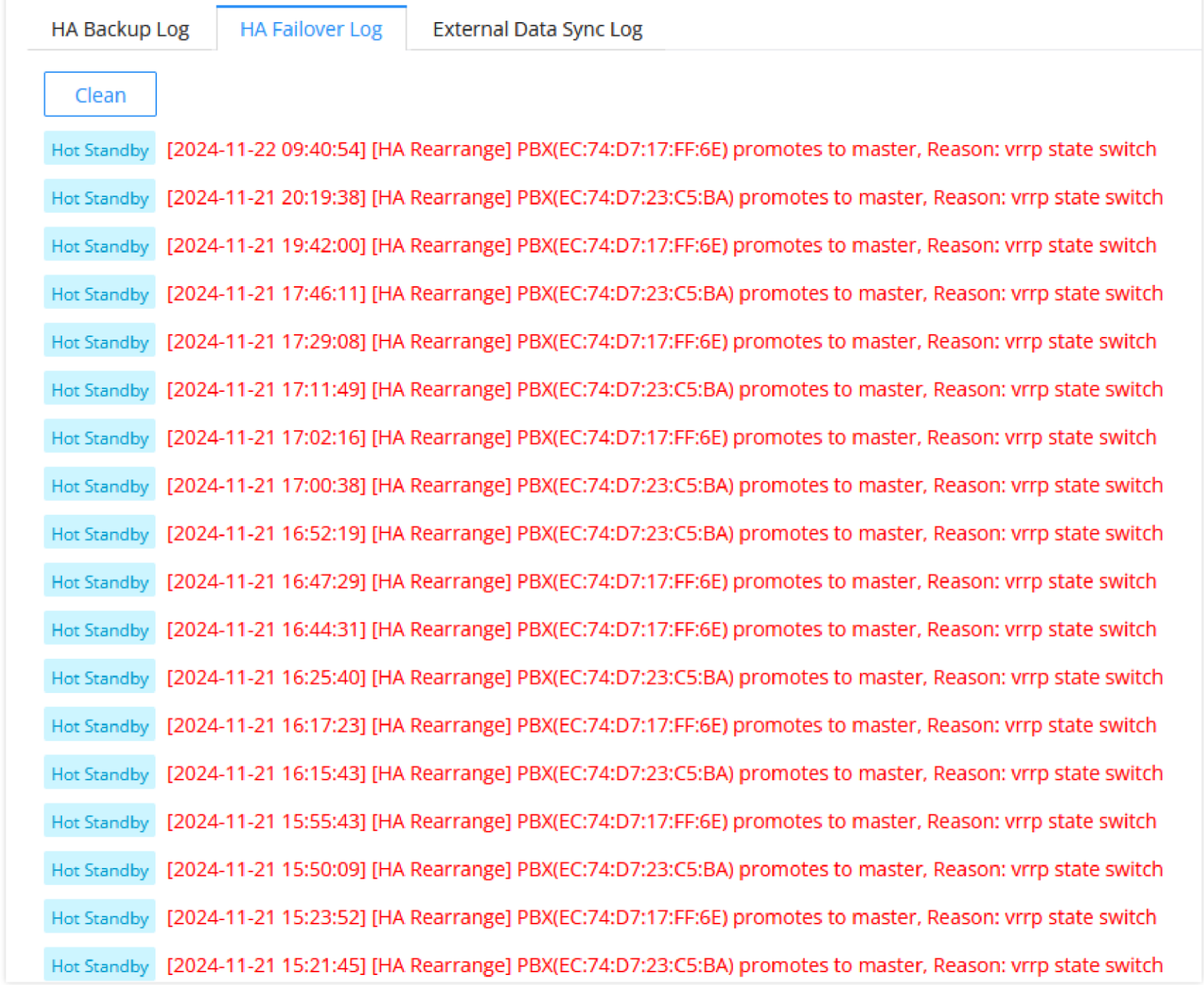
Hot Standby [2024-11-21 16:22:47] HA backup success!!

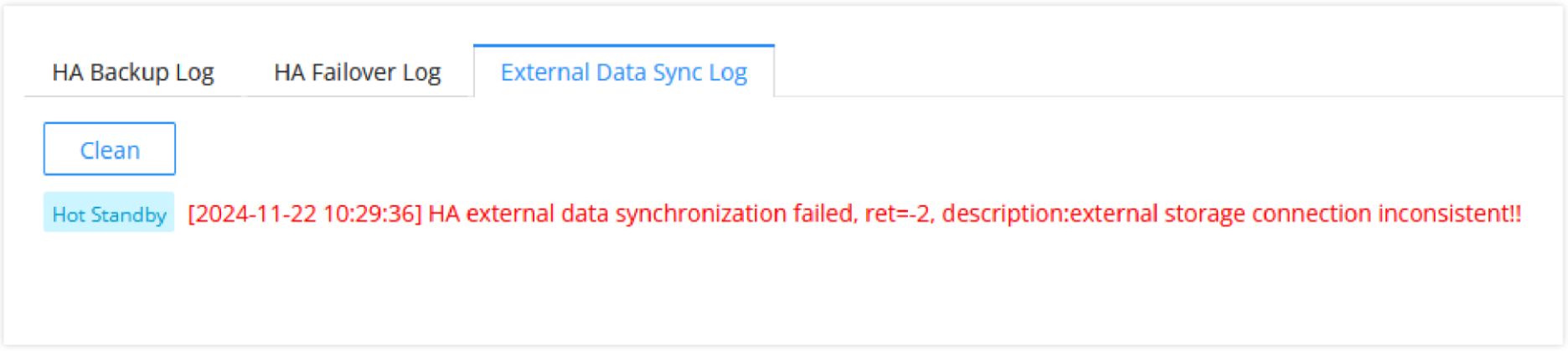
Hot Standby [2024-11-21 16:18:42] HA backup success!!

Hot Standby [2024-11-2116:f?:06] HA backup success!!

Hot Standby [2024-11-2116:06:49] HA backup success!!

Hot Standby [2024-11-21 15:57:14] HA backup success!!





Since the PBX HA master/slave roles are consistent with the VRRP master/slave roles, when the VRRP master/slave switches, the HA switches accordingly. In the HA switchover log, only the switchover record can be seen, but the specific switchover reason needs to be checked on the network component, **VRRP → Log** page: