FortiVoice™ 200D/200D-T/2000E-T2 High Availability Technical Note

FortiVoice 200D/200D-T/2000E-T2 High Availability Technical Note

February 21, 2018

2nd Edition

Technical Documentation	docs.fortinet.com
Knowledge Base	kb.fortinet.com
Customer Service & Support	support.fortinet.com
Training Services	training.fortinet.com
FortiGuard	fortiguard.com
Document Feedback	techdocs@fortinet.com

High Availability Failover Examples

You can configure the FortiVoice unit to act as a high availability (HA) member in order to increase availability.

For information on configuring and using FortiVoice HA, see the *FortiVoice Phone System Administration Guide.*

This technical note describes basic FortiVoice active-passive HA failover scenarios.

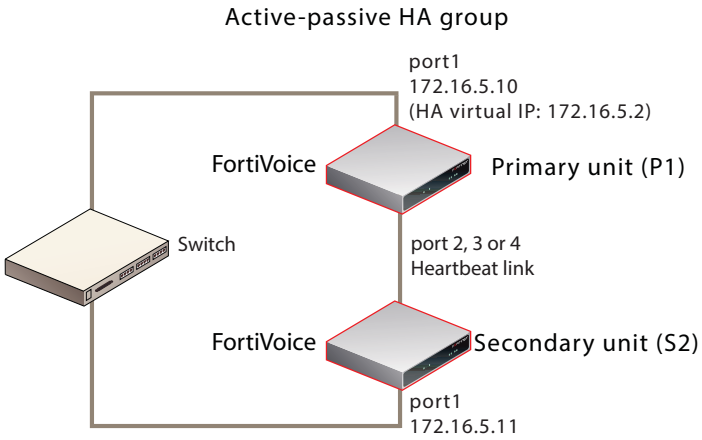
This technical note assumes that you use the FortiVoice Phone System 5.3.0 or later software.

To simplify the descriptions of the HA failover scenarios, the following abbreviations are used:

- P1 is the configured primary unit.
- S2 is the configured secondary unit.

For each scenario, refer to the HA group shown in Figure 1.

Figure 1: Example active-passive HA group



The following HA failover scenarios are described:

- Failover scenario 1: Temporary failure of the primary unit
- Failover scenario 2: System reboot or reload of the primary unit
- Failover scenario 3: System reboot or reload of the secondary unit
- Failover scenario 4: System shutdown of the secondary unit
- Failover scenario 5: Primary heartbeat link fails
- Failover scenario 6: Network connection between primary and secondary units fails (remote service monitoring detects a failure)

Failover scenario 1: Temporary failure of the primary unit

In this scenario, the primary unit (P1) fails because of a software failure or a recoverable hardware failure (in this example, the P1 power cable is unplugged). HA logging and alert email are configured for the HA group.

When the secondary unit (S2) detects that P1 has failed, S2 becomes the new primary unit and continues processing phone calls.

There is no data loss when failover happens although active calls are disconnected and line appearance and extension appearance take time to restore. Call data consists of the FortiVoice

call detailed records, recorded calls, voicemail, call directories, fax, and voice prompts. The user web portal is not affected.

Here is what happens during this process:

1. The FortiVoice HA group is operating normally.
2. The power is accidentally disconnected from P1.
3. S2's heartbeat test detects that P1 has failed.

   How soon this happens depends on the HA daemon configuration of S2.
4. The effective HA operating mode of S2 changes to *master*.
5. S2 sends an alert email similar to the following, indicating that S2 has determined that P1 has failed and that S2 is switching its effective HA operating mode to *master*.

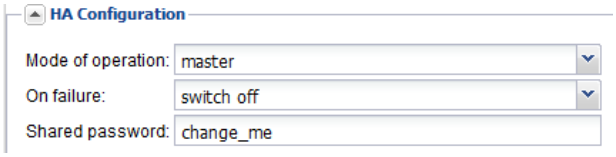
   This is the HA machine at 172.16.5.11.

   The following event has occurred
   'MASTER heartbeat disappeared'
   The state changed from 'SLAVE' to 'MASTER'
6. S2 records event log messages (among others) indicating that S2 has determined that P1 has failed and that S2 is switching its effective HA operating mode to *master*.

Recovering from temporary failure of the primary unit

After P1 recovers from the hardware failure, what happens next to the HA group depends on P1's HA *On failure* settings under *System* > *High Availability* > *Configuration*.

Figure 2: HA On Failure settings



- *switch off*

  P1 will not process calls or join the HA group until you manually select the effective HA operating mode.
- *wait for recovery then restore original role*

  On recovery, P1's effective HA operating mode resumes its configured master role. This also means that S2 needs to give back the master role to P1. This behavior may be useful if the cause of failure is temporary and rare, but may cause problems if the cause of failure is permanent or persistent.

  In the case, the S2 will send out another alert email similar to the following:

  This is the HA machine at 172.16.5.11.

  The following event has occurred
  'SLAVE asks us to switch roles (recovery after a restart)
  The state changed from 'MASTER' to 'SLAVE'

  After recovery, P1 also sends out an alert email similar to the following:

  This is the HA machine at 172.16.5.10.

The following critical event was detected
The system was shutdown!

- *wait for recovery then restore slave role*

  On recovery, P1's effective HA operating mode becomes *slave*, and S2 continues to assume the *master* role. P1 then synchronizes with the current master unit, S2.

Failover scenario 2: System reboot or reload of the primary unit

If you need to reboot or reload (not shut down) P1 for any reason, such as a firmware upgrade or a process restart, by using the CLI commands `execute reboot` or `execute reload`, or by clicking the *Restart* button under *Status* > *Dashboard* > *System Command* on the GUI:

- P1 will send a holdoff command to S2 so that S2 will not take over the master role during P1's reboot.
- P1 will also send out an alert email similar to the following:

  This is the HA machine at 172.16.5.10.

  The following critical event on system (FOV-1K0000000001 [172.16.5.10]) version v5.3-build0362 was detected
  The system is rebooting!
- S2 will hold off checking the services and heartbeat with P1. Note that S2 will only hold off for about 5 minutes. In case P1 never boots up, S2 will take over the master role.
- S2 will send out an alert email, indicating that S2 received the holdoff command from P1.

  This is the HA machine at 172.16.5.11.

  The following event has occurred
  'peer rebooting'
  The state changed from 'SLAVE' to 'HOLD_OFF'

After P1 is up again:

- P1 will send another command to S2 and ask S2 to change its state from holdoff to slave and resume monitoring P1's services and heartbeat.
- S2 will send out an alert email, indicating that S2 received instruction commands from P1.

  This is the HA machine at 172.16.5.11.

  The following event has occurred
  'peer command appeared'
  The state changed from 'HOLD_OFF' to 'SLAVE'
- S2 logs the event in the HA logs.

Failover scenario 3: System reboot or reload of the secondary unit

If you need to reboot or reload (not shut down) S2 for any reason, such as a firmware upgrade or a process restart, by using the CLI commands `execute reboot` or `execute reload`, or by clicking the *Restart* button under *Monitor* > *System Status* > *Status* on the GUI, the behavior of P1 and S2 is as follows:

- P1 will send out an alert email similar to the following, informing the administrator of the heartbeat loss with S2.

  This is the HA machine at 172.16.5.10.

The following event has occurred
'ha: SLAVE heartbeat disappeared'

- S2 will send out an alert email similar to the following:

  This is the HA machine at 172.16.5.11.

  The following critical event on system (FOV-1K0000000002 [192.168.3.210]) version v5.3-build0362 was detected
  The system is rebooting!
- P1 will also log this event in the HA logs.

Failover scenario 4: System shutdown of the secondary unit

If you shut down S2:

- P1 will send out an alert email similar to the following, informing the administrator of the heartbeat loss with S2.

  This is the HA machine at 172.16.5.10.

  The following event has occurred

  SLAVE heartbeat disappeared
- P1 will log this event in the HA logs.

Failover scenario 5: Primary heartbeat link fails

If the primary heartbeat link fails, such as when the cable becomes accidentally disconnected, and if you have not configured a secondary heartbeat link, the FortiVoice units in the HA group cannot verify that other units are operating and assume that the other has failed. As a result, the secondary unit (S2) changes to operating as a primary unit, and ***both*** FortiVoice units are acting as primary units.

Two primary units connected to the same network may cause address conflicts on your network. Additionally, because the heartbeat link is interrupted, the FortiVoice units in the HA group cannot synchronize configuration changes or voice data changes.

Even after reconnecting the heartbeat link, both units will continue operating as primary units. To return the HA group to normal operation, you must connect to the web-based manager of S2 to restore its effective HA operating mode to *slave* (secondary unit).

1. The FortiVoice HA group is operating normally.
2. The heartbeat link Ethernet cable is accidently disconnected.
3. S2's HA heartbeat test detects that the primary unit has failed.

   How soon this happens depends on the HA daemon configuration of S2.
4. The effective HA operating mode of S2 changes to *master*.
5. S2 sends an alert email similar to the following, indicating that S2 has determined that P1 has failed and that S2 is switching its effective HA operating mode to *master*.

   This is the HA machine at 172.16.5.11.

   The following event has occurred
   'MASTER heartbeat disappeared'
   The state changed from 'SLAVE' to 'MASTER'
6. S2 records event log messages (among others) indicating that S2 has determined that P1 has failed and that S2 is switching its effective HA operating mode to *master*.

To prevent this scenario from happening, more than one heartbeat links should be configured, so that the slave can still communicate to the master in case the primary heartbeat link is down.

Recovering from a heartbeat link failure

Because the hardware failure is not permanent (that is, the failure of the heartbeat link was caused by a disconnected cable, not a failed port on one of the FortiVoice units), you may want to return both FortiVoice units to operating in their configured modes when rejoining the failed primary unit to the HA group.

To return to normal operation after the heartbeat link fails

1. Reconnect the primary heartbeat interface by reconnecting the heartbeat link Ethernet cable.

   Even though the effective HA operating mode of S2 is *master*, S2 continues to attempt to find the other primary unit. When the heartbeat link is reconnected, S2 finds P1 and determines that P1 is also operating as a primary unit. So S2 switches back to Slave Mode.
2. S2 sends an alert email similar to the following, indicating that S2 has stopped operating as the primary unit.

   This is the HA machine at 172.16.5.10

   The following event has occurred:

   2 devices with same mode, fixing

   The state changed from 'MASTER' to 'SLAVE'
3. S2 records event log messages (among others) indicating that S2 is switching to *slave* mode.

Failover scenario 6: Network connection between primary and secondary units fails (remote service monitoring detects a failure)

Depending on your network configuration, the network connection between the primary and secondary units can fail for a number of reasons. In the network configuration shown in Figure 1 on page 1, the connection between port1 of primary unit (P1) and port1 of the secondary unit (S2) can fail if a network cable is disconnected or if the switch between P1 and S2 fails.

A more complex network configuration could include a number of network devices between the primary and secondary unit's non-heartbeat network interfaces. In any configuration, remote service monitoring can only detect a communication failure. Remote service monitoring cannot determine where the failure occurred or the reason for the failure.

In this scenario, remote service monitoring has been configured to make sure that S2 can connect to P1. The *On failure* setting located in the HA main configuration section is *wait for recovery then restore slave role*.

The failure occurs when power to the switch that connects the P1 and S2 port1 interfaces is disconnected. Remote service monitoring detects the failure of the network connection between the primary and secondary units. Because of the *On failure* setting, P1 changes its effective HA operating mode to *failed*.

When the failure is corrected, P1 detects the correction because while operating in failed mode P1 has been attempting to connect to S2 using the port1 interface. When P1 can connect to S2, the effective HA operating mode of P1 changes to *slave* and the voice data on P1 will be synchronized to S2. S2 can now deliver the calls. The HA group continues to operate in this manner until an administrator resets the effective HA modes of operation of the FortiVoice units.

1. The FortiVoice HA group is operating normally.
2. The power cable for the switch between P1 and S2 is accidently disconnected.

3. S2's remote service monitoring cannot connect to the primary unit.

   How soon this happens depends on the remote service monitoring configuration of S2.
4. Through the HA heartbeat link, S2 signals P1 to stop operating as the primary unit.
5. The effective HA operating mode of P1 changes to *failed*.
6. The effective HA operating mode of S2 changes to *master*.
7. S2 sends an alert email similar to the following, indicating that S2 has determined that P1 has failed and that S2 is switching its effective HA operating mode to *master*.

   This is the HA machine at 172.16.5.11.

   The following event has occurred
   remote problem detected (SIP_UDP=FAILED;HTTP=DISABLED), telling MASTER to fail
   The state changed from 'SLAVE' to 'MASTER'
8. S2 logs the event (among others) indicating that S2 has determined that P1 has failed and that S2 is switching its effective HA operating mode to *master*.
9. P1 sends an alert email similar to the following, indicating that P1 has stopped operating in HA mode.

   This is the HA machine at 172.16.5.10.

   The following event has occurred
   'SLAVE asks us to switch roles (user requested takeover)'

   The state changed from 'MASTER' to 'FAILED'
10. P1 records the log messages (among others) indicating that P1 is switching to *Failed* mode.

Recovering from a network connection failure

Because the network connection failure was not caused by failure of either FortiVoice unit, you may want to return both FortiVoice units to operating in their configured modes when rejoining the failed primary unit to the HA group.

To return to normal operation after the heartbeat link fails

1. Reconnect power to the switch.

   Because the effective HA operating mode of P1 is *failed*, P1 is using remote service monitoring to attempt to connect to S2 through the switch.
2. When the switch resumes operating, P1 successfully connects to S2.

   P1 has determined the S2 can connect to the network and process calls.
3. The effective HA operating mode of P1 switches to *slave*.
4. P1 logs the event.
5. P1 sends an alert email similar to the following, indicating that P1 is switching its effective HA operating mode to *slave*.

   This is the HA machine at 172.16.5.10.

   The following event has occurred
   remote problem recovered

   The state changed from 'FAILED' to 'SLAVE'
6. Connect to the web-based manager of P1 and go to *System* > *High Availability* > *Status*.
7. Check for synchronization messages.

   Do not proceed to the next step until P1 has synchronized with S2.
8. Connect to the web-based manager of S2, go to *System* > *High Availability* > *Status* and select *click HERE to restore configured operating mode*.

9. Connect to the web-based manager of P1, go to *System* > *High Availability* > *Status* and select *click HERE to restore configured operating mode*.

   P1 should return to operating as the primary unit and S2 should return to operating as the secondary unit.

   P1 and S2 synchronize again. P1 can now process phone calls normally.