High Availability

Feature History for High Availability

This table provides release and related information for the features explained in this module.

These features are available in all the releases subsequent to the one they were introduced in, unless noted otherwise.

Table 1: Feature History for High Availability

Release	Feature	Feature Information
Cisco IOS XE Amsterdam 17.1.1s	Redundant Management Interface	The Redundancy Management Interface (RMI) is used as a secondary link between the active and standby controllers. This interface is the same as the Wireless Management Interface and the IP address on this interface is configured in the same subnet as the Wireless Management Interface.

Information About High Availability

High Availability (HA) allows you to reduce the downtime of wireless networks that occurs due to the failover of controllers. The HA Stateful Switch Over (SSO) capability on the controller allows AP to establish a CAPWAP tunnel with the active controller. The active controller shares a mirror copy of the AP and client database with the standby controller. The APs won’t go into the discovery state and clients don’t disconnect when the active controller fails. The standby controller takes over the network as the active controller. Only one CAPWAP tunnel is maintained between the APs and the controller that is in an active state.

HA supports full AP and client SSO. Client SSO is supported only for clients that have completed the authentication and DHCP phase, and have started passing traffic. With Client SSO, the client information is synced to the standby controller when the client associates to the controller or when the client parameters change. Fully authenticated clients, for example, the ones in RUN state, are synced to the standby. Thus, client reassociation is avoided on switchover making the failover seamless for the APs and clients, resulting in zero client service downtime and zero SSID outage. This feature reduces major downtime in wireless networks due to failure conditions such as box failover, network failover, or power outage on the primary site.

Note

Note When the controller works as a host for spanning tree, ensure that you configure portfast trunk, using **spanning-tree port type edge trunk** or **spanning-tree portfast trunk** commands, in the uplink switch to ensure faster convergence.

Note You can configure FIPS in HA setup. For information, see the Configuring FIPS in HA Setup.

Prerequisites for High Availability

External Interfaces and IPs

Because all the interfaces are configured only on the Active box, but are synchronized with the Standby box, the same set of interfaces are configured on both controllers. From external nodes, the interfaces connect to the same IP addresses, irrespective of the controllers they are connected to.

For this purpose, the APs, clients, DHCP, Cisco Prime Infrastructure, Cisco Catalyst Centre, and Cisco Identity Services Engine (ISE) servers, and other controller members in the mobility group always connect to the same IP address. The SSO switchover is transparent to them. But if there are TCP connections from external nodes to the controller, the TCP connections need to be reset and reestablished.

HA Interfaces

The HA interface serves the following purposes:

- Provides connectivity between the controller pair before an IOSd comes up.
- Provides IPC transport across the controller pair.
- Enables redundancy across control messages exchanged between the controller pair. The control messages can be HA role resolution, keepalives, notifications, HA statistics, and so on.

You can select either SFP or RJ-45 connection for HA port. Supported Cisco SFPs are:

- GLC-SX-MMD

- GLC-LH-SMD

When either SFP or RJ-45 connection is present, HA works between the two controllers. The SFP HA connectivity takes priority over RJ-45 HA connectivity. If SFP is connected when RJ-45 HA is up and running, the HA pair reloads. The reload occurs even if the link between the SFPs isn't connected.

Restrictions on High Availability

- For a fail-safe SSO, wait till you receive the switchover event after completing configuration synchronization on the standby controller. If the standby controller has just been booted up, we recommend that you wait *x* minutes before the controller can handle switchover events without any problem. The value of *x* can change based on the platform. For example, a Cisco 9800-80 Series Controller running to its maximum capacity can take up to 24 minutes to complete the configuration synchronization before being ready for SSO. You can use the **show wireless stats redundancy config database** command to view the database-related statistics.
- The flow states of the NBAR engine are lost during a switchover in an HA scenario in local mode. Because of this, the classification of flows will restart, leading to incorrect packet classification as the first packet of the flow is missed.
- The HA connection supports only IPv4.
- Switchover and an active reload and forces a high availability link down from the new primary.
- Two HA interfaces (RMI and RP) must be configured on the same subnet, and the subnet cannot be shared with any other interfaces on the device.
- It is not possible to synchronize a TCP session state because a TCP session cannot survive after a switchover, and needs to be reestablished.
- The Client SSO does not address clients that have not reached the RUN state because they are removed after a switchover.
- Statistics tables are not synced from active to standby controller.
- Machine snapshot of a VM hosting controller HA interfaces is not supported. It may lead to a crash in the HA controller.
- Mobility-side restriction: Clients which are not in RUN state will be forcefully reauthenticated after switchover.
- The following application classification may not be retained after the SSO:
  - AVC limitation—After a switchover, the context transfer or synchronization to the Standby box does not occur and the new active flow needs to be relearned. The AVC QoS does not take effect during classification failure.
  - A voice call cannot be recognized after a switchover because a voice policy is based on RTP or RTCP protocol.
  - Auto QoS is not effective because of AVC limitation.
- The active controller and the standby controller must be paired with the same interface for virtual platforms. For hardware appliance, there is a dedicated HA port.

- Static IP addressing can synch to standby, but the IP address cannot be used from the standby controller.
- You can map a dedicated HA port to a 1 GB interface only.
- To use EtherChannels in HA mode in releases until, and including, Cisco IOS XE Gibraltar 16.12.x, ensure that the channel mode is set to On.
- EtherChannel Auto-mode is not supported in HA mode in releases until, and including, Cisco IOS XE Gibraltar 16.12.x.
- LACP and PAGP is not supported in HA mode in releases until, and including, Cisco IOS XE Gibraltar 16.12.x.
- When the controller works as a host for spanning tree, ensure that you configure portfast trunk in the uplink switch using s**panning-tree port type edge trunk** or **spanning-tree portfast trunk** command to ensure faster convergence.
- The **clear chassis redundancy** and **write erase** commands will not reset the chassis priority to the default value.
- While configuring devices in HA, the members must not have wireless trustpoint with the same name and different keys. In such a scenario, if you form an HA pair between the two standalone controllers, the wireless trustpoint does not come up after a subsequent SSO. The reason being the *rsa keypair* file exists but it is incorrect as the *nvram:private-config* file is not synched with the actual *WLC_WLC_TP* key pair.

  As a best practice, before forming an HA, it is recommended to delete the existing certificates and keys in each of the controllers which were previously deployed as standalone.
- After a switchover, when the recovery is in progress, do not configure the WLAN or WLAN policy. In case you configure, the controller can crash.
- After a switchover, clients that are not in RUN state and not connected to an AP are deleted after 300 seconds.

Configuring High Availability (CLI)

Before you begin

The active and standby controller should be in the same mode, either Install mode or Bundle mode, with same image version. We recommend that you use Install mode.

Procedure

	Command or Action	Purpose
Step 1	**chassis** *chassis-num* **priority** *chassis-priority* **Example:** `Device# chassis 1 priority 1`	(Optional) Configures the priority of the specified device. **Note** From Cisco IOS XE Gibraltar 16.12.x onwards, device reload is not required for the chassis priority to become effective.

	Command or Action	Purpose
		• *chassis-num*—Enter the chassis number. The range is from 1 to 2. • *chassis-priority*—Enter the chassis priority. The range is from 1 to 2. The default value is 1. **Note** When both the devices boot up at the same time, the device with higher priority(2) becomes active, and the other one becomes standby. If both the devices are configured with the same priority value, the one with the smaller MAC address acts as active and its peer acts as standby.

Step 2	**chassis redundancy ha-interface GigabitEthernet** *num***local-ip** *local-chassis-ip-addr network-mask* **remote-ip** *remote-chassis-ip-addr*
	Example:
	`Device# chassis redundancy ha-interface`
	`GigabitEthernet 2 local-ip 4.4.4.1 /24 remote-ip 4.4.4.2`
		Configures the chassis high availability parameters.
		• *num*—GigabitEthernet interface number. The range is from 0 to 32.
		• *local-chassis-ip-addr*—Enter the IP address of the local chassis HA interface.
		• *network-mask*—Enter the network mask or prefix length in the */nn* or *A.B.C.D* format.
		• *remote-chassis-ip-addr*—Enter the remote chassis IP address.

Step 3	**chassis redundancy keep-alive timer** *timer* **Example:** `Device# chassis redundancy keep-alive timer 6`	Configures the peer keepalive timeout value. Time interval is set in multiple of 100 ms (enter 1 for default).
Step 4	**chassis redundancy keep-alive retries** *retry-value* **Example:** `Device# chassis redundancy keep-alive retries 8`	Configures the peer keepalive retry value before claiming peer is down. Default value is 5.

Disabling High Availability

If the controller is configured using RP method of SSO configuration, use the following command to clear all the HA-related parameters, such as local IP, remote IP, HA interface, mask, timeout, and priority:

clear chassis redundancy

If the controller is configured using RMI method, use the following command:

no redun-management interface vlan chassis

Note Reload the devices for the changes to take effect.

After the HA unpairing, the standby controller startup configuration and the HA configuration will be cleared and standby will go to Day 0.

Before the command is executed, the user is prompted with the following warning on the active controller:

```
Device# clear chassis redundancy

WARNING: Clearing the chassis HA configuration will result in both the chassis move into
Stand Alone mode. This involves reloading the standby chassis after clearing its HA
configuration and startup configuration which results in standby chassis coming up as a
totally
clean after reboot. Do you wish to continue? [y/n]? [yes]:

*Apr 3 23:42:22.985: received clear chassis.. ha_supported:1yes
WLC#
*Apr 3 23:42:25.042: clearing peer startup config
*Apr 3 23:42:25.042: chkpt send: sent msg type 2 to peer..
*Apr 3 23:42:25.043: chkpt send: sent msg type 1 to peer..
*Apr 3 23:42:25.043: Clearing HA configurations
*Apr 3 23:42:26.183: Successfully sent Set chassis mode msg for chassis 1.chasfs file updated
*Apr 3 23:42:26.359: %IOSXE_REDUNDANCY-6-PEER_LOST: Active detected chassis 2 is no
longer standby
```

On the standby controller, the following messages indicate that the configuration is being cleared:

```
Device-stby#

*Apr 3 23:40:40.537: mcprp_handle_spa_oir_tsm_event: subslot 0/0 event=2
*Apr 3 23:40:40.537: spa_oir_tsm subslot 0/0 TSM: during state ready, got event 3(ready)
*Apr 3 23:40:40.537: @@@ spa_oir_tsm subslot 0/0 TSM: ready -> ready
*Apr 3 23:42:25.041: Removing the startup config file on standby

!Standby controller is reloaded after clearing the chassis.
```

System and Network Fault Handling

If the standby controller crashes, it reboots and comes up as the standby controller. Bulk sync follows causing the standby to become hot. If the active controller crashes, the standby becomes active. The new active controller assumes the role of primary and tries to detect a dual active.

The following matrices provide a clear picture of the conditions the controller switchover would trigger:

Table 2: System and Network Fault Handling

System Issues			
Trigger	**RP Link Status**	**Switchover**	**Result**
Critical process crash	Up	Yes	Switchover happens
Forced switchover	Up	Yes	Switchover happens
Critical process crash	Up	Yes	Switchover happens
Forced switchover	Up	Yes	Switchover happens
Critical process crash	Down	No	Double fault – as mentioned in Network Error handling
Forced switchover	Down	N/A	Double fault – as mentioned in Network Error handling

Verifying High Availability Configurations

To view the HA configuration details, use the following command:

```
Device# show romvar
ROMMON variables:
 LICENSE_BOOT_LEVEL =
 MCP_STARTUP_TRACEFLAGS = 00000000:00000000
 BOOTLDR =
 CRASHINFO = bootflash:crashinfo_RP_00_00_20180202-034353-UTC
 STACK_1_1 = 0_0
 CONFIG_FILE =
 BOOT =
bootflash:boot_image_test,1;bootflash:boot_image_good,1;bootflash:rp_super_universalk9.vwlc.bin,1;

 RET_2_RTS =
 SWITCH_NUMBER = 1
 CHASSIS_HA_REMOTE_IP = 10.0.1.9
 CHASSIS_HA_LOCAL_IP = 10.0.1.10
 CHASSIS_HA_LOCAL_MASK = 255.255.255.0
 CHASSIS_HA_IFNAME = GigabitEthernet2
 CHASSIS_HA_IFMAC = 00:0C:29:C9:12:0B
 RET_2_RCALTS =
 BSI = 0
 RANDOM_NUM = 647419395
```

Verifying AP or Client SSO Statistics

To view the AP SSO statistics, use the following command:

```
Device# show wireless stat redundancy statistics ap-recovery wnc all
AP SSO Statistics
```

```
Inst    Timestamp      Dura(ms)   #APs  #Succ  #Fail  Avg(ms)  Min(ms)  Max(ms)
------------------------------------------------------------------------------
   0    00:06:29.042         98     34     34      0        2        1       35
   1    00:06:29.057         56     33     30      3        1        1       15
   2    00:06:29.070         82     33     33      0        2        1       13


Statistics:

WNCD Instance   : 0
No. of AP radio recovery failures          : 0
No. of AP BSSID recovery failures          : 0
No. of CAPWAP recovery failures            : 0
No. of DTLS recovery failures              : 0
No. of reconcile message send failed       : 0
No. of reconcile message successfully sent : 34
No. of Mesh BSSID recovery failures: 0
No. of Partial delete cleanup done : 0
.
.
.
```

To view the Client SSO statistics, use the following command:

```
Device# show wireless stat redundancy client-recovery wncd all
Client SSO statistics
----------------------

WNCD instance  : 1
Reconcile messages received from AP                    : 1
Reconcile clients received from AP                     : 1
Recreate attempted post switchover                     : 1
Recreate attempted by SANET Lib                        : 0
Recreate attempted by DOT1x Lib                        : 0
Recreate attempted by SISF Lib                         : 0
Recreate attempted by SVC CO Lib                       : 1
Recreate attempted by Unknown Lib                      : 0
Recreate succeeded post switchover                     : 1
Recreate Failed post switchover                        : 0
Stale client entries purged post switchover            : 0

Partial delete during heap recreate                    : 0
Partial delete during force purge                      : 0
Partial delete post restart                            : 0
Partial delete due to AP recovery failure              : 0
Partial delete during reconcilation                    : 0

Client entries in shadow list during SSO               : 0
Client entries in shadow default state during SSO      : 0
Client entries in poison list during SSO               : 0

Invalid bssid during heap recreate                     : 0
Invalid bssid during force purge                       : 0
BSSID mismatch with shadow rec during reconcilation    : 0
BSSID mismatch with shadow rec reconcilation(WGB client): 0
BSSID mismatch with dot11 rec during heap recreate     : 0

AID mismatch with dot11 rec during force purge         : 0
AP slotid mismatch during reconcilation                : 0
Zero aid during heap recreate                          : 0
AID mismatch with shadow rec during reconcilation      : 0
AP slotid mismatch shadow rec during reconcilation     : 0
Client shadow record not present                       : 0
```

To view the mobility details, use the following command:

```
Device# show wireless stat redundancy client-recovery mobilityd
Mobility Client Deletion Reason Statistics
-------------------------------------------
Mobility Incomplete State         : 0
Inconsistency in WNCD & Mobility  : 0
Partial Delete                    : 0

General statistics
--------------------
Cleanup sent to WNCD, Missing Delete case   : 0
```

To view the Client SSO statistics for SISF, use the following command:

```
Device# show wireless stat redundancy client-recovery sisf
Client SSO statistics for SISF
--------------------------------
Number of recreate attempted post switchover    : 1
Number of recreate succeeded post switchover    : 1
Number of recreate failed because of no mac     : 0
Number of recreate failed because of no ip      : 0
Number of ipv4 entry recreate success           : 1
Number of ipv4 entry recreate failed            : 0
Number of ipv6 entry recreate success           : 0
Number of ipv6 entry recreate failed            : 0
Number of partial delete received               : 0
Number of client purge attempted                : 0
Number of heap and db entry purge success       : 0
Number of purge success for db entry only       : 0
Number of client purge failed                   : 0
Number of garp sent                             : 1
Number of garp failed                           : 0
Number of IP entries validated in cleanup       : 0
Number of IP entry address errors in cleanup    : 0
Number of IP entry deleted in cleanup           : 0
Number of IP entry delete failed in cleanup     : 0
Number of IP table create callbacks on standby  : 0
Number of IP table modify callbacks on standby  : 0
Number of IP table delete callbacks on standby  : 0
Number of MAC table create callbacks on standby : 1
Number of MAC table modify callbacks on standby : 0
Number of MAC table delete callbacks on standby : 0
```

To view the HA redundancy summary, use the following command:

```
Device# show wireless stat redundancy summary
HA redundancy summary
---------------------

AP recovery duration (ms)        : 264
SSO HA sync timer expired        : No
```

Verifying High Availability

Table 3: Commands for Monitoring Chassis and Redundancy

Command Name	Description
show chassis	Displays the chassis information. **Note** When the peer timeout and retries are configured, the **show chassis ha-status** command output may show incorrect values. To check the peer keep-alive timer and retries, use the following commands: • **show platform software stack-mgr chassis active r0 peer-timeout** • **show platform software stack-mgr chassis standby r0 peer-timeout**
show redundancy	Displays details about Active box and Standby box.
show redundancy switchover history	Displays the switchover counts, switchover reason, and the switchover time.

To start the packet capture in the redundancy HA port (RP), use the following commands:

- test wireless redundancy packet dump start
- test wireless redundancy packet dump stop
- test wireless redundancy packet dump start filter port 2300

```
Device# test wireless redundancy packetdump start
Redundancy Port PacketDump Start
Packet capture started on RP port.

Device# test wireless redundancy packetdump stop
Redundancy Port PacketDump Start
Packet capture started on RP port.
Redundancy Port PacketDump Stop
Packet capture stopped on RP port.
Device# dir bootflash:
Directory of bootflash:/
1062881  drwx           151552  Oct 20 2020 23:15:25 +00:00  tracelogs
47      -rw-            20480  Oct 20 2020 23:15:24 +00:00  haIntCaptureLo.pcap
1177345  drwx             4096  Oct 20 2020 19:56:14 +00:00  certs
294337  drwx             8192  Oct 20 2020 19:56:05 +00:00  license_evlog
15      -rw-              676  Oct 20 2020 19:56:01 +00:00  vlan.dat
14      -rw-               30  Oct 20 2020 19:55:16 +00:00  throughput_monitor_params
13      -rw-           134808  Oct 20 2020 19:54:57 +00:00  memleak.tcl
1586145  drwx             4096  Oct 20 2020 19:54:45 +00:00  .inv
1103761  drwx             4096  Oct 20 2020 19:54:39 +00:00  dc_profile_dir
17      -r--              114  Oct 20 2020 19:54:17 +00:00  debug.conf
1389921  drwx             4096  Oct 20 2020 19:54:17 +00:00  .installer
46      -rw-       1104760207  Oct 20 2020 19:26:41 +00:00  leela_katar_rping_test.SSA.bin
49057   drwx             4096  Oct 20 2020 16:11:21 +00:00  .prst_sync
```

```
45      -rw-       1104803200  Oct 20 2020 15:39:19 +00:00
C9800-L-universalk9_wlc.2020-10-20_14.57_yavadhan.SSA.bin
269809  drwx             4096  Oct 19 2020 23:41:49 +00:00  core
44      -rw-       1104751981  Oct 19 2020 17:42:12 +00:00
C9800-L-universalk9_wlc.BLD_POLARIS_DEV_LATEST_20201018_053825_2.SSA.bin
43      -rw-       1104286975  Oct 16 2020 12:05:47 +00:00
C9800-L-universalk9_wlc.BLD_POLARIS_DEV_LATEST_20201010_001654_2.SSA.bin

Device# test wireless redundancy packetdump start filter port 2300
Redundancy Port PacketDump Start
Packet capture started on RP port with port filter 2300.
```

To check connection between the two HA Ports (RP) and check if there are any drops, delays, or jitter in the connection, use the following command:

```
Device# test wireless redundancy rping
Redundancy Port ping
PING 169.254.64.60 (169.254.64.60) 56(84) bytes of data.
64 bytes from 169.254.64.60: icmp_seq=1 ttl=64 time=0.083 ms
64 bytes from 169.254.64.60: icmp_seq=2 ttl=64 time=0.091 ms
64 bytes from 169.254.64.60: icmp_seq=3 ttl=64 time=0.074 ms

--- 169.254.64.60 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2041ms
rtt min/avg/max/mdev = 0.074/0.082/0.091/0.007 ms
test wireless redundancy
```

To see the HA port interface setting status, use the **show platform hardware slot R0 ha_port interface stats** command.

```
Device# show platform hardware slot R0 ha_port interface stats
HA Port
ha_port   Link encap:Ethernet  HWaddr 70:18:a7:c8:80:70
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
          Memory:e0900000-e0920000

Settings for ha_port:
        Supported ports:            [ TP ]
        Supported link modes:       10baseT/Half 10baseT/Full
                                    100baseT/Half 100baseT/Full
                                    1000baseT/Full
        Supported pause frame use:   Symmetric
        Supports auto-negotiation:   Yes
        Supported FEC modes:         Not reported
        Advertised link modes:       10baseT/Half 10baseT/Full
                                     100baseT/Half 100baseT/Full
                                     1000baseT/Full
        Advertised pause frame use:  Symmetric
        Advertised auto-negotiation: Yes
        Advertised FEC modes:        Not reported
        Speed:                       Unknown!
        Duplex:                      Unknown! (255)
        Port:                        Twisted Pair
        PHYAD:                       1
        Transceiver:                 internal
        Auto-negotiation:            on
        MDI-X:                       off (auto)
        Supports Wake-on:            pumbg
        Wake-on:                     g
        Current message level:       0x00000007 (7)
```

```
                                     drv probe link
        Link detected:               no

NIC statistics:
     rx_packets:             0
     tx_packets:             0
     rx_bytes:               0
     tx_bytes:               0
     rx_broadcast:           0
     tx_broadcast:           0
     rx_multicast:           0
     tx_multicast:           0
     multicast:              0
     collisions:             0
     rx_crc_errors:          0
     rx_no_buffer_count:     0
     rx_missed_errors:       0
     tx_aborted_errors:      0
     tx_carrier_errors:      0
     tx_window_errors:       0
     tx_abort_late_coll:     0
     tx_deferred_ok:         0
     tx_single_coll_ok:      0
     tx_multi_coll_ok:       0
     tx_timeout_count:       0
     rx_long_length_errors:  0
     rx_short_length_errors: 0
     rx_align_errors:        0
     tx_tcp_seg_good:        0
     tx_tcp_seg_failed:      0
     rx_flow_control_xon:    0
     rx_flow_control_xoff:   0
     tx_flow_control_xon:    0
     tx_flow_control_xoff:   0
     rx_long_byte_count:     0
     tx_dma_out_of_sync:     0
     tx_smbus:               0
     rx_smbus:               0
     dropped_smbus:          0
     os2bmc_rx_by_bmc:       0
     os2bmc_tx_by_bmc:       0
     os2bmc_tx_by_host:      0
     os2bmc_rx_by_host:      0
     tx_hwtstamp_timeouts:   0
     rx_hwtstamp_cleared:    0
     rx_errors:              0
     tx_errors:              0
     tx_dropped:             0
     rx_length_errors:       0
     rx_over_errors:         0
     rx_frame_errors:        0
     rx_fifo_errors:         0
     tx_fifo_errors:         0
     tx_heartbeat_errors:    0
     tx_queue_0_packets:     0
     tx_queue_0_bytes:       0
     tx_queue_0_restart:     0
     tx_queue_1_packets:     0
     tx_queue_1_bytes:       0
     tx_queue_1_restart:     0
     rx_queue_0_packets:     0
     rx_queue_0_bytes:       0
     rx_queue_0_drops:       0
     rx_queue_0_csum_err:    0
```

```
rx_queue_0_alloc_failed:0
rx_queue_1_packets:     0
rx_queue_1_bytes:       0
rx_queue_1_drops:       0
rx_queue_1_csum_err:    0
rx_queue_1_alloc_failed:0
```