Configuring System-Level High Availability

This chapter contains the following sections:

Information About System-Level High Availability

Information About Single and Dual Supervisor Roles

The Cisco Nexus 1000V can be configured with a single Virtual Supervisor Module (VSM) or dual VSMs. The following table describes the HA supervisor roles for single and dual VSM operation.

Single VSM Operation	Dual VSM Operation
• Stateless—In case of failure, service restarts from the startup configuration. • Stateful—In case of failure, service resumes from previous state.	• Redundancy is provided by one active VSM and one standby VSM. • The active VSM runs all the system applications and controls the system. • On the standby VSM, the applications are started and initialized in standby mode. The applications are synchronized and kept up to date with the active VSM in order to be ready to run. • On a switchover, the standby VSM takes over for the active VSM. • The control interface of the VSMs are used to pass heartbeats between the two VSMs. • The management interface is used to prevent split-brain scenarios.

HA Supervisor Roles

The redundancy role indicates not only whether the VSM interacts with other VSMs, but also the module number it occupies. The following table shows the available HA roles for VSMs.

role	Module Number	Description
Standalone	1	• This role does not interact with other VSMs. • You assign this role when there is only one VSM in the system. • This role is the default.
Primary	1	• This role coordinates the active/standby state with the secondary VSM. • This role takes precedence during bootup when negotiating active/standby mode. That is, if the secondary VSM does not have the active role at bootup, the primary VSM takes the active role. • You assign this role to the first VSM that you install in a dual VSM system.
Secondary	2	• This role coordinates the active/standby state with the primary VSM. • You assign this role to the second VSM that you install in a dual VSM system.

Dual Supervisor Active and Standby Redundancy States

Independent of its role, the redundancy state of a VSM can be one of the following described in this table.

Redundancy State	Description
Active	Controls the system and is visible to the outside world.
Standby	Synchronizes its configuration with that of the active VSM so that it is continuously ready to take over in case of a failure or manual switchover. You cannot use Telnet or Secure Shell (SSH) protocols to communicate with the standby VSM. Instead, you can use the **attach module** command from the active VSM to access the standby VSM console. Only a subset of the CLI commands are available from the standby VSM console.

Dual Supervisor Synchronization

The active and standby VSMs are in the operationally HA state and can automatically synchronize when the internal state of one supervisor module is Active with HA Standby and the internal state of the other supervisor module is HA Standby.

If the output of the **show system redundancy** command indicates that the operational redundancy mode of the active VSM is None, the active and standby VSMs are not yet synchronized.

This example shows the VSM internal state of dual supervisors as observed in the output of the **show system redundancy status** command:

```
switch# show system redundancy status
Redundancy role
---------------
      administrative:   standalone
         operational:   standalone

Redundancy mode
---------------
      administrative:   HA
         operational:   None

This supervisor (sup-1)
-----------------------
    Redundancy state:   Active
    Supervisor state:   Active
      Internal state:   Active with no standby

Other supervisor (sup-2)
------------------------
    Redundancy state:   Not present
switch#
```

Information About VSM Restarts and Switchovers

Restarts on Standalone VSMs

In a system with only one supervisor, when all HA policies have been unsuccessful in restarting a service, the supervisor restarts. The supervisor and all services restart with no prior state information.

Restarts on Dual VSMs

When a VSM fails in a system with dual supervisors, the system performs a switchover rather than a system restart in order to maintain a stateful operation. In some cases, a switchover might not be possible at the time of the failure. For example, if the standby VSM is not in a stable standby state, a restart rather than a switchover is performed.

Switchovers on Dual VSMs

A dual VSM configuration allows uninterrupted traffic forwarding with a stateful switchover (SSO) when a failure occurs in the VSM. The two VSMs operate in an active/standby capacity in which only one is active at any given time, while the other acts as a standby backup. The two VSMs constantly synchronize the state and configuration to provide a seamless and stateful switchover of most services if the active VSM fails.

Switchover Characteristics

A switchover occurs when the active supervisor fails (for example, if repeated failures occur in an essential service or if the system that is hosting the VSM fails).

A user-triggered switchover could occur (for example, if you need to perform maintenance tasks on the system hosting the active VSM).

An HA switchover has the following characteristics:

- It is stateful (nondisruptive) because the control traffic is not affected.
- It does not disrupt data traffic because the VEMs are not affected.

Automatic Switchovers

When a stable standby VSM detects that the active VSM has failed, it initiates a switchover and transitions to active. When a switchover begins, another switchover cannot be started until a stable standby VSM is available.

If a standby VSM that is not stable detects that the active VSM has failed, then, instead of initiating a switchover, it tries to restart the system.

Manual Switchovers

Before you can initiate a manual switchover from the active to the standby VSM, the standby VSM must be stable.

Once you have verified that the standby VSM is stable, you can manually initiate a switchover.

Once a switchover process begins, another switchover process cannot be started until a stable standby VSM is available.

Guidelines and Limitations

- Although primary and secondary VSMs can reside in the same host, to improve redundancy, install them in separate hosts and, if possible, connect the VSMs to different upstream switches.
- The console for the standby VSM is available through the vSphere client or by entering the **module attach** *x* command, but configuration is not allowed and many commands are restricted. Enter this command at the console of the active VSM.
- You cannot use Telnet or Secure Shell (SSH) protocols to communicate with the standby VSM because the management interface IP is unconfigured until the VSM becomes active.
- The active and standby VSMs must be on the same management subnet.

Configuring System-Level High Availability

Changing the VSM Role

The Cisco Nexus 1000V VSM software installation provides an opportunity for you to designate the role for each VSM. You can use this procedure to change that initial configuration.

⚠

Caution Changing the role of a VSM can result in a conflict between the VSM pair. If a primary and secondary VSM see each other as active at the same time, the system resolves this problem by resetting the primary VSM.

Use this procedure to change the role of a VSM to one of the following after it is already in service:

- Standalone
- Primary
- Secondary

Before you begin

- Log in to the CLI in EXEC mode.
- If you are changing a standalone VSM to a secondary VSM, be sure to first isolate it from the other VSM in the pair to prevent any interaction with the primary VSM during the change. Power the VM off from the vSphere Client before reconnecting it as standby.

For an example on how to change the port groups and port profiles assigned to the VSM interfaces in the vSphere Client, see the*Cisco Nexus 1000V Installation and Upgrade Guide*.

You must understand the following information:

- The possible HA roles are standalone, primary, and secondary.

- The possible HA redundancy states are active and standby.
- To activate a change from primary to secondary VSM, you must reload the VSM by doing one of the following:
  - Enter the **reload** command.
  - Power the VM off and then on from the vSphere Client.
- A change from a standalone to a primary VSM takes effect immediately.

Procedure

	Command or Action	Purpose
Step 1	switch# **system redundancy role** {*standalone* | *primary* | *secondary*}	Designates the HA role of the VSM.
Step 2	(Optional) switch# **show system redundancy status**	Displays the current redundancy status for the VSMs.
Step 3	(Optional) switch# **copy running-config startup-config**	Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

Example

This example shows how to change the VSM role:

```
switch# system redundancy role standalone
switch# show system redundancy status
Redundancy role
---------------
      administrative:   standalone
         operational:   standalone

Redundancy mode
---------------
      administrative:   HA
         operational:   None

This supervisor (sup-1)
-----------------------
   Redundancy state: Active
   Supervisor state: Active
   Internal state:Active with no standby

Other supervisor (sup-2)
------------------------
   Redundancy state:   Not present
switch#
```

Configuring a Switchover

Guidelines and Limitations for Configuring a Switchover

- When you manually initiate a switchover, system messages are generated that indicate the presence of two VSMs and identify which one is becoming active.
- A switchover can only be performed when both VSMs are functioning.

Verifying that a System is Ready for a Switchover

Use one of the following commands to verify the configuration:

Command	Purpose
show system redundancy status	Displays the current redundancy status for the VSM(s). If the output indicates the following, you can proceed with a system switchover: • The presence of an active VSM • The presence of a standby VSM in the HA standby redundancy state
show module	Displays information about all available VEMs and VSMs in the system. If the output indicates the following, you can proceed with a system switchover: • The presence of an active VSM • The presence of a standby VSM in the HA standby redundancy state

Manually Switching the Active VSM to Standby

Be sure you know the following about manually switching the active VSM to a standby VSM:

- A switchover can be performed only when two VSMs are functioning in the switch.
- If the standby VSM is not in a stable state (ha-standby), you cannot initiate a manual switchover and will see the following error message:

```
Failed to switchover (standby not ready to takeover in vdc 1)
```

- If a switchover does not complete successfully within 28 seconds, the supervisors reset.

Before you begin

- Log in to the active VSM CLI in EXEC mode.

- Complete the steps in Verifying that a System is Ready for a Switchover, on page 7 and verify that the system is ready for a switchover.

Procedure

	Command or Action	Purpose
Step 1	switch# **system switchover**	On the active VSM, initiates a manual switchover to the standby VSM. Once you enter this command, you cannot start another switchover process on the same system until a stable standby VSM is available. Before proceeding, wait until the switchover completes and the standby supervisor becomes active.
Step 2	(Optional) switch# **show running-config diff**	Verifies the difference between the running and startup configurations. Any unsaved running configuration in an active VSM is also unsaved in the VSM that becomes active after switchover. Save that configuration in the startup if needed.
Step 3	(Optional) switch# **copy running-config startup-config**	Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

Example

This example shows how to switch an active VSM to the standby VSM and displays the output that appears on the standby VSM as it becomes the active VSM:

```
switch# system switchover
---------------------------
2009 Mar 31 04:21:56 n1000v %$ VDC-1 %$ %SYSMGR-2-HASWITCHOVER_PRE_START:
This supervisor is becoming active (pre-start phase).
2009 Mar 31 04:21:56 n1000v %$ VDC-1 %$ %SYSMGR-2-HASWITCHOVER_START:
This supervisor is becoming active.
2009 Mar 31 04:21:57 n1000v %$ VDC-1 %$ %SYSMGR-2-SWITCHOVER_OVER: Switchover completed.
2009 Mar 31 04:22:03 n1000v %$ VDC-1 %$ %PLATFORM-2-MOD_REMOVE: Module 1 removed (Serial
number )
```

This example shows how to display the difference between the running and startup configurations:

```
switch# show running-config diff
*** Startup-config
--- Running-config
***************
*** 1,38 ****
  version 4.0(4)SV1(1)
  role feature-group name new
  role name testrole
  username admin password 5 $1$S7HvKc5G$aguYqHl0dPttBJAhEPwsy1  role network-admin
```

```
telnet server enable
ip domain-lookup
```

Configuring the VSM-to-VSM Heartbeat Interval

If the communication network between two VSMs in an HA pair experiences interruptions longer than the 15-second default, you can change the VSM-to-VSM heartbeat interval so that it is less sensitive to falsely detecting active VSM failures.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **system inter-sup-heartbeat time** *time-interval*	Configures the VSM-to-VSM heartbeat with a time interval from 6 to 30 seconds. The default is 15 seconds.
Step 3	switch(config)# **show running-config | grep heartbeat**	Displays the heartbeat interval setting in the running configuration.
Step 4	(Optional) switch(config)# **copy running-config startup-config**	Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

Example

The following example shows how to set the VSM-to-VSM interval to 10 seconds and verify this setting:

```
switch# configure terminal
switch(config)# system inter-sup-heartbeat time 10
switch(config)# show running-config | grep heartbeat
system inter-sup-heartbeat time 10
switch(config)# copy running-config startup-config
```

Adding a Second VSM to a Standalone System

Adding a Second VSM to a Standalone System

The following list is designed to guide you through the process of adding a second VSM to a standalone system.

1. Change the standalone VSM to a primary VSM. For more information , see Changing the Standalone VSM to a Primary VSM, on page 10.
2. Install the second VSM. For more information, see http://www.cisco.com/en/US/products/ps9902/prod_installation_guides_list.html

3. Verify the change to the dual VSM system. For more information, see Verifying the Change to a Dual VSM System, on page 11.

Changing the Standalone VSM to a Primary VSM

You can change the role of a VSM from standalone in a single VSM system to primary in a dual VSM system.

A change from a standalone to a primary VSM takes effect immediately.

Before you begin

Log in to the CLI in EXEC mode.

Procedure

	Command or Action	Purpose
Step 1	switch# **system redundancy role primary**	Changes the standalone VSM to a primary VSM. The role change occurs immediately.
Step 2	switch#**peer-sup mac-address clear**	Clears old peer VSM MAC addresses, if any.
Step 3	(Optional) switch# **show system redundancy status**	It also displays peer VSM MAC addresses as not learned.
Step 4	(Optional) switch# **copy running-config startup-config**	Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

Example

This example shows how to display the current system redundancy status for the VSM:

```
switch# system redundancy role primary
switch# peer-sup mac-address clear
switch# show system redundancy status
Redundancy role
---------------
      administrative:   primary
         operational:   primary

Redundancy mode
---------------
      administrative:   HA
         operational:   None

This supervisor (sup-1)
-----------------------
    Redundancy state:   Active
    Supervisor state:   Active
      Internal state:   Active with no standby

Other supervisor (sup-2)
------------------------
    Redundancy state:   Not present
```

```
Peer Sup Mac Addresses Learnt
-------------------------------------------
   Control Interface:   Not Learnt
      Mgmt Interface:   Not Learn

switch# copy running-config startup-config
```

Verifying the Change to a Dual VSM System

Use one of the following commands to verify the configuration:

Command	Purpose
show system redundancy status	Displays the current redundancy status for VSMs in the system.
show module	Displays information about all available VSMs and VEMs in the system.

Replacing the Secondary VSM in a Dual VSM System

Note Equipment Outage—This procedure requires that you power down and reinstall a VSM. During this time, your system will operate with a single VSM.

If have your VSM HA Pair in 5.2(1)SV3(1.1) with Domain Id > 1023 [Setup created Via upgrade] , then kindly change your domain ID to less than 1024 before replacing Primary or Secondary VSM in an Dual VSM system.

Procedure

Step 1 Ensure that the primary VSM is active (see the output of the **show system redundancy status**command).

Note Do a system switchover if necessary.

Step 2 Power off the secondary VSM.

Step 3 Log into the CLI in EXEC mode on the active primary VSM. Enter **peer-sup mac-addresses-clear**command.

Step 4 Verify that the "Peer Sup Mac Addresses Learnt" section in the **show system redundancy status** command displays "Not Learnt."

Step 5 Install the new VSM as a secondary, with the same domain ID as the existing VSM, using the procedure in the “Installing and Configuring the VSM VM” section in the *Cisco Nexus 1000V Installation and Upgrade Guide*.

After the new VSM is added to the system, both VSMs learn the peer VSM MAC addresses and the new VSM synchronizes with the existing VSM.

Replacing the Primary VSM in a Dual VSM System

You can replace an active/primary VSM in a dual VSM system.

Note Equipment Outage—This procedure requires that you power down and reinstall a VSM. During this time, your system will operate with a single VSM.

If have your VSM HA Pair in 5.2(1)SV3(1.1) with Domain Id > 1023 [Setup created Via upgrade] , then kindly change your domain ID to less than 1024 before replacing Primary or Secondary VSM in an Dual VSM system.

Before you begin

- Log in to the CLI in EXEC mode.
- Power off the primary VSM.
- Configure the port groups so that the new primary VSM cannot communicate with the secondary VSM or any of the VEMs during the setup. VSMs with a primary or secondary redundancy role have built-in mechanisms for detecting and resolving the conflict between two VSMs in the active state. To avoid these mechanisms during the configuration of the new primary VSM, you must isolate the new primary VSM from the secondary VSM.

Procedure

Step 1 Ensure that the secondary VSM is active.

Note Do a system switchover if necessary.

Step 2 Log into CLI in EXEC mode on the active secondary VSM. Enter **peer-sup mac-addresses-clear** command.

Step 3 Verify that the "Peer Sup Mac Addreses Learnt" section in the **show system redundancy status** command displays "Not Learnt."

Step 4 On the vSphere Client, change the port group configuration for the new primary VSM VM to prevent communication with the secondary VSM and the VEMs during the setup.

For an example on how to change the port groups and port profiles assigned to the VSM interfaces in the vSphere Client, see the *Cisco Nexus 1000V Installation and Upgrade Guide.*

Step 5 Install the new VSM, change the HA role from standalone to primary and set the same domain ID as the existing VSM, using the **Installing the Cisco Nexus 1000V Software Using ISO or OVA Files** section in the *Cisco Nexus 1000V Installation and Upgrade Guide*.

Step 6 Save the configuration.

Step 7 Power off the VM.

Step 8 On the vSphere Client, change the port group configuration for the new primary VSM to permit communication with the secondary VSM and the VEMs.

Step 9 Power up the new primary VSM. Both VSMs will learn the peer VSM's MAC addresses.

The new primary VSM starts and automatically synchronizes all configuration data with the secondary VSM, which is currently the active VSM. Because the existing VSM is active, the new primary VSM becomes the standby VSM and receives all configuration data from the existing active VSM.

Changing the Domain ID in a Dual VSM System

Before you begin

- Have access to the console of both the active and standby VSM.
- Isolate the standby VSM from the active VSM to avoid the built-in mechanisms that detect and resolve conflict between two VSMs with a primary or secondary redundancy role. This procedure has a step for isolating the VSMs.

Note Equipment Outage—This procedure requires that you power down a VSM. During this time, your system will operate with a single VSM.

Procedure

Step 1 On the vSphere Client for the standby VSM, do one of the following to isolate the VSMs and prevent their communication while completing this procedure:

- Change the port group configuration for the interfaces using port groups that prevent the VSMs from communicating with each other.
- Unmark the “Connected” option for the interfaces.

The standby VSM becomes active but cannot communicate with the other active VSM or the VEM

Step 2 At the console of the standby VSM, change the domain ID and save the configuration.

Example:

This example shows how to change the domain ID and save the configuration:

```
switch# configure terminal
switch(config)# svs-domain
switch(config-svs-domain)# domain id 100
Successfully cleared old Peer VSM's MAC Addresses
================================================================================
IMPORTANT NOTE: If this VSM is replacing a Standby VSM which was in HA
pair then, please execute "peer mac-addresses clear" CLI on Active VSM
to clear old Peer VSM's MAC Addresses on Active VSM as well.
================================================================================
switch(config-svs-domain)# copy running-config startup-config
```

The domain ID is changed on the standby VSM and the VEM connected to it

Step 3 Power down the standby VSM.

Step 4 At the console of the active VSM, change the domain ID and save the configuration.

Example:

```
switch# configure terminal
switch(config)# svs-domain
switch(config-svs-domain)# domain id 100
Successfully cleared old Peer VSM's MAC Addresses
======================================================================
IMPORTANT NOTE: If this VSM is replacing a Standby VSM which was in HA
pair then, please execute "peer mac-addresses clear" CLI on Active VSM
to clear old Peer VSM's MAC Addresses on Active VSM as well.
======================================================================

switch(config-svs-domain)# copy running-config startup-config
```

The domain ID is changed on the active VSM and the VEM that is connected to it.

Step 5 On the vSphere Client for the standby VSM, do one of the following to permit communication with the active VSM:

- Change the port group configuration for the interfaces.
- Make sure that the "Connect at power on" option is marked for the interfaces.

When the standby VSM is powered up, it will be able to communicate with the active VSM.

Step 6 Power up the standby VSM.

Both VSMs are now using the new domain ID and will synchronize.

Changing the Domain ID in a Dual VSM System for VSMs Hosted on Cisco Nexus 1010

Before you begin

- Have access to the CLI of the active VSM (primary VSB) and standby VSM (secondary VSB).
- Have access to the Cisco Nexus 1010 CLI.

Procedure

Step 1 On the Cisco Nexus 1010 CLI, complete the following tasks:

a) Power down the secondary VSB.

Example:

```
switch# configure terminal
switch(config)# virtual-service-blade VSM1
switch(config-vsb-config)# shutdown secondary
```

b) Check the status of the secondary VSB and verify that the status is **VSB POWERED OFF**.

Example:

```
switch(config-vsb-config)# show virtual-service-blade summary

--------------------------------------------------------------------------------
Name Role State Nexus1010-Module
--------------------------------------------------------------------------------
VSM1 PRIMARY VSB POWERED ON Nexus1010-PRIMARY
VSM1 SECONDARY VSB POWERED OFF Nexus1010-SECONDARY
```

c) Delete the secondary VSB and verify that the status is **VSB NOT PRESENT**.

Example:

```
switch(config-vsb-config)# no enable secondary
switch(config-vsb-config)# show virtual-service-blade summary

--------------------------------------------------------------------------------
Name Role State Nexus1010-Module
--------------------------------------------------------------------------------
VSM1 PRIMARY VSB POWERED ON Nexus1010-PRIMARY
VSM1 SECONDARY VSB NOT PRESENT Nexus1010-SECONDARY
```

Step 2 On the primary VSB, complete the following tasks:

a) Verify that the secondary VSB is not connected.

b) Verify that the operational status of primary VSB is **Connected**.

Example:

```
switch# show svs connections
connection VC:
ip address: 192.168.0.1
protocol: vmware-vim https
certificate: default
datacenter name: Hamilton-DC
DVS uuid: ac 36 07 50 42 88 e9 ab-03 fe 4f dd d1 30 cc 5c
config status: Enabled
operational status: Connected
```

c) Change the domain ID and save the configuration.

Example:

```
switch# configure terminal
switch(config)# svs-domain
switch(config-svs-domain)# domain id 100
Successfully cleared old Peer VSM's MAC Addresses
================================================================================
IMPORTANT NOTE: If this VSM is replacing a Standby VSM which was in HA
pair then, please execute "peer mac-addresses clear" CLI on Active VSM
to clear old Peer VSM's MAC Addresses on Active VSM as well.
================================================================================
switch(config-svs-domain)# copy running-config startup-config
```

d) Verify the new domain ID.

Example:

```
switch(config)# show svs domain
SVS domain config:
Domain id: 100
L2/L3 Control mode: L2
```

```
L3 control interface: NA
Status: Config push to VC successful.
```

e) Verify that the domain ID is updated on VEMs by running the following command on the VEM modules:

Example:

```
switch# vemcmd show card
 ard UUID type  2: 58f8afd7-e1e3-3c51-85e2-6e6f2819a7b8
 Card name: sfish-srvr-1
 Switch name: n1000v
 Switch alias: DvsPortset-0
 Switch uuid: 56 e0 36 50 91 1c 32 7a-e9 9f 31 59 88 0c 7f 76
 Card domain: 100
 Card slot: 4
 VEM Control (Control VLAN) MAC: 00:02:3d:14:00:03
 VEM Packet (Inband) MAC: 00:02:3d:24:00:03
 VEM Control Agent (DPA) MAC: 00:02:3d:44:00:03
 VEM SPAN MAC: 00:02:3d:34:00:03
 Management IP address: 172.23.232.102
 Max physical ports: 32
 Max virtual ports: 216
 Card control VLAN: 3002
 Card packet VLAN: 3003
        Processors: 4
   Processor Cores: 4
 Processor Sockets: 2
   Physical Memory: 4290351104
```

Step 3 On the Cisco Nexus 1010 CLI, complete the following tasks:

a) Deploy a secondary VSB.

Example:

```
switch# configure terminal
switch(config)# virtual-service-blade VSM1
switch(config-vsb-config)# enable secondary
 Enter vsb image: [dcos_vsm.iso]
 Enter domain id[1-4095]: 100
 Management IP version [V4/V6]: [V4]
 Enter Management IP address: 10.78.109.67
 Enter Management subnet mask length: 27
 IPv4 address of the default gateway: 10.78.109.65
 Enter HostName: switch
 Enter the password for 'admin': xz35vb1zx
```

b) Check the status of the secondary VSB and verify that the status is **VSB POWERED ON**.

Example:

```
switch(config-vsb-config)# show virtual-service-blade summary

--------------------------------------------------------------------------------
Name Role State Nexus1010-Module
--------------------------------------------------------------------------------
VSM1 PRIMARY VSB POWERED ON Nexus1010-PRIMARY
VSM1 SECONDARY VSB POWERED ON Nexus1010-SECONDARY
```

Step 4 On the primary VSB, verify that the HA pair is formed.

Example:

```
switch# show system redundancy status
Redundancy role
```

```
---------------
administrative: primary
operational: primary
Redundancy mode
---------------
administrative: HA
operational: HA
This supervisor (sup-1)
-----------------------
Redundancy state: Active
Supervisor state: Active
Internal state: Active with HA standby
Other supervisor (sup-2)
------------------------
Redundancy state: Standby
Supervisor state: HA standby
Internal state: HA standby
```

Disabling Domain ID Collision

Procedure

Step 1 Log in to the primary VSM console in EXEC mode.

Step 2 Disable the domain ID collision detection.

Example:

```
switch# peer-sup mac-addresses check disable
```

Step 3 Verify that the check is disabled.

Example:

```
switch# show peer-sup mac-addresses details
Peer MAC Address Check = Disabled
Peer HA0 MAC Address = 00:50:56:b5:3a:99
Peer HA1 MAC Address = 00:50:56:b5:5e:05
```

Step 4 Log in to the secondary VSM console in EXEC mode

Step 5 Disable the domain id collision detection.

Example:

```
switch# peer-sup mac-addresses check disable
```

Step 6 Verify that the check is disabled.

Example:

```
switch# show peer-sup mac-addresses details
Peer MAC Address Check = Disabled
Peer HA0 MAC Address = 00:50:56:b5:3a:99
Peer HA1 MAC Address = 00:50:56:b5:5e:05
```

Verifying the HA Status

Use one of the following commands to verify the configuration:

Command	Purpose
show system redundancy status	Displays the HA status of the system.
show module	Displays information about all available VSMs and VEMs in the system.
show processes	Displays the state of all processes and the start count of the process. The states and types are described as follows: • State: R (runnable), S (sleeping), Z (defunct) • Type: U (unknown), O (non sysmgr), VL (vdc-local), VG (vdc-global), VU (vdc-unaware), NR (not running), ER (terminated)

Starting with Release 5.2(1)SV3(1.1), the VSM drops the HA packets when the source MAC address is not known.If the peer VSM's MAC addresses are not learned correctly (such as when a standby VSM is replaced without following a correct procedure), the VSM is not formed.

The **show system redundancy status** command displays a note in this case output. After clearing the old MAC addresses, HA should be formed if the problem was due to incorrect MAC addresses.

```
switch# show system redundancy status

Redundancy role
---------------
      administrative:   primary
         operational:   primary

Redundancy mode
---------------
      administrative:   HA
         operational:   None

This supervisor (sup-1)
-----------------------
    Redundancy state:   Active
    Supervisor state:   Active
      Internal state:   Active with no standby

Other supervisor (sup-2)
------------------------
    Redundancy state:   Not present

Peer Sup Mac Addresses Learnt
-----------------------------------------------
   Control Interface:   00:50:56:91:44:c8
      Mgmt Interface:   00:50:56:91:1f:6f
```

```
HA Packet Drops Due to Domain id Collision
-------------------------------------------
   Control Interface:   36
      Mgmt Interface:   51
------------------------------------------------------------------------------
IMPORTANT NOTE: Please compare Peer Sup MAC addresses learnt above
with the actual Peer Sup's MAC addresses. If they are not same, execute
"peer-sup mac-addresses clear" on this VSM to form HA again
------------------------------------------------------------------------------

switch#
```

Related Documents

Related Topic	Document Title
Software upgrades	*Cisco Nexus 1000V Installation and Upgrade Guide*
Cisco Nexus 1000V commands	*Cisco Nexus 1000V Command Reference*

Standards

No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.

MIBs

MIBs	MIBs Link
CISCO-PROCESS-MIB	To locate and download MIBs, go to the following URL: http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

RFCs

No RFCs are supported by this feature.

Technical Assistance

Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.

Go to the following URL: http://www.cisco.com/cisco/web/support/index.html

Feature History for System-Level High Availability

This table includes only the updates for those releases that have resulted in additions or changes to the feature.

Feature Name	Releases	Feature Information
Enhancements for Domain ID Collision	5.2(1)SV3(1.1)	This feature was introduced.
System - Level High Availability	4.0(4)SV1(1)	This feature was introduced.