CHAPTER 3

Single IP Infrastructure

This chapter discusses concepts related to Single IP Infrastucture and Manageability requirements for the Service Provider Home Agent application. This application is resident on the SAMI service blade of the Cisco 7600 Switch and is part of the Msef product family. This chapter also provides details about how to configure this feature.

This chapter includes the following sections:

Overview of Single IP Feature

The current mSEF gateway-on-SAMI solutions, (Cisco Mobile Wireless Home Agent, WiMax BWG, Cisco GGSN, and PDSN) all offer a multiple-routers-on-a-stick model with the attendant manageability and operational issues. The system design for Home Agent Single IP allows you to manage the gateway-on-SAMI on a per-blade basis. This results in a “factor-of-6 decrease” in operational complexity compared to the previous presentation of six individual processors per blade.

The Single IP feature reapportions functionality on a SAMI service blade from the current model of six independent IOS processors, each executing both control and traffic plane functions, to a model where one IOS processor is designated as a Control Plane (CP) processor and the other 5 designated as Traffic Plane (TP) processors.

Here is an additional targeted subset of functionality that is presented in a per-chassis model. The presentation of a per-blade model applies to the following areas:

- Access Network Protocol
- Authentication/Authorization interactions
- Network Management interaction through SNMP for MIB retrieval
- Retrieval of “load parameters”, through SNMP, as a basis for per-subscriber dynamic gateway assignment
- Configuration, Show and Debug functionality
- Failure detection and failover of a blade
- AAA server response time determinations and alarm indications

Additionally, the presentation of a per-chassis model applies to the following targeted functionality:

- Show subscribers present across a chassis with various output filtering capabilities.
- Display the session activity for one or more subscribers across a chassis.
- Monitor Subscriber (Call Trace) for one or more specific subscribers for the purposes of troubleshooting.
- Collation, transfer and storage of bulk statistics for a chassis.

The Home Agent feature behavior as perceived by external systems does not change. The Single IP Home Agent on a blade will look and feel the same as one Home Agent 4.0 image executing on a single processor.

Single IP Interface

The following features fall under the umbrella of Single IP per blade:

- Single Interface for MIP
- Single Interface for Configuration
- Single Interface for SNMP Management
- Single Interface for Trouble Shooting and Debug
- Single Interface for AAA
  - Single Interface for MIP and AAA
- Single Interface for Failover

Single Interface for MIP

The service blade presents a distinct IP address that is the Home Agent IP address. This address is configured the same as in Home Agent Release 4.0. This same IP address is also the endpoint address for the tunnel between the Home Agent and the Care-of-Address (CoA), whether that is a Foreign Agent CoA, or a Collocated CoA. This IP address configuration is present on both control plane and traffic plane processors. This allows configuration of one Mobile IP security association per blade for each of MN-HA and FA-HA, instead of the current six.

The Home Agent IP address should be the loopback address, and this same IP address is also the endpoint address for the tunnel between the Home Agent and the Care-of-Address (CoA)

The service blade implements a packet distribution function in IXP ucode that ensures that user traffic packets are dispatched to the correct traffic plane processor. Packets identified as control plane traffic are sent to the control plane processor. Packets that do not match a specific identification are sent to the control plane processor for treatment.

Single Interface for Configuration

The service blade provides a single point of configuration for blade functionality. This means that you can establish a session to the service blade, the same as performed in Home Agent Release 4.0. The session is established to the control processor on the service blade. From that single session to the service blade, it is possible to configure the Home Agent features with a single execution of each command required for a feature. That configuration is then propagated to all processors that require the same configuration without you having to perform any additional configuration tasks.

The default treatment for any IOS configuration command is that the configuration takes effect on all IOS processors on the service blade. It is possible to define a set of commands that will only execute on the processor hosting the configuration session. Some examples of filtered configuration commands are those relating to OSPF and HSRP.

Single Interface for SNMP Management

The service blade provides a distinct configurable IP address that is the target address for SNMP operations. This IP address is hosted on the control plane processor. All MIBs on a service blade related to Home Agent functionality are accessible through this IP address. Information required from processors other than the control plane processor is either Pushed or Pulled depending on the MIB target.

There are two MIBs related to processor resource usage and memory usage that present information on a per-processor basis. There will be a single Processor Resource MIB result returned with six individual entries, one per processor. Similarly, this also occurs for memory usage.

Single Interface for Trouble Shooting and Debug

The service blade provides a single point of entry (session into the control plane processor) to execute **show** and **debug** commands. By default, **show** commands are executed on the Control Plane processor only. Each command that requires execution on 1 or more traffic plane processors is individually instrumented.

For commands that require additional information from the traffic plane processor, and are qualified per user (either NAI or IP address), the traffic plane processor hosting that user is identified and the command executed on that specific processor.

The results from the various processors are combined into a single presentation before a response to the command is provided.

Conditional debug commands use a similar approach. To support the chassis-wide “Debug a Subscriber” feature, it is necessary to preset a trigger for the identified subscriber before a Mobile IP binding registration request is received for that subscriber. Once the registration request is received, the preset trigger can be removed for all processors except the one where the request was received.

Single Interface for AAA

The service blade presents a single IP address for AAA interactions. This may be one IP address for both Radius-based and Diameter-based interactions, or separate IP address configurations for each protocol.

Radius-based Authentication and Authorization is executed solely from the Control Plane processor.

Radius-based Change of Authorization and Packet of Disconnect exchanges occur with the Control Plane which then triggers the execution of the resulting action on the relevant Traffic Processor. These functions are provided independent of support for Radius-based accounting.

Diameter-based interactions for policy support also execute solely on the Control Plane processor. This is supported as part of the Home Agent 5.0 release.

Radius-based and/or Diameter-based accounting is not supported in this release of Single IP for Home Agent. The service blade packet distribution function does provide for directing of Radius traffic to a specific processor based on the destination UDP port.

Single Interface for MIP and AAA

For the Single IP-based Home Agent, the CP terminates the interface towards AAA servers. For all subscribers, the Authentication is performed by the CP. Note that only Authentication is performed.

To update the information from active/standby CP to the TP, the CP uses the IPC mechanism. The CP waits on process for some control messages while updating to the TP. The following sections contain the specific approach for each control plane messaging case.

Procedures on Active HA

The following control messages are handled by CP of the active Home Agent.

- Registration Request (RRQ) -Registration, Re-Registration and De-Registration of subscriber
- Registration Revocation messages
- Registration Revocation Acknowledgement Messages
- Change of Authorization(COA)
- Packet of Disconnect (POD)

Registration Request of MN on Active-HA CP

1. The CP on the active-HA receives RRQ and the CP performs Authorization for the MN. The interface between the CP and AAA servers remains same as HA4.0.
2. If the authorization failed for the MN, the CP sends a Registration Reply with Error Code to FA.
3. On successful authorization, an IP address assignment is made for the binding. The mechanisms for IP address assignment are the same as for Home Agent 4.0. The CP looks at the Hash Table to get one TP ID based on the assigned MN address.
4. The CP updates binding information to the corresponding TP using an IPC reliable mechanism without waiting for response. And, it will send update information to standby-HA CP over UDP/IP and respond to FA with a Registration Reply.
5. If an acknowledgment is received by the CP without error code from the TP, the CP does not take any action.
6. If failure happens due to timeout or received invalid response from the TP, the CP deletes the binding and as well initiate “binddeleterequest” to the standby-HA and sends a Registration Revocation Message to the FA if revocation is enabled on the HA.

The following information is updated from CP to TP for binding:

- RRQ Header - Is based on RFC 3344.
- SPI of MHAE as an extension
- NAI extension
- Multipath NVSE
- Address Type CVSE - Indicates DHCP Address allocation for MN
- MR dynamic Network NVSE
- Static/Dynamic pool name
- Class attribute—if received, this is only for Accounting purposes
- CUI—if received, this is only for Accounting purpose and wimax subscribers
- Accounting multi session ID, accounting interim interval - for Wimax subscribers.

- VRF name and corresponding HA IP address, if present.
- In and Out Acl Names
- Hotline basic Information
- Hotline accounting Indication
- List of Hotline rule/profile based as NVSEs.

De-Registration of MN on Active-HA

The following call flow describes the de-registration of a MN on the active HA:

1. The CP on the active-HA receives a RRQ for De-Registration and the CP does Authorization for the MN. The interface between the CP and AAA servers is the same as HA Release 4.0 functionality.
2. If the authorization fails for the MN, the CP send a Registration Reply with Error Code to FA.
3. On successful authorization, the CP sends binding information to the corresponding TP using IPC reliable mechanism to delete the binding. During De-Registration the CP does not wait for the response from the TP.
4. The CP sends a Registration Reply with MN address and error code as **0**.
5. The CP on the active-HA sends a binding delete request to its peer.

The following information is updated from the CP to the TP for binding,

- Message Type and Error Code
- MN Home-Address
- Home-Agent Address
- Care-of-Address

Registration Revocation Message on Active-HA

The following call flow identifies the procedure for Registration Revocation on the active HA:

1. The CP on the active-HA receives a Registration Revocation Message. The CP sends a Registration Revocation ACK with error code to the FA, if any parsing failure or authentication failure with FHAE.
2. The CP sends binding information to the corresponding TP using IPC reliable mechanism to delete the binding. During Delete Request, the CP does not wait for the response from TP.
3. The CP on the active-HA sends a binding delete request to it's peer.
4. The CP delete binding information for the MN.
5. The CP sends a Registration Revocation Ack with MN address and error code as **0.**

The following information is updated from the CP to the TP for binding:

- Message Type and Error Code
- MN Home-Address
- Home-Agent Address
- Care-of-Address

Registration Revocation Acknowledgement on Active-HA

The CP on the active-HA receives a Registration Revocation ACK for corresponding Registration Revocation Message that is sent by the active-HA. The CP does not take any action to update the TP for updating binding information, but it does complete FHAE or IPSec Authentication.

COA Received on Active-HA

The following call flow highlights the procedure for COAs received on the active HA:

1. The CP on the active-HA receives a COA and the CP does authorization for the MN. The interface between the CP and AAA servers is identical to that of Home Agent Release 4.0.
2. If the authorization fails for the MN, the CP sends COA NAK Error Code to the AAA Server.
3. The CP sends COA NAK if any failure occurs while parsing hotline information to the AAA Server. The CP does not update any information to the TP, or to the standby-HA.
4. The CP sends interim update information to the corresponding TP using IPC reliable mechanism without waiting for response. It also sends interim update information to the standby-HA CP over UDP/IP, and respond to AAA with COA Ack.
5. If acknowledgment is received by the CP without an error code from the TP, the CP does not take any further action.
6. If failure happens due to timeout or received invalid response from the TP, the CP deletes the binding and initiates a “binddeleterequest” to the standby-HA. A Registration Revocation Message is sent to the FA if revocation is enabled on HA.

The following information is updated from the CP to the TP for binding,

- MN Address
- HA IP Address
- Hotline basic Information
- Hotline accounting Indication
- List of Hotline rules/profiles as NVSEs.

POD Received on Active-HA

The following call flow identifies the procedure when POD is received on an active HA:

1. The CP on the active-HA receives a POD and CP does authorization for the MN. The interface between the CP and AAA servers is identical to that of Home Agent 4.0.
2. If the suthorization fails for the MN, the CP sends a POD NAK Error Code to the AAA Server.
3. The CP constructs a Registration Revocation Message for the MN Address and sends it to the corresponding care-of-address.
4. The CP sends binding information to the corresponding TP using IPC reliable mechanism to delete the binding. During Delete Request, the CP does not wait for the response from the TP.
5. The CP on the active-HA sends a binding delete request to its peer.
6. The CP deletes the binding information for the MN.
7. The CP waits to receive a Registration Revocation Ack with MN address and error code as **0**. If a timeout occurs before getting a response, the HA re-tries with a Registration Revocation to the PDSN.

Procedures on Standby Home Agent

The CP on the standby Home Agent will update Traffic Processors in two cases of active/standby synchronization.

- Dynamic Sync
- Bulk Sync

Bind UpdateRequest received by CP on Standby-HA during Dynamic-Sync

The following call flow describes how the standy-HA will handle a “BindUpdate Request” from the active-HA for Registration/Re-Registration of MN.

1. The standby-CP receives “BindUpdateRequest” from the active-CP, and the standby-CP does authorization for the MN. This validates the received “BindUpdateRequest”.
2. If the HHAE authentication failed between the active/standby-HA, the standby CP sends a “BindUpdate Ack” with finite error code.
3. On successful authorization, the CP creates binding on received Home-Address. And the CP looks at the hash table to get the one TP ID based on the assigned MN address.
4. The CP updates binding information to the corresponding TP using IPC reliable mechanism without waiting for response. It acknowledges the active-HA with “bindudpate ack”.
5. If acknowledgment is received by the CP without error code from the TP, the CP does not take any action.
6. If failure happens due to timeout or received invalid response from the TP, the CP deletes the binding on the standby-HA. The binding deletion on standy-HA should not interfere with the active-HA binding information.

The following information shall be updated from the CP to the TP for binding,

- RRQ Header - Is based on RFC 3344.
- SPI of MHAE as an extension
- NAI extension
- Multipath NVSE
- Revocation Support Extension,
- Address Type CVSE - It will indicate DHCP Address allocation for MN
- MR dynamic Network NVSE
- Static/Dynamic pool name
- Class attribute - if received, this is only for Accounting purpose
- CUI - if received, this is only for Accounting purpose and wimax subscribers
- Accounting multi session id, accounting interim interval - for wimax subscribers.
- VRF name and corresponding HA IP address, if present.
- In and Out Acl Names
- Hotline basic Information
- Hotline accounting Indication
- List of Hotline rule/profile based as NVSEs.

BindDeleteRequest received by CP on Standby-HA during Dynamic-Sync

The following call flow describes how the standby-HA handles a “BindDelete Request” from the active-HA after receivinga De-Registration/Revocation Request/POD for MN.

1. The standby-CP receives a “BindDeleteRequest” from the active-CP, and the standby-CP does authorization for the MN.
2. If the HHAE authentication fails between the active/standby HA, the standby CP sends a “BindDelete Ack” with finite error code.

3. On successful authorization, the CP sends binding information to the corresponding TP using IPC reliable mechanism to delete the binding. During the Delete Request, the CP does not wait for the response from the TP.
4. The CP sends "BindDelete Ack" with MN address and error code of **0** to the active-HA.

The following information is updated from the CP to the TP for binding:

- Message Type and Error Code
- MN Home-Address
- Home-Agent Address
- Care-of-Address

BindInterimUpdate received by CP on Standby-HA during Dynamic-Sync

The following call flow describes how the standby CP handles a "BindInterimUpdate" message during dynamic-sync:

1. The standby-CP receives "InterimUpdateRequest" from the active-CP, and the standby-CP performs authorization for the MN.
2. If the HHAE authentication fails between the active/standby-HA, the standby-CP sends "InterimUpdateAck" with finite error code.
3. On successful authorization, the CP updates the Interim Update information with hot-lining rules to a binding that was already created on the CP.
4. The CP updates the binding information to the corresponding TP using IPC reliable mechanism without waiting for response. It acknowledges the active-HA with a "interimupdate Ack" with error code of **0**.
5. If acknowledgment is received by the CP without an error code from the TP, the CP does not take any action.
6. If failure occurs due to a timeout or it receives invalid response from the TP, the CP deletes the binding on the standby-HA. The binding deletion on the standy-HA should not interfere with active-HA binding information.

The following information is updated from the CP to the TP for binding:

- MN Address
- HA IP Address
- Hotline basic Information
- Hotline Accounting Indication
- List of Hotline rules/profiles as NVSEs.

BindUpdateRequest received by CP on Standby-HA during BulkSync

During Bulksync, the active-HA CP sends binding information for multiple bindings to the CP on the standby-HA. After successful creation of each binding on the standby-HA CP, the binding information is updated to the TP through IPC mechanism without waiting for the response.

At any stage, the CP-TP response message status should not interfere with the bulk sync message flow. Once the response is received, the "bindupdaterequest" message treatment is applicable on that binding.

Miscellaneous Cases

During a MIP Session Termination due to Hotline Timer Expire, no update is sent from the CP to the TP on the active/standby HA. The binding information is automatically deleted on the CP/TP of the active/standby HA once the hotline timer expires.

During a MIP Session expire based on Registration Lifetime, the above functionality is also applicable on the binding.

Single Interface for Failover

The current SAMI failure mode is for a per-processor failure whenever possible. For the single IP model, a failure detected on the blade will result in a blade level failover, even if a processor-level failover is sufficient. This includes interface failures in so far as they are detectable by the SAMI platform. This requires platform support for such a failure mode.

Operation and Management

This section discusses features that fall under the umbrella of Operation and Management.

Chassis-Wide MIB for Application Related Parameters

This feature provides a single MIB within which all application related parameters are reported across the chassis. For the Home Agent, this functionality is provided on a per-Home Agent instance basis.

For all Home Agent instances on a single service blade, this information is available through a SNMP Get to a single IP address. The information is available in the CISCO-MOBILE-IP-MIB and in the CISCO-IP-LOCAL-POOL-MIB. The SNMP manager is responsible for executing the necessary number of SNMP GET operations to retrieve a MIB per Home Agent instance. This release of the Single IP Home Agent feature supports one Home Agent instance per service blade, thereby reducing the number of Get operations from 12 per service blade to 2.

Reporting of Chassis-Wide Loading on a Per Application Instance Basis

Service Provider networks typically use AAA capabilities to dynamically assign a Home Agent for a subscriber at the time of subscriber network entry. The criteria for Home Agent selection varies by Service Provider. Service Providers want proof of the loading of each Home Agent instance configured in a chassis, not the chassis as a whole. This loading is based on IP address pool usage within that Home Agent instance.

This information is contained in the CISCO-IP-LOCAL-POOL-MIB. This information allows Home Agent instance selection based solely on IP address pool usage. The MIB contains statistics of InUse addresses and Free Addresses on both a per-pool and a per-pool group basis. The AAA server is responsible to use this information per-IP pool and pool-group configured at the Home Agent instance.

In addition, the SNMP traps triggered on pool usage threshold crossing are sent to the same SNMP host that retrieves the CISCO-IP-LOCAL-POOL-MIB.

Trap Generation for AAA Unresponsiveness

This feature allows the HA to send a new SNMP trap/notification to the NMS server when the HA is authenticating MNs, and notices that the AAA is unresponsive. The trap is added when a timeout occurs. It is now possible to set a threshold (defined as a percentage of the maximum response time) on round trip delay, and generate a trap when that threshold is exceeded. An additional trap is generated when the round-trip delay falls below a second threshold.

For each RADIUS server, you can configure the threshold percentage values (*normal* or *high*). When the round-trip time of RADIUS messages between the HA and AAA server goes above or below the configured threshold values, a notification is sent to the NMS server indicating AAA server un/responsiveness. Similarly, when the number of RADIUS retransmit messages goes above or below the configured threshold values, an SNMP trap/message is sent to the NMS server indicating AAA server un/responsiveness.

The RADIUS-CLIENT-AUTHENTICATION-MIB contains entries for timeout on AAA access. The trap is added in the CISCO-RADIUS-MIB.

To enable this feature, perform the following tasks:

	Command	Purpose
Step 1	`Router(config)# radius-server snmp-trap timeout-threshold normal high`	Enables you to generate SNMP traps that denote AAA unresponsiveness. *normal* is the normal threshold in percentage, used to generate traps. *high* is the high threshold in percentage, used to generate traps.
Step 2	`Router(config)# radius-server snmp-trap retrans-threshold normal high`	When this command is configured, a trap (SNMP notification) is generated when round trip time or retransmit value goes above the high threshold value and comes below the normal threshold value. The trap is generated for either round trip time or retransmits time. *normal* is the normal threshold in percentage, used to generate traps. *high* is the high threshold in percentage, used to generate traps.

Note This feature is only supported only on the Cisco SAMI card on the 7600.

The RADIUS-CLIENT-AUTHENTICATION-MIB contains entries for timeout on AAA access. A trap is added based on this timeout occurring. It is also possible to set a threshold on round trip delay (defined as a percentage of the maximum response time), and generate a trap when that threshold is exceeded. An additional trap is generated when the round-trip delay falls below a second threshold. This provides a level of delay for trap generation.

Show Subscriber

This feature provides—from a single point in the chassis—summary listings of subscribers hosted by the Home Agent instances in the chassis. The Home Agent 5.0 Release supports a single Home Agent instance per service blade, so the sequence of steps necessary is limited to requesting the desired information using IOS CLI commands for one, or all, service blades.

The HA Named Service corresponds to the name configured using the IOS **hostname** command for the Home Agent instance on the service blade.

Table 3-1 lists the feature's functionality:

Table 3-1 List of Show Subscriber Functionality

All	Summary of all users on the chassis	To display the total of all registered users on the chassis, use the **show ip mobile binding summary** command on the control processor once per active service blade. The total from each blade is then summed, and the result displayed at the supervisor where the capability was initiated. There is a maximum number of subscribers that can be displayed for a single command. We recommend a value of 1000. If the number of registered subscribers is greater than that, the output is saved to a file, and the name and location of the file is indicated to the user.
Card	Summary of all users on one specific Card/Slot	To display the total of all registered users on one service blade, use the **show ip mobile binding summary** command on the control processor of the service blade identified with the desired result being the **total** line
CPU	Summary of all users on one specific CPU	To display the total of all registered users on a given traffic processor on a service blade, use the **show ip mobile binding summary** command on the service blade, plus the TP identified in the command.
Lifetime	Summary of all users with MIP Lifetime >, <, = to a value	This option filters the output by Granted Registration Lifetime. The raw output is generated using the **show ip mobile binding** command. This can be executed for All, Card or CPU.
LifetimeRem	Summary of all users with MIP Lifetime Remaining >, <, = to a value	This option filters the output by Remaining Registration Lifetime. The raw output is generated using the **show ip mobile binding** command. This can be executed for All, Card or CPU.
Connect	Summary of all users with A Connect Time >, <, = to a time value	This option displays the time since the subscriber first registered, not the time since the last re-registration

Table 3-1 List of Show Subscriber Functionality (continued)

FA	Summary of all users from a specific FA IP address	This option filters the output by Foreign Agent IP address. The raw output can be generated using the **show ip mobile binding** command. This can be executed for All, Card or CPU.
HA	Summary of all users from a specific HA IP address	Use this option to determine the Home Agent instance corresponding to the Home Agent IP address, and then configure the **show ip mobile binding** command on the control plane processor of that Home Agent.
HA-Name	Summary of all users from a specific HA Named Service	Use this option to determine the Home Agent instance corresponding to the Home Agent Name, and then configure the **show ip mobile binding** command on the control plane processor of that Home Agent. The Home Agent name is defined by the **hostname** command in the service blade configuration.
Pool	Summary of all users from a specific Pool Name or Pool Group	The raw output for this command is provided by the **show ip local pool** command which will provide the ip address range(s) of those pools. Based on this, the relevant information can be retrieved using the show ip mobile binding and show ip mobile host commands.
CallType	Summary of all users for this Call Type (could be something like MIP, WiMax, 3G, PDIF, etc)	This is filtering by Access-Type. The raw output can be generated using **show ip mobile binding**. The access type supported by a Foreign Agent is determined by the **show ip mobile** command. This can be executed for All, Card or CPU.
NAI/User	Summary of all users for this NAI (must support wildcards in the NAI). Example “show user summary nai *ptt*” for finding Push to Talk users on the box.	This is filtering by wild-carded NAI. Native IOS CLIs do not support such a wild-carding concept. The raw output can be generated using ‘show ip mobile binding’. This can be executed for All, Card or CPU.
ACL-IN	Summary of all users that were assigned this Input ACL	This is filtering by Input ACL. The raw output can be generated using **show ip mobile binding**. This can be executed for All, Card or CPU.
ACL-OUT	Summary of all users that were assigned this Input ACL	This is filtering by Output ACL. The raw output can be generated using **show ip mobile binding**. This can be executed for All, Card or CPU.

Here is a list of the possible output display formats:

- Summary - Totals without reporting per user information
- Summary Traffic - adds traffic totals, Bytes In/Out, Packet In/Out, Dropped In, Dropped Out by ACL, provided by show ip mobile host command.
- Brief - Single line of output per user matching the command filters. The output comprises the assigned IP address, NAI, Home Agent IP address, Foreign Agent IP address, Remaining Registration Lifetime
- Brief Traffic - As for 3 above plus the traffic totals, Bytes In/Out, Packet In/Out, Dropped In, Dropped Out by ACL, from the show ip mobile host command.
- Verbose - Full display as provided by the combined outputs of the show ip mobile binding and show ip mobile host commands
- Verbose MIP - Full display as provided by the output of the show ip mobile binding command

The output of the **summary** command gives you a count of the number users that match the query option. It also tallies of Bytes In/Out, Packet In/Out, Dropped in.Out by ACL etc.

This feature is supported under the umbrella of OSLER for Home Agent. Please refer to the OSLER section of this chapter for more information.

This functionality is not supported through SNMP.

Intra-Chassis Configuration Synchronization

This feature provides that any configuration command executed on the active blade will automatically be synchronized on the partner standby blade. This applies to all commands except those used to configure the active/standby partnering model (**ip mobile home-agent redundancy**), and those for configuring HSRP (**standby**) as a failure detection mode for redundancy.

Note It is not possible to execute configuration commands on the standby Home Agent. EXEC commands are permitted.

How an active or standby HA is determined is based on the RF infrastructure used for SSO support, as well as for Session Redundancy support for various mSEF gateways.

Initialization

The SSO configuration synchronization happens automatically during bootup without any pre-required configurations. The same cannot be applied to the Home Agent as IP connectivity between the redundant units is required prior to RF negotiation, so different yet related configurations are necessary for the Active and Standby blades.

Additionally, the SSO configuration sync feature does not support any unique configuration on each of the redundant units. On the Home Agent, HSRP and RF Interdev protocols are required, both of which require certain unique configurations on the redundant units.

The existing commands that require unique configurations for each unit are modified to accommodate configurations for the peer unit in that same command. A new command identifies the peer slots. These commands are parsed and the RF negotiation state RF_PROG_STANDBY_CONFIG is used to trigger configuration sync automatically.

RF Client

As in the case of SSO configuration sync, the Home Agent configuration sync is also an RF client. The configuration sync feature registers a callback with RF for the progression events and status events. The RF notifies each of these registered clients in order with the progression of events and any status events. This allows the HA to know when to sync the configuration files.

Configuration Files and Synchronization

Here is a brief explanation of the startup configuration and running configuration process that comprises the configuration synchronization feature.

The startup configuration is stored in NVRAM as a text file. This file is synced whenever you perform operations such as “write memory”, “copy running startup”, etc. If the file is opened for a write operation, when it is closed the sync is initiated.

A running configuration sync is dynamically generated by certain operations, so any time the sync is performed the running configuration must be generated.

In the SSO implementation, before the sync process begins, the primary is locked. A bulk sync of the startup configuration and the running configuration is performed. After that is completed, the parser mode sync is done.

After both the processors are in sync and the primary is unlocked, the line-by-line sync begins.

All of the above syncing processes require a transport mechanism to communicate between the redundant units, and currently each of the platforms uses either IPC or some other transport mechanisms.

The Home Agent configuration sync feature could use one the following transport mechanisms:

- Reliable IPC mechanism currently being used for CP-TP messaging
- RF/CF SCTP-based approach for IPC messaging
- New SCTP-based approach for IPC messaging

The first is the fastest solution from an implementation perspective but it does not scale well for an Inter-chassis solution. Currently we use the second option, RF/CF SCTP.

Startup Configuration Sync

In the SSO implementation the Startup config is synced during bootup right when the RF state is ready to perform bulk sync. You must lock the router prior to initiating the startup config sync. The same design is adopted for the Single IP Home Agent configuration sync feature.

When a **write memory** or **copy** *file1* **startup-config** is executed there are two ways to hande the scenario:

- Bulk sync the startup configuration file.
- Perform a line-by-line sync of the EXEC command.

The second option is used for the SSO feature, but for the Single IP Home Agent the first option is used because it allows the active unit to save configuration changes to the standby location.

Running Configuration Sync

With a running configuration sync, the redundancy units carry the same state of information.

Initially, after the secondary unit establishes RF Interdev communication, the running config file is bulk synchronized. The bulk sync will induce a self-reload of the standby unit if the running configuration has changed on the active unit prior to its bootup. After the reload, the standby will come up with the running config of the active unit.

After this the line-by-line sync occurs between the two units. As you configure each command, the same command is passed on to the secondary side after executing the same on the primary.

The bulk sync of the running configuration is done using the RCSF in the SSO implementation, and the same is done (using the RF Interdev SCTP) for the Single IP Home Agent feature.

Bulk Sync

RF Interdev communication needs to be established between the two units prior to initiating the bulk sync. Each unit will parse it's startup configuration and this will cause the unit to become active / standby. The active unit will then bulk sync its running and private configuration files to the standby if there has been running/private config modifications on it post bootup. After the bulk sync, the standby will reload itself and come up with the altered configs. During this standby reload phase, no configurations are allowed on the active unit.

The configurations that are synced during initialization include:

- Private configuration
- Running configuration

The startup configuration is not synced because the startup config files in the SUP are always in sync.

If a private configuration is changed after bootup, the active unit copies its private configuration file into a buffer and transports the same using RF Interdev SCTP to the standby

If running configs change after bootup, the active unit copies its running config file into a buffer and transports it using RF Interdev SCTP to the standby end

After both the previous steps are complete, the active sends a message to the standby to commence parsing the received buffers

The standby unit save the received buffer contents locally, and reloads itself so as to apply the modified to itself.

Line by Line Sync

When both active and standby units are up and running, the CLI entered from the active unit is executed first, the same command is propagated to the standby and executed, and returns the result back to active.

The Parser Return Code (PRC) scheme is used in the SSO implementation to have all the parser action routine for each CLI command set the return code. This return code is a combined form of all the following information including the class of the error code, component id, sync-bit, sub-code, etc.

Parser Mode Synchronization is an effort to maintain the same parser mode between Active and Standby units before a command is sent to Slave for synchronization.

In the SSO implementation syncing Process is done through RPC, which is blocking the current process until active RP receives return code message from standby RP. Thus, the commands are executed in order for both units.

If a command fails on standby unit, then the result is conveyed back to active. On the active, a stub registry for policy maker is invoked, and leaves the decision on what to do with the returned result to the calling/upper layer.

The Single IP Home Agent configuration sync feature will use the SSO line by line sync implementation as is.

Configuration Details

Since configurations must be synced as is, the CLIs on both the units should be the same. The following commands are currently unique to each redundant unit, and have been modified:

- **ipc zone default**
- **association** *no>*
- **protocol sctp**
- **unit1-port** *port1*
- **unit1-ip** *ip1*
- **unit2-port** *port2*
- **unit2-ip** *ip2*

The following new CLI's are introduced:

```
interface GigabitEthernet0/0.23
redundancy ip address unit1 <ip1> <mask1> unit2 <ip2> <mask2>
```

The **redundancy ip address** command CLI is a per-interface CLI. The HSRP protocol uses this IP address configured for its negotiation, and not the one configured using the regular **ip address** command. The **ip address** configuration is not required for a sub-interface which is dedicated for HSRP negotiation with the peer.

```
redundancy unit1 slot <x> unit2 slot <y>
```

This is a global configuration and is used for identifying the peer slot.

To configure Intra-chassis Configuration Synchronization, perform the following tasks:

```
redundancy unit1 slot <x> unit2 slot <y>

unit1-port <portnum> , unit2-port <portnum> under the ipc-assoc-protocol-sctp mode

unit1-ip <address1> , unit2-ip <address2> under the ipc-unit1-port and ipc-unit2-port
modes respectively

redundancy ip address unit1 <address1> <mask1> unit2 <address2> <mask2> Under the
interface and sub-interface modes
```

Here is the sequence of configuration steps, and must be performed on each of the cards.

	Command	Purpose
Step 1	`Router#show redundancy states`	Execute the following commands on both SAMIs before running any redundancy commands. **my state** should be active on both the cards.

Step 1	`Router(config)# redundancy inter-device`
	
	`redundancy unit1 slot 9 unit2 slot 6`
	
	`interface GigabitEthernet0/0.2`
	`encapsulation dot1Q 20`
	`redundancy ip address unit1 4.0.0.1`
	`255.255.255.0`
	`unit2 4.0.0.2 255.255.255.0`
	`standby 0 ip 4.0.0.4`
	`standby 0 name hsrp`
		Enables intra-chassis configuration synchronization.
		
		Configures global redundancy unit-slot mapping.
		
		Configures an interface for HSRP.
		
		HSRP needs unique IPs for the standby and active units and you need to use the **redundancy ip address** command.
		
		Note Do not configure the **ip address** command on this interface.

Step 2	`Router(donfig)# redundancy unit1` *hostname name 1* `unit2` *hostname name2*	Used to identify and configure the peer slot in the same chassis.

Step 3	`Router(config)# redundancy inter-device`
	`scheme standby hsrp`
	
	`ipc zone default`
	`association 1`
	`no shutdown`
	`protocol sctp`
	`unit2-port 5000`
	`unit2-ip 4.0.0.2`
	`unit1-port 5000`
	`unit1-ip 4.0.0.1`
		Associates the HSRP scheme name to the RF Interdevice.
		
		Configures ipc information for the RF Interdevice.

After you execute the above configuration, save the configs and reload one of the cards (standby is preferred). Once they come up they will do an HSRP negotiation followed by an RF Interdev negotiation after which the configuration sync feature sets in. The above steps are the same as are needed to get RF Interdev working on a fresh card for the first time.

Monitor Subscriber

This feature allows you from a single point in the chassis to establish conditional debugs based on NAI or assigned IP address. This is possible without knowing which Home Agent instance in the chassis hosts the subscriber session or is selected to host the subscriber session for cases when the session is not yet established. This feature make use of the OSLER tool that allows centralized execution of IOS commands with the ability to receive responses and present those responses in a clear and concise format.

There will be two output formats, **brief**, where the debug output is succinctly presented, and **verbose** which is the full debug output available.

The operator must login to the Supervisor of the 7600, and then execute the command debug condition “qualifier” protocols, or something similar.

A two-stage process will result.

1. Determine the Home Agent instance in the chassis hosting the session.
2. If a session is present, apply the **debug** conditional command on that Home Agent instance and then apply the specific **debug** commands requested. If no session is present, establish a pre-trigger condition for debug followed by the requested **debug** commands on all Home Agent instances configured in the chassis.

It is possible to specify the protocol subsystems for which conditional debugging applies. The choices are all, mobile-ip or aaa (including Radius).

There is a limit of 10 simultaneous monitored subscribers per chassis. But there is no restriction on distribution of those monitored subscribers across blades within a chassis.

Only 1 subscriber can be monitored per monitoring session. To monitor 10 subscribers, you must establishe10 independent monitoring sessions.

The **verbose** output format comprises all debugs generated by IOS for the selected protocols. This is a large amount of information that requires expert analysis to be useful. The **brief** format is a subset of the possible debugs.

There are no changes required to the **debugs** available within the Home Agent IOS code base.

This feature is supported under the umbrella of OSLER for Home Agent. Please refer to the OSLER section for more specific information.

Show Subscriber Session

You “login” to the Supervisor of the 7600 and then execute the **show subscriber session** command where the subscriber is identified by NAI or IP address.

This results in a two step process:

- Determine the Home Agent instance in the chassis hosting the session
- Execute the commands for **show ip mobile host** ***ip-address*** **| nai**, **show ip mobile secure host** *ip-address* **| nai**, **show ip mobile violation address | nai** *string* and **show ip mobile host-counters**.

Bulk Statistics Collection

This feature is capable at a single point, to perform the following functions:

- To initiate the periodic collection of the available Home Agent statistics, identifiable by name, from each active service blade in the chassis.
- To collect the specified statistics by enabling IOS Bulk Statistics collection at each selected service blade. This mechanism allows the collection of statistics for MIB variables. If the required measure is not part of a MIB, it cannot be collected as part of the bulk statistics collection feature.
- To transfer the file to an external TFTP server identified by a URL.

You can set the statistics collection period in 15 minute increments, the minimum collection period being 30 minutes. The maximum collection period is 24 hours.

The file content contains summary statistics for each blade except for the CPU usage and memory occupation information which are available on a per-CPU basis collected per blade. The per-blade file has an entry for each application CPU on that blade.

The file format comprises a sequence of “variable_name value” pairs separated by commas.

In HA Release 5.0, the variable name will be the OID of the variable as this is the level of support available from the IOS Bulk Statistics Collection CLI.

There are a predefined set of statistics that are collected, including the variables available in the MIBs supported by the Home Agent application. The OID assigned to the statistic corresponds directly to the OID in the related MIB.

The following variables of interest are not present in a MIB. These will not be supported as part of the Bulk Statistics Collection feature:

- HARegRevocationsSent
- HARegRevocationsReceived
- HARegRevocationsIgnored
- HARegRevocationAcksSent
- HARegRevocationAcksReceived
- HARegRevocationAcksIgnored

The time-period over which collection is made is indicated in the file in the form of period yy:mm:dd:hh:mm:ss yy:mm:dd:hh:mm:ss. The first date is the start, the second date the end.

If you want to alter the set of subsystems for which statistics collection is enabled, you must first cancel the ongoing statistics collection and initiate and a new collection. Any information that you collect during the cancelled session will be saved.

In the event that the external server is unavailable, the file is saved in local non-volatile memory. The last transferred file is saved locally until the next file is successfully transferred. On successful transfer of the new file, the currently saved file is replaced with the new one.

No new IOS commands are used to support the bulk statistics feature in the Single IP Home Agent Release 5.0.

Redundancy Support in Home Agent Release 5.0

Redundancy support for Home Agent 5.0 features is identical to Release 4.0 of the Home Agent with the exception of the Home Agent Accounting, MIP-LAC, Mobile Router, VRF, and Home Agent as LNS features.

The active—standby redundancy interaction is between the control processors of the active and standby service blades.

Performance Requirements

The Single IP Home Agent will support the following performance figures:

- 500,000 registered subscribers per service blade
- 5 Gbps throughput.
- The time required to bulk-sync an Active Home Agent service blade hosting 500,000 subscriber registrations to a reloaded Standby Home Agent service blade will take no longer than the time taken to bulk-sync a fully loaded Active to Standby service blade in the “six independent processor” model. There is no intention to proportionately reduce the bulk-sync time from x to x * (500,000 / 1,400,000).
- The call per second rate is no slower than for a single processor in the “six independent processor model”. The call per second rate meets or exceeds the rate measured during performance verification for Sprint.

Single IP Support - Reused and New CLIs

The following CLIs are provided to allow IPC to communicate with IXP, and to allow GTP and IPC over GTP modules to provide the reliable, acknowledged and unacknowledged communication capability between the SAMI PPCs:

EXEC Mode

- **debug sami ipc gtp ipc 3-8>**
- **debug sami ipc gtp ipc**
- **debug sami ipc gtp any**
- **debug sami ipc detail**
- **debug sami ipc**
- **debug sami ipc stats detail**
- **debug sami ipc stats**
- **debug sami configuration sync**
- **test sami tp-config [enable|disable]** (available on TPs in SingleIP image)

Show Commands

- **show sami ipcp ipc gtp**
- **show sami ipcp ipc ixp**
- **show sami ipcp ipc processor**

Config Mode:

- **default sami ipc crashdump**
- **default sami ipc keepalive**
- **default sami ipc retransmit**
- **default sami ipc retries**
- **sami ipc crashdump**

- **sami ipc keepalive**
- **sami ipc retransmit**
- **sami ipc retries**

Distributed Configuration on Single IP Home Agent

The Distributed CLI agent distributes the configuration information from the CP to each of the TPs using the IPC protocol.

By default, the CLI agent allows all the commands, but only filter the ones that might trigger some functionality on the TP that is not needed.

For the single IP model, an EXEC banner is displayed when logging in to a TP and warns the user to be aware that "normal" maintenance activities should be run from CP.

Table 3-2 lists the commands that Home Agent Single IP supports, and indicates whether they are filtered at the CP or also sent to the TPs.

If the command is sent to the TPs, then it is executed at each of the TPs.

Table 3-2 Home Agent Commands for Single IP

Command (Config Commands)	Purpose	To be filtered at Control Processor
aaa authentication ppp default group radius	Enables authentication of PPP users using RADIUS.	No
aaa authentication login default group radius	Specifies RADIUS as the default method for user authentication during login.	No
aaa authorization commands	Reestablish the default created when the **aaa authorization commands** command was issued,	No
aaa authorization ipmobile default group radius	Authorizes Mobile IP to retrieve security associations from the AAA server using RADIUS	No
aaa authorization network default group radius	Restricts network access to a user. Runs authorization for all network-related service requests. Uses the group radius authorization method as the default method for authorization.	No
aaa accounting network default start-stop group radius	Enables accounting by sending a "start" accounting notice at the beginning of a process and "stop" accounting notice at the end of a process to RADIUS servers.	No
aaa accounting system default start-stop group radius	Enables the HA to send system messages.	No

Table 3-2 Home Agent Commands for Single IP (continued)

aaa accounting update newinfo	Enables an interim accounting record to be sent to the accounting server whenever there is new accounting information to report relating to the user in question.	No
aaa session-id common	Ensures that all session identification (ID) information that is sent out for a given call will be made identical.	No
aaa server radius dynamic author	Enables support for received Change of Authorization message	No
radius-server host *ip-addr* **key** *sharedsecret*	Specifies the IP address of the RADIUS server host and specifies the shared secret text string used between the router and the RADIUS server.	No
radius-server retransmit *retries*	Specifies the number of times the Cisco IOS software searches the list of RADIUS server hosts before giving up.	No
radius-server vsa send authentication 3gpp2	Enables the use of vendor-specific attributes (VSA) as defined by RADIUS IETF attribute 26. Limits the set of recognized vendor- specific attributes to only authentication attributes.	No
radius-server vsa send accounting 3gpp2	Enables the use of vendor-specific attributes (VSA) as defined by RADIUS IETF attribute 26. Limits the set of recognized vendor-specific attributes to only accounting attributes.	No
radius-server vsa send authentication wimax	Enables use of WiMax specific attributes	No
radius-server vsa send accounting wimax	Enables use of WiMax specific attributes	No
radius-server snmp-trap retrans-threshold *50 - 75*	Generates a trap (SNMP notification) when a retransmit value goes above the high threshold value, and comes below the normal threshold value.	No
radius-server snmp-trap timeout-threshold *50 - 75*	Generates a trap (SNMP notification) when a round trip value goes above the high threshold value, and comes below the normal threshold value.	No

Table 3-2 Home Agent Commands for Single IP (continued)

router mobile	Enables mobile IP on the router	No
ip mobile host {*lower* [*upper*] | **nai** *string* [**static-address** {*addr1* [*addr2*] [*addr3*] [*addr4*] [*addr5*] | **local-pool** *name*}] [**address** {*addr* | **pool** {**local** *name* | **dhcp-proxy- client** [**dhcp-server** *addr*]}]} {**interface** ***name*** | **virtual-network** *network-address mask*} [**aaa** [**load-sa** [**permanent**]]] [**authorized-pool** *name*] [**skip-aaa-reauthentication**][**care-of-access** *access-list*] [**lifetime** *seconds*]	Configures mobile host or mobile node group (ranging from lower address to *upper* address group) to be supported by the home-agent.	No
ip mobile virtual-network *netmask* [**address** *address*]	Defines a virtual network	No
router(config-if)#standby [*group-number*] **ip** ***ip-address***	Enables HSRP	Yes
router(config-if)#standby [*group-number*] [**priority** *priority*] **preempt** [**delay** [**minimum** | **sync**] *delay*]	Sets the Hot Standby priority used in choosing the active router.	Yes
router(config-if)# standby name *hsrp-group-name*	Sets the name of the standby group	Yes
ip mobile home-agent redundancy *hsrp-group-name*	Configures the Home Agent for redundancy using the HSRP group name.	Yes
ip mobile secure home-agent *address* **spi** *spi* **key hex** *string*	Sets up the Home Agent security association between peer routers.	Yes
ip mobile home-agent dynamic-address *ip address*	Sets the Home Agent Address field in the Registration Response packet. The Home Agent Address field will be set to ip address.	No
ip mobile home-agent revocation	Enables support for MIPv4 Registration Revocation on the HA	Yes
interface tunnel *10*	Configures a tunnel template.	No
ip mobile home-agent template tunnel *10* **address** *10.0.0.1*	Configures a Home Agent to use the template tunnel.	No

Table 3-2 Home Agent Commands for Single IP (continued)

ip mobile home-agent accounting *list*	Enables HA accounting, and applies the previously defined accounting method list for Home Agent. List is the AAA Accounting method used to generate HA accounting records.	Nn
ip mobile home-agent *method* **redundancy [virtual-network address** *address*] **periodic-sync**	Syncs the byte and packet counts for each binding to the standby unit using an accounting update event. This sync only occurs if the byte counts have changed since the last sync.	No
ip mobile realm *realm* **hotline redirect** *redirect-server-ipaddress*	Enables inbound user sessions to be disconnected when specific session attributes are presented.	No
ip mobile home-agent dfp-max-weight *dfp-max-weight-value*	This command enables the maximum dfp weight that can be allowed on HA. By default, the max dfp weight value is 24.	**No**
ip mobile home-agent max-cps *max-cps-value*	This command enables the maximum cps that can be allowed on HA. By default, the max cps value is 160cps with accounting support.	**No**
ip mobile home-agent max-binding *max-binding-value*	Limits the number of bindings that can be opened on the HA. The default value of max-binding-value is 235,000.	No
ip mobile home-agent host-config url *url*	As part of this feature, a new CLI has been introduced to configure the URL on the HA. This is needed as sometimes HA will not be able to provide the configs requested by MN. To address this situation this generic site specified by the URL will help MN to download its configs parameters. Sample configuration: **ip mobile home-agent host-config** url http://www.cisco.com	No
ip mobile realm *realm* **hotline capability profile-based redirect ip**	This command configures a profile-based hot-lining for users with ip-redirection rules. Here, the realm can be nai/realm. The no version of this CLI will delete the profile-based ip-redirection rules.	No

Table 3-2 Home Agent Commands for Single IP (continued)

ip mobile realm *realm* **hotline capability profile-based redirect http**	This command configures a profile-based hot-lining for users with http-redirection rules. Here, the realm can be nai/realm. The no version of this CLI will delete the profile-based http-redirection rules.	No
ip mobile home-agent aaa attribute framed-pool	Support the download of the RADIUS Framed Pool name downloaded during the authentication	No
Router(config-cmap)#**match flow mip-bind** Router(config-pmap-c)#**police rate mip-binding [bc** *bytes***] [peak-rate mip-binding [be** *bytes***]]**	To classify packets for each binding, belonging to a class of MN users with a specified rate, the following CLI is configured in MQC class-map config mode. To police the individual MN binding already identified to MQC, based on the specified rate, the following CLI is specified in policy-map config mode specific to a configured class. Sample Configuration: class-map class-mip match flow mip-binding policy-map policy-mip-flow class class-mip police rate mip-binding [bc <bytes>] [peak-rate mip-binding [be <byes>]] conform-action <action> exceed-action <action> violate-action <action>	No
ip mobile home-agent service-policy [input *policy-name* **[output** *policy-name***]**	This CLI attaches the HA to QoS police function through the service-policy command. It helps identify HA by associating service-policy to the HA virtual interface object. The command is configured for both traffic directions.	No
ip local pool *poolname start_address end_address* **group** *customer-x* **priority** *0..255*	The new option “priority 0..255” is an optional to ip local pool. By configuring this option, priority will be assigned to the newly created pool and the same will be used in assigning IP Address.	No

Table 3-2 Home Agent Commands for Single IP (continued)

ip mobile realm *@xyz.com* **vrf** *vrf-name* **ha-addr** *ip-address* **[aaa-group [accounting** *aaa-acct-group* **| authentication** *aaa-auth-group*]] [**dns dynamic-update method** *word*] [**dns server** *primary dns server address secondary dns server address* [**assign**]] [**hotline**] [**ppp-regeneration** [**setup-time** *number*]]	Defines the VRF for the domain @xyz.com. The option "ppp-regeneration <setup-time <number>" will be optional to "ip mobile realm" command. By configuring this option, PPP regeneration feature will be enabled and every MIP session matching this realm will be mapped to a corresponding L2TP session.	No
router ospf *process-id*	Enables OSPF routing, which places you in router configuration mode.	Yes
network *ip-address wildcard-mask* **area** *area-id*	Defines an interface on which OSPF runs and define the area ID for that interface.	Yes
ip ospf cost *cost*	Explicitly specifies the cost of sending a packet on an OSPF interface.	Yes
ip ospf retransmit-interval *seconds*	Specifies the number of seconds between link-state advertisement (LSA) retransmissions for adjacencies belonging to an OSPF interface.	Yes
ip ospf transmit-delay *seconds*	Sets the estimated number of seconds required to send a link-state update packet on an OSPF interface.	Yes
ip ospf priority *number-value*	Sets priority to help determine the OSPF designated router for a network.	Yes
ip ospf hello-interval *seconds*	Specifies the length of time between the hello packets that the Cisco IOS software sends on an OSPF interface.	Yes
ip ospf dead-interval *seconds*	Sets the number of seconds that a device must wait before it declares a neighbor OSPF router down because it has not received a hello packet.	Yes
ip ospf authentication-key *key*	Assigns a password to be used by neighboring OSPF routers on a network segment that is using the OSPF simple password authentication.	Yes
ip ospf message-digest-key *key-id* **md5** *key*	Enables OSPF MD5 authentication. The values for the *key-id* and *key* arguments must match values specified for other neighbors on a network segment.	Yes

Table 3-2 Home Agent Commands for Single IP (continued)

ip ospf authentication [**message-digest** | **null**]	Specifies the authentication type for an interface.	Yes
access-list *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*] [**log**]	Defines a standard IP access list.	No
ip access-list {**standard** | **extended**} *access-list-name*	Define an IP access list by name.	No
snmp-server enable traps ipsec [**cryptomap** [**add** | **delete** | **attach** | **detach**] | **tunnel** [**start** | **stop**] | **too-many-sas**]	Enables the router to send IP Security (IPSec) Simple Network Management Protocol (SNMP) Notifications.	Yes
snmp-server enable traps ipmobile	Enables Simple Network Management Protocol (SNMP) security notifications for Mobile IP	Yes
snmp mib [bulkstat | community-map | notification-log | persist]	Defines bulk statistics collection	Yes

Note For any configuration command that is filtered, its sub configuration commands are also filtered.

Distributed Show and Debug

By default, all the **debug** commands are executed in the TPs, and the trace gets displayed from the CP. The CP does not perform any aggregation for distributed debug.

For debug AAA / RADIUS commands, these are executed on the TP as well as the CP but as no Radius transactions occur on the TP, the debugs will not be displayed. For example, the radius transaction corresponding to a received PoD or CoA is only handled at the CP. An internal event is passed from CP to the appropriate TP indicating that a PoD/CoA has occurred but this is not in the form of a Radius transaction.

debug ip mobile commands are not executed at the TP as, when a subscriber binding is created, this occurs at both the CP and the selected TP. Only one set of debug output is necessary.

Distributed Show - By default the show commands are not executed at all TPs. Only for the commands listed in Table 3-3 is aggregation done periodically at the CP for the data collected from the TPs (traffic counters are maintained by the TPs).

Note The **Execute On … clear** command is now a Service Internal command

The Table 3-3 lists the show and debug commands that are supported on the Single IP Home Agent for Release 5.0:

Table 3-3 show and debug Commands That are Supported on the Single IP Home Agent

Command (Show and Debug)	Purpose	Aggregation Required? (Yes/No)	Is the exec command sent to TP ?
show ip mobile binding [**home-agent** *ip-address* | **nai** *string* [**session-id** *string*] | **police [nai** *string* **]** | **summary**]	Displays the mobility binding table on the home agent (HA).	Yes	No
show ip mobile host [*address* | **interface** *interface* | **network** *address* | **nai** *string* | **group** | **summary**]	Displays mobile node information.	Yes	No
show ip mobile traffic	Displays HA protocol counters	Yes	No
show ip mobile tunnel [*interface*]	Displays information about the mobile IP tunnels.	Yes	No
show policy-map [apn *mn-apn-index* **[realm** *string* **]]**	CLI in exec mode will display aggregate policing statistics for flows across the MN-APN interface.	No	No
show ip mobile hot-line capability [realm *word***] [all]**	Display hot-line capability of username/nai or realm. If the username or realm is not specified, display information all the user or realms currently hot-lined on HA.	No	No
show ip mobile globals	Displays global information for Mobile Agents.	No	No
show ip mobile secure	Displays mobility security associations for Mobile IP.	No	No
show ip route vrf	Displays the routing table information corresponding to a VRF.	No	No
show ip mobile redundancy	Displays the redundancy status of the Home Agent.	No	No
show ip mobile secure	Displays mobility security associations for Mobile IP.	No	No
show ip mobile ipc	Displays ipc information for CP-TP interface	No	No
debug ip mobile advertise	Displays advertisement information.	No	No
debug aaa authentication	Displays information on AAA/TACACS+ authorization.	No	Yes
debug aaa pod	Displays debug information for Radius Disconnect message processing at AAA subsystem level.	No	Yes

Table 3-3 show and debug Commands That are Supported on the Single IP Home Agent (continued) (continued)

debug ip mobile [advertise | dfp | host | local-area | redundancy | router | upd-tunneling | vpdn-tunneling [events | detail]| ipc | mib]	Displays IP mobility activities.	No	No
debug ip mobile host [*acl* | **nai** | **mac** *H.H.H*]	Displays mobility event information.	No	No
debug ip mobile redundancy {**events** | **error** | **detail** | **periodic-sync**}	Displays IP mobility events.	No	No
debug radius [accounting | **authentication** | **brief** | **elog** | **failover** | **periodic-sync** | **retrans-mit** | **verbose**]	Displays information associated with RADIUS.	No	Yes
debug tacacs [**accounting** | **authentication** | **authorization** | **events** | **packet**]	Displays information associated with TACACS.	No	Yes

Only for the **show ip mobile binding** [**nai** string | ip address] command and the **show ip mobile host** [**nai** *string* | *ip address*] command, the CP will use a Pull mechanism to get the current counters from the TPs. The interval for the counters displayed in these **show** commands is too long to make them irrelevant.

Note The **clear mobile ip binding all load** command is no longer available for the Home Agent product. This is replaced by the requirement to perform a reload rather than using this command.

Show CLI Enhancements for Chassis Management

Table 3-4 lists the **show** commands are added to support the chassis-wide management interface for the Single IP Home Agent. Refer to the section for further details.

Table 3-4 Chassis Management-related show Commands

CLI Command	Purpose	Does it collect info from the TPs? (Yes/No)
show ip mobile binding fa [*coa-ip*]	Displays the mobility binding table on the home-agent with the matching care-of-address.	No
show ip mobile binding fa [*coa-ip*] **summary**	Displays the summary of mobility binding table on the home-agent with the matching care-of-address.	No
show ip mobile binding granted-lifetime greater [*time*]	Displays the of mobility binding table on the home-agent with the granted-lifetime greater than *time*.	No

Table 3-4 Chassis Management-related show Commands (continued)

show ip mobile binding granted-lifetime greater [*time*] **summary**	Displays the summary of mobility binding table on the home-agent with the granted-lifetime greater than *time*.	No
show ip mobile binding granted-lifetime equals [*time*]	Displays the of mobility binding table on the home-agent with the granted-lifetime equal to *time*.	No
show ip mobile binding granted-lifetime equals [*time*] **summary**	Displays the summary of mobility binding table on the home-agent with the grated-lifetime equal to *time*.	No
show ip mobile binding granted-lifetime less [*time*]	Displays the mobility binding table on the home-agent with the granted-lifetime less than *time*.	No
show ip mobile binding granted-lifetime less [*time*] **summary**	Displays the summary of mobility binding table on the home-agent with the granted-lifetime less than *time*.	No
show ip mobile binding remaining-lifetime greater [*time*]	Displays the mobility binding table on the home-agent with the remaining-lifetime greater than *time*.	No
show ip mobile binding remaining-lifetime greater [*time*] **summary**	Displays the summary of mobility binding table on the home-agent with the remaining-lifetime greater than *time*.	No
show ip mobile binding remaining-lifetime equals [*time*]	Displays the mobility binding table on the home-agent with the remaining-lifetime equals to *time*.	No
show ip mobile binding remaining-lifetime equals [*time*] **summary**	Displays the summary of mobility binding table on the home-agent with the remaining-lifetime equals to *time*.	No
show ip mobile binding remaining-lifetime less [*time*]	Displays the mobility binding table on the home-agent with the remaining-lifetime less than *time*.	No
show ip mobile binding remaining-lifetime less [*time*] **summary**	Displays the summary of mobility binding table on the home-agent with the remaining-lifetime less than *time*.	No

Network Management and MIBs

One focus of the Single IP design is to provide single MIB access per service blade. The result is that a number of MIBs will now have six entries, one per processor, rather than a single entry. This applies specifically to the CISCO-PROCESS-MIB and the CISCO-ENHANCED-MEMPOOL-MIB.

The other MIBs used for Home Agent management, RFC 2002 MIB, CISCO-MOBILE-IP-MIB, CISCO-IP-LOCAL-POOL-MIB, RADIUS Authentication Client MIB are not affected by this system design.

Here is a list of MIBs that are used as a source of key performance indicators (KPIs):

- RFC 2002 MIB
- CISCO-MOBILE-IP-MIB
- RFC 2618 RADIUS Authentication Client MIB
- IF-MIB
- CISCO-IP-LOCAL-POOL-MIB
- CISCO-PROCESS-MIB
- CISCO-MEMORY-POOL-MIB - Replaced by ENHANCED-MEMPOOL-MIB
- CISCO-ENHANCED-MEMPOOL-MIB

Both the CISCO-PROCESS-MIB and the CISCO-MEMORY-POOL-MIB are required to provide a single MIB report per service blade. Both of these MIBs contain per-processor content. Because the design requires that the information for all six application processors is reported with one SNMP GET, each MIB will contain six entries, one per application processor.

The IF-MIB will contain information for interfaces of the Traffic Plane processors in addition to the interfaces of the Control Plane processor.

The CISCO-PROCESS-MIB already contains a facility to provide information for one or more CPUs. The CISCO-MEMORY-POOL-MIB does not support this capability. Nor does the the Home Agent currently support the CISCO-ENHANCED-MEMPOOL-MIB.

The RADIUS Authentication Client MIB is not currently supported in the Home Agent image and is required.

Table 3-5 lists the supported MIBs:

Table 3-5 Single IP MIBs for HA Release 5.0

MIB	Description	Does it need info from TP?	If Yes, Mechanism
RFC2006-MIB	This uses the definitions defined in RFC 2006, *The Definitions of Managed Objects for IP Mobility Support Using SMIv2*	No, there are no traffic counters.	
CISCO-MOBILE-IP-MIB	This allows you to monitor the total number of HA mobility bindings and the total number of FA visitor bindings using an NM	No, it has only counters for control messages.	
RFC2618 RADIUS Authentication Client MIB	This uses the definitions defined in RFC 2618.	No, there are no traffic counters.	
IF-MIB	This contains information for interfaces of the Traffic Plane processors in addition to the interfaces of the Control Plane processor	Yes	Data Aggregator on CP, Data Provider on TP, follows PUSH paradigm. TP sends update to CP every minute.
CISCO-IP-LOCAL-POOL-MIB	This MIB defines the configuration and monitoring capabilities relating to local IP pools.	No, there are no traffic counters.	
CISCO-ENHANCED-MEMPOOL-MIB	This is for monitoring the memory pools of all physical entities on a managed system.	Yes	Data Aggregator on CP, Data Provider on TP, follows PUSH paradigm. Each TP sends update every second to CP.
CISCO-PROCESS-MIB	This describes the statistic of active system processes on processors running IOS, the six processor on the two daughter cards.	Yes	Data Aggregator on CP, Data Provider on TP, follows PUSH paradigm. CPU stats from TP are sent every second, other stats are sent every minute to CP.
CISCO-ENTITY-MIB	The MIB module for representing multiple logical entities supported by a single SNMP agent	Yes	Data Aggregator on CP, Data Provider on TP

Resource Requirements and Limitations

The re-architecture from a six "do-everything" processor model to a one control, multiple traffic plane model imposes some new resource constraints:

- Calls per Second figure will be bounded by the capability of a single CPU versus the previous six
- The number of supported Mobile IP bindings is limited by the memory available to the control plane processor. Home Agent 4.0 currently supports 235,000 subscribers per processor based on a memory limitation of 1Gigabyte. SAMI platform support of the Single IP Home Agent will provide 2 Gigabytes of memory per processor. Given that I/O memory does not need to be duplicated when combining the session capacity of two processors into one, HA Release 5.0 supports 500,000 subscribers per blade and does not require memory requirements in excess of 2 Gigabytes.
- Reducing the number of processors supporting user traffic from 6 to 5 requires a corresponding increase in throughput per processor of 20%. This is achieved as a result of the CEF/MFI rewrite activities of Home Agent 5.0.
- Decoupling of the control and traffic planes significantly reduces the inter-dependency of calls per second ratings and throughput achieved. The decoupling is not complete though.
- Establishing and and releasing mobile IP bindings requires inter-processor messaging between the control plane processor and the traffic plane processor chosen to provide packet routing for the user.
- The push/pull nature of the control plane to traffic plane interactions for MIB population on the control plane processor impacts both calls per second and throughput.
- The per-chassis features that require periodic retrieval of information from the service blade will impact the calls per second rating. Throughput is also affected as variables relevant to the per-chassis statistics collection are provided from the traffic plane in either a Push or Pull model.
- A tradeoff in performance occurs between Supervisor processing and service blade processing to support the various **show subscriber** command combinations.

Features Not Supported

The following features are not supported on the Home Agent 5.0 Single IP software release:

- MIP-LAC
- Mobile Router
- Home Agent as LNS
- Hotlining

Chassis Managment

The Single IP functionality depends on chassis management to provide a single OAM viewpoint for a defined set of functionality. This allows you to see whole chassis as a single black box without worrying about the multiple service blades having multiple processors, and separate active/standby configurations.

In order to get or set the right information on the right HA instance, the management commands check all the modules in the chassis, figure out the right module (active SAMI blades) and the HA instance(s) on these active blades. The Home Agent 5.0 release will have only one HA instance per service blade.

The following commands provide chassis management information, and are initiated from the active SUP card.

- **Show Subscriber**
- **Monitor Subscriber**
- **Show Subscriber Session**
- **Statistics Collection**

Restrictions

The Single IP model places some restrictions on packet routing configurations, both internal and external to the chassis.

Note You must configure the **no auto-sync all** command for an inter-chassis SR setup. For inter-chassis, the "unit1/unit2" style of configuration commands do not apply.

Note
- Dynamic routing protocols for advertizing routes for mobile subnets run at the supervisor.

Note
- OSPF runs on the CP only of each SAMI blade for the purpose of advertizing mobile subnets to the Supervisor only.

Note
- Dynamic route updates are not propagated from the CP to the TP.

Note
- Static routes must be configured from the SAMI blade to the Supervisor.

Note
- All MN-sourced traffic will be routed from the same blade to the Supervisor. This applies to both MN-Network traffic and MN-MN traffic.

Note
- Routing MN-MN traffic within a TP on a SAMI blade is not possible.

Note
- An HSRP Virtual IP Address is no longer used as the IP address of the Mobile IP tunnel termination of the Home Agent.

Note
- You must configure a loopback address at the Home Agent for use as the Mobile IP tunnel termination address.

Note
- You must configure a loopback address for interfaces to external servers such as DHCP and Radius servers. Do not use the HSRP virtual IP address.

Note
- The Standby Home Agent does not advertize routes to the Supervisor.

Note

- The Supervisor routes packets to the Home Agent blade on the SAMI using the HSRP Virtual IP address and associated HSRP Virtual Mac address.

Note

- Any physical interface used for external routing of packets must have the IP address assigned using the **redundancy ip address** command so that the active and standby have the correct address assigned when using the config-sync feature.