

IP Pool Sharing Protocol

This chapter provides information on configuring an enhanced, or extended, service. The product administration guides provide examples and procedures for configuration of basic services on the system. It is recommended that you select the configuration example that best meets your service model, and configure the required elements for that model before using the procedures in this chapter.

This chapter contains the following topics:

- Overview, on page 1
- How IPSP Works, on page 3
- Configuring IPSP Before the Software Upgrade, on page 6
- Configuring IPSP After the Software Upgrade, on page 8
- Disabling IPSP, on page 9

Overview

The IP Pool Sharing Protocol (IPSP) is a protocol that system-based HA services can use during an offline-software upgrade to avoid the assignment of duplicate IP addresses to sessions while allowing them to maintain the same address, and to preserve network capacity.

In order for IPSP to be used, at least two system-based HAs with identical configurations must be present on the same LAN. IPSP uses a primary & secondary model to manage the IP pools between the HAs. When used, this protocol ensures the following:

- In-progress sessions can be handed-off to the secondary HA when an offline-software upgrade is being performed on the primary and receive the same IP address that it was originally assigned.
- New sessions can be redirected to the secondary HA when an offline-software upgrade is being performed on the primary and receive a non-duplicate IP address.

The protocol is enabled at the interface level. Each system-based HA must have an IPSP-enabled interface configured in the same context as the HA service for this protocol to function properly.

Primary HA Functionality

The primary HA is the system that is to be upgraded. It performs the following functions for IPSP:

- Queries the pool information from the secondary HA the pool configurations on both HAs must be identical

- Assigns an IP address or address block to the secondary HA when requested by the secondary HA the primary HA releases sessions if they have an IP address requested by the secondary
- For graceful termination conditions (e.g. an administrative user issues the **reload** command), sends a termination message to the secondary HA causing it to assume the responsibilities of the primary HA until the primary is available again.
- Sends a trap when the number of calls drops to zero after starting IPSP

Secondary HA Functionality

The secondary HA is the system that takes over Mobile IP sessions from the primary HA that is being upgraded. It performs the following functions for IPSP:

- Locks the IP pools until it receives an address or address block assignment from the primary HA it unlocks the IP pools after busying out the addresses that are not assigned to it
- Processes address requests for sessions that are within the address block assigned to it
- Communicates with the primary HA, as needed, to request IP addresses that are not currently assigned to it it does not assign the address until the primary HA approves it
- For graceful termination conditions (e.g. an administrative user issues the **reload** command), it notifies the primary HA that it is going out of service
- Assumes the responsibility of the primary HA when requested to
- In the event that it determines that primary HA is not available, it assumes the responsibility of the primary HA if there is at least one address allocated to verify that the AAA server is re-configured to direct the calls

Requirements, Limitations, & Behavior

- One IPSP interface can be configured per system context.
- The IPSP interfaces for both the primary and secondary HAs must be configured to communicate on the same network.
- If IP pool busyout is enabled on any configured address pool, IPSP can not be configured.
- The IP pool configuration (pool name, addresses, priority, pool group, etc.) on both the HAs must be identical.
- IP pools cannot be modified on either the primary or the secondary HAs once IPSP is enabled.
- Sessions are dropped during the IPSP setup process if:
  - the primary HA has not yet approved an IP address or address block.
  - the primary HA is not known to the secondary HA.
- Once an address is assigned to the secondary HA, all the information about that address is erased on the primary HA and that address becomes unusable by the primary HA.
- LRU is not supported across the systems. Although, LRU continues to be supported within the system.

- If the IPSP configuration is not disabled before removing the HA from the IPSP network link, sessions may be rejected if the system's VPN Manager is rebooted or restarts.
- IPSP does not control static IP pools. An external application (AAA, etc.) must be responsible for ensuring that duplicate addresses are not assigned.
- IPSP ignores interface failures allowing the configured dead-interval timer to determine when the HA should become the primary and control the pool addresses. Before the dead-interval timer starts, the secondary HA maintains its state and any busied out addresses remain busied out. After the dead-interval timer starts, IPSP marks the neighboring peer HA as down, becomes primary, and will unbusy out all pool addresses.

How IPSP Works

IPSP operation requires special configuration in both the primary and secondary HAs. As mentioned previously, both HAs must have identical configurations. This allows the secondary HA to process sessions identically to the primary when the primary is taken offline for upgrade.

Configuration must also be performed on the AAA server. Whereas subscriber profiles on the AAA server originally directed sessions to the primary HA, prior to using IPSP, subscriber profiles must be re-configured to direct sessions to the secondary HA.

There are two scenarios in which IPSP takes effect:

- **New sessions:** Once IPSP is configured, new sessions are directed to a secondary HA (HA2) allowing the primary HA to go through a software upgrade without degrading network capacity. The secondary HA requests addresses from the primary HA's (HA1) pools as needed. As the addresses are allocated, they are busied out on the primary HA. This procedure is displayed below.
- **Session handoffs:** Once IPSP is configured, sessions originally registered with the primary HA (HA1) are re-registered with the secondary HA (HA2). To ensure the session is assigned the same IP address, the secondary HA requests the address from the primary HA. The primary HA verifies the binding and releases it to the secondary HA which, in turn, re-assigns it to the session. As the addresses are allocated, they are busied out on the primary HA. This procedure is displayed below.

IPSP Operation for New Sessions

The following figure and text describe how new sessions are handled when IPSP is enabled.

Figure 1: IPSP Operation for New Sessions

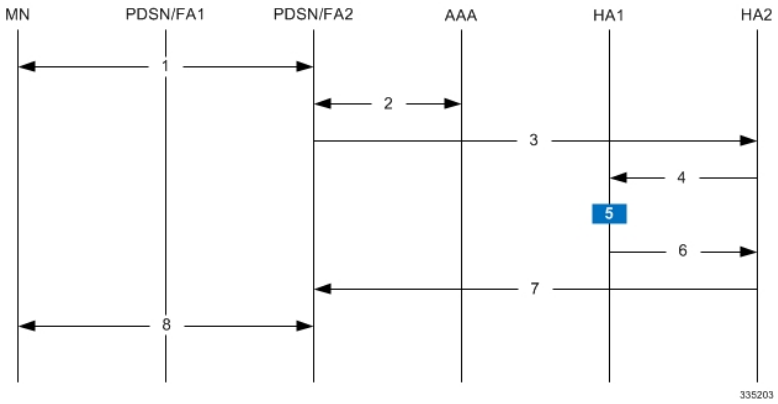


Table 1: IPSP Operation for New Sessions Description

Step	Description
1	A mobile node (MN) attempting to establish a data session is connected to PDSN/FA 2.
2	PDSNFA 2 authenticates the subscriber with the AAA server. One of the attributes returned by the AAA server as part of a successful authentication is the IP address of the secondary HA.
3	PDSN/FA 2 forwards the session request to HA2 for processing. HA2 processes the session as it would for any Mobile IP session.
4	With IPSP enabled, prior to assigning an IP address, HA2 sends a request to HA1 for an IP address.
5	HA1 allocates the address to HA2 and busies it out so it can not be re-assigned.
6	HA1 responds to HA2 with the IP address for the session.
7	HA2 proceeds with session processing and provides PDSN/FA 2 with the IP address for the MN.
8	The MN and PDSN/FA 2 complete session processing.

IPSP Operation for Session Handoffs

The following figure and text describe how session handoffs are handled when IPSP is enabled.

Figure 2: IPSP Operation for Session Handoffs

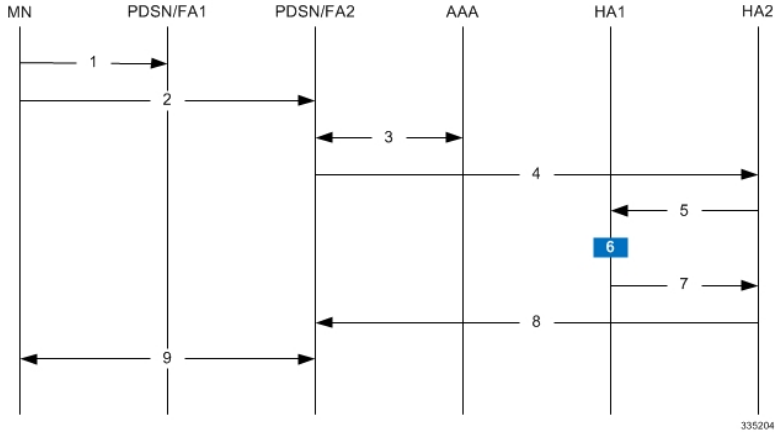


Table 2: IPSP Operation for Session Handoffs Description

Step	Description
1	A mobile node (MN) is connected to PDSN/FA 1.
2	The MN's session is handed-off to PDSN/FA2 and goes through the re-registration process.
3	PDSN/FA 2 authenticates the subscriber with the AAA server as part of the re-registration process. One of the attributes returned by the AAA server as part of a successful authentication is the IP address of the secondary HA.
4	PDSN/FA 2 forwards the session request to HA2 for processing. Included in the request is the MN's current IP address.
5	With IPSP enabled, prior to assigning an IP address, HA2 sends a request to HA1 for an IP address.
6	HA1 verifies the MN's information and releases the binding. It then busies out the address so it can not be re-assigned.
7	HA1 allocates the original IP address to HA2 for the session.
8	HA2 proceeds with session processing and provides PDSN/FA 2 with the IP address for the mobile node.
9	The mobile node and PDSN/FA 2 complete session processing.

Configuring IPSP Before the Software Upgrade

Configuring IPSP requires changes to the primary HA (the HA on which the software upgrade is to occur), the secondary HA (the HA to which subscribers sessions are to be directed), and the AAA server.

This section provides information and instructions for configuring IPSP before the software upgrade.

Important This section provides the minimum instruction set for configuring IPSP on the system. For more information on commands that configure additional parameters and options, refer to the *IPSP Configuration Mode Commands* chapter in the *Command Line Interface Reference*.

To enable the IP pool sharing during software upgrade:

Step 1 Configure the AAA servers by applying the example configuration in Configuring the AAA Server for IPSP, on page 6.

Step 2 Configure an interface on the system for use by IPSP according to the instructions found in the *Creating and Configuring Ethernet Interfaces and Ports* section of the *System Administration Guide*.

Step 3 Enable the IPSP on secondary HA by applying the example configuration in Enabling IPSP on the Secondary HA, on page 7.

Step 4 Perform the boot system priority and SPC/SMC card synchronization as described in *Off-line Software Upgrade* section in the *System Administration Guide*.

Step 5 Enable the IPSP on primary HA by applying the example configuration in Enabling IPSP on the Primary HA, on page 7.

Step 6 Verify your ACL configuration by following the steps in the *Verifying the IPSP Configuration* section.

Step 7 Proceed for software upgrade as described in Off-line Software Upgrade section in the *System Administration Guide*.

Step 8 Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

Configuring the AAA Server for IPSP

For subscriber session establishment, the AAA server provides the IP address of the HA that is to service the session. This information exists in the 3GPP2_MIP_HA_Address RADIUS attribute configured for the subscriber.

Because the primary HA has been responsible for facilitating subscriber sessions, its IP address is the one configured via this attribute. For IPSP however, the attribute configuration must change in order to direct sessions to the secondary HA.

To do this, reconfigure the 3GPP2_MIP_HA_Address RADIUS attribute for each subscriber on the AAA server with the IP address of the secondary HA.

The precise instructions for performing this operation vary depending on the AAA server vendor. Refer to the documentation for your AAA server for more information.

Enabling IPSP on the Secondary HA

The secondary HA is the alternate HA that is to take responsibility while the primary HA is upgraded.



Important This section provides the minimum instruction set for configuring IPSP on the system. For more information on commands that configure additional parameters and options, refer to the *IPSP Configuration Mode Commands* chapter in the *Command Line Interface Reference*.

Use the following example to enable the IPSP on secondary HA:

```
configure
 context <ipsp_ctxt_name> [ -noconfirm ]
 interface <ipsp_if_name>
 pool-share-protocol primary <pri_ha_address> [ mode {active | inactive |
check-config } ]
 dead-interval <dur_sec>
 end
```

Notes:

- The interface must be configured in the same context as the HA service and must be on the same network as the primary HA's IPSP interface.
- *ipsp_if_name* is the name of the interface on which you want to enable IPSP.
- dead-interval is an optional command to configure time to wait before retrying the primary HA for the IP Pool Sharing Protocol.

Enabling IPSP on the Primary HA

The primary HA is the HA that is to be upgraded.



Important This section provides the minimum instruction set for configuring IPSP on the system. For more information on commands that configure additional parameters and options, refer to the *IPSP Configuration Mode Commands* chapter in the *Command Line Interface Reference*.

Use the following example to enable the IPSP on primary HA:

```
configure
 context <ipsp_ctxt_name> [ -noconfirm ]
 interface <ipsp_if_name>
 pool-share-protocol secondary <sec_ha_address> [ mode {active | inactive |
check-config } ]
 dead-interval <dur_sec>
 end
```

Notes:

- The interface must be configured in the same context as the HA service and must be on the same network as the secondary HA's IPSP interface.

- *ipsp_if_name* is the name of the interface on which you want to enable IPSP.
- dead-interval is an optional command to configure time to wait before retrying the secondary HA for the IP Pool Sharing Protocol.

Important Once this configuration is done, the primary HA begins to hand responsibility for sessions and release IP addresses to the secondary HA. Prior to performing the software upgrade, all IP addresses must be released. When IPSP has released all IP pool addresses from the primary HA an SNMP trap (**starIPSPAllAddrsFree**) is triggered.

Verifying the IPSP Configuration

These instructions are used to verify the IPSP configuration.

Verify that IPSP has released all IP addresses by entering the following command in Exec Mode with in specific context:

```
show ip ipsp
```

The output of this command provides the list of used addresses and released addresses. The system will send the **starIPSPAllAddrsFree** trap once all IP addresses are released. When the value in the *Used Addresses* column reaches 0 for all IP pools listed, then the primary HA sends the SNMP trap and notifies the secondary HA to take over as the primary HA.

Configuring IPSP After the Software Upgrade

If desired, IP pool addresses can be migrated from the original secondary HA back to the original primary HA once the upgrade process is complete.

Important It is important to note that the HA that was originally designated as the secondary is now functioning as the primary HA. Conversely, the HA that was originally designated as the primary is now functioning as the secondary.

In order to migrate the addresses, both HAs and the AAA server must be configured according to the instructions in this section.

This section provides information and instructions for configuring IPSP after the software upgrade.

Important This section provides the minimum instruction set for configuring IPSP on the system. For more information on commands that configure additional parameters and options, refer *IPSP Configuration Mode Commands* chapter in the *Command Line Interface Reference*.

To enable the IP pool sharing after software upgrade:

Step 1 Configure the AAA servers by applying the example configuration in Configuring the AAA Server for IPSP, on page 6.

Step 2 Configure an interface on the system for use by IPSP according to the instructions found in the Creating and Configuring Ethernet Interfaces and Ports section of *System Administration Guide*.

Step 3 Enable the IPSP on secondary HA by applying the example configuration in Enabling IPSP on the Secondary HA, on page 7.

Step 4 Enable the IPSP on primary HA by applying the example configuration in Enabling IPSP on the Primary HA, on page 7.

Step 5 Verify your ACL configuration by following the steps in the *Verifying the IPSP Configuration*.

Step 6 Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

Disabling IPSP

Once all IP addresses on the primary HA have been released, IPSP must be disabled on both the primary and secondary HAs.



Caution Prior to disabling IPSP, ensure that the primary HA has released all IP addresses to secondary HA.

Follow the instructions in this section to disable IPSP on primary and secondary HA after migration of all IP addresses.



Important This section provides the minimum instruction set for disabling IPSP on the HAs. For more information on commands, refer to the *IPSP Configuration Mode Commands* chapter in the *Command Line Interface Reference*.

Use the following example to enable the IPSP on primary/secondary HA:

```
configure
 context <ipsp_ctxt_name> [ -noconfirm ]
 interface <ipsp_if_name>
 no pool-share-protocol
 end
```

Notes:

- The interface must be configured in the same context as the primary/secondary HA service and must be on the same network as the primary/secondary HA's IPSP interface.
- *ipsp_if_name* is the name of the interface on which you want to disable IPSP.
- IPSP must be disabled on both the HAs.