Configuring L2TP HA Session SSO ISSU on a LAC LNS

The L2TP HA Session SSO/ISSU on a LAC/LNS feature provides a generic stateful switchover/In Service Software Upgrade (SSO/ISSU) mechanism for Layer 2 Tunneling Protocol (L2TP) on a Layer 2 Access Concentrator (LAC) and a Layer 2 Network Server (LNS). This feature preserves all fully established PPP and L2TP sessions during an SSO switchover or an ISSU upgrade or downgrade.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for L2TP HA Session SSO ISSU on a LAC LNS

- Configure a VPDN deployment. For an overview of VPDN deployments, see the VPDN Technology Overview module.
- This implementation does not require the peer L2TP node to be HA or redundancy aware. It does not require the peer L2TP node to implement L2TP failover RFC.
- Ensure that the peer L2TP node is L2TP RFC compliant.

Restrictions for L2TP HA Session SSO ISSU on a LAC LNS

- Cisco IOS XE Release 2.2 provides support for the L2TP HA Session SSO/ISSU on a LAC/LNS feature on Cisco ASR 1000 Series Routers only.
- Cisco IOS XE Release 2.4 provides support for VPDN Multihop nodes for VPDN tunnels and sessions. VPDN tunnels and sessions are preserved after a Route Processor (RP) failover in a dual RP ASR set up.
- L2TP HA Session SSO/ISSU on a LAC/LNS does not support HA/SSO on the following software features, and sessions with these will be lost following an RP failover:
    - L2TP Dialout
    - L2TP Active Discovery Relay for PPPoE
    - Multilink PPP on LNS

Information About L2TP HA Session SSO ISSU on a LAC LNS

Stateful Switchover

Development of the stateful switchover (SSO) feature is an incremental step within an overall program to improve the availability of networks constructed with Cisco IOS routers.

In specific Cisco networking devices that support dual RPs, stateful switchover takes advantage of RP redundancy to increase network availability. The feature establishes one of the RPs as the active processor and designating the other RP as the standby processor, and then synchronizing critical state information between them. Following an initial synchronization between the two processors, SSO dynamically maintains RP state information between them.

A switchover from the active to the standby processor occurs when the active RP fails, is removed from the networking device, or is manually taken down for maintenance.

SSO is particularly useful at the network edge. Traditionally, core routers protect against network faults using router redundancy and mesh connections that allow traffic to bypass failed network elements. SSO provides protection for network edge devices with dual RPs that represent a single point of failure in the network design, and where an outage might result in loss of service for customers.

Note If a new L2TP session request is received on a tunnel that is in the resync phase after switchover, it is rejected. A new Cisco vendor-specific disconnect cause code (611) provides the reason for this session disconnect. The **show vpdn history failure** command displays the Failure Type field as *Tunnel in HA resync* .

Checkpointing Data

SSO is always checkpointing or saving and resynchronizing client-specific state data that transfers to a peer client on a remote RP for HA switchover and on the local RP for ION restart. Once a valid checkpointing session is established, the checkpointed state data is established without error.

ISSU Software Superpackage and Rolling Upgrade Requirements

This section describes the affects on L2TP when performing an ISSU superpackage or subpackage software upgrade or downgrade on a Cisco ASR 1000 Series Router. During the ISSU operation of software upgrades and downgrades, there can be control traffic interruption in some scenarios of ISSU, causing the L2TP resynchronization operation (with L2TP silent switchover) to fail, resulting in a loss of an L2TP tunnel or session.

In general, there is no effect on the data traffic while performing an ISSU superpackage or subpackage software upgrade or downgrade. Data traffic interruptions are contained within a managed and expected operating set. For example, when you upgrade the software for a given spa, the software upgrade only affects the data traffic serviced by that spa; the remaining network continues to operate normally.

Software Upgrades and Downgrades

When you are configuring a superpackage software upgrade or downgrade, L2TP sessions and tunnels might be lost. To help mitigate any potential loss of L2TP tunnels or sessions, use a rolling-upgrade method to help minimize any L2TP tunnel or session outages.

Note You can help minimize any tunnel or session outage as seen by the IP layer, by either configuring a backup interface for IP routing or an Ether-channel interface towards the L2TP peer.

For the Cisco ASR 1000 Series Routers, it is important to realize that ISSU-compatibility depends on the software sub-package being upgraded and the hardware configuration. Consolidated packages are ISSU-compatible in dual RP configurations only and have other limitations. The SPA and SIP software sub-packages must be upgraded on a per-SPA or per-SIP basis.

If you are upgrading a software package on the Cisco ASR 1000 Series Router that requires a reload of the standby Route Processor (RP), you must manually initiate a upgrade of the standby FP, SPA and SIP software with the same version of software provisioned on the new active RP following the switchover, to prevent any reload when the standby RP takes over as the new active RP.

Adjusting Receive Window Size

When configuring L2TP HA Session SSO/ISSU on a LAC/LNS, Cisco IOS software internally adjusts the L2TP receive window size to a smaller value. This adjusted receive-window value displays when using the **show vpdn tunnel detail** command. If required, use the **l2tp tunnel resync** command to increase the size of the L2TP receive window.

How to Configure L2TP HA Session SSO ISSU on a LAC LNS

You can configure L2TP HA globally using the **l2tp sso enable** command. You can also configure L2TP HA sessions for a specific VPDN group by using the **sso enable** command in VPDN group configuration mode. Both global and VPDN group L2TP HA sessions are enabled, by default. You must configure both the **l2tp sso enable** command and the **sso enable** command for VPDN groups for protocol L2TP to execute L2TP HA session functionality.

Global and VPDN group-specific L2TP HA sessions are hidden from the output of the **show running-config** command, because they are enabled by default. If you use the **no l2tp sso enable** command, the HA commands will display as NVGEN and appear in the output of the **show running-config** command.

After an SSO switchover, L2TP HA sessions determines the sequence numbers used by L2TP peers. Determining sequence numbers can be time consuming if peers send a large number of unacknowledged messages. You can use the **l2tp tunnel resync** command to control the number of unacknowledged messages sent by a peer. Increasing the value of the number of packets can improve the session setup rate for L2TP HA tunnels with a large number of sessions.

Configuring SSO on a Route Processor

Cisco series Internet routers operate in SSO mode by default after reloading the same version of SSO-aware images on the device.

Before you can use SSO, use must enable SSO on an RP. This task explains how to use the **redundancy** command to enable SSO on an RP. This task ensures that all redundancy session data, following a SSO, is used to re-create and reestablishes existing sessions to their peer connections.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **redundancy**
4. **mode sso**
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**redundancy** **Example:** `Router(config)# redundancy`	Enters redundancy configuration mode.
Step 4	**mode sso** **Example:** `Router(config-red)# mode sso`	Specifies the mode of redundancy.
Step 5	**end** **Example:**	Returns to privileged EXEC mode.

	Command or Action	Purpose
	`Router(config-red)# end`	

Configuring Global L2TP HA SSO Mode

Cisco series Internet routers operate in L2TP HA SSO mode by default after reloading the same version of SSO-aware images on the device. No configuration is necessary to enable L2TP HA SSO sessions.

This procedure shows how to use the **l2tp sso enable** command to enable or disable HA globally. The **l2tp sso enable** command is enabled by default.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **l2tp sso enable**
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**l2tp sso enable** **Example:** `Router(config)# l2tp sso enable`	Enables L2TP HA SSO.
Step 4	**end** **Example:** `Router(config)# end`	Returns to privileged EXEC mode.

Configuring VPDN Groups or VPDN Templates for L2TP HA SSO

Perform this task when configuring a VPDN group or a VPDN template for L2TP HA SSO. This configuration example provides recommended scaling parameters to use when the number of VPDN tunnels in use is high, such as 8000 tunnels, with each tunnel supporting only a few VPDN sessions (two or less).

Conversely, if the number of VPDN tunnels is low and the number of VPDN sessions per VPDN tunnel is high, use the **l2tp tunnel resync** command to increase the resynchronization value. For example, if the number of VPDN session per VPDN tunnel are in the hundreds, use the **l2tp tunnel resync** command to increase the resynchronization value to a matching value in the hundreds.

Beginning with Cisco IOS XE Release 2.3, you can set the retransmit retries and timeout values to default values.

For HA functionality for a VPDN group, both the **l2tp sso enable** and **sso enable** commands must be enabled (default). If either command is disabled, no HA functionality is available for the VPDN group.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **l2tp sso enable**
4. **vpdn enable**
5. **vpdn-group** *name*
6. **sso enable**
7. **l2tp tunnel resync** *packets*
8. **l2tp tunnel retransmit retries** *number*
9. **l2tp tunnel retransmit timeout min** *seconds*
10. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**l2tp sso enable** **Example:** `Router(config)# l2tp sso enable`	Enables L2TP SSO mode.
Step 4	**vpdn enable** **Example:** `Router(config)# vpdn enable`	Enters VPDN configuration mode.
Step 5	**vpdn-group** *name* **Example:**	Creates a VPDN group and enters VPDN group configuration mode.

	Command or Action	Purpose
	`Router(config-vpdn)# vpdn-group example`	
Step 6	**sso enable** **Example:** `Router(config-vpdn)# sso enable`	Enables L2TP SSO for the VPDN group.
Step 7	**l2tp tunnel resync** *packets* **Example:** `Router(config-vpdn)# l2tp tunnel resync 4`	Configures the number of packets after an SSO, an L2TP HA tunnel sends before waiting for an acknowledgement.
Step 8	**l2tp tunnel retransmit retries** *number* **Example:** `Router(config-vpdn)# l2tp tunnel retransmit retries 30`	Configures the number of retransmission attempts made for an L2TP control packet.
Step 9	**l2tp tunnel retransmit timeout min** *seconds* **Example:** `Router(config-vpdn)# l2tp tunnel retransmit timeout min 8`	Configures the amount of time that the router waits before resending an L2TP control packet.
Step 10	**exit** **Example:** `Router(config-vpdn)# exit`	Exits VPDN group configuration mode.

Controlling Packet Resynchronization for L2TP HA

After a SSO switchover, L2TP HA determines the sequence numbers used by L2TP peers. Determining sequence numbers can be time consuming, if peers send a large number of unacknowledged messages. You can use the **l2tp tunnel resync** command to control the number of unacknowledged messages sent by a peer. Increasing the value of the number of packets can improve the session setup rate for L2TP HA tunnels with a large number of sessions.

You can use the **show l2tp redundancy** command to display the time taken to resynchronize with the peer L2TP node.

This procedure shows how to use the **l2tp tunnel resync** command, in VPDN-group configuration mode, to control the number of packets a L2TP HA tunnel sends before waiting for an acknowledgement.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **vpdn enable**

4. **vpdn-group** *name*
5. **l2tp tunnel resync** *packets*
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**vpdn enable** **Example:** `Router(config)# vpdn enable`	Enters VPDN configuration mode.
Step 4	**vpdn-group** *name* **Example:** `Router(config-vpdn)# vpdn-group example`	Creates a VPDN group and enters VPDN group configuration mode.
Step 5	**l2tp tunnel resync** *packets* **Example:** `Router(config-vpdn)# l2tp tunnel resync 250`	Specifies the number of packets to be processed after an SSO before an acknowledgment message is sent. This example specifies that 250 packets will process before an acknowledgment message is sent.
Step 6	**end** **Example:** `Router(config-vpdn)# end`	Returns to privileged EXEC mode.

Verifying the Checkpoint Status of L2TP HA Sessions

The **show l2tp redundancy** command provides information regarding the global state of the L2TP or specific L2TP sessions, with regard to their checkpointing status. You can display detailed information on:

- L2TP HA protocol state:
  - Standby readiness
  - Received message counter
  - Number of tunnels and sessions, compared to the number of HA-enabled tunnels and sessions

    - Number of tunnels that successfully resynchronized with the peer L2TP node after the last switchover, and the number that failed to resynchronize.

- L2TP control channel (tunnel) redundancy information:
    - Tunnel state
    - Local ID
    - Remote ID
    - Remote name
    - Class or group name
    - Number of sessions using this tunnel
- L2TP Session redundancy information:
    - Local session ID
    - Remote session ID
    - Tunnel ID
    - Status of assignment of logical tunnel and logical session handles

The L2TP HA protocol state information for tunnels configured for HA (HA-enabled) and HA tunnels established successfully (HA-established) should match on the active and standby RP, unless there is a failure.

The output of the **show l2tp redundancy** command on the standby RP does not display total counter values or values for L2TP resynchronized tunnels. Total counter values would include non-HA protected tunnels and sessions, and these are not present on the standby RP.

To display global L2TP or specific L2TP sessions having checkpoint status, follow this procedure.

SUMMARY STEPS

1. **enable**
2. **show l2tp redundancy** [**all** | [**detail**] [**id** *local-tunnel-ID* [*local-session-ID*]]]
3. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show l2tp redundancy** [**all** | [**detail**] [**id** *local-tunnel-ID* [*local-session-ID*]]] **Example:** `Router# show l2tp redundancy all`	Display the status of L2TP session with redundancy data.
Step 3	**exit** **Example:**	Exits privileged EXEC mode.

	Command or Action	Purpose
	`Router# exit`	

Verifying the Checkpoint Status of VPDN Sessions

SUMMARY STEPS

1. **enable**
2. **show vpdn redundancy** [**all** \| [**detail**] [**id** *local-tunnel-ID* [*local-session-ID*]]]
3. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show vpdn redundancy** [**all** | [**detail**] [**id** *local-tunnel-ID* [*local-session-ID*]]] **Example:** `Router# show vpdn redundancy all`	Displays the status of VPDN session with checkpointed data.
Step 3	**exit** **Example:** `Router# exit`	Exits privileged EXEC mode.

Troubleshooting L2TP or VPDN Redundancy Sessions

There is extensive troubleshooting for L2TP or VPDN redundancy sessions. For example, if the standby RP does not initialize, the **show l2tp redundancy** command displays a warning message and will display no tunnel or session information.

```
Router# show l2tp redundancy

L2TP HA support: Silent Failover
L2TP HA Status:
  Checkpoint Messaging on: FALSE
  Standby RP is up:        TRUE
  Recv'd Message Count:    0

No HA CC of Session data to display until Standby RP is up.
```

You can use the **debug l2tp redundancy** or **debug vpdn redundancy** commands to display debug information relating to L2TP- or VPDN-checkpointing events or errors. Debug information includes:

- cf--L2TP redundancy checkpointing-facility events (cf-events)
- detail--L2TP redundancy details
- error--L2TP redundancy errors
- event--L2TP redundancy events
- fsm--L2TP redundancy fsm-events
- resync--L2TP redundancy resynchronizations
- rf--L2TP redundancy-facility events (rf-events)

To debug an L2TP or VPDN session having redundancy event errors, follow this procedure.

SUMMARY STEPS

1. **enable**
2. **debug** {**l2tp** | **vpdn**} **redundancy** {**cf** | **detail** | **error** | **event** | **fsm** | **resync** | **rf**}
3. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**debug** {**l2tp** | **vpdn**} **redundancy** {**cf** | **detail** | **error** | **event** | **fsm** | **resync** | **rf**} **Example:** `Router# debug vpdn redundancy cf`	Displays debug information for VPDN session with redundancy data.
Step 3	**exit** **Example:** `Router# exit`	Exits privileged EXEC mode.

Configuring L2TP HA SSO ISSU on a RADIUS Server

You can configure L2TP HA SSO/ISSU on a RADIUS server, using the following RADIUS attribute-value (AV) pair:

```
cisco:cisco-avpair="vpdn:l2tp-silent-switchover=1"
```

You can configure the L2TP HA SSO/ISSU resynchronous parameter on a RADIUS server, using the following RADIUS AV pair:

```
cisco:cisco-avpair="vpdn:l2tp-tunnel-resync-packet=<num>"
```

Configuration Examples for L2TP HA Session SSO ISSU on a LAC LNS

Example Configuring SSO on a Route Processor

This example shows how to configure SSO on a route processor:

```
Router# configure terminal
Router(config)# redundancy
Router (config-red)# mode sso
Router (config-red)# end
```

Example Configuring L2TP High Availability

This example shows how to configure L2TP SSO:

```
Router# configure terminal
Router(config)# l2tp sso enable
Router (config-red)# end
```

Examples Displaying L2TP Checkpoint Status

Example Displaying L2TP Redundancy Information

The following example shows an L2TP redundancy information request:

```
Router# show l2tp redundancy
L2TP HA support: Silent Failover
L2TP HA Status:
  Checkpoint Messaging on: TRUE
  Standby RP is up:        TRUE
  Recv'd Message Count:    189
  L2TP Tunnels:            2/2/2/0 (total/HA-enabled/HA-est/resync)
  L2TP Sessions:           20/20/20 (total/HA-enabled/HA-est)
  L2TP Resynced Tunnels:   2/0 (success/fail)
  Resync duration 0.63 secs (complete)
```

Example Displaying L2TP Redundancy Detail Information

The following example shows an L2TP redundancy detail information request:

```
Router# show l2tp redundancy detail id 44233 2
 Local session ID        : 2
 Remote session ID        : 2
 Local CC ID        : 44233
 Local UDP port        : 1701
 Remote UDP port        : 1701
```

```
 Waiting for VPDN application        : No
 Waiting for L2TP protocol        : No
```

Example Displaying All L2TP Redundancy Information

The following example shows an L2TP redundancy all-information request:

```
Router# show l2tp redundancy all

L2TP HA support: Silent Failover
L2TP HA Status:
  Checkpoint Messaging on: FALSE
  Standby RP is up:         TRUE
  Recv'd Message Count:     0
  L2TP Active Tunnels:      1/1/0 (total/HA-enabled/resync)
  L2TP Active Sessions:     1/1 (total/HA-enabled)
 L2TP Resynced Tunnels:  1/0 (success/fail)
L2TP HA CC Check Point Status:
State  LocID RemID Remote Name      Class/Group              Num. Sessions
est    33003 26355 LAC-1            1                        1
L2TP HA Session Status:
LocID      RemID      TunID     Waiting for    Waiting for
                                 VPDN app?     L2TP proto?
28017      10         33003       No             No
```

Example Displaying L2TP Redundancy ID Information

The following example shows how to limit the information displayed by providing a tunnel ID:

```
Router# show l2tp redundancy id 33003
 L2TP HA Session Status:
LocID  RemID  TunID   Waiting for     Waiting for
       VPDN app?     L2TP proto?
2  2  33003   No     No
```

Example Displaying L2TP Redundancy Detail ID Information

The following example shows how to limit the information displayed by providing a session ID:

```
Router# show l2tp redundancy detail id 33003 3
Local session ID        : 3
 Remote session ID        : 3
 Local CC ID        : 33003
 Local UDP port        : 1701
 Remote UDP port        : 1701
 Waiting for VPDN application        : No
 Waiting for L2TP protocol        : No
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases

Related Topic	Document Title
VPDN commands	*Cisco IOS VPDN Command Reference*
Layer 2 Tunnel Protocol	Layer 2 Tunnel Protocol Technology Brief
Stateful switchover and high availability	Configuring Stateful Switchover module
ISSU on Cisco ASR 1000 Series Routers	http://www.cisco.com/en/US/docs/routers/asr1000/configuration/guide/chassis
VPDN technology overview	VPDN Technology Overview module

Standards

Standard	Title
None	--

MIBs

MIB	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
RFC 2661	*Layer 2 Tunneling Protocol (L2TP)*
RFC 4591	Fail Over for Layer 2 Tunneling Protocol (L2TP)

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for L2TP HA Session SSO ISSU on a LAC LNS

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 1: Feature Information for L2TP HA Session SSO/ISSU on a LAC/LNS

Feature Name	Releases	Feature Information
L2TP HA Session SSO/ISSU on a LAC/LNS	Cisco IOS XE Release 2.2 Cisco IOS XE Release 2.3 Cisco IOS XE Release 2.4	Provides a generic SSO/ISSU mechanism for Layer 2 Tunneling Protocol (L2TP) on a LAC and a LNS. This feature was introduced on the Cisco ASR 1000 Series Routers. The following commands were introduced by this feature: **debug l2tp redundancy**, **debug vpdn redundancy**, **l2tp sso enable**, **l2tp tunnel resync**, **show l2tp redundancy**, **show vpdn redundancy**, **sso enable**. In 2.3, support was added for scaling parameters for VPDN groups and templates. In 2.4, support was added for support for Multihop VPDN for VPDN tunnels and sessions.