



Configuring L2TP HA Session SSO/ISSU on a LAC/LNS

First Published: September 22, 2008

Last Updated: September 22, 2008

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 feature information and caveats, see 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 for L2TP HA Session SSO/ISSU on a LAC/LNS](#)” section on [page 343](#).

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

Contents

- [Prerequisites for L2TP HA Session SSO/ISSU on a LAC/LNS, page 328](#)
- [Information About L2TP HA Session SSO/ISSU on a LAC/LNS, page 328](#)
- [How to Configure L2TP HA Session SSO/ISSU on a LAC/LNS, page 329](#)
- [Configuration Examples for L2TP HA Session SSO/ISSU on a LAC/LNS, page 337](#)
- [Troubleshooting Tips, page 340](#)
- [Additional References, page 341](#)



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2008 Cisco Systems, Inc. All rights reserved.

- [Feature Information for L2TP HA Session SSO/ISSU on a LAC/LNS, page 343](#)

Prerequisites for L2TP HA Session SSO/ISSU on a LAC/LNS

Before you can provide for the L2TP HA Session SSO/ISSU on a LAC/LNS feature, you must:

- Configure a VPDN deployment. For an overview of VPDN deployments, refer to the “[VPDN Technology Overview](#)” module.
- Configure redundancy and SSO. For more information on SSO, refer to the [Cisco IOS High Availability Configuration Guide](#).
- Ensure the peer L2TP node is L2TP RFC compliant. For more information, refer to the “[RFCs](#)” section.

Information About L2TP HA Session SSO/ISSU on a LAC/LNS

To implement L2TP HA Session SSO/ISSU on a LAC/LNS feature, you need to understand the following concepts:

- [Stateful Switchover](#)
- [Checkpointing Data](#)

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 Route Processor (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. 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.

For complete information of SSO on Cisco IOS routers, see the [Stateful Switchover](#) module in the [Cisco IOS High Availability Configuration Guide](#).

Checkpointing Data

SSO 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.

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.

This section contains the following procedures:

- [Configuring SSO on a Route Processor, page 329](#) (required)
- [Configuring Global L2TP HA SSO Mode, page 330](#) (optional)
- [Configuring VPDN Group-Specific L2TP HA SSO Mode, page 331](#) (optional)
- [Controlling Packet Resynchronization for L2TP HA, page 332](#) (optional)
- [Verifying the Checkpoint Status of L2TP HA Sessions, page 333](#) (optional)
- [Verifying the Checkpoint Status of VPDN Sessions, page 335](#) (optional)
- [Configuring Debugging for L2TP or VPDN Redundancy Sessions, page 336](#) (optional)

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, you 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. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">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	exit Example: Router# exit	Exits redundancy configuration mode.

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.

The following 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. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">• 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	exit Example: Router# exit	Exits global configuration mode.

Configuring VPDN Group-Specific L2TP HA SSO Mode

The following procedure shows how to use the **l2tp sso enable** and **sso enable** commands to enable or disable high availability (HA) for a VPDN group. 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 *id***
6. **sso enable**
7. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>enable</code> Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">Enter your password if prompted.
Step 1	<code>configure terminal</code> Example: Router# configure terminal	Enters global configuration mode.
Step 2	<code>l2tp sso enable</code> Example: Router(config)# l2tp sso enable	Enables L2TP SSO mode.
Step 3	<code>vpdn enable</code> Example: Router(config)# vpdn enable	Enters VPDN configuration mode.
Step 4	<code>vpdn-group id</code> Example: Router(config-vpdn)# vpdn-group example	Enters VPDN group configuration mode.
Step 5	<code>sso enable</code> Example: Router(config-vpdn)# sso enable	Enables L2TP SSO for the VPDN group.
Step 6	<code>exit</code> 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.



Note

If you use the **l2tp tunnel resync** command to increase the value of the resync number, this action might cause a slowdown in the recovery of an L2TP tunnel after a stateful switchover.

The following 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** *vpdn-group-id*
5. **l2tp tunnel resync** *number-of-packets*
6. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">• Enter your password if prompted.
Step 1	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 2	vpdn enable Example: Router(config)# vpdn enable	Enters VPDN configuration mode.
Step 3	vpdn-group <i>vpdn-group-id</i> Example: Router(config-vpdn)# vpdn-group example	Enters VPDN group configuration mode.
Step 4	l2tp tunnel resync <i>number-of-packets</i> Example: Router(config-vpdn)# l2tp tunnel resync 250	Specifies the number of packets to be processed before an acknowledgment message is sent. This example specifies that 250 packets will process before an acknowledgment message is sent.
Step 5	exit Example: Router(config-vpdn)# exit	Exits VPDN group configuration 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** [**detail** | **all** | **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. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	show l2tp redundancy [<i>detail all id local-tunnel-id local-session-id</i>] Example: Router# show l2tp redundancy all	Display the status of L2TP session with redundancy data.
Step 3	exit Example: Router# exit	Exits privileged EXEC mode.

Verifying the Checkpoint Status of VPDN Sessions

To verify the checkpoint status of VPDN sessions, follow this procedure.

SUMMARY STEPS

- enable**
- show vpdn redundancy** [*detail | all | id local-tunnel-id local-session-id*]
- exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	show vpdn redundancy [<i>detail all id local-tunnel-id local-session-id</i>] 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.

Configuring Debugging for L2TP or VPDN Redundancy Sessions

There is extensive debugging 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> enable
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	<p><code>enable</code></p> <p>Example: Router> <code>enable</code></p>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	<p><code>debug {l2tp vpdn} redundancy {cf detail error event fsm resync rf}</code></p> <p>Example: Router# <code>debug vpdn redundancy cf</code></p>	<p>Displays debug information for VPDN session with redundancy data.</p>
Step 3	<p><code>exit</code></p> <p>Example: Router# <code>exit</code></p>	<p>Exits privileged EXEC mode.</p>

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

This section includes the following examples:

- [Configuring SSO on a Route Processor: Example, page 337](#)
- [Configuring L2TP High Availability: Example, page 337](#)

Configuring SSO on a Route Processor: Example

This example shows how to configure L2TP SSO:

```
Router> enable
Router# configure terminal
Router(config)# redundancy
Router (config-red)# mode sso
Router (config-red)# exit
```

Configuring L2TP High Availability: Example

This example shows how to configure L2TP SSO:

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

Displaying L2TP Checkpoint Status: Examples

This section provides the following configuration examples:

- [Displaying L2TP Redundancy Information: Example, page 338](#)
- [Displaying L2TP Redundancy Detail Information: Example, page 338](#)
- [Displaying All L2TP Redundancy Information: Example, page 339](#)
- [Displaying L2TP Redundancy ID Information: Example, page 339](#)
- [Displaying L2TP Redundancy Detail ID Information: Example, page 339](#)

Displaying L2TP Redundancy Information: Example

The following example shows an L2TP redundancy information request:

```
Router> enable
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
  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)
```

Displaying L2TP Redundancy Detail Information: Example

The following example shows an L2TP redundancy detail information request:

```
Router> enable
Router# show l2tp redundancy detail

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:
  Local ID      : 33003
  Remote ID     : 26355
  Control Channel state: established
  Remote name   : LAC-1
  Class Name    : 1
  Number of sessions : 1
  Logical CC ID : 4096
  Local UDP port : 1701
  Remote UDP port : 1701
  Current Ns    : 8
  Current Nr    : 10
  Check pointed Ns/Nr values available on Standby RP
```

```

Local session ID       : 28017
Remote session ID     : 10
Local CC ID           : 33003
Local UDP port        : 1701
Remote UDP port       : 1701
Waiting for VPDN application: No
Waiting for L2TP protocol  : No

```

Displaying All L2TP Redundancy Information: Example

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

```

Router> enable
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

```

Displaying L2TP Redundancy ID Information: Example

The following example shows an L2TP redundancy information request for ID 33003:

```

Router> enable
Router# show l2tp redundancy id 33003

L2TP HA Session Status:

LocID    RemID    TunID    Waiting for      Waiting for
         VPDN app?    L2TP proto?
28017    10       33003    No               No

```

Displaying L2TP Redundancy Detail ID Information: Example

The following example shows an L2TP redundancy detail information request for ID 33003:

```

Router> enable
Router# show vpdn redundancy detail id 33003

Local session ID       : 28017
Remote session ID     : 10
Local CC ID           : 33003
Local UDP port        : 1701
Remote UDP port       : 1701
Waiting for VPDN application: No

```

```
Waiting for L2TP protocol : No
```

Troubleshooting Tips

This section provides debugging commands you can use to help troubleshoot an L2TP HA SSO session.

The following example configuration shows a debugging session for an LNS:

```
LNS1> debug enable  
LNS1# debug l2tp redundancy cf  
L2TP redundancy cf debugging is on  
LNS1# debug l2tp redundancy detail  
L2TP redundancy details debugging is on  
LNS1# debug l2tp redundancy error  
L2TP redundancy errors debugging is on  
LNS1# debug l2tp redundancy event  
L2TP redundancy events debugging is on  
LNS1# debug l2tp redundancy fsm  
L2TP redundancy fsm debugging is on  
LNS1# debug l2tp redundancy resync  
L2TP redundancy resync debugging is on  
LNS1# debug l2tp redundancy rf  
L2TP redundancy rf debugging is on
```

Additional References

The following sections provide references related to the L2TP HA Session SSO/ISSU on a LAC/LNS feature.

Related Documents

Related Topic	Document Title
Layer 2 Tunnel Protocol	<i>Layer 2 Tunnel Protocol Technology Brief</i>
Cisco IOS high availability	<i>Cisco IOS High Availability Configuration Guide</i>
VPDN technology overview	“VPDN Technology Overview,” <i>Cisco VPDN Configuration Guide</i>

Standards

Standard	Title
None	—

MIBs

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

RFCs

RFC	Title
RFC 2661	<i>Layer 2 Tunneling Protocol (L2TP)</i>
RFC 4591	<i>Fail Over for Layer 2 Tunneling Protocol (L2TP)</i>

Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register on Cisco.com.</p>	<p>http://www.cisco.com/techsupport</p>

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

Table 1 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



Note

Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 23 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.	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.

CCDE, CCVP, Cisco Eos, Cisco StadiumVision, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn is a service mark; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0801R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2008 Cisco Systems, Inc. All rights reserved.