



# Session Scalability Enhancements

---

This feature module describes enhancements to session scalability and stability. It includes information on the benefits of the enhancements, supported platforms, related documents, and new commands.

This document includes the following sections:

- Feature Overview, page 1
- Supported Platforms, page 2
- Supported Standards, MIBs, and RFCs, page 2
- Recommendations, page 2
- Configuration Tasks, page 3
- Configuration Example, page 6
- Command Reference, page 7
- Glossary, page 12

## Feature Overview

The session scalability enhancements described in this document are included in Cisco IOS Release 12.1(1) DC1. They can be used in addition to the L2TP scalability enhancements in Cisco IOS Release 12.0(7) DC to achieve high numbers of PPP sessions and L2TP tunnels.

## Benefits

### **Increased Default Output Hold-Queue Limit**

Before this release, the default output hold-queue limit was 40 packets. Now the default is 80 packets.

### **Limiting the Number of Simultaneous Link Control Protocol Session Initiations**

A new command enables you to limit the number of simultaneous link control protocol (LCP) session initiations. You can reduce the client session recovery time after a dropout by preventing a chain reaction of LCP session initiation timeouts.

### **Limiting the Load Metric**

A new command enables you to limit the load metric based on the length of the PPP manager process input queue.

### Control of PPP Authentication and Retry Timeouts

New commands enable you to modify the PPP authentication timeout and PPP retry timeout.

## Related Documents

- *Cisco 6400 Software Configuration Guide*

## Supported Platforms

These session scalability enhancements are supported on the Cisco 6400 node route processor (NRP).

## Supported Standards, MIBs, and RFCs

### Standards

None

### MIBs

None

### RFCs

No new or modified RFCs are supported by these feature enhancements.

## Recommendations

### Cisco Express Forwarding

To support more than 1000 sessions, enable Cisco Express Forwarding (CEF) with the **ip cef** global configuration command. For more information on CEF, see the “Cisco Express Forwarding” chapter of the *Cisco IOS Switching Services Configuration Guide*.

### Memory

Make sure you have at least 128 MB of DRAM on the Cisco 6400 NRP while using these feature enhancements.

### NSP Image Version

Make sure that the NSP and NRP simultaneously run the same software release version while using these enhancements.

### System and Console Logging

Disable logging to the console terminal by using the **no logging console** global configuration command:

```
Router(config)# no logging console
```

Also, log messages to an internal buffer by using the **logging buffered** *buffer-size* global configuration command. Choose a buffer size appropriate for the available memory and volume of messages logged on your systems:

```
Router(config)# logging buffered 131072
```

For more information on system and console logging, see the “Redirecting debug and error message Output” section of the “Using Debug Commands” chapter of the *Cisco IOS Debug Command Reference, Cisco IOS Release 12.1*.

## Configuration Tasks

See the following sections for configuration tasks for the session scalability enhancements. Each task is optional.

- Increasing the Input Hold-Queue Limit
- Increasing the Output Hold-Queue Limit
- Limiting the Number of LCP Session Initiations
- Limiting the Load Metric
- Modifying the PPP Authentication Timeout
- Modifying the PPP Retry Timeout

### Increasing the Input Hold-Queue Limit

If the **show interfaces EXEC** command reveals an excessive number of discarded packets because of input hold-queue overflows, increase the input hold-queue limit by completing the following steps, beginning in global configuration mode.

	Command	Purpose
Step 1	Router(config)# <b>interface atm slot/subslot/port</b>	Select the ATM interface.
Step 2	Router(config-if)# <b>hold-queue length in</b>	Specify the maximum number of packets in the input hold-queue.

### Verifying the Input Hold-Queue Limit

To display the current input hold-queue setting and the number of packets discarded because of input hold-queue overflows, use the **show interfaces EXEC** command.

## Increasing the Output Hold-Queue Limit

If the **show interfaces EXEC** command reveals an excessive number of discarded packets because of output hold-queue overflows, increase the output hold-queue limit by completing the following steps, beginning in global configuration mode.

	Command	Purpose
Step 1	Router(config)# <b>interface atm slot/subslot/port</b>	Select the ATM interface.
Step 2	Router(config-if)# <b>hold-queue length out</b>	Specify the maximum number of packets in the output hold-queue.

### Verifying the Output Hold-Queue Limit

To display the current output hold-queue setting and the number of packets discarded because of output hold-queue overflows, use the **show interfaces EXEC** command.

## Limiting the Number of LCP Session Initiations

By default, the system does not limit the number of simultaneously active LCP sessions. Allowing a large number of LCP sessions to start in parallel causes many sessions to timeout and retry, and can result in a chain reaction of LCP session negotiations and excessive session recovery times. The chain reaction can be controlled by limiting the number of simultaneous LCP session initiations. This allows sessions to be established prior to additional initiations.

To limit the number of simultaneous LCP session initiations, use the following command in global configuration mode.

Command	Purpose
Router(config)# <b>lcp max-session-starts number</b>	Specifies the maximum number of simultaneous LCP sessions to be negotiated. Value must be between 100 and 3000.



#### Note

The nominal value depends on many factors. Cisco recommends that you start with the lowest value of 100. Try several numbers and select the one that results in the shortest session recovery time after a link dropout.

### Verifying the LCP Session Initiation Limit

To check the configured limit of LCP session initiations, use the **show running-config EXEC** command.

## Limiting the Load Metric

To limit the load metric, use the following command in global configuration mode.

Command	Purpose
Router(config)# <b>lcp max-load-metric</b> <i>number</i>	Specifies the maximum load metric based on the length of the PPP manager process input queue.



### Note

The nominal value depends on many factors. Cisco recommends that you start with 100. Try several numbers and select the one that results in the shortest session recovery time after a link dropout.

## Verifying the Load Metric Limit

To check the configured limit of LCP session initiations, use the **show running-config EXEC** command.

## Modifying the PPP Authentication Timeout

The PPP authentication timeout determines how long to wait for a response from the remote peer before retransmitting one of the following packets:

- Password Authentication Protocol (PAP) authentication request
- Challenge Handshake Authentication Protocol (CHAP) challenge
- CHAP response

The default PPP authentication timeout is 10 seconds. To modify the PPP authentication timeout, complete the following steps beginning in global configuration mode:

	Command	Purpose
Step 1	NRP(config)# <b>interface virtual-template</b> <i>number</i>	Selects or creates the virtual template interface and enters interface configuration mode.
Step 2	NRP(config-if)# <b>ppp timeout authentication</b> <i>seconds</i>	0 - 255. Specifies the PPP authentication timeout, in seconds.



### Note

The nominal value depends on many factors. Cisco recommends that you start with a PPP authentication timeout of 15 seconds. Try several numbers and select the one that results in the highest number of stable sessions.

## Verifying the PPP Authentication Timeout

To check the configured PPP authentication timeout, use the **show running-config EXEC** command.

## Modifying the PPP Retry Timeout

The PPP retry timeout determines how long the PPP state machine (for LCP and all NCP's) waits for a response from the remote peer before retransmitting one of the following packets:

- Configuration request
- Connection termination request

The default PPP retry timeout is 2 seconds. To modify the PPP retry timeout, complete the following steps beginning in global configuration mode:

	Command	Purpose
Step 1	<code>NRP(config)# interface virtual-template number</code>	Selects or creates the virtual template interface and enters interface configuration mode.
Step 2	<code>NRP(config-if)# ppp timeout retry seconds</code>	1 - 255. Specifies the PPP retry timeout, in seconds.



### Note

The nominal value depends on many factors. Cisco recommends that you start with a PPP retry timeout of 15 seconds. Try several numbers and select the one that results in the highest number of stable sessions.

## Verifying the PPP Retry Timeout

To check the configured PPP retry timeout, use the **show running-config EXEC** command.

## Configuration Example

For general L2TP configuration examples, see the *Layer 2 Tunnel Protocol* feature module.

The following example shows a configuration implementing the enhancements documented in this feature module as well as in the *Layer 2 Tunnel Protocol Scalability Enhancements* feature module. The input hold queue limit on an ATM interface is set to 1200, and virtual template 1 is used to preclone 2000 virtual access interfaces. VPDN group 1 is set to use 7 retransmission attempts, with the retransmission timeouts beginning at 2 seconds and ending at 4 seconds, and the L2TP tunnel timeout

is set to 10 seconds. The local RWS is set to 500 packets. The number of simultaneous LCP session initiations are limited to 100, and the load metric is limited to 100. Both the PPP authentication and retry timeouts are set to 15 seconds.

```
!  
vpdn enable  
!  
vpdn-group 1  
  accept-dialin  
  protocol l2tp  
  virtual-template 1  
  terminate from hostname LAC1  
  local name LNS1  
  l2tp tunnel receive-window 500  
  l2tp tunnel nosession-timeout 10  
  l2tp tunnel retransmit retries 7  
  l2tp tunnel retransmit timeout min 2  
  l2tp tunnel retransmit timeout max 4  
!  
virtual-template 1 pre-clone 2000  
!  
interface ATM 0/0/0  
  hold-queue 1200 in  
!  
interface FastEthernet 0/0/0  
  ip address negotiated  
  no ip directed-broadcast  
!  
interface Virtual-Template 1  
  ip unnumbered FastEthernet 0/0/0  
  no ip directed-broadcast  
  no logging event link-status  
  no keepalive  
  peer default ip address pool pool-1  
  ppp authentication chap  
→ ppp timeout retry 15  
→ ppp timeout authentication 15  
!  
→ lcp max-session-starts 100  
→ lcp max-load-metric 100  
!
```

## Command Reference

This section documents new commands. All other commands used with this feature are documented in the Cisco IOS Release 12.1 command reference publications.

- **lcp max-load-metric**
- **lcp max-session-starts**
- **ppp timeout authentication**
- **ppp timeout retry**

# lcp max-load-metric

To limit load metric, use the **lcp max-load-metric** global configuration command. To disable this limit, use the **no** form of the command.

**lcp max-load-metric** *number*

**no lcp max-load-metric**

Syntax Description	<i>number</i>	Maximum load metric based on the length of the PPP manager process input queue.
--------------------	---------------	---

Defaults	Unlimited
----------	-----------

Command Modes	Global configuration
---------------	----------------------

Command History	Release	Modification
	12.1(1) DC1	This command was introduced on the Cisco 6400 NRP.

Usage Guidelines	The nominal limit depends on many factors. Try several numbers and select the one that results in the shortest session recovery time after a link dropout.
------------------	--

Examples	The following example limits the load metric to 100:
----------	--

```
lcp max-load-metric 100
```

# lcp max-session-starts

To limit the number of simultaneous link control protocol (LCP) session initiations, use the **lcp max-session-starts** global configuration command. To disable this limit, use the **no** form of the command.

**lcp max-session-starts** *number*

**no lcp max-session-starts**

<b>Syntax Description</b>	<i>number</i>	Maximum number of simultaneous LCP session initiations.				
<b>Defaults</b>	Unlimited number of simultaneous LCP sessions initiations					
<b>Command Modes</b>	Global configuration					
<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>12.1(1) DC1</td> <td>This command was introduced on the Cisco 6400 NRP.</td> </tr> </tbody> </table>	Release	Modification	12.1(1) DC1	This command was introduced on the Cisco 6400 NRP.	
Release	Modification					
12.1(1) DC1	This command was introduced on the Cisco 6400 NRP.					
<b>Usage Guidelines</b>	<p>Range of possible values: 100 to 3000.</p> <p>The nominal limit depends on many factors. Try several numbers and select the one that results in the shortest session recovery time after a link dropout.</p>					
<b>Examples</b>	<p>The following example limits the number of simultaneous LCP session initiations to 100:</p> <pre>lcp max-session-starts 100</pre>					

# ppp timeout authentication

To set the amount of time to wait for a response from the remote peer before retransmitting a PAP authenticate request, CHAP challenge, or CHAP response, use the **ppp timeout authentication** interface configuration command. To return to the default timeout, use the **no** form of the command.

**ppp timeout authentication** *seconds*

**no ppp timeout authentication**

<b>Syntax Description</b>	<i>seconds</i>	0 - 255. Time between retransmissions.
---------------------------	----------------	--

<b>Defaults</b>	10 seconds
-----------------	------------

<b>Command Modes</b>	Interface configuration
----------------------	-------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	11.3(2)T	This command was introduced.
12.1(1)DC1	This command was modified for the Cisco 6400 NRP.	

<b>Usage Guidelines</b>	The nominal value depends on many factors. Cisco recommends that you start with a PPP authentication timeout of 15 seconds. Try several values and select the one that results in the highest number of stable sessions.
-------------------------	--

<b>Examples</b>	In the following example, the authentication timeout is set to 15 seconds:
-----------------	--

```

!
interface Virtual-Template1
  no ip address
  no logging event link-status
  keepalive 200
  no peer default ip address
  ppp authentication chap
  ppp timeout retry 15
→ ppp timeout authentication 15
!

```

# ppp timeout retry

To set the amount of time the PPP state machine (for LCP and NCP) waits for a response from the remote peer before retransmitting a configuration request or connection termination request, use the **ppp timeout retry** interface configuration command. To return to the default timeout, use the **no** form of the command.

**ppp timeout retry** *seconds*

**no ppp timeout retry**

<b>Syntax Description</b>	<i>seconds</i>	1 - 255. Time between retransmissions.
---------------------------	----------------	--

<b>Defaults</b>	2 seconds
-----------------	-----------

<b>Command Modes</b>	Interface configuration
----------------------	-------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	11.3(2) T	This command was introduced.
12.1(1)DC1	This command was modified for the Cisco 6400 NRP.	

<b>Usage Guidelines</b>	The nominal value depends on many factors. Cisco recommends that you start with a PPP retry timeout of 15 seconds. Try several values and select the one that results in the highest number of stable sessions.
-------------------------	---

<b>Examples</b>	In the following example, the retry timeout is set to 15 seconds:
-----------------	---

```

!
interface Virtual-Template1
no ip address
no logging event link-status
keepalive 200
no peer default ip address
ppp authentication chap
ppp timeout retry 15
→ ppp timeout authentication 15
!
```

# Glossary

**CHAP**—Challenge Handshake Authentication Protocol. Security feature supported on lines using PPP encapsulation that prevents unauthorized access. CHAP does not itself prevent unauthorized access; it merely identifies the remote end. The router or access server then determines whether that user is allowed access. Compare to PAP.

**control messages**—Signaling messages that provide the control of setup, maintenance, and tear-down of L2TP sessions and tunnels.

**L2TP**—Layer 2 Tunnel Protocol. An Internet Engineering Task Force (IETF) standards track protocol defined in RFC 2661 that provides tunneling of PPP. Based upon the best features of L2F and PPTP, L2TP provides an industry-wide interoperable method of implementing VPDN.

**L2TP access concentrator**—See LAC.

**L2TP network server**—See LNS.

**L2TP session**—Communications transactions between the LAC and LNS that support tunneling of a single PPP connection. There is a one-to-one relationship among the PPP connection, L2TP session, and L2TP call.

**LAC**—L2TP access concentrator. A node that acts as one side of an L2TP tunnel endpoint and is a peer to the L2TP network server (LNS). The LAC sits between an LNS and a remote system and forwards packets to and from each. Packets sent from the LAC to the LNS require tunneling with the L2TP protocol as defined in this document. The connection from the LAC to the remote system is either local or a PPP link.

**LCP**—Link control protocol. Protocol that establishes, configures, and tests data-link connections for use by PPP. See also PPP.

**link control protocol**—See LCP.

**LNS**—L2TP network server. A node that acts as one side of an L2TP tunnel endpoint and is a peer to the L2TP access concentrator (LAC). The LNS is the logical termination point of a PPP session that is being tunneled from the remote system by the LAC. Analogous to the Layer 2 Forwarding (L2F) home gateway (HGW).

**Layer 2 Tunnel Protocol**—See L2TP.

**NCP**—Network Control Protocol. Series of protocols for establishing and configuring different network layer protocols, such as for AppleTalk over PPP.

**PAP**—Password Authentication Protocol. Authentication protocol that allows PPP peers to authenticate one another. The remote router attempting to connect to the local router is required to send an authentication request. Unlike CHAP, PAP passes the password and host name or username in the clear (unencrypted). PAP does not itself prevent unauthorized access, but merely identifies the remote end. The router or access server then determines if that user is allowed access. PAP is supported only on PPP lines. Compare with CHAP.

**Point-to-Point Protocol**—See PPP.

**PPP**—Point-to-Point Protocol. A protocol that encapsulates network layer protocol information over point-to-point links. PPP is defined in RFC 1661.

**Virtual Private Dialup Networking**—See VPDN.

**VPDN**—Virtual Private Dialup Networking. A system that permits the physical dialup connection to appear to be connected directly to a home network while actually residing elsewhere on the network. A virtual pipe is connected between the physical dialup connections and the termination point at the home network.