

Managing the L2TP Destination Lockout Process

When multiple sets of tunneling parameters are available, L2TP uses a selection algorithm to choose the best tunnel for subscriber traffic. As part of this selection process, the JUNOS software's L2TP implementation includes a lockout feature in which the router locks out, or disregards, destinations that are assumed to be unavailable.

By default, when a destination becomes unavailable, L2TP locks out that destination for a lockout timeout of 300 seconds (5 minutes). After the lockout timeout expires, L2TP assumes that the destination is now available and includes the destination when performing the selection algorithm.

Tasks to manage the L2TP lockout process include:

1. Modifying the Lockout Procedure on page 1
2. Verifying that a Locked-Out Destination is Available on page 2
3. Configuring a Lockout Timeout on page 2
4. Unlocking a Destination that is Currently Locked Out on page 3
5. Starting an Immediate Lockout Test on page 3

Modifying the Lockout Procedure

You can optionally configure your own lockout procedure by specifying the lockout timeout you want to use or enabling a lockout test, or both. When the lockout timeout expires, the destination is either immediately unlocked (if lockout testing is not enabled) or begins the lockout test to verify that the destination is available.

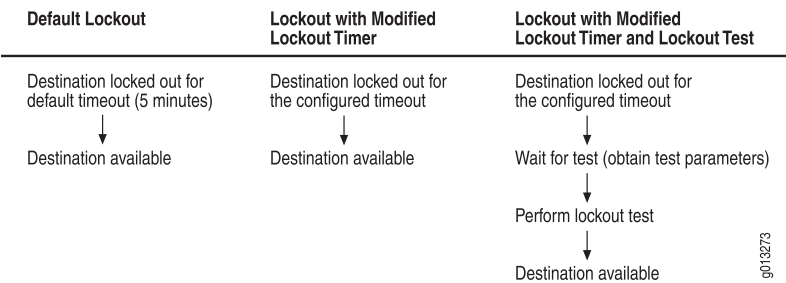
L2TP performs the lockout test by attempting to establish a tunnel to the unavailable destination. For the test, L2TP must first obtain the parameters for a tunnel to the destination. If no such tunnel currently exists, L2TP must wait until it receives a new session request that has tunnel parameters for the locked out destination. The destination remains locked out while L2TP waits for the tunnel parameters and becomes available only after successful completion of the lockout test. Therefore, if lockout testing is enabled, the destination is actually locked out longer than the lockout timer you specify.



NOTE: Always configure the lockout timeout to be shorter than the destruct timeout. The destruct timeout (as described in Specifying a Destruct Timeout for L2TP Tunnels and Sessions) overrides the lockout timeout—when the destruct timeout expires, all information about the locked out destination is deleted, including the time remaining on the destination's lockout timeout and the requirement to run a lockout test prior to returning the destination to service. As a result, the locked out destination might be returned to service prior to expiration of your configured lockout timeout and without completion of the lockout test you specified.

Figure 1 on page 2 shows how locked-out destinations transition from a locked-out state to available status when using the default lockout configuration, a configuration that includes a modified lockout timer, and a configuration with both a modified timer and the lockout test.

Figure 1: Lockout States



You can use the following commands to manage L2TP destination lockout and configure a lockout process that meets the needs of your network environment:

- Use the **`I2tp destination lockout-timeout`** command to modify the default lockout timeout period.
- Use the **`I2tp destination lockout-test`** command to configure L2TP to perform a lockout test, which verifies that a currently locked out destination is now available and to include it in the selection algorithm.
- Use the **`I2tp unlock destination`** command to force L2TP to immediately unlock the specified locked out destination; the destination is then considered to be available by the selection algorithm. L2TP disregards any time remaining in the existing lockout timeout and also disregards the lockout test (if configured).
- Use the **`I2tp unlock-test destination`** command to force L2TP to immediately begin the lockout testing procedure for the specified destination; any time remaining in the existing lockout timeout is not taken into account.
- Use the **`show I2tp`** and **`show I2tp destination lockout`** commands to view information about the L2TP configuration and statistics.

Verifying that a Locked-Out Destination is Available

You can use the **`I2tp destination lockout-test`** command to configure L2TP to test locked-out destinations; this verifies that a previously locked-out destination is available before the router changes the destination’s status.

- To verify the availability of locked out destinations:

host1(config)#**`I2tp destination lockout-test`**

Configuring a Lockout Timeout

You use the **`I2tp destination lockout-timeout`** command to configure the amount of time (in seconds) between when an L2TP destination is found to be unavailable and when it is eligible for unlocking. When the timeout period expires, L2TP either begins the lockout test procedure (if configured to do so) or immediately returns the destination to available state.



BEST PRACTICE: Always configure the lockout timeout to be shorter than the destruct timeout. The destruct timeout (as described in *Specifying a Destruct Timeout for L2TP Tunnels and Sessions*) overrides the lockout timeout—when the destruct timeout expires, all information about the locked out destination is deleted, including the time remaining on the destination's lockout timeout and the requirement to run a lockout test prior to returning the destination to service.

You can specify a lockout timeout in the range 60–3600 seconds (1 minute–1 hour). The router uses a timeout value of 300 seconds by default.

- To configure an L2TP lockout timeout:

```
host1(config)#l2tp destination lockout-timeout 500
```

The new lockout timeout only affects future locked-out destinations; it does not affect destinations that are currently locked out.

Unlocking a Destination that is Currently Locked Out

You use the **l2tp unlock destination** command to force L2TP to immediately unlock the specified L2TP destination, which is currently locked out and unavailable. L2TP then considers the destination to be available. Any remaining lockout time and the lockout test setting (if configured) are not taken into account.

You must be at privilege level 10 or higher to use this command.

- To unlock a currently locked-out destination:

```
host1(config)#l2tp unlock destination ip 192.168.1.98
```

Starting an Immediate Lockout Test

You use the **l2tp unlock-test destination** command to force L2TP to immediately start the lockout test for the specified destination—any remaining lockout time for the destination is ignored.

You must be at privilege level 10 or higher to use this command.



NOTE: If lockout testing is not configured, this command immediately unlocks the destination and L2TP then considers the destination to be available

- To force an immediate lockout test for a specific destination:

```
host1(config)#l2tp unlock-test destination ip 192.169.110.8
```

