CHAPTER 16

Configuring Port Security

This chapter describes how to configure port security on the Catalyst enterprise LAN switches.

Note
For complete syntax and usage information for the commands that are used in this chapter, refer to the Catalyst 4500 Series, Catalyst 2948G, Catalyst 2948G-GE-TX, and Catalyst 2980G Switches Command Reference.

This chapter consists of these sections:

- Understanding How Port Security Works, page 16-1
- Port Security Configuration Guidelines, page 16-3
- Configuring Port Security on the Switch, page 16-3
- Monitoring Port Security, page 16-10

Understanding How Port Security Works

You can use port security to block input to an Ethernet, Fast Ethernet, or Gigabit Ethernet port when the MAC address of the station attempting to access the port is different from any of the MAC addresses that are specified for that port. Alternatively, you can use port security to filter traffic that is destined to or received from a specific host that is based on the host MAC address.

Allowing Traffic Based on the Host MAC Address

The total number of MAC addresses that can be specified per port is limited to the global resource of 1024 plus 1 default MAC address. That is, the total number of MAC addresses on any port cannot exceed 1025.

The maximum number of MAC addresses that you can allocate for each port depends on your network configuration. The following combinations are valid allocations:

- 1025 (1 + 1024) addresses on one port and 1 address each on the rest of the ports
- 513 (1 + 512) each on two ports in a system and 1 address each on the rest of the ports
- 901 (1 + 900) on one port, 101 (1 + 100) on another port, 25 (1 + 24) on a third port, and 1 address on each of the rest of the ports
After you allocate the maximum number of MAC addresses on a port, you can either specify the secure MAC address for the port manually or have the port dynamically configure the MAC address of the connected devices. Out of a maximum allocated number of MAC addresses on a port, you can manually configure all, allow all to be autoconfigured, or configure some manually and allow the rest to be autoconfigured. Once you manually configure or autoconfigure the addresses, they are stored in nonvolatile RAM (NVRAM) and are maintained after a reset.

When you manually change the maximum number of MAC addresses that are associated to a port greater than the default value and then manually enter the authorized MAC addresses, any remaining MAC addresses are automatically configured. For example, if you configure the port security for a port to have a maximum of ten MAC addresses but add only two MAC addresses, the next eight new source MAC addresses that are received on that port are added to the secured MAC address list for the port.

After you allocate a maximum number of MAC addresses on a port, you can also specify how long the addresses on the port will remain secure. After the age time expires, the MAC addresses on the port become insecure. By default, all addresses on a port are secured permanently.

If a security violation occurs, you can configure the port to go either into shutdown mode or restrictive mode. The shutdown mode option allows you to specify whether the port is to be permanently disabled or disabled for only a specified time. The default is for the port to shut down permanently. The restrictive mode allows you to configure the port to remain enabled during a security violation and drop only packets that are coming in from insecure hosts.

**Note**
If you configure a secure port in restrictive mode, and a station is connected to the port whose MAC address is already configured as a secure MAC address on another port on the switch, the port in restrictive mode shuts down instead of restricting traffic from that station. For example, if you configure MAC-1 as the secure MAC address on port 2/1 and MAC-2 as the secure MAC address on port 2/2 and then connect the station with MAC-1 to port 2/2 when port 2/2 is configured for restrictive mode, port 2/2 shuts down instead of restricting traffic from MAC-1.

When a secure port receives a packet, the source MAC address of the packet is compared to the list of secure source addresses that were manually configured or autoconfigured (learned) on the port. If a MAC address of a device that is attached to the port differs from the list of secure addresses, the port either shuts down permanently (default mode), shuts down for the time that you have specified, or drops incoming packets from the insecure host.

The behavior of a port depends on how you configure it to respond to a security violation. If a security violation occurs, the LED labeled Link for that port turns orange, and a link-down trap is sent to the Simple Network Management Protocol (SNMP) manager. An SNMP trap is not sent if you configure the port for restrictive violation mode. A trap is sent only if you configure the port to shut down during a security violation.

**Restricting Traffic Based on the Host MAC Address**

You can filter traffic based on a host MAC address, so that packets tagged with a specific source MAC address are discarded. When you specify a MAC address filter with the `set cam filter` command, incoming traffic from that host MAC address is dropped, and packets that are addressed to that host are not forwarded. You cannot filter traffic for multicast addresses with this command.

**Note**
The `set cam filter` command allows filtering for unicast addresses only.
Blocking Unicast Flood Packets on Secure Ports

You can block unicast flood packets on a secure Ethernet port by disabling the unicast flood feature. If you disable unicast flood on a port, the port will drop unicast flood packets when the port reaches the allowed maximum number of MAC addresses.

The port automatically restarts unicast flood packet learning when the number of MAC addresses drops below the maximum number that is allowed. The learned MAC address count decreases when a configured MAC address is removed or a time to live counter (TTL) is reached.

For more information about unicast flood packets, see Chapter 17, “Configuring Unicast Flood Blocking.”

Port Security Configuration Guidelines

This section lists the guidelines for configuring port security:

- Do not configure port security on a SPAN destination port.
- Do not configure SPAN destination on a secure port.
- Do not configure dynamic, static, or permanent CAM entries on a secure port.

Configuring Port Security on the Switch

The following sections describe how to configure port security.

Enabling Port Security

Port security is either autoconfigured or enabled manually by specifying a MAC address. If a MAC address is not specified, the source address from the incoming traffic is autoconfigured and secured, up to the maximum number of MAC addresses allowed. These autoconfigured MAC addresses remain secured for a time, depending upon the aging timer set. The autoconfigured MAC addresses are cleared from the port in case of a link-down event.

When you enable port security on a port, any dynamic CAM entries that are associated with the port are cleared. If there are any currently configured static or permanent CAM entries on that same port, you may not be able to enable the port-security on that port. If this is the case, clear the configured static and permanent earl entries on that port and then enable port-security.

To enable port security, perform this task in privileged mode:

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 Enable port security on the desired ports. If desired, specify the secure MAC address.</td>
<td>set port security mod_num/port_num enable [mac_addr]</td>
</tr>
<tr>
<td>Step 2 You can add MAC addresses to the list of secure addresses.</td>
<td>set port security mod_num/port_num mac_addr</td>
</tr>
<tr>
<td>Step 3 Verify the configuration.</td>
<td>show port [mod_num[/port_num]]</td>
</tr>
</tbody>
</table>
This example shows how to enable port security using the learned MAC address on a port:

```
Console> (enable) set port security 2/1 enable
Port 2/1 port security enabled with the learned mac address.
Trunking disabled for Port 2/1 due to Security Mode
```

This example shows how to verify the port security:

```
Console> (enable) show port 2/1
Port Name               Status     Vlan       Level  Duplex Speed Type
----- ------------------ ---------- ---------- ------ ------ ----- ------------
2/1                     connected  522        normal   half   100 100BaseTX
Port Security Secure-Src-Addr   Last-Src-Addr     Shutdown Trap     IfIndex
----- -------- ----------------- ----------------- -------- -------- -------
2/1  enabled  00-90-2b-03-34-08 00-90-2b-03-34-08 No       disabled 1081
Port Broadcast-Limit Broadcast-Drop
---------- ----------------- ------------
2/1  -              0
Port Align-Err FCS-Err Xmit-Err Rcv-Err UnderSize
---------- ---------- ---------- ---------- ----------
2/1  0          0          0          0         0
Port Single-Col Multi-Coll Late-Coll Excess-Col Carri-Sen Runts Giants
---------- ---------- ---------- ---------- --------- ---------
2/1  0          0          0          0         0         0
Last-Time-Cleared
--------------------------
Fri Jul 10 1998, 17:53:38
```

This example shows how to enable port security on a port and manually specify the secure MAC address:

```
Console> (enable) set port security 2/1 enable 00-90-2b-03-34-08
Port 2/1 port security enabled with 00-90-2b-03-34-08 as the secure mac address
Trunking disabled for Port 2/1 due to Security Mode
```

**Setting the Maximum Number of Secure MAC Addresses**

You can set the number of MAC addresses to secure on a port. By default, at least one MAC address per port can be secured. In addition to this default, a global resource of up to 1024 MAC addresses is available to be shared by the ports. If the entire global resource of 1024 MAC addresses is used on some ports, you can still enable port security on the rest of the ports with a maximum of one MAC per port.

If you reduce the maximum number of MAC addresses, the system clears the specified number of MAC addresses and displays the list of removed addresses.

To set the number of MAC addresses to be secured on a port, perform this task in privileged mode:

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set the number of MAC addresses to be secured on a port.</td>
<td><code>set port security mod_num/port_num maximum num_of_mac</code></td>
</tr>
</tbody>
</table>
This example shows how to set the number of MAC addresses to be secured:

```
Console> (enable) set port security 4/7 maximum 20
Maximum number of secure addresses set to 20 for port 4/7.
Console> (enable)
```

This example shows how to reduce the number of MAC addresses; it also shows how to display the list of cleared MAC addresses:

```
Console> (enable) set port security 4/7 maximum 18
Maximum number of secure addresses set to 18 for port 4/7
00-11-22-33-44-55 cleared from secure address list for port 4/7
00-11-22-33-44-66 cleared from secure address list for port 4/7
Console> (enable)
```

### Setting the Port Security Age Time

The age time on a port specifies how long all addresses on that port will be secured. This age time is activated when a MAC address initiates traffic on the port. After the age time expires for a MAC address, the entry for that MAC address on the port is removed from the secure address list. The valid range is from 1–1440 minutes. Setting the age time to zero disables aging of secure addresses.

To set the age time on a port, perform this task in privileged mode:

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set the age time for which addresses on a port will be secured.</td>
<td><code>set port security</code> mod_num/port_num age time</td>
</tr>
</tbody>
</table>

```
Console> (enable) set port security 4/7 age 600
Secure address age time set to 600 minutes for port 4/7.
Console> (enable)
```

### Clearing MAC Addresses

Enter the `clear port security` command to clear MAC addresses from a list of secure addresses on a port.

**Note**

If you enter the `clear` command on a MAC address that is in use, the network may relearn that MAC address and make the MAC address secure again. We recommend that you disable port security before you clear the MAC addresses.

To clear all of the MAC addresses or one particular address from the list of secure MAC addresses, perform this task in privileged mode:

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clear all of the MAC addresses or one particular address from the list of secure MAC addresses.</td>
<td><code>clear port security</code> mod_num/port_num [mac_addr</td>
</tr>
</tbody>
</table>

```
```
This example removes one MAC address from the secure address list on port 4/7:

```console
Console> (enable) clear port security 4/7 00-11-22-33-44-55
00-11-22-33-44-55 cleared from secure address list for port 4/7
Console> (enable)
```

This example removes all MAC addresses from ports 4/5–7:

```console
Console> (enable) clear port security 4/5-7 all
All addresses cleared from secure address list for ports 4/5-7
Console> (enable)
```

### Configuring Unicast Flood Blocking on Secure Ports

To configure unicast flood blocking, you must disable the unicast flood feature.

**Note**
The port disables unicast flooding once the MAC address limit is reached.

To configure unicast flood blocking on a secure port, perform this task in privileged mode:

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 Disable unicast flood blocking on the desired secure ports.</td>
<td>set port security mod/port unicast-flood disable</td>
</tr>
<tr>
<td>Step 2 Verify the configuration of unicast flood blocking.</td>
<td>show port security mod/port</td>
</tr>
<tr>
<td>Step 3 Verify the status of unicast flood blocking.</td>
<td>show port unicast-flood mod/port</td>
</tr>
</tbody>
</table>

This example shows how to configure the switch to disable unicast flood packets on a port and verify its configuration:

```console
Console> (enable) set port security 4/1 unicast-flood disable
Port 4/1 security flood mode set to disable.
Console> (enable) show port security 4/1
Port Security Violation Shutdown-Time Age-Time Max-Addr Trap IfIndex
-------- ----- --------- ------------- -------- -------- --------- -------
4/1 disabled shutdown 0 0 1 disabled 50
Port Num-Addr Secure-Src-Addr Age-Left Last-Src-Addr Shutdown/Time-Left
-------- ------------- ----------- --------- ----------------- ---------
4/1 0 - - - -
```

**Note**
The `show port unicast-flood` command displays the run-time status of unicast flood blocking. The output can show unicast flooding as either enabled or disabled depending upon if the port has exceeded its address limitation.
Enabling MAC Address Notification

Enabling MAC address notification allows you to monitor MAC addresses at the module and port level that were added by the switch or removed from the CAM table.

A new MAC address is added when either of the following occurs:
- When a packet is received from a new device on one of the ports of the switch with a new source address
- When the MAC address is added to the CAM table by the CLI

A MAC address is removed from the CAM table when one of the following is true:
- When the MAC address receives no packets during the time-out period
- When the switch invalidates a CAM table entry and replaces the entry with a new entry
- When the MAC address is removed from the CAM table by the CLI

**Note**
MAC address notification settings are ignored on PAgP and LACP EtherChannel ports.

To enable MAC address notification globally, perform this task in privileged mode:

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Enable MAC address notification globally. set cam notification { enable</td>
</tr>
<tr>
<td>Step 2</td>
<td>Set the history log size. set cam notification historysize log_size</td>
</tr>
<tr>
<td>Step 3</td>
<td>Enable notification of added MAC addresses. set cam notification added { enable</td>
</tr>
<tr>
<td>Step 4</td>
<td>Enable notification of removed MAC addresses. set cam notification removed { enable</td>
</tr>
<tr>
<td>Step 5</td>
<td>Verify the configuration. show cam notification all</td>
</tr>
</tbody>
</table>

MAC addresses are stored in memory between notifications. To set the interval time between notifications and verify the configuration, perform this task in privileged mode:

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Set the interval time between notifications. set cam notification interval time</td>
</tr>
<tr>
<td>Step 2</td>
<td>Verify the configuration. show cam notification all</td>
</tr>
</tbody>
</table>

If the `set cam notification interval` is set to 0, the switch will send notification immediately. If the notifications are sent immediately, they will have an impact on the performance of the switch.

You can generate SNMP traps whenever a MAC address change occurs; do so by enabling the `set snmp trap enable macnotification`, `set cam notification`, and `set cam notification historysize` commands.
To set the SNMP trap MAC address notification, perform this task in privileged mode:

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set the SNMP traps on the system.</td>
<td>set snmp trap enable macnotification</td>
</tr>
</tbody>
</table>

This example shows how to enable MAC address notification globally, enable notification of added and removed MAC addresses, and set the interval time between notifications:

```
Console> (enable) set cam notification enable
MAC address change detection globally enabled

Be sure to specify which ports are to detect MAC address changes with the 'set cam notification [added|removed] enable <m/p> command.

SNMP traps will be sent if 'set snmp trap enable macnotification' has been set.

Console> (enable) set cam notification historysize 300
MAC address change history log size set to 300 entries

Console> (enable) set cam notification added enable 3/1-4
MAC address change notifications for added addresses are enabled on port(s) 3/1-4

Console> (enable) set cam notification removed enable 3/3-6
MAC address change notifications for removed addresses are enabled on port(s) 3/3-6

Console> (enable) set cam notification interval 10
MAC address change notification interval set to 10 seconds

Console> (enable) show cam notification all
MAC address change detection enabled
CAM notification interval = 10 second(s).
MAC addresses added = 3
MAC addresses removed = 5
MAC addresses added overflowed = 0
MAC addresses removed overflowed = 0
MAC address SNMP traps generated = 0

Console> (enable) set snmp trap enable macnotification
SNMP MAC notification trap enabled.
```

**Setting the Security Violation Action**

You can set a port to the following two modes to handle a security violation:

- **Shutdown**—Shuts down the port permanently or for a specified time. Permanent shutdown is the default mode.
- **Restrict**—Drops all packets from insecure hosts, but remains enabled.

To set the security violation action to be taken, perform this task in privileged mode:

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set the security violation action on a port.</td>
<td>set port security mod_num/port_num violation {shutdown</td>
</tr>
</tbody>
</table>
Chapter 16 Configuring Port Security

Configuring Port Security on the Switch

This example shows how to set the port to drop all packets that are coming in on the port from insecure hosts:

```
Console> (enable) set port security 4/7 violation restrict
Port security violation on port 4/7 will cause insecure packets to be dropped.
```

### Setting the Shutdown Time

You can specify how long a port is to remain disabled in the event of a security violation. By default, the port is shut down permanently. The valid range is from 1–1440 minutes.

If you set the time to zero, the shut down is disabled for this port.

**Note**

When the shutdown timeout expires, the port is reenabled and all port security-related configuration is maintained.

To set the shutdown timeout, perform this task in privileged mode:

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set the shutdown timeout on a port.</td>
<td><code>set port security mod_num/port_num shutdown time</code></td>
</tr>
</tbody>
</table>

This example shows how to set the shutdown time to 600 minutes on port 4/7:

```
Console> (enable) set port security 4/7 shutdown 600
Secure address shutdown time set to 600 minutes for port 4/7.
```

### Disabling Port Security

To disable port security, perform this task in privileged mode:

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Disable port security on the desired ports.</td>
<td><code>set port security mod_num/port_num disable</code></td>
</tr>
<tr>
<td>Step 2</td>
<td>Verify the configuration.</td>
<td><code>show port security [mod_num/port_num]</code></td>
</tr>
</tbody>
</table>

This example shows how to disable security on a port:

```
Console> (enable) set port security 2/1 disable
Port 2/1 port security disabled.
Console> (enable) show port security 2/1
Port Security Violation Shutdown-Time Age-Time Max-Addr Trap IfIndex
------ ------ ------------- -------------- -------- -------- ------- -------
3/24 disabled restrict 20 300 10 disabled 921
Port Num-Addr Secure-Src-Addr Age-Left Last-Src-Addr Shutdown/Time-Left
------ ------ --------- ------ -------------- -----------
3/24 00-e0-4f-ac-b4-00 - - - -
```

Console> (enable)
Restricting Traffic for a Host MAC Address

To restrict incoming or outgoing traffic for a specific MAC address, perform this task in privileged mode:

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Restrict traffic that is destined to or originating from a specific MAC address.</td>
</tr>
<tr>
<td></td>
<td>set cam {static</td>
</tr>
<tr>
<td>Step 2</td>
<td>Clear the filter.</td>
</tr>
<tr>
<td></td>
<td>clear cam {static</td>
</tr>
<tr>
<td></td>
<td>clear cam mac_address vlan</td>
</tr>
<tr>
<td>Step 3</td>
<td>Verify the configuration.</td>
</tr>
<tr>
<td></td>
<td>show cam mac_address vlan</td>
</tr>
<tr>
<td></td>
<td>show cam {static</td>
</tr>
</tbody>
</table>

This example shows how to create a filter for a specific MAC address:

```
Console> (enable) set cam static filter 00-02-03-04-05-06 1
Filter entry added to CAM table.
Console> (enable)
```

This example shows how to clear the filter:

```
Console> (enable) clear cam 00-02-03-04-05-06 1
CAM entry cleared.
Console> (enable)
```

This example shows how to display the static CAM entries:

```
Console> show cam static
VLAN Dest MAC/Route Des [CoS] Destination Ports or VCs / [Protocol Type]
---- ------------------ ----- -------------------------------------------
3 04-04-05-06-07-08 * FILTER
```

Monitoring Port Security

You can view the following port security information:

- List of secure MAC addresses for a port
- Maximum number of secure addresses that are allowed on a port
- Total number of secure MAC addresses
- Age and shutdown timeout
- Shutdown and security mode
- Statistics data related to port security

To display port security configuration information and statistics, perform this task in privileged mode:
Chapter 16  Configuring Port Security

Monitoring Port Security

These examples show how to display port security configuration information and statistics:

Task | Command
--- | ---
Step 1 | Display the configuration.
Step 2 | Display the port security statistics.

These examples show how to display port security configuration information and statistics:

```
Console> (enable) show port security 3/24
Port  Security Violation Shutdown-Time Age-Time Max-Addr Trap     IfIndex
----- -------- --------- ------------- -------- -------- -------- -------
3/24  enabled shutdown           300       60       10 disabled     921

Port  Num-Addr Secure-Src-Addr   Age-Left Last-Src-Addr     Shutdown/Time-Left
----- -------- ----------------- -------- ----------------- ------------------
3/24        4 00-e0-4f-ac-b4-00       60 00-e0-4f-ac-b4-00       no         -
00-11-22-33-44-55        0
00-11-22-33-44-66        0
00-11-22-33-44-77        0

Console> (enable) show port security statistics 3/24
Port  Total-Addrs Maximum-Addrs
----- ----------- -------------
3/24           4            10

Console> (enable)
Port  Total-Addrs Maximum-Addrs
----- ----------- -------------
3/24           1            10

Console> (enable)

This example shows how to display port security statistics on a module:

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```

```
Total global address space used (out of 1024): 0
Status: installed
Console> (enable)