



Release Notes for the Catalyst 3750G Integrated Wireless LAN Controller Switch, Cisco IOS Release 12.2(25)FZ

June 12, 2006

The Catalyst 3750 Integrated Wireless LAN Controller Switch is an integrated Catalyst 3750 switch and Cisco 4400 series wireless LAN controller that supports up to 25 or 50 lightweight access points. The switch and the internal controller run separate software versions, which must be upgraded separately. These release notes contain information that applies to the software running on the switch, and describes only features that are specific to the wireless LAN controller switch.

- Cisco IOS Release 12.2(25)FZ runs on all Catalyst 3750 switches. When using the wireless LAN controller switch in a stack, you should load this image on all switches in the stack. However, wireless capability is available only on the Catalyst 3750 Integrated Wireless LAN Controller Switch. Cisco IOS Release 12.2(25)FZ is based on and contains all features of Cisco IOS Release 12.2(25)SEE. For information about these features, as well as software upgrade procedure, caveats, resolved caveats, limitations, and so on, see the [Release Notes for the Catalyst 3750 switch for Cisco IOS Release 12.2\(25\)SEE](#).
- The integrated controller runs software release 4.0.x.0 for the 4402 wireless controller. For information about this controller software release, see the [Release Notes for Cisco Wireless LAN Controllers and Lightweight Access Point, Release 4.0.x.0](#). For controller software upgrade procedure, see the [Cisco Wireless LAN Controller Configuration Guide Release 4.0](#).

The Catalyst 3750 switches support stacking through Cisco StackWise technology. Unless otherwise noted, the term *switch* refers to a standalone switch and to a switch stack.

These release notes include important information about Cisco IOS Release 12.2(25)FZ and any features, limitations, restrictions, and caveats that apply specifically to this release. Verify that these release notes are correct for your switch:

- If you are installing a new switch, see the Cisco IOS release label on the rear panel of your switch.
- If your switch is on, use the **show version** privileged EXEC command.



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

© 2006 Cisco Systems, Inc. All rights reserved.

- If you are upgrading to a new release, see the software upgrade filename for the software version. See the “[Switch Software Versions](#)” section on page 5.

Registered cisco.com users with a login password can download the switch software from this site:

<http://www.cisco.com/kobayashi/sw-center/sw-lan.shtml>



Note

For IPv6 capability on the Catalyst 3750 switches, you must order the advanced IP services image upgrade from Cisco.

The switch software release is part of a special release of Cisco IOS software that is not released on the same 8-week maintenance cycle that is used for other platforms. As maintenance releases and future software releases become available, they will be posted to Cisco.com in the Cisco IOS software area.

Cisco IOS Release 12.2(25)FZ is based on Cisco IOS Release 12.2(25)SEE. Open caveats in Cisco IOS Release 12.2(25)SEE also affect Cisco IOS Release 12.2(25)FZ, unless they are listed in the Cisco IOS Release 12.2(25)FZ resolved caveats list. The list of open caveats in Cisco IOS Release 12.2(25)SEE is available at this URL:

http://www.cisco.com/en/US/products/hw/switches/ps5023/prod_release_note09186a00805f29ad.html#wp708755

Registered users can download the integrated wireless controller software from this site:

<http://www.cisco.com/kobayashi/sw-center/sw-wireless.shtml>

For information about the Cisco wireless controller software release 4.0.x.0, including the list of open caveats for the release, see the *[Release Notes for Cisco Wireless LAN Controllers and Lightweight Access Point, Release 4.0.x.0](#)*.

For the complete list of documentation for the Catalyst 3750 switch and the integrated wireless controller, see the “[Related Documentation](#)” section on page 19.

Contents

This information is in the release notes:

- “[System Requirements](#)” section on page 3
- “[Understanding the Integrated Wireless LAN Controller Switch](#)” section on page 7
- “[Configuring the Integrated Wireless LAN Controller Switch](#)” section on page 9
- “[Catalyst 3750 Integrated Wireless LAN Controller Switch Specific Commands](#)” section on page 12
- “[Open Caveats](#)” section on page 18
- “[Resolved Caveats](#)” section on page 19
- “[Related Documentation](#)” section on page 19
- “[Obtaining Documentation](#)” section on page 20
- “[Documentation Feedback](#)” section on page 21
- “[Obtaining Technical Assistance](#)” section on page 22
- “[Obtaining Additional Publications and Information](#)” section on page 23

System Requirements

The system requirements are described in these sections:

- “Hardware Supported” section on page 3
- “Device Manager System Requirements” section on page 4
- “CNA Compatibility” section on page 5
- “Switch Software Versions” section on page 5
- “Switch and Controller Software Compatibility” section on page 6

For Device Manager requirements, see the [Release Notes for the Catalyst 3750 switch for Cisco IOS Release 12.2\(25\)SEE](#).

Hardware Supported

Table 1 lists the hardware supported by Cisco IOS Release 12.2(25)FZ and Cisco wireless controller release 4.0.x.0.



Note

Although you can download the Cisco IOS Release 12.2(25)FZ image on any Catalyst 3750 switch, the controller functionality is supported only on the Catalyst 3750 Integrated Wireless LAN Controller Switches listed in the table. When the Cisco IOS Release 12.2(25)FZ image is run on any other Catalyst 3750 switch, the switch has the same functionality as the corresponding Cisco IOS Release 12.2(25)SEE image (IP base, IP services, or advanced IP services image). However, when a stack of switches includes a Catalyst 3750 Integrated Wireless LAN Controller Switch, you should load the Cisco IOS Release 12.2(25)FZ image on all switches in the stack.

Table 1 Catalyst 3750 Wireless LAN Controller Switch Supported Hardware

Switch	Description
Catalyst 3750G-24WS-S25	24 10/100/1000 PoE ¹ ports, 2 SFP ² module slots, and an integrated wireless LAN controller supporting up to 25 access points.
Catalyst 3750G-24WS-S50	24 10/100/1000 PoE ports, 2 SFP module slots, and an integrated wireless LAN controller supporting up to 50 access points
SFP modules	1000BASE-CWDM ³ , -LX, SX, -T, -ZX 100BASE-FX MMF ⁴
Redundant power systems	Cisco RPS 675 Redundant Power System
Access points	Cisco Lightweight Access Points

1. PoE = Power over Ethernet
2. SFP = small form-factor pluggable
3. CWDM = coarse wavelength-division multiplexer
4. MMF = multimode fiber

Device Manager System Requirements

These sections describes the hardware and software requirements for using the device manager:

- “[Hardware Requirements](#)” section on page 4
- “[Software Requirements](#)” section on page 4

Hardware Requirements

[Table 2](#) lists the minimum hardware requirements for running the device manager.

Table 2 Minimum Hardware Requirements

Processor Speed	DRAM	Number of Colors	Resolution	Font Size
Intel Pentium II ¹	64 MB ²	256	1024 x 768	Small

1. We recommend Intel Pentium 4.
2. We recommend 256-MB DRAM.

Software Requirements

[Table 3](#) lists the supported operating systems and browsers for using the device manager. The device manager verifies the browser version when starting a session to ensure that the browser is supported.



Note

The device manager does not require a plug-in.

Table 3 Supported Operating Systems and Browsers

Operating System	Minimum Service Pack or Patch	Microsoft Internet Explorer ¹	Netscape Navigator
Windows 2000	None	5.5 or 6.0	7.1
Windows XP	None	5.5 or 6.0	7.1

1. Service Pack 1 or higher is required for Internet Explorer 5.5.

CNA Compatibility

Cisco IOS Release 12.2(25)FZ and later are only compatible with Cisco Network Assistant (CNA) 4.0 and later.

You can download CNA 4.0 from this URL:

<http://www.cisco.com/cgi-bin/tablebuild.pl/NetworkAssistant>

For more information about Cisco Network Assistant, see the *Release Notes for Cisco Network Assistant* on cisco.com.

Switch Software Versions

The Cisco IOS switch image is stored as a bin file in a directory that is named with the Cisco IOS release. A subdirectory contains the files needed for web management. The image is stored on the system board flash device (flash:).

You can use the **show version** privileged EXEC command to see the software version that is running on your switch. The second line of the display shows the version.



Note

For Catalyst 3750 switches, although the **show version** output always shows the software image running on the switch, the model name shown at the end of this display is the factory configuration (IP base image or IP services image) and does not change if you upgrade the software image.

You can also use the **dir filesystem:** privileged EXEC command to see the directory names of other software images that you might have stored in flash memory.

Table 4 lists the switch software filenames for this software release.

For IPv6 capability on the Catalyst 3750 switch, you must order the advanced IP services image upgrade from Cisco.

Table 4 *Catalyst 3750G Integrated Wireless LAN Controller Switch Cisco IOS Software Image Files*

Filename	Description
c3750-ipbase-tar.122-25.FZ.tar	Catalyst 3750 IP base image with controller functionality and device manager files. This image has Layer 2+ and basic Layer 3 routing features.
c3750-ipservices-tar.122-25.FZ.tar	Catalyst 3750 IP services image with controller functionality and device manager files. This image has both Layer 2+ and full Layer 3 routing features.
c3750-ipbasek9-tar.122-25.FZ.tar	Catalyst 3750 IP base cryptographic image with controller functionality and device manager files. This image has the Kerberos, SSH ¹ , Layer 2+, and basic Layer 3 routing features.

Table 4 *Catalyst 3750G Integrated Wireless LAN Controller Switch Cisco IOS Software Image Files (continued)*

Filename	Description
c3750-ipservicesk9-tar.122-25.FZ.tar	Catalyst 3750 IP services cryptographic image with controller functionality and device manager files. This image has the Kerberos, SSH, Layer 2+, and full Layer 3 features.
c3750-advipservicesk9-tar.122-25.FZ.tar	Catalyst 3750 advanced IP services image with controller functionality, cryptographic file, and device manager files. This image has all the IP services image features and the capability for unicast routing of IPv6 packets.

1. SSH = Secure Shell

See the [Release Notes for the Catalyst 3750 switch for Cisco IOS Release 12.2\(25\)SEE](#) on cisco.com for switch software upgrade procedures.

Switch and Controller Software Compatibility

The switch and controller run two different software images and interaction between them is minimal. These software images are packaged and upgraded separately. These images must be compatible for the wireless LAN controller switch to operate correctly. If the image versions are not compatible, the wireless LAN controller switch could stop functioning. [Table 5](#) is the compatibility matrix for Catalyst 3750 and wireless controller.

Table 5 *Catalyst 3750G Wireless LAN Controller Switch Software Compatibility*

Switch Software Release	Compatible Controller Software Release
Cisco IOS Release 12.2(25)FZ	Cisco Software Release 4.0.x.0

If the switch and controller software are not compatible, you need to upgrade or downgrade the software so that they are compatible:

- When the Wireless LAN Control Protocol (WCP) version in the Catalyst 3750 image and the controller image do not match, the switch generates syslog message. If the system still functions, you should upgrade or downgrade software to synchronize the images.
- If WCP stops working, you can use the second console port on the switch to upgrade or downgrade controller software.



Note If WCP stops working, the switch resets the wireless LAN controller approximately every 320 seconds.

You upgrade the Catalyst 3750 software as with any other Catalyst 3750 switch. See the [Release Notes for the Catalyst 3750 switch for Cisco IOS Release 12.2\(25\)SEE](#) for the procedure. You can upgrade the controller software directly by using TFTP after the controller management IP address is configured or directly from the Wireless Control System (WCS), an application using SNMP, as you would for a standalone 4402 controller. See the [Cisco Wireless LAN Controller Configuration Guide Release 4.0](#) on cisco.com.

Understanding the Integrated Wireless LAN Controller Switch

The Catalyst 3750 Integrated Wireless LAN Controller Switch is a Layer 3 IEEE 802.3af-compliant switch with an integrated wireless LAN controller capable of supporting up to 25 or 50 lightweight access points. The switch combines the Catalyst 3750 infrastructure with wireless LAN controller and access points to provide an IEEE 802.11 mobile wireless solution.

The wireless LAN controller switch has these features:

- Layer 2 and Layer 3 wireless mobility
- wireless LAN controller in appliance mode using Layer 3 Lightweight Access Point Protocol (LWAPP) to control access points in the same or different subnet than the controller
- Layer 3 roaming
- single point of ingress for wireless traffic
- integration of wireless traffic with existing wired network infrastructure.
- Layer 2 switching and Layer 3 routing capability
- software parity with the Catalyst 3750 IP base, IP services, and advanced IP services crypto and noncrypto images
- optimized for 25 and 50 access points and up to 500 wireless users
- Power over Ethernet ports for powering access points or other network appliances, such as IP phones

The Catalyst 3750 switch software handles all the switch features, including routing, bridging, access control lists (ACLs), and quality of service (QoS). The controller handles all wireless functionality. The Catalyst 3750 switch and the internal wireless controller are connected internally through two Gigabit Ethernet links. These links are automatically configured to direct the switch wireless traffic toward the controller, requiring minimal configuration by the user.

You can manage the switch by the switch CLI, eXpresso, or CNA. You can manage the controller from the controller CLI, the embedded controller GUI, or WCS. You can access the controller command-line interface (CLI) from the switch CLI.

The Wireless LAN Controller Switch and Switch Stacks

The wireless LAN controller switch can coexist with other Catalyst 3750 switches in a switch stack. However, for controller functionality, all switches in the stack should be running Cisco IOS Release 12.2(25)FZ. To support wireless controller redundancy, there should be at least two wireless LAN controller switches in a stack. A stack should contain no more than four wireless LAN controller switches.

The wireless LAN controller switch can be a master switch or a member switch in a stack. Stacking behavior for a wireless LAN controller switch is consistent with that of other Catalyst 3750 switches. For wireless functionality, you can configure the access points so that if one wireless LAN controller switch in a stack shuts down, the access points and wireless clients controlled by the controller in this switch automatically migrate to the controller of another wireless LAN controller switch in the stack. The traffic for wireless clients experiences a short interruption due to reassociation and reauthentication.

In a switch stack, each switch holds a unique switch number (1 to 9). This same switch number is used to access the controller in a switch in a stack or a standalone switch, where the switch number is 1 by default. For example, to access the controller in stack member 3, use the **session 3 processor 1** privileged EXEC command (where processor 1 represents the controller). To access the controller in a standalone switch, use the command **session 1 processor 1**.

**Note**

Always power off a switch before adding or removing it from a switch stack.

Controller and Switch Interaction

The Catalyst 3750 switch and its internal controller are managed separately. You can manage the switch by using the 3750 CLI, eXpresso, or CNA. You can manage the controller by using the controller CLI, the embedded controller GUI, or WCS. To use the GUI or WCS, you must configure the controller management interface, either through the 3750 CLI, the controller CLI, eXpresso, or Express Setup. See the *Catalyst 3750 Integrated Wireless LAN Controller Switch Getting Started Guide* for how to use eXpresso and express setup. To access the controller CLI, enter the **session switch-number processor 1** privileged EXEC command.

When you power on the wireless LAN controller switch, POST is performed separately by both the Catalyst 3750 switch and by the wireless controller. Both maintain separate configuration files, which must be separately saved or cleared.

Note these switch and controller interactions:

- The Catalyst 3750 switch and the controller maintain separate configuration files. They are not automatically synchronized.
- When the switch resets, this automatically resets the controller. When the controller is reset by the switch, the controller configuration is not automatically saved.
- Password recovery functions separately on the switch and on the controller.
 - You can trigger the password recovery procedure on the switch by pressing the switch Mode button. (See the “Troubleshooting” chapter in the *Catalyst 3750 Software Configuration Guide* for information about the switch password recovery procedure.)
 - Password recovery on the controller can be performed by selecting **clear config** from a hidden boot-up menu accessible if the user initiates an escape from the controller bootup process. This requires serial console access to the controller through the second console port.

Internal Ports

The two internal Gigabit Ethernet ports connect the switch and controller hardware. These ports carry the wireless control and data traffic, as well as the switch and controller management traffic. The links are automatically configured to allow internal traffic between the switch and the controller. In addition, an internal VLAN ID is chosen by the Catalyst 3750 switch and communicated to the controller. You cannot configure the internal VLAN.

In order to operate correctly with the controller, the internal ports (identified as Gigabit Ethernet ports 27 and 28) must have these characteristics:

- IEEE 802.1Q trunk mode
- static Ether Channel ports with Port Aggregation Protocol (PAgP) and Link Aggregation Control Protocol (LACP) disabled

- generation of Dynamic Trunking Protocol (DTP) frames disabled
- spanning tree protocol (STP) Port Fast mode enabled
- Cisco Discovery Protocol (CDP) disabled
- UniDirectional Link Detection (UDLD) disabled

The ports are automatically configured with these parameters, including membership in an EtherChannel port group, and you should not change these configurations. However, it is important that the EtherChannel port group should be unique on the switch and in the stack; no other ports should belong to the port group that contains the internal ports. If a switch stack includes more than one wireless LAN controller switch, the internal port channel number must be different within each switch.

You can reconfigure the port channel number if necessary, and you can explicitly configure these ports with other parameters. However, you should not configure features that limit traffic flow, such as ACLs, VLAN maps, and IP source guard.

Configuring the Integrated Wireless LAN Controller Switch

You configure the wireless LAN controller switch by using the same commands that you use to configure any Catalyst 3750 switch (standalone or in a switch stack). This section describes only the configuration specific to the wireless LAN controller switch.

Configuring the Internal Ports

As explained in the [“Internal Ports” section on page 8](#), the internal ports connecting the switch and controller are Gigabit Ethernet ports 27 and 28. You should not change the parameters defined in that section as required for switch and controller interaction. This is a sample configuration for the internal ports:

```
!
interface Port-channel41
  switchport trunk encapsulation dot1q
  switchport mode trunk
  switchport nonegotiate
end

!
interface GigabitEthernet2/0/27
  description This interface is permanently connected to wireless controller
  switchport trunk encapsulation dot1q
  switchport mode trunk
  switchport nonegotiate
  no cdp enable
  channel-group 41 mode on
  spanning-tree portfast trunk
end

!
interface GigabitEthernet2/0/28
  description This interface is permanently connected to wireless controller
  switchport trunk encapsulation dot1q
  switchport mode trunk
  switchport nonegotiate
  no cdp enable
  channel-group 41 mode on
  spanning-tree portfast trunk
```

end

You can also configure other parameters on these ports in interface configuration mode. For example, by default, all traffic on all VLANs are sent to the controller. You should limit the VLANs that are allowed on the internal trunk by using the **switchport trunk allowed vlan** interface configuration command. You enter interface configuration mode for an internal port the same as any other port. For example, if the wireless LAN controller switch is a standalone switch or switch number 1 in a stack, use this command to enter interface configuration mode for internal port 27:

```
Switch(config)# gigabitethernet1/0/27
Switch(config-if)#
```

The internal ports are automatically configured to belong to a static Ether Channel that has PAgP and LACP disabled. No other ports (internal or otherwise) in the switch stack should be members of this EtherChannel. To identify the internal port channel number that the switch has automatically configured, use the **show etherchannel summary** privileged EXEC command.

This output shows that the internal ports on switch 1 in the stack belong to port channel 40. You should not use this port channel for any other ports in the stack.

```
Switch# show etherchannel summary
Flags:  D - down          P - in port-channel
        I - stand-alone  s - suspended
        H - Hot-standby (LACP only)
        R - Layer3       S - Layer2
        U - in use       f - failed to allocate aggregator
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port

Number of channel-groups in use: 36
Number of aggregators:          36

Group  Port-channel  Protocol    Ports
-----+-----+-----+-----
1      Po1(SD)         LACP        Gi2/0/1(D)
<output truncated>
33     Po33(SD)        LACP        Gi2/0/17(D)
40     Po40(SU)        -           Gi1/0/27(P) Gi1/0/28(P)
```

Reconfiguring the Internal Ports

You should not modify the automatic configuration of the internal ports, but if they somehow lose the automatic configuration, you should reconfigure the ports to that configuration.

Beginning in privileged EXEC mode, follow these steps to configure the internal ports to the automatic configuration:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	interface interface-id	Specify one of the internal ports, and enter interface configuration mode. The internal ports are gigabitethernet switch-number/0/27 and gigabitethernet switch-number/0/28 .

	Command	Purpose
Step 3	channel-group <i>channel-group-number</i> mode on	Assign the port to a channel group, and disable PAgP and LACP. <ul style="list-style-type: none"> For <i>channel-group-number</i>, the range is 1 to 48. Selecting mode on forces the port to channel without PAgP or LACP. <p>Note No other ports in the switch stack should be members of this channel group.</p>
Step 4	exit	Return to privileged EXEC mode.
Step 5	interface <i>interface-id</i>	Specify the other internal port, and enter interface configuration mode.
Step 6	channel-group <i>channel-group-number</i> mode on	Assign the port to the same channel group used in Step 3.
Step 7	exit	Return to privileged EXEC mode.
Step 8	interface port-channel <i>channel-group-number</i>	Enter interface configuration mode for the port channel that includes the internal ports.
Step 9	channel-group <i>channel-group-number</i> mode on	Assign the port to the same channel group used in Step 3.
Step 10	switchport mode trunk	Set the internal ports to trunk mode.
Step 11	switchport trunk encapsulation dot1q	Set the trunk encapsulation method to IEEE 802.1Q.
Step 12	switchport no negotiate	Disable generation of DTP frames.
Step 13	spanning tree portfast	Enable STP Port Fast mode.
Step 14	no cdp	Disable CDP.
Step 15	no uddl	Disable UDLD (the default is disabled).
Step 16	switchport trunk allowed vlan remove <i>vlan-list</i>	Control the VLAN traffic sent to the controller by not allowing VLAN traffic on the trunk from specified VLANs.
Step 17	exit	Return to privileged EXEC mode.
Step 18	show running-config	Verify your entries.
Step 19	copy running-config startup-config	(Optional) Save your entries in the configuration file.

Accessing the Controller

You can configure the internal wireless controller by using the embedded controller GUI, WCS, or the controller CLI. You use the management interface IP address to access the controller GUI from a browser or from WCS.

You access the controller CLI from the master switch in a switch stack or from a standalone wireless LAN controller switch by using the **session** *stack-member-number* **processor 1** privileged EXEC command. This command takes you to the controller CLI to enter controller configuration commands. This example assumes that switch 2 in a stack is the wireless LAN controller switch:

```
Switch# session 1 processor 1
(Cisco Controller)
User:
```

See the [Cisco Wireless LAN Controller Configuration Guide Release 4.0](#) for controller CLI configuration information.

Displaying Internal Wireless Controller Information

To use access the controller GUI, you need to enter the management interface IP address. From the switch CLI, you can enter the **show platform wireless-controller** privileged EXEC command with or without keywords to display the management IP address, as well as other information about the internal controller as shown in this example.

```
Switch# show platform wireless-controller
Wireless Controller in Switch 2
Operational Status of the Controller : operational
Service VLAN : 4095
Service Port Mac Address : 000b.8540.3783
Service IP Address : 127.0.1.2
Management IP Address : 22.2.2.2
Management VLAN : 7
Software Version : 3.3.0.3
Keepalive Version(controller/switch) : 1/1
Keepalives Missed : 0
Controller accepts http/https : 0/1
Controller's Status Line : up
Watchdog resets of Controller : 0
Controller resets total : 0
Unacknowledged control messages : 0

Wireless Controller in Switch 3
Operational Status of the Controller : operational
Service VLAN : 4095
Service Port Mac Address : 000b.8540.33e3
Service IP Address : 127.0.1.3
Management IP Address : 8.8.8.8
Management VLAN : 8
Software Version : 3.3.0.3
Keepalive Version(controller/switch) : 1/1
Keepalives Missed : 0
Controller accepts http/https : 0/1
Controller's Status Line : up
Watchdog resets of Controller : 0
Controller resets total : 0
Unacknowledged control messages : 0
```

See the [“show platform wireless-controller”](#) section on page 15.

Catalyst 3750 Integrated Wireless LAN Controller Switch Specific Commands

The new commands and keywords described in this section apply only to the Catalyst 3750 Integrated Wireless LAN Controller Switch. These commands are visible only in switches running Cisco IOS Release 12.2(25)FZ. Note that for switches in a stack, the commands should be entered on the master switch, even if it is not a wireless LAN controller switch.

These commands are new or modified for the wireless LAN controller switch:

- [session](#), page 13
- [show platform wireless-controller](#), page 15
- [debug platform wireless-controller](#), page 17

session

Use the **session** privileged EXEC command on the stack master to access a specific stack member or to access the controller on a Catalyst 3750 Integrated Wireless LAN Controller Switch.

session *stack-member-number* [**processor 1**]

Syntax Description	
<i>stack-member-number</i>	Specify the stack member number. The range is 1 to 9.
processor 1	(Optional) Specify the destination processor for the session, that is, the embedded controller in the Catalyst 3750 Integrated Wireless LAN Controller Switch. Entering this keyword puts you in the controller CLI.

Defaults No default is defined.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(11)AX	This command was introduced.
	12.2(25)FZ	The processor 1 keyword was added for Catalyst 3750 Integrated Wireless LAN Controller Switch.

Usage Guidelines

When you access the stack member, its stack member number is appended to the system prompt.

Use the **session** command from the stack master to access a stack member switch.

Use the **session** command with **processor 1** from the stack master or a standalone switch to access the internal controller. A standalone switch is always stack member 1.

Use the **processor 1** keyword to change to the controller command-line interface. See the [Cisco Wireless LAN Controller Configuration Guide Release 4.0](#) for controller configuration information.

Examples This example shows how to access stack member 6:

```
Switch(config)# session 6
Switch-6#
```

This example shows how to access the controller on stack member 1, which is a Catalyst 3750 wireless LAN controller switch (standalone or stack master):

```
Switch# session 1 processor 1

(Cisco Controller)
User:
```

Related Commands

Command	Description
reload	Reloads the stack member and puts a configuration change into effect.
switch priority	Changes the stack member priority value.
switch renumber	Changes the stack member number.
show platform wireless-controller	Displays information about the internal wireless controller.
show switch	Displays information about the switch stack and its stack members.

show platform wireless-controller

Use the **show platform wireless-controller** privileged EXEC command to display information about the internal wireless controller in a Catalyst 3750 Integrated Wireless LAN Controller Switch.

```
show platform wireless-controller [management-info | status | summary] [switch-number]
[ | {begin | exclude | include} expression]
```

Syntax Description	
management-info	(Optional) Display information about the management interface of the wireless controller.
status	(Optional) Display wireless controller status information.
summary	(Optional) Display wireless controller summary information.
<i>switch-number</i>	(Optional) Display wireless controller information for the specified stack member. The range is from 1 to 9.
 begin	(Optional) Display begins with the line that matches the <i>expression</i> .
 exclude	(Optional) Display excludes lines that match the <i>expression</i> .
 include	(Optional) Display includes lines that match the specified <i>expression</i> .
<i>expression</i>	Expression in the output to use as a reference point.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.2(25)FZ	This command was introduced.

Usage Guidelines You should use this command only when you are working directly with your technical support representative while troubleshooting a problem. Do not use this command unless your technical support representative asks you to do so.

Enter the **show platform wireless-controller** commands to determine the stack number of the switch or switches in the stack that contain the integrated wireless LAN controller. The command outputs also display the MAC address and IP address of the controller to be used in accessing and configuring the controller.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

Examples

This is an example of output from the **show platform wireless-controller** privileged EXEC command with no keywords:

```
Switch# show platform wireless-controller
Wireless Controller in Switch 2
Operational Status of the Controller : operational
Service VLAN : 4095
Service Port Mac Address : 000b.8540.3783
Service IP Address : 127.0.1.2
Management IP Address : 22.2.2.2
Management VLAN : 7
Software Version : 3.3.0.3
Keepalive Version(controller/switch) : 1/1
Keepalives Missed : 0
Controller accepts http/https : 0/1
Controller's Status Line : up
Watchdog resets of Controller : 0
Controller resets total : 0
Unacknowledged control messages : 0
```

```
Wireless Controller in Switch 3
Operational Status of the Controller : operational
Service VLAN : 4095
Service Port Mac Address : 000b.8540.33e3
Service IP Address : 127.0.1.3
Management IP Address : 8.8.8.8
Management VLAN : 8
Software Version : 3.3.0.3
Keepalive Version(controller/switch) : 1/1
Keepalives Missed : 0
Controller accepts http/https : 0/1
Controller's Status Line : up
Watchdog resets of Controller : 0
Controller resets total : 0
Unacknowledged control messages : 0
```

This is an example of output from the **show platform wireless-controller management-info** command:

```
Switch# show platform wireless-controller management-info
sw vlan ip gateway http https mac version
2 7 22.2.2.2/24 22.2.2.1 0 1 000b.8540.3783 3.3.0.3
3 8 8.8.8.8/24 8.8.8.1 0 1 000b.8540.33e3 3.3.0.3
```

This is an example of output from the **show platform wireless-controller status** command:

```
Switch# show platform wireless-controller status 1
Switch Service IP Management IP SW Version Status
-----+-----+-----+-----+-----+-----+-----+-----+-----+
2 127.0.1.2 22.2.2.2 3.3.0.3 operational
3 127.0.1.3 8.8.8.8 3.3.0.3 operational
```

This is an example of output from the **show platform wireless-controller summary** command:

```
Switch# show platform wireless-controller summary
Switch Status State
2 up operational
3 up operational
```

debug platform wireless-controller

Use the **debug platform wireless-controller** privileged EXEC command to enable debugging of the internal wireless LAN controller on a Catalyst 3750 Integrated Wireless LAN Controller Switch. Use the **no** form of this command to disable debugging.

```
debug platform wireless-controller {all | packets | session | sm | wcp}
```

```
no debug platform wireless-controller {all | packets | session | sm | wcp}
```

Syntax Description

all	Display all wireless controller debug messages.
packets	Display Wireless LAN Control Protocol (WCP) packet debug messages.
session	Display wireless controller session debug messages.
sm	Display wireless controller state machine debug messages.
wcp	Display all WCP debug messages.

Defaults

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(25)FZ	This command was introduced.

Usage Guidelines

The **undebug platform wireless-controller** command is the same as the **no debug platform wireless-controller** command.

When you enable debugging, it is enabled only on the stack master. To enable debugging on a stack member, you can start a session from the stack master by using the **session switch-number** privileged EXEC command. Then enter the **debug** command at the command-line prompt of the stack member. You also can use the **remote command stack-member-number LINE** privileged EXEC command on the stack master switch to enable debugging on a member switch without first starting a session.

Related Commands

Command	Description
show debugging	Displays information about the types of debugging that are enabled. For syntax information, see the Cisco IOS Release 12.2 Configuration Guides and Command References > Cisco IOS Configuration Fundamentals Configuration Guide, Release 12.2 > System Management > Troubleshooting and Fault Management .
show platform wireless-controller	Displays information about the internal wireless controller.

Catalyst 3750 Integrated Wireless LAN Controller Switch Specific System Messages

The system messages described in this section apply only to the Catalyst 3750 Integrated Wireless LAN Controller switch. These messages are visible only in switches running Cisco IOS Release 12.2(25)FZ.

Error Message WRLSCNTR-3-INIT_ERR: Initialization failed. [chars]

Explanation Part of initialization required for the normal operation of the wireless LAN controller failed.

Recommended Action Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information. For more information about these online tools and about contacting Cisco, see the system message guide.

Error Message WRLSCNTR-3-CONFIG_ERR: No available channel-group to configure internal interfaces [chars] and [chars].

Explanation The interfaces connected to the wireless LAN controller must be configured as part of a channel group. The switch tried to apply the configuration, but it failed because all channel-group numbers have been assigned. You cannot correctly configure interfaces connected to the wireless LAN controller without removing a channel group.

Recommended Action Modify the EtherChannel configuration to remove a channel group, and use that channel-group number to configure interfaces connected to the wireless LAN controller.

Error Message WRLSCNTR-3-VERSION_ERR: Switch and wireless controller are using incompatible versions.

Explanation The switch software is not fully compatible with the software on the wireless LAN controller. Some functionality might not be available.

Recommended Action Update the software on the switch or on the wireless LAN controller so that the software versions are compatible.

Open Caveats

For open caveats relating to the switch software, see the [Release Notes for the Catalyst 3750 switch for Cisco IOS Release 12.2\(25\)SEE](#) on cisco.com.

For open caveats relating to the controller software, see the [Release Notes for Cisco Wireless LAN Controllers and Lightweight Access Point, Release 4.0.x.0](#) on Cisco.com.

Resolved Caveats

For resolved caveats relating to the switch software, see the [Release Notes for the Catalyst 3750 switch for Cisco IOS Release 12.2\(25\)SEE](#) on cisco.com.

For resolved caveats relating to the controller software, see the [Release Notes for Cisco Wireless LAN Controllers and Lightweight Access Point, Release 4.0.x.0](#) on Cisco.com.

Related Documentation

These documents provide complete information about the Catalyst 3750 switch and are available at Cisco.com:

- http://www.cisco.com/en/US/products/hw/switches/ps5023/tsd_products_support_series_home.html

You can order printed copies of documents with a DOC-xxxxxx= number from the Cisco.com sites and from the telephone numbers listed in the “[Obtaining Documentation](#)” section on page 20.

These documents provide complete information about the Catalyst 3750 switches:

- Release Notes for the Catalyst 3750 switch for Cisco IOS Release 12.2(25)SEE on cisco.com
- *Catalyst 3750 Integrated Wireless LAN Controller Switch Getting Started Guide* (order number DOC-7817540=)
- *Catalyst 3750 Switch Hardware Installation Guide* (not orderable but available on Cisco.com)
- *Catalyst 3750 Switch Software Configuration Guide* (not orderable but available on Cisco.com)
- *Catalyst 3750 Switch Command Reference* (not orderable but available on Cisco.com)
- *Catalyst 3750, 3560, 3550, 2970, and 2960 Switch System Message Guide* (not orderable but available on Cisco.com)
- Device manager online help (available on the switch)
- *Regulatory Compliance and Safety Information for the Catalyst 3750 Switch* (order number DOC-7816664)

These documents provide complete information about the integrated wireless LAN controller and are available at cisco.com:

- *Release Notes for Cisco Wireless LAN Controller and Lightweight Access Point, Release 4.0.x.0*
- *Cisco Wireless LAN Controller Configuration Guide, Release 4.0*
- *Cisco Wireless LAN Controller Command Reference, Release 4.0*

For other information about related products, see these documents:

- *Getting Started with Cisco Network Assistant* (not orderable but available on Cisco.com)
- *Release Notes for Cisco Network Assistant* (not orderable but available on Cisco.com)
- *Cisco Small Form-Factor Pluggable Modules Installation Notes* (order number DOC-7815160=)
- *Cisco CWDM GBIC and CWDM SFP Installation Note* (not orderable but available on Cisco.com)
- *Cisco RPS 675 Redundant Power System Hardware Installation Guide* (order number DOC-7815201=)
- *Network Admission Control Software Configuration Guide* (not orderable but is available on Cisco.com)

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation at this URL:

<http://www.cisco.com/techsupport>

You can access the Cisco website at this URL:

<http://www.cisco.com>

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Product Documentation DVD

The Product Documentation DVD is a comprehensive library of technical product documentation on a portable medium. The DVD enables you to access multiple versions of installation, configuration, and command guides for Cisco hardware and software products. With the DVD, you have access to the same HTML documentation that is found on the Cisco website without being connected to the Internet. Certain products also have .PDF versions of the documentation available.

The Product Documentation DVD is available as a single unit or as a subscription. Registered Cisco.com users (Cisco direct customers) can order a Product Documentation DVD (product number DOC-DOCDVD= or DOC-DOCDVD=SUB) from Cisco Marketplace at this URL:

<http://www.cisco.com/go/marketplace/>

Ordering Documentation

Registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:

<http://www.cisco.com/go/marketplace/>

Nonregistered Cisco.com users can order technical documentation from 8:00 a.m. to 5:00 p.m. (0800 to 1700) PDT by calling 1 866 463-3487 in the United States and Canada, or elsewhere by calling 011 408 519-5055. You can also order documentation by e-mail at tech-doc-store-mkpl@external.cisco.com or by fax at 1 408 519-5001 in the United States and Canada, or elsewhere at 011 408 519-5001.

Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.

You can submit comments about Cisco documentation by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you will find information about how to:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories, security notices, and security responses for Cisco products is available at this URL:

<http://www.cisco.com/go/psirt>

To see security advisories, security notices, and security responses as they are updated in real time, you can subscribe to the Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed. Information about how to subscribe to the PSIRT RSS feed is found at this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you have identified a vulnerability in a Cisco product, contact PSIRT:

- For Emergencies only—security-alert@cisco.com

An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

- For Nonemergencies—psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

**Tip**

We encourage you to use Pretty Good Privacy (PGP) or a compatible product (for example, GnuPG) to encrypt any sensitive information that you send to Cisco. PSIRT can work with information that has been encrypted with PGP versions 2.x through 9.x.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

The link on this page has the current PGP key ID in use.

If you do not have or use PGP, contact PSIRT at the aforementioned e-mail addresses or phone numbers before sending any sensitive material to find other means of encrypting the data.

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, at this URL:

<http://www.cisco.com/techsupport>

Access to all tools on the Cisco Technical Support & Documentation 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 at this URL:

<http://tools.cisco.com/RPF/register/register.do>

**Note**

Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

<http://www.cisco.com/techsupport/servicerequest>

For S1 or S2 service requests, or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)

EMEA: +32 2 704 55 55

USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

<http://www.cisco.com/techsupport/contacts>

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—An existing network is down, or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operations are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of the network is impaired, while most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- The *Cisco Product Quick Reference Guide* is a handy, compact reference tool that includes brief product overviews, key features, sample part numbers, and abbreviated technical specifications for many Cisco products that are sold through channel partners. It is updated twice a year and includes the latest Cisco offerings. To order and find out more about the Cisco Product Quick Reference Guide, go to this URL:

<http://www.cisco.com/go/guide>

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:
<http://www.cisco.com/go/marketplace/>
- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:
<http://www.ciscopress.com>
- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:
<http://www.cisco.com/packet>
- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:
<http://www.cisco.com/go/iqmagazine>
or view the digital edition at this URL:
<http://cisoiq.texterity.com/cisoiq/sample/>
- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:
<http://www.cisco.com/ipj>
- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:
<http://www.cisco.com/en/US/products/index.html>
- Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:
<http://www.cisco.com/discuss/networking>
- World-class networking training is available from Cisco. You can view current offerings at this URL:
<http://www.cisco.com/en/US/learning/index.html>

This document is to be used in conjunction with the documents listed in the “[Related Documentation](#)” section.

CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, The Fastest Way to Increase Your Internet Quotient, and TransPath 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. (0601R)

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.

© 2006 Cisco Systems, Inc. All rights reserved.

