



## **VideoStream Configuration Guide Cisco IOS XE Release 3SE Cisco 3850 Series Catalyst Switch**

**First Published:** September 13, 2013

**Last Modified:** September 13, 2013

### **Americas Headquarters**

Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
<http://www.cisco.com>  
Tel: 408 526-4000  
800 553-NETS (6387)  
Fax: 408 527-0883

Text Part Number: OL-28533-02

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

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

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <http://www.cisco.com/go/trademarks>. Third-party trademarks mentioned 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. (1110R)

© Cisco Systems, Inc. All rights reserved.



## CONTENTS

---

### Preface

### Preface v

**Document Conventions 7**

**Related Documentation 9**

**Obtaining Documentation and Submitting a Service Request 11**

---

### CHAPTER 1

### Using the Command-Line Interface 1

Information About Using the Command-Line Interface 1

Command Modes 1

Using the Help System 3

Understanding Abbreviated Commands 4

No and Default Forms of Commands 4

CLI Error Messages 4

Configuration Logging 5

How to Use the CLI to Configure Features 5

Configuring the Command History 5

Changing the Command History Buffer Size 6

Recalling Commands 6

Disabling the Command History Feature 7

Enabling and Disabling Editing Features 7

Editing Commands Through Keystrokes 8

Editing Command Lines That Wrap 9

Searching and Filtering Output of show and more Commands 10

Accessing the CLI Through a Console Connection or Through Telnet 11

---

### CHAPTER 2

### Configuring VideoStream 13

Finding Feature Information 13

Prerequisites for VideoStream 13

Restrictions for Configuring VideoStream 14

Information about VideoStream 14

How to Configure VideoStream 14

    Configuring Multicast-Direct Globally for Media-Stream 14

    Configuring Media-Stream for 802.11 bands 16

    Configuring WLAN to Stream Video 18

    Deleting a Media-Stream 19

Monitoring Media Streams 19

---

**CHAPTER 3**

**Configuring VideoStream GUI 21**

    Configuring VideoStream (GUI) 21



# Preface

---





## Document Conventions

This document uses the following conventions:

Convention	Description
^ or Ctrl	Both the ^ symbol and Ctrl represent the Control (Ctrl) key on a keyboard. For example, the key combination ^ <b>D</b> or <b>Ctrl-D</b> means that you hold down the Control key while you press the D key. (Keys are indicated in capital letters but are not case sensitive.)
<b>bold font</b>	Commands and keywords and user-entered text appear in <b>bold font</b> .
<i>Italic font</i>	Document titles, new or emphasized terms, and arguments for which you supply values are in <i>italic font</i> .
Courier font	Terminal sessions and information the system displays appear in <code>courier font</code> .
<b>Bold Courier font</b>	<b>Bold Courier font</b> indicates text that the user must enter.
[x]	Elements in square brackets are optional.
...	An ellipsis (three consecutive nonbolded periods without spaces) after a syntax element indicates that the element can be repeated.
	A vertical line, called a pipe, indicates a choice within a set of keywords or arguments.
[x   y]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
{x   y}	Required alternative keywords are grouped in braces and separated by vertical bars.
[x {y   z}]	Nested set of square brackets or braces indicate optional or required choices within optional or required elements. Braces and a vertical bar within square brackets indicate a required choice within an optional element.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.

Convention	Description
< >	Nonprinting characters such as passwords are in angle brackets.
[ ]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

### Reader Alert Conventions

This document may use the following conventions for reader alerts:



#### Note

Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the manual.



#### Tip

Means *the following information will help you solve a problem*.



#### Caution

Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.



#### Timesaver

Means *the described action saves time*. You can save time by performing the action described in the paragraph.



#### Warning

Means *reader be warned*. In this situation, you might perform an action that could result in bodily injury.





## Related Documentation

---



---

**Note**

Before installing or upgrading the switch, refer to the switch release notes.

---

- Error Message Decoder, located at:  
<https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi>





## Obtaining Documentation and Submitting a Service Request

---

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.





## CHAPTER

# 1

## Using the Command-Line Interface

---

- [Information About Using the Command-Line Interface, page 1](#)
- [How to Use the CLI to Configure Features, page 5](#)

## Information About Using the Command-Line Interface

### Command Modes

The Cisco IOS user interface is divided into many different modes. The commands available to you depend on which mode you are currently in. Enter a question mark (?) at the system prompt to obtain a list of commands available for each command mode.

You can start a CLI session through a console connection, through Telnet, a SSH, or by using the browser.

When you start a session, you begin in user mode, often called user EXEC mode. Only a limited subset of the commands are available in user EXEC mode. For example, most of the user EXEC commands are one-time commands, such as **show** commands, which show the current configuration status, and **clear** commands, which clear counters or interfaces. The user EXEC commands are not saved when the switch reboots.

To have access to all commands, you must enter privileged EXEC mode. Normally, you must enter a password to enter privileged EXEC mode. From this mode, you can enter any privileged EXEC command or enter global configuration mode.

Using the configuration modes (global, interface, and line), you can make changes to the running configuration. If you save the configuration, these commands are stored and used when the switch reboots. To access the various configuration modes, you must start at global configuration mode. From global configuration mode, you can enter interface configuration mode and line configuration mode.

This table describes the main command modes, how to access each one, the prompt you see in that mode, and how to exit the mode.

Table 1: Command Mode Summary

Mode	Access Method	Prompt	Exit Method	About This Mode
User EXEC	Begin a session using Telnet, SSH, or console.	Switch>	Enter <b>logout</b> or <b>quit</b> .	Use this mode to <ul style="list-style-type: none"> <li>• Change terminal settings.</li> <li>• Perform basic tests.</li> <li>• Display system information.</li> </ul>
Privileged EXEC	While in user EXEC mode, enter the <b>enable</b> command.	Switch#	Enter <b>disable</b> to exit.	Use this mode to verify commands that you have entered. Use a password to protect access to this mode.
Global configuration	While in privileged EXEC mode, enter the <b>configure</b> command.	Switch(config)#	To exit to privileged EXEC mode, enter <b>exit</b> or <b>end</b> , or press <b>Ctrl-Z</b> .	Use this mode to configure parameters that apply to the entire switch.
VLAN configuration	While in global configuration mode, enter the <b>vlan</b> <i>vlan-id</i> command.	Switch(config-vlan)#	To exit to global configuration mode, enter the <b>exit</b> command. To return to privileged EXEC mode, press <b>Ctrl-Z</b> or enter <b>end</b> .	Use this mode to configure VLAN parameters. When VTP mode is transparent, you can create extended-range VLANs (VLAN IDs greater than 1005) and save configurations in the switch startup configuration file.
Interface configuration	While in global configuration mode, enter the <b>interface</b> command (with a specific interface).	Switch(config-if)#	To exit to global configuration mode, enter <b>exit</b> . To return to privileged EXEC mode, press <b>Ctrl-Z</b> or enter <b>end</b> .	Use this mode to configure parameters for the Ethernet ports.

Mode	Access Method	Prompt	Exit Method	About This Mode
Line configuration	While in global configuration mode, specify a line with the <b>line vty</b> or <b>line console</b> command.	Switch(config-line)#	To exit to global configuration mode, enter <b>exit</b> .  To return to privileged EXEC mode, press <b>Ctrl-Z</b> or enter <b>end</b> .	Use this mode to configure parameters for the terminal line.

## Using the Help System

You can enter a question mark (?) at the system prompt to display a list of commands available for each command mode. You can also obtain a list of associated keywords and arguments for any command.

### SUMMARY STEPS

1. **help**
2. *abbreviated-command-entry ?*
3. *abbreviated-command-entry <Tab>*
4. **?**
5. *command ?*
6. *command keyword ?*

### DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>help</b>  <b>Example:</b> Switch# <b>help</b>	Obtains a brief description of the help system in any command mode.
<b>Step 2</b>	<i>abbreviated-command-entry ?</i>  <b>Example:</b> Switch# <b>di?</b> dir disable disconnect	Obtains a list of commands that begin with a particular character string.
<b>Step 3</b>	<i>abbreviated-command-entry &lt;Tab&gt;</i>  <b>Example:</b> Switch# <b>sh conf&lt;tab&gt;</b> Switch# <b>show configuration</b>	Completes a partial command name.

	Command or Action	Purpose
Step 4	?  <b>Example:</b> Switch> ?	Lists all commands available for a particular command mode.
Step 5	<i>command</i> ?  <b>Example:</b> Switch> <b>show</b> ?	Lists the associated keywords for a command.
Step 6	<i>command keyword</i> ?  <b>Example:</b> Switch(config)# <b>cdp holdtime</b> ? <10-255> Length of time (in sec) that receiver must keep this packet	Lists the associated arguments for a keyword.

## Understanding Abbreviated Commands

You need to enter only enough characters for the switch to recognize the command as unique.

This example shows how to enter the **show configuration** privileged EXEC command in an abbreviated form:

```
Switch# show conf
```

## No and Default Forms of Commands

Almost every configuration command also has a **no** form. In general, use the **no** form to disable a feature or function or reverse the action of a command. For example, the **no shutdown** interface configuration command reverses the shutdown of an interface. Use the command without the keyword **no** to reenable a disabled feature or to enable a feature that is disabled by default.

Configuration commands can also have a **default** form. The **default** form of a command returns the command setting to its default. Most commands are disabled by default, so the **default** form is the same as the **no** form. However, some commands are enabled by default and have variables set to certain default values. In these cases, the **default** command enables the command and sets variables to their default values.

## CLI Error Messages

This table lists some error messages that you might encounter while using the CLI to configure your switch.



**Table 2: Common CLI Error Messages**

Error Message	Meaning	How to Get Help
% Ambiguous command: "show con"	You did not enter enough characters for your switch to recognize the command.	Reenter the command followed by a question mark (?) without any space between the command and the question mark.  The possible keywords that you can enter with the command appear.
% Incomplete command.	You did not enter all of the keywords or values required by this command.	Reenter the command followed by a question mark (?) with a space between the command and the question mark.  The possible keywords that you can enter with the command appear.
% Invalid input detected at '^' marker.	You entered the command incorrectly. The caret (^) marks the point of the error.	Enter a question mark (?) to display all of the commands that are available in this command mode.  The possible keywords that you can enter with the command appear.

## Configuration Logging

You can log and view changes to the switch configuration. You can use the Configuration Change Logging and Notification feature to track changes on a per-session and per-user basis. The logger tracks each configuration command that is applied, the user who entered the command, the time that the command was entered, and the parser return code for the command. This feature includes a mechanism for asynchronous notification to registered applications whenever the configuration changes. You can choose to have the notifications sent to the syslog.




---

**Note** Only CLI or HTTP changes are logged.

---

## How to Use the CLI to Configure Features

### Configuring the Command History

The software provides a history or record of commands that you have entered. The command history feature is particularly useful for recalling long or complex commands or entries, including access lists. You can customize this feature to suit your needs.

## Changing the Command History Buffer Size

By default, the switch records ten command lines in its history buffer. You can alter this number for a current terminal session or for all sessions on a particular line. This procedure is optional.

### SUMMARY STEPS

1. **terminal history** [*size number-of-lines*]

### DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>terminal history</b> [ <i>size number-of-lines</i> ]  <b>Example:</b> Switch# <b>terminal history size 200</b>	Changes the number of command lines that the switch records during the current terminal session in privileged EXEC mode. You can configure the size from 0 to 256.

## Recalling Commands

To recall commands from the history buffer, perform one of the actions listed in this table. These actions are optional.



### Note

The arrow keys function only on ANSI-compatible terminals such as VT100s.

### SUMMARY STEPS

1. **Ctrl-P** or use the **up arrow** key
2. **Ctrl-N** or use the **down arrow** key
3. **show history**

### DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>Ctrl-P</b> or use the <b>up arrow</b> key	Recalls commands in the history buffer, beginning with the most recent command. Repeat the key sequence to recall successively older commands.
<b>Step 2</b>	<b>Ctrl-N</b> or use the <b>down arrow</b> key	Returns to more recent commands in the history buffer after recalling commands with <b>Ctrl-P</b> or the up arrow key. Repeat the key sequence to recall successively more recent commands.

	Command or Action	Purpose
<b>Step 3</b>	<b>show history</b>  <b>Example:</b> Switch# <code>show history</code>	Lists the last several commands that you just entered in privileged EXEC mode. The number of commands that appear is controlled by the setting of the <b>terminal history</b> global configuration command and the <b>history</b> line configuration command.

## Disabling the Command History Feature

The command history feature is automatically enabled. You can disable it for the current terminal session or for the command line. This procedure is optional.

### SUMMARY STEPS

1. `terminal no history`

### DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>terminal no history</b>  <b>Example:</b> Switch# <code>terminal no history</code>	Disables the feature during the current terminal session in privileged EXEC mode.

## Enabling and Disabling Editing Features

Although enhanced editing mode is automatically enabled, you can disable it and reenble it.

### SUMMARY STEPS

1. `terminal editing`
2. `terminal no editing`

### DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>terminal editing</b>  <b>Example:</b> Switch# <code>terminal editing</code>	Reenables the enhanced editing mode for the current terminal session in privileged EXEC mode.

	Command or Action	Purpose
Step 2	<b>terminal no editing</b>  <b>Example:</b> Switch# <code>terminal no editing</code>	Disables the enhanced editing mode for the current terminal session in privileged EXEC mode.

## Editing Commands Through Keystrokes

The keystrokes help you to edit the command lines. These keystrokes are optional.



### Note

The arrow keys function only on ANSI-compatible terminals such as VT100s.

**Table 3: Editing Commands**

Editing Commands	Description
<b>Ctrl-B</b> or use the <b>left arrow</b> key	Moves the cursor back one character.
<b>Ctrl-F</b> or use the <b>right arrow</b> key	Moves the cursor forward one character.
<b>Ctrl-A</b>	Moves the cursor to the beginning of the command line.
<b>Ctrl-E</b>	Moves the cursor to the end of the command line.
<b>Esc B</b>	Moves the cursor back one word.
<b>Esc F</b>	Moves the cursor forward one word.
<b>Ctrl-T</b>	Transposes the character to the left of the cursor with the character located at the cursor.
<b>Delete</b> or <b>Backspace</b> key	Erases the character to the left of the cursor.
<b>Ctrl-D</b>	Deletes the character at the cursor.
<b>Ctrl-K</b>	Deletes all characters from the cursor to the end of the command line.
<b>Ctrl-U</b> or <b>Ctrl-X</b>	Deletes all characters from the cursor to the beginning of the command line.
<b>Ctrl-W</b>	Deletes the word to the left of the cursor.

<b>Esc D</b>	Deletes from the cursor to the end of the word.
<b>Esc C</b>	Capitalizes at the cursor.
<b>Esc L</b>	Changes the word at the cursor to lowercase.
<b>Esc U</b>	Capitalizes letters from the cursor to the end of the word.
<b>Ctrl-V</b> or <b>Esc Q</b>	Designates a particular keystroke as an executable command, perhaps as a shortcut.
<b>Return</b> key	Scrolls down a line or screen on displays that are longer than the terminal screen can display.  <b>Note</b> The More prompt is used for any output that has more lines than can be displayed on the terminal screen, including <b>show</b> command output. You can use the <b>Return</b> and <b>Space</b> bar keystrokes whenever you see the More prompt.
<b>Space</b> bar	Scrolls down one screen.
<b>Ctrl-L</b> or <b>Ctrl-R</b>	Redisplays the current command line if the switch suddenly sends a message to your screen.

## Editing Command Lines That Wrap

You can use a wraparound feature for commands that extend beyond a single line on the screen. When the cursor reaches the right margin, the command line shifts ten spaces to the left. You cannot see the first ten characters of the line, but you can scroll back and check the syntax at the beginning of the command. The keystroke actions are optional.

To scroll back to the beginning of the command entry, press **Ctrl-B** or the left arrow key repeatedly. You can also press **Ctrl-A** to immediately move to the beginning of the line.



### Note

The arrow keys function only on ANSI-compatible terminals such as VT100s.

The following example shows how to wrap a command line that extends beyond a single line on the screen.

## SUMMARY STEPS

1. **access-list**
2. **Ctrl-A**
3. **Return** key

## DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>access-list</b>  <b>Example:</b>  <pre>Switch(config)# access-list 101 permit tcp 10.15.22.25 255.255.255.0 10.15.22.35 Switch(config)# \$ 101 permit tcp 10.15.22.25 255.255.255.0 10.15.22.35 255.25 Switch(config)# \$t tcp 10.15.22.25 255.255.255.0 131.108.1.20 255.255.255.0 eq Switch(config)# \$15.22.25 255.255.255.0 10.15.22.35 255.255.255.0 eq 45</pre>	<p>Displays the global configuration command entry that extends beyond one line.</p> <p>When the cursor first reaches the end of the line, the line is shifted ten spaces to the left and redisplayed. The dollar sign (\$) shows that the line has been scrolled to the left. Each time the cursor reaches the end of the line, the line is again shifted ten spaces to the left.</p>
<b>Step 2</b>	<b>Ctrl-A</b>  <b>Example:</b>  <pre>Switch(config)# access-list 101 permit tcp 10.15.22.25 255.255.255.0 10.15.25\$</pre>	<p>Checks the complete syntax.</p> <p>The dollar sign (\$) appears at the end of the line to show that the line has been scrolled to the right.</p>
<b>Step 3</b>	<b>Return key</b>	<p>Execute the commands.</p> <p>The software assumes that you have a terminal screen that is 80 columns wide. If you have a different width, use the <b>terminal width</b> privileged EXEC command to set the width of your terminal.</p> <p>Use line wrapping with the command history feature to recall and modify previous complex command entries.</p>

## Searching and Filtering Output of show and more Commands

You can search and filter the output for **show** and **more** commands. This is useful when you need to sort through large amounts of output or if you want to exclude output that you do not need to see. Using these commands is optional.

## SUMMARY STEPS

1. `{show | more} command | {begin | include | exclude} regular-expression`

## DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<code>{show   more} command   {begin   include   exclude} regular-expression</code>	Searches and filters the output.

	Command or Action	Purpose
	<p><b>Example:</b>  Switch# <code>show interfaces   include protocol</code>  Vlan1 is up, line protocol is up  Vlan10 is up, line protocol is down  GigabitEthernet1/0/1 is up, line protocol is down  GigabitEthernet1/0/2 is up, line protocol is up</p>	<p>Expressions are case sensitive. For example, if you enter <code>  exclude output</code>, the lines that contain <b>output</b> are not displayed, but the lines that contain <b>output</b> appear.</p>

## Accessing the CLI Through a Console Connection or Through Telnet

Before you can access the CLI, you must connect a terminal or a PC to the switch console or connect a PC to the Ethernet management port and then power on the switch, as described in the hardware installation guide that shipped with your switch.

If your switch is already configured, you can access the CLI through a local console connection or through a remote Telnet session, but your switch must first be configured for this type of access.

You can use one of these methods to establish a connection with the switch:

- Connect the switch console port to a management station or dial-up modem, or connect the Ethernet management port to a PC. For information about connecting to the console or Ethernet management port, see the switch hardware installation guide.
- Use any Telnet TCP/IP or encrypted Secure Shell (SSH) package from a remote management station. The switch must have network connectivity with the Telnet or SSH client, and the switch must have an enable secret password configured.
  - The switch supports up to 16 simultaneous Telnet sessions. Changes made by one Telnet user are reflected in all other Telnet sessions.
  - The switch supports up to five simultaneous secure SSH sessions.

After you connect through the console port, through the Ethernet management port, through a Telnet session or through an SSH session, the user EXEC prompt appears on the management station.







## Configuring VideoStream

---

- [Finding Feature Information, page 13](#)
- [Prerequisites for VideoStream, page 13](#)
- [Restrictions for Configuring VideoStream, page 14](#)
- [Information about VideoStream, page 14](#)
- [How to Configure VideoStream, page 14](#)
- [Monitoring Media Streams, page 19](#)

### Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release.

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

### Prerequisites for VideoStream

Make sure that the multicast feature is enabled. We recommend configuring IP multicast on the controller with multicast-multicast mode.

Check for the IP address on the client machine. The machine should have an IP address from the respective VLAN.

Verify that the access points have joined the controllers.

# Restrictions for Configuring VideoStream

## Information about VideoStream

The IEEE 802.11 wireless multicast delivery mechanism does not provide a reliable way to acknowledge lost or corrupted packets. As a result, if any multicast packet is lost in the air, it is not sent again which may cause an IP multicast stream unviewable.

The VideoStream feature makes the IP multicast stream delivery reliable over the air, by converting the multicast frame to a unicast frame over the air. Each VideoStream client acknowledges receiving a video IP multicast stream.

## How to Configure VideoStream

### Configuring Multicast-Direct Globally for Media-Stream

#### SUMMARY STEPS

1. **configure terminal**
2. **wireless multicast**
3. **IP igmp snooping**
4. **IP igmp snooping querier**
5. **wireless media-stream multicast-direct**
6. **wireless media-stream message**
7. **wireless media-stream group** <name> <startIp> <endIp>
8. **end**

#### DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b>  <b>Example:</b> Switch# <code>configure terminal</code>	Enters global configuration mode.
<b>Step 2</b>	<b>wireless multicast</b>	Enables multicast for wireless forwarding.
<b>Step 3</b>	<b>IP igmp snooping</b>	Enables IGMP snooping on a per-VLAN basis. If the global setting is disabled, then all VLANs are treated as disabled, whether they are enabled or not.

	Command or Action	Purpose
Step 4	IP igmp snooping querier	Configures a snooping querier on an interface when there is no multicast router in the VLAN to generate queries.
Step 5	<b>wireless media-stream multicast-direct</b>  <b>Example:</b> Switch(config)# <b>wireless media-stream multicast-direct</b>	Configures the global multicast-direct feature for the controller.
Step 6	<b>wireless media-stream message</b>  <b>Example:</b> Switch(config)# <b>wireless media-stream message ?</b> Email Configure Session Announcement Email Notes Configure Session Announcement notes URL Configure Session Announcement URL phone Configure Session Announcement Phone number <cr>	Configures various message configuration parameters like phone, URL, email and notes. That is, when a media stream is refused (due to bandwidth constraints), a message can be sent to the user. These parameters configure the messages to send IT support email address, notes (message to display explaining why the stream was refused), URL to which the user can be redirected and the phone number that the user can call about the refused stream.
Step 7	<b>wireless media-stream group</b> <name><startIp><endIp>  <b>Example:</b> Switch(config)# <b>wireless media-stream group grp1 231.1.1.1 239.1.1.3</b> Switch(config-media-stream)#?  avg-packet-size Configures average packet size default Set a command to its defaults  exit Exit sub-mode max-bandwidth Configures maximum Expected Stream Bandwidth in Kbps no Negate a command or set its defaults policy Configure media stream admission policy qos Configure Over the AIR QoS class, <'video'> ONLY  <cr>	configures each media stream and its parameters like expected multicast destination addresses, stream bandwidth consumption and stream priority parameters.
Step 8	<b>end</b>  <b>Example:</b> Switch(config)# <b>end</b>	Returns to privileged EXEC mode. Alternatively, you can also press <b>Ctrl-Z</b> to exit global configuration mode.

## Configuring Media-Stream for 802.11 bands

### SUMMARY STEPS

1. `configure terminal`
2. `ap dot11 24ghz | 5ghz media-stream multicast-direct`
3. `ap dot11 24ghz | 5ghz media-stream video-redirect`
4. `ap dot11 24ghz | 5ghz media-stream multicast-direct admission-besteffort`
5. `ap dot11 24ghz | 5ghz media-stream multicast-direct client-maximum [<value >]`
6. `ap dot11 24ghz | 5ghz media-stream multicast-direct radio-maximum 20`
7. `ap dot11 24ghz | 5ghz cac multimedia max-bandwidth [<bandwidth>]`
8. `ap dot11 24ghz | 5ghz cac media-stream multicast-direct min_client_rate [<dot11_rate> ]`
9. `ap dot11 5ghz cac media-stream`
10. `ap dot11 5ghz cac multimedia`
11. `ap dot11 5ghz cac video`
12. `ap dot11 5ghz cac voice`
13. `end`

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>configure terminal</code>  <b>Example:</b> <code>Switch# configure terminal</code>	Enters global configuration mode.
Step 2	<code>ap dot11 24ghz   5ghz media-stream multicast-direct</code>  <b>Example:</b> <code>Switch(config)#ap dot11 24ghz media-stream multicast-direct</code>	Configures if media stream (mc2uc) is allowed for 802.11 band
Step 3	<code>ap dot11 24ghz   5ghz media-stream video-redirect</code>  <b>Example:</b> <code>Switch(config)#ap dot11 24ghz media-stream video-redirect</code>	Configures to redirect unicast video traffic to best effort queue.
Step 4	<code>ap dot11 24ghz   5ghz media-stream multicast-direct admission-besteffort</code>  <b>Example:</b> <code>Switch(config)#ap dot11 24ghz media-stream multicast-direct admission-besteffort</code>	Configures the media stream to still be sent through the best effort queue if a media stream cannot be prioritized due to bandwidth availability limitations. Add <b>no</b> in the command to drop the stream if the media stream cannot be prioritized due to bandwidth availability limitations.

	Command or Action	Purpose
<b>Step 5</b>	<b>ap dot11 24ghz   5ghz media-stream multicast-direct client-maximum [&lt;value&gt;]</b>  <b>Example:</b> <pre>Switch(config)#ap dot11 24ghz media-stream multicast-direct client-max 15</pre>	Configures maximum number of allowed media streams per individual client. The maximum is 15 and the default is 0. Value 0 denotes unlimited streams.
<b>Step 6</b>	<b>ap dot11 24ghz   5ghz media-stream multicast-direct radio-maximum 20</b>	Configures maximum number of radio streams. The range is from 1 to 20. Default is 0. Value 0 denotes unlimited streams.
<b>Step 7</b>	<b>ap dot11 24ghz   5ghz cac multimedia max-bandwidth [&lt;bandwidth&gt;]</b>  <b>Example:</b> <pre>Switch(config)#ap dot11 24ghz cac multimedia max-bandwidth 60</pre>	Configure maximum media (voice + video) bandwidth in %. The range is between 5% and 85%.
<b>Step 8</b>	<b>ap dot11 24ghz   5ghz cac media-stream multicast-direct min_client_rate [&lt;dot11_rate&gt; ]</b>  <b>Example:</b> <pre>Switch(config)#ap dot11 24ghz cac media-stream multicast-direct min_client_rate</pre>	Configures the minimum PHY rate needed for a client to send media-stream as unicast. Clients communicating below this rate will not receive the media stream as a unicast flow. Typically, this PHY rate is equal to or higher than the rate at which multicast frames are sent.
<b>Step 9</b>	<b>ap dot11 5ghz cac media-stream</b>	Configures CAC parameters for media stream access category.
<b>Step 10</b>	<b>ap dot11 5ghz cac multimedia</b>	Configures CAC parameters for media access category, used for voice and video.
<b>Step 11</b>	<b>ap dot11 5ghz cac video</b>	Configures CAC parameters for video access category, used for voice signaling.
<b>Step 12</b>	<b>ap dot11 5ghz cac voice</b>	Configures CAC parameters for voice access category.
<b>Step 13</b>	<b>end</b>  <b>Example:</b> <pre>Switch(config)# end</pre>	Returns to privileged EXEC mode. Alternatively, you can also press <b>Ctrl-Z</b> to exit global configuration mode.

## Configuring WLAN to Stream Video

### SUMMARY STEPS

1. **configure terminal**
2. **wlan wlan\_name**
3. **shutdown**
4. **media-stream multicast-direct**
5. **no shutdown**
6. **end**

### DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b>  <b>Example:</b> Switch# <b>configure terminal</b>	Enters global configuration mode.
<b>Step 2</b>	<b>wlan wlan_name</b>  <b>Example:</b> Switch(config)# <b>wlan wlan50</b>	Enters the WLAN configuration mode.
<b>Step 3</b>	<b>shutdown</b>  <b>Example:</b> Switch(config-wlan)# <b>shutdown</b>	Disables the WLAN for configuring it parameters.
<b>Step 4</b>	<b>media-stream multicast-direct</b>  <b>Example:</b> Switch(config)# <b>media-stream multicast-direct</b>	Configures the multicast-direct feature on media-stream for the WLAN.
<b>Step 5</b>	<b>no shutdown</b>  <b>Example:</b> Switch(config-wlan)# <b>no shutdown</b>	Enables the WLAN.
<b>Step 6</b>	<b>end</b>  <b>Example:</b> Switch(config)# <b>end</b>	Returns to privileged EXEC mode. Alternatively, you can also press <b>Ctrl-Z</b> to exit global configuration mode.

## Deleting a Media-Stream

### Before You Begin

The media-stream should be enabled and configured for it to be deleted.

### SUMMARY STEPS

1. `configure terminal`
2. `no wireless media-stream group media_stream_name`
3. `end`

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>configure terminal</b>  <b>Example:</b> Switch# <code>configure terminal</code>	Enters global configuration mode.
Step 2	<b>no wireless media-stream group media_stream_name</b>  <b>Example:</b> Switch(config)# <code>no wireless media-stream grp1</code>	Deletes the media-stream which bears the name mentioned in the command.
Step 3	<b>end</b>  <b>Example:</b> Switch(config)# <code>end</code>	Returns to privileged EXEC mode. Alternatively, you can also press <b>Ctrl-Z</b> to exit global configuration mode.

## Monitoring Media Streams

*Table 4: Commands for monitoring media streams*

Commands	Description
<code>show wireless media-stream client detail group name</code>	Displays media stream client details of the particular group.
<code>show wireless media-stream client summary</code>	Displays the media stream information of all the clients.
<code>show wireless media-stream group detail group name</code>	Displays the media stream configuration details of the particular group.

Commands	Description
show wireless media-stream group summary	Displays the media stream configuration details of all the groups.
show wireless media-stream message details	Displays the session announcement message details.
show wireless multicast	Displays the multicast-direct configuration state.
show ap dot11 24ghz   5ghz media-stream rrc	Displays 802.11 media Resource-Reservation-Control configurations.





## Configuring VideoStream GUI

- [Configuring VideoStream \(GUI\), page 21](#)

### Configuring VideoStream (GUI)

Complete the following steps to configure VideoStream using GUI.

#### Step 1

Configure the multicast feature by following these steps:

- Choose **Wireless > MediaStream > General**.
- Select or unselect the **Multicast Direct feature** check box. The default value is disabled.  
**Note** Enabling the multicast direct feature does not automatically reset the existing client state. The wireless clients must rejoin the multicast stream after enabling the multicast direct feature on the controller.
- In the **Session Message Config** area, select **Session announcement State** check box to enable the session announcement mechanism. If the session announcement state is enabled, clients are informed each time a controller is not able to serve the multicast direct data to the client.
- In the **Session announcement URL** text box, enter the URL where the client can find more information when an error occurs during the multicast media stream transmission.
- In the **Session announcement e-mail** text box, enter the e-mail address of the person who can be contacted.
- In the **Session announcement Phone** text box, enter the phone number of the person who can be contacted.
- In the **Session announcement Note** text box, enter a reason as to why a particular client cannot be served with a multicast media.
- Click **Apply**.

#### Step 2

Add a media stream by following these steps:

- Choose **Wireless > Media Stream > Streams** to open the Media Stream page.
- Click **Add New** to configure a new media stream. The **Media Stream > New page** appears.  
**Note** The Stream Name, Multicast Destination Start IP Address (IPv4 or IPv6), and Multicast Destination End IP Address (IPv4 or IPv6) text boxes are mandatory. You must enter information in these text boxes.
- In the **Stream Name** text box, enter the media stream name. The stream name can be up to 64 characters.
- In the **Multicast Destination Start IP Address (IPv4 or IPv6)** text box, enter the start (IPv4 or IPv6) address of the multicast media stream.

- e) In the **Multicast Destination End IP Address (IPv4 or IPv6)** text box, enter the end (IPv4 or IPv6) address of the multicast media stream.

**Example:**

**Note** Ensure that the Multicast Destination Start and End IP addresses are of the same type, that is both addresses should be of either IPv4 or IPv6 type.

- f) In the **Maximum Expected Bandwidth** text box, enter the maximum expected bandwidth that you want to assign to the media stream. The values can range between 1 to 35000 kbps.

**Example:**

**Note** We recommend that you use a template to add a media stream to the controller.

- g) From the Select from Predefined Templates drop-down list under Resource Reservation Control (RRC) Parameters, choose one of the following options to specify the details about the resource reservation control:

- Very Coarse (below 300 kbps)
- Coarse (below 500 kbps)
- Ordinary (below 750 kbps)
- Low (below 1 Mbps)
- Medium (below 3 Mbps)
- High (below 5 Mbps)

**Note** When you select a predefined template from the drop-down list, the following text boxes under the Resource Reservation Control (RRC) Parameters list their default values that are assigned with the template.

- Average Packet Size (100-1500 bytes)—Specifies the average packet size. The value can be in the range of 100 to 1500 bytes. The default value is 1200.
- RRC Periodic update—Enables the RRC (Resource Reservation Control Check) Periodic update. By default, this option is enabled. RRC periodically updates the admission decision on the admitted stream according to the correct channel load. As a result, it may deny certain low priority admitted stream requests.
- RRC Priority (1-8)—Specifies the priority bit set in the media stream. The priority can be any number between 1 and 8. The larger the value means the higher the priority is. For example, a priority of 1 is the lowest value and a value of 8 is the highest value. The default priority is 4. The low priority stream may be denied in the RRC periodic update.
- Traffic Profile Violation—Specifies the action to perform in case of a violation after a re-RRC. Choose an action from the drop-down list. The possible values are as follows:
  - Drop—Specifies that a stream is dropped on periodic reevaluation.
  - Fallback—Specifies that a stream is demoted to Best Effort class on periodic reevaluation.
 The default value is **drop**.

- h) Click **Apply**.

**Step 3** Enable the media stream for multicast-direct by following these steps:

- a) Choose **WLANs > WLAN ID** to open the **WLANs > Edit** page.
- b) Click the **QoS** tab and select Gold (Video) from the Quality of Service (QoS) drop-down list.
- c) Click **Apply**.

**Step 4** Set the EDCA parameters to voice and video optimized (optional) by following these steps:

- a) Choose **Wireless > 802.11a/n/ac** or **802.11b/g/n > EDCA Parameters**.
- b) From the **EDCA Profile** drop-down list, choose the Voice and Video Optimized option.
- c) Click **Apply**.

**Step 5** Enable the admission control on a band for video (optional) by following these steps:

**Note** Keep the voice bandwidth allocation to a minimum for better performance.

- a) Choose **Wireless > 802.11a/n/ac** or **802.11b/g/n > Media** to open the 802.11a/n (5 GHz) or 802.11b/g/n > Media page.
- b) Click the **Video** tab.
- c) Select the **Admission Control (ACM)** check box to enable bandwidth-based CAC for this radio band. The default value is disabled.
- d) Click **Apply**.

**Step 6** Configure the video bandwidth by following these steps:

**Note** The template bandwidth that is configured for a media stream should be more than the bandwidth for the source media stream. The voice configuration is optional. Keep the voice bandwidth allocation to a minimum for better performance.

- a) Disable all WMM WLANs.
- b) Choose **Wireless > 802.11a/n/ac** or **802.11b/g/n > Media** to open the 802.11a/n/ac (5 GHz) or 802.11b/g/n > Media page.
- c) Click the **Video** tab.
- d) Select the **Admission Control (ACM)** check box to enable the video CAC for this radio band. The default value is disabled.
- e) In the Max RF Bandwidth field, enter the percentage of the maximum bandwidth allocated to clients for video applications on this radio band. Once the client reaches the value specified, the access point rejects new requests on this radio band.  
The range is 5 to 85%. The default value is 9%.
- f) Click **Apply**.
- g) Reenable all WMM WLANs and click **Apply**.

**Step 7** Configure the media bandwidth by following these steps:

- a) Choose **Wireless > 802.11a/n/ac** or **802.11b/g/n > Media** to open the 802.11a (or 802.11b) > Media > Parameters page.
- b) Click the **Media** tab to open the Media page.
- c) Select the **Unicast Video Redirect** check box to enable Unicast Video Redirect. The default value is disabled.
- d) In the **Maximum Media Bandwidth (0-85%)** text box, enter the percentage of the maximum bandwidth to be allocated for media applications on this radio band. Once the client reaches a specified value, the access point rejects new calls on this radio band.  
The default value is 85%; valid values are from 0% to 85%.
- e) In the **Client Minimum Phy Rate** text box, enter the minimum transmission data rate to the client. If the transmission data rate is below the phy rate, either the video will not start or the client may be classified as a bad client. The bad client video can be demoted for better effort QoS or subject to denial.

- f) In the **Maximum Retry Percent (0-100%)** text box, enter the percentage of maximum retries that are allowed. The default value is 80. If it exceeds 80, either the video will not start or the client might be classified as a bad client. The bad client video can be demoted for better effort QoS or subject to denial.
- g) Select the **Multicast Direct Enable** check box to enable the Multicast Direct Enable field. The default value is enabled.
- h) From the **Max Streams per Radio** drop-down list, choose the maximum number of streams allowed per radio from the range 0 to 20. The default value is set to No-limit. If you choose No-limit, there is no limit set for the number of client subscriptions.
- i) From the **Max Streams per Client** drop-down list, choose the maximum number of streams allowed per client from the range 0 to 20. The default value is set to No-limit. If you choose No-limit, there is no limit set for the number of client subscriptions.
- j) Select the **Best Effort QoS Admission** check box to enable best-effort QoS admission.
- k) Click **Apply**.

**Step 8** Enable a WLAN by following these steps:

- a) Choose **WLANS > WLAN ID**. The **WLANs > Edit** page appears.
- b) Select the **Status** check box.
- c) Click **Apply**.

**Step 9** Enable the 802.11 a/n/ac or 802.11 b/g/n network by following these steps:

- a) Choose **Wireless > 802.11a/n/ac** or **802.11b/g/n > Network**.
- b) Select the **802.11a** or **802.11b/g Network Status** check box to enable the network status.
- c) Click **Apply**.

**Step 10** Verify that the clients are associated with the multicast groups and group IDs by following these steps:

- a) Choose **Monitor > Clients**. The **Clients** page appears.
  - b) Check if the 802.11a/n/ac or 802.11b/g/n network clients have the associated access points.
  - c) Choose **Monitor > Multicast**. The **Multicast Groups** page appears.
  - d) Select the **MGID** check box for the VideoStream to the clients.
  - e) Click **MGID**. The **Multicast Group Detail** page appears. Check the Multicast Status details.
-