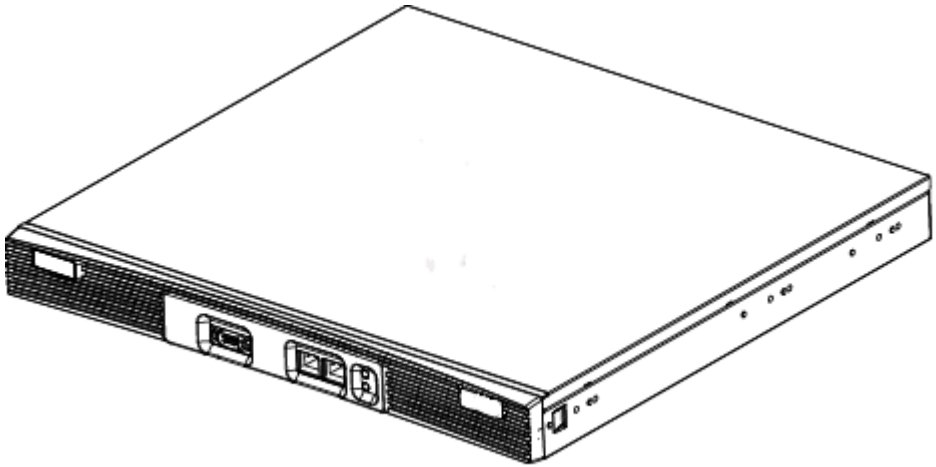
MOTOROLA

WS5100 Series Switch

CLI Reference Guide



About This Guide

This preface introduces the *WS5100 Series CLI Reference Guide* and contains the following sections:

Who Should Use this Guide

The *WS5100 Series CLI Reference Guide* is intended for system administrators responsible for the implementing, configuring, and maintaining the WS5100 switch using the switch's *command line interface* (CLI). It also serves as a reference for configuring and modifying most common system settings. The administrator should be familiar with wireless technologies, network concepts, ethernet concepts, as well as IP addressing and SNMP concepts.

How to Use this Guide

This guide will help you implement, configure, and administer the WS5100 switch and associated network elements. This guide is organized into the following sections:

Chapter	***Jump to this section if you want to...***
Chapter 1, "Introduction"	Review the overall feature-set of the WS5100 switch, as well as the many configuration options available.
Chapter 2, "Common Commands"	Summarizes the commands common amongst many contexts and instance contexts within the WS5100 switch command line interface.
Chapter 3, "User Exec Commands"	Summarizes the User Exec commands within the WS5100 switch command line interface.
Chapter 4, "Privileged Exec Commands"	Summarizes the Priv Exec commands within the WS5100 switch command line interface.
Chapter 5, "Global Configuration Commands"	Summarizes the Global Config commands within the WS5100 switch command line interface.
Chapter 6, "crypto-isakmp"	Summarizes the **`crypto-isakmp`** commands within the WS5100 switch command line interface.
Chapter 7, "crypto-group"	Summarizes the **`crypto-group`** commands within the WS5100 switch command line interface.
Chapter 8, "crypto-peer"	Summarizes the **`crypto-peer`** commands within the WS5100 switch command line interface.
Chapter 9, "crypto-ipsec"	Summarizes the **`crypto-ipsec`** commands within the WS5100 switch command line interface.
Chapter 10, "crypto-map"	Summarizes the **`crypto-map`** commands within the WS5100 switch command line interface.
Chapter 11, "crypto-trustpoint Instance"	Summarizes the **`crypto trustpoint`** commands within the WS5100switch command line interface.

Chapter	*Jump to this section if you want to...*
Chapter 12, "interface Instance"	Summarizes the **`config-if`** commands within the WS5100 switch command line interface.
Chapter 13, "spanning tree-mst Instance"	Summarizes the **`(config-mst)`** instance commands within the WS5100 switch command line interface.
Chapter 14, "Extended ACL Instance"	Summarizes the **`config-ext-nacl`** commands within the WS5100 switch command line.
Chapter 15, "Standard ACL Instance"	Summarizes the **`config-std-nacl`** commands within the WS5100 switch command line.
Chapter 16, "Extended MAC ACL Instance"	Summarizes the **`config-ext-macl`** commands within the WS5100 switch command line.
Chapter 17, "DHCP Server Instance"	Summarizes the **`(config-dhcp pool)`** commands within the WS5100 switch command line.
Chapter 18, "DHCP Class Instance"	Summarizes the **`(config-dhcp-class)`** instance commands within the WS5100 switch command line interface.
Chapter 19, "Radius Server Instance"	Summarizes the **`(config-radsrv)`** instance commands within the WS5100 switch command line interface.
Chapter 20, "Wireless Instance"	Summarizes the **`(config-wireless)`** instance commands within the WS5100 switch command line interface.
Chapter 21, "SOLE Instance"	Summarizes the **`(config-sole)`** instance commands within the WS5100 switch command line interface.

Conventions Used in this Guide

This section describes the following topics:

- *Annotated Symbols*
- *Notational Conventions*

Annotated Symbols

The following document conventions are used in this document:

NOTE: Indicate tips or special requirements.

CAUTION: Indicates conditions that can cause equipment damage or data loss.

WARNING! Indicates a condition or procedure that could result in personal injury or equipment damage.

Notational Conventions

The following notational conventions are used in this document:

- Italics are used to highlight specific items in the general text, and to identify chapters and sections in this and related documents.
- Bullets (•) indicate:
  - action items
  - lists of alternatives
  - lists of required steps that are not necessarily sequential
- Sequential lists (those describing step-by-step procedures) appear as numbered lists.

Convention	*Example Token*	*Description*	*Valid Inputs*
bold		Bold text indicates commands and keywords that you enter literally	
italics		Italic text indicates arguments for which you supply values.	
()	(on|off)	Grouping (exactly one of a list of tokens)	on

Convention	*Example Token*	*Description*	*Valid Inputs*
{}	{key1|key2|key 3}	Selective recursive (multiple tokens allowed, but each can only be used once)	key1 key3
[ ]	[key1|key2|key 3]	Infinite recursive (multiple tokens allowed, each can be used multiple times)	key1 key1 key2 key3 key2 key3
.	.<1-10>	Simple infinite recursive	1 2 6
?	[key1|?key2]	Selective keyword in infinite recursive (multiple tokens, but you can pick one that's only allowed once)	key1 key1 key2

Motorola Service Information

Use the Motorola Support Center as the primary contact for any technical problem, question, or support issue involving Motorola products. Motorola Support Center responds to calls by email, telephone or fax within the time limits set forth in individual contractual agreements:

Telephone (North America): 1-800-653-5350

Telephone (International): +1-631-738-6213

Fax: (631) 738-5410

Email: *emb.support@motorola.com*

When contacting Motorola Support Center, please provide the following information:

- Serial number of the unit.
- Model number or product name.
- Software type and version number.

Customer Support Website

Comprehensive on-line support is available at the MySymbolCare Web site at http://www.symbol.com/support/ . Registration is free and a variety of services can be linked through this Web portal.

Product Sales and Product Information

North America	International
Motorola, Inc. One Symbol Plaza Holtsville, New York 11742-1300 Tel: 1-631-738-2400 or 1-800-722-6234 Fax: 1-631-738-5990	Motorola, Inc. Symbol Place Winnersh Triangle, Berkshire, RG41 5TP United Kingdom Tel: 0800-328-2424 (Inside UK) +44 118 945 7529 (Outside UK)

General Information

For general information, contact Motorola at:

Telephone (North America): 1-800-722-6234

Telephone (International): +1-631-738-5200

Website: http://www.motorola.com

Motorola, Inc.
End-User License Agreement

BY DOWNLOADING, INSTALLING, OR USING THE SOFTWARE DESCRIBED IN THIS DOCUMENT, YOU OR THE ENTITY OR COMPANY THAT YOU REPRESENT ("LICENSEE") ARE UNCONDITIONALLY CONSENTING TO BE BOUND BY AND ARE BECOMING A PARTY TO THIS LICENSE AGREEMENT ("AGREEMENT"). LICENSEE'S USE OR CONTINUED USE OF THE DOWNLOADED OR INSTALLED MATERIALS SHALL ALSO CONSTITUTE ASSENT TO THE TERMS OF THIS AGREEMENT. IF LICENSEE DOES NOT UNCONDITIONALLY AGREE TO ALL OF THE TERMS OF THIS AGREEMENT, DO NOT CONTINUTE THE INSTALLATION PROCESS. IF THESE TERMS ARE CONSIDERED AN OFFER, ACCEPTANCE IS EXPRESSLY LIMITED TO AND EXPRESSLY CONTINGENT UPON THESE TERMS. IF YOU ARE ACCEPTING THESE TERMS ON BEHALF OF A COMPANY, ANOTHER PERSON OR ANY OTHER LEGAL ENTITY, YOU REPRESENT AND WARRANT THAT YOU HAVE THE AUTHORITY TO BIND THAT COMPANY, PERSON OR ENTITY.

1. LICENSE GRANT. Subject to the terms of this Agreement, Motorola, Inc. and/or its subsidiaries ("Licensor") hereby grants Licensee a limited, personal, non-sublicensable, non transferable, nonexclusive license to use the software that Licensee is about to download or install and the documentation that accompanies it (collectively, the "Software") for Licensee's personal use in connection with hardware produced by Licensor and only in accordance with the accompanying documentation. Licensee may download, install and use the Software only on a single computer. Licensee may make one copy of the Software (excluding any documentation) for backup purposes, provided that copyright and other restricted rights notices of Licensor and its suppliers are reproduced exactly.
2. LICENSE RESTRICTIONS. Except as expressly permitted by this Agreement, Licensee shall not, nor permit anyone else to, directly or indirectly: (i) copy (except for one backup copy), modify, distribute or create derivative works based upon the Software; (ii) reverse engineer, disassemble, decompile or otherwise attempt to discover the source code or structure, sequence and organization of the Software; or (iii) rent, lease, or use the Software for timesharing or service bureau purposes, or otherwise use the Software for any commercial purpose/on behalf of any third party. Licensee shall maintain and not remove or obscure any proprietary notices on the Software, and shall reproduce such notices exactly on all permitted copies of the Software. All title, ownership rights, and intellectual property rights in and to the Software, and any copies or portions thereof, shall remain in Licensor and its suppliers or licensors. Licensee understands that Licensor may modify or discontinue offering the Software at any time. The Software is protected by the copyright laws of the United States and international copyright treaties. The Software is licensed, not sold. This Agreement does not give Licensee any rights not expressly granted herein.

3. INTELLECTUAL PROPERTY; CONTENT. All title and intellectual property rights in and to the Software (including but not limited to any images, photographs, animations, video, audio, music, text and "applets" incorporated into the Software), and any copies you are permitted to make herein are owned by Licensor or its suppliers. All title and intellectual property rights in and to the content which may be accessed through use of the Software is the property of the respective content owner and may be protected by applicable copyright or other intellectual property laws and treaties. This EULA grants you no rights to use such content. As a condition to Licensee's use of the Software, Licensee represents, warrants and covenants that Licensee will not use the Software: (i) to infringe the intellectual property rights or proprietary rights, or rights of publicity or privacy, of any third party; (ii) to violate any applicable law, statute, ordinance or regulation; (iii) to disseminate information or materials in any form or format ("Content") that are harmful, threatening, abusive, harassing, tortuous, defamatory, vulgar, obscene, libelous, or otherwise objectionable; or (iv) to disseminate any software viruses or any other computer code, files or programs that mayinterrupt, destroy or limit the functionality of any computer software or hardware or telecommunications equipment. Licensee, not Licensor, remains solely responsible for all Content that Licensee uploads, posts, e-mails, transmits, or otherwise disseminates using, or in connection with, the Software.
4. FEES; SUPPORT AND UPGRADES. Licensor may, at Licensor's sole option, provide support services related to the Software ("Support Services"). Nothing in this Agreement grants Licensee any right to receive any Support Services. Use of any Support Services provided is governed by the Licensor policies and programs described in the user manual, in "online" documentation, and/or in other Licensor-provided materials or support agreements. Any supplemental software code provided to you as part of any Support Services shall be considered part of the Software and subject to the terms and conditions of this EULA. With respect to technical information you provide to Licensor as part of any Support Services, Licensor may use such information for its business purposes, including for product support and development. Licensor will not utilize such technical information in a form that personally identifies Licensee.
5. TERMINATION. Either party may terminate this Agreement at any time, with or without cause, upon written notice. Any termination of this Agreement shall also terminate the licenses granted hereunder. Upon termination of this Agreement for any reason, Licensee shall return all copies of the Software to Licensor, or destroy and remove from all computers, hard drives, networks, and other storage media all copies of the Software, and shall so certify to Licensor that such actions have occurred. Sections 2-13 shall survive termination of this Agreement.

6. DISCLAIMER OF WARRANTIES. To the maximum extent permitted by applicable law, Licensor and its suppliers provide the Software and any (if any) Support Services AS IS AND WITH ALL FAULTS, and hereby disclaim all warranties and conditions, either express, implied or statutory, including, but not limited to, any (if any) implied warranties or conditions of merchantability, of fitness for a particular purpose, of lack of viruses, of accuracy or completeness of responses, of results, and of lack of negligence or lack of workmanlike effort, all with regard to the Software, and the provision of or failure to provide Support Services. ALSO, THERE IS NO WARRANTY OR CONDITION OF TITLE, QUIET ENJOYMENT, QUIET POSSESSION, CORRESPONDENCE TO DESCRIPTION, OR NONINFRINGEMENT WITH REGARD TO THE SOFTWARE. THE ENTIRE RISK AS TO THE QUALITY OF OR ARISING OUT OF USE OR PERFORMANCE OF THE SOFTWARE AND SUPPORT SERVICES, IF ANY, REMAINS WITH LICENSEE.
7. EXCLUSION OF INCIDENTAL, CONSEQUENTIAL AND CERTAIN OTHER DAMAGES. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL LICENSOR OR ITS SUPPLIERS BE LIABLE FOR ANY GENERAL, SPECIAL, INCIDENTAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES WHATSOEVER (INCLUDING, BUT NOT LIMITED TO, DAMAGES FOR LOSS OF PROFITS OR CONFIDENTIAL OR OTHER INFORMATION, FOR BUSINESS INTERRUPTION, FOR PERSONAL INJURY, FOR LOSS OF PRIVACY, FOR FAILURE TO MEET ANY DUTY INCLUDING OF GOOD FAITH OR OF REASONABLE CARE, FOR NEGLIGENCE, AND FOR ANY OTHER PECUNIARY OR OTHER LOSS WHATSOEVER) ARISING OUT OF OR IN ANY WAY RELATED TO THE USE OF OR INABILITY TO USE THE SOFTWARE, THE PROVISION OF OR FAILURE TO PROVIDE SUPPORT SERVICES, OR OTHERWISE UNDER OR IN CONNECTION WITH ANY PROVISION OF THIS AGREEMENT, EVEN IN THE EVENT OF THE FAULT, TORT (INCLUDING NEGLIGENCE), STRICT LIABILITY, BREACH OF CONTRACT OR BREACH OF WARRANTY OF LICENSOR OR ANY SUPPLIER, AND EVEN IF LICENSOR OR ANY SUPPLIER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.
8. LIMITATION OF LIABILITY AND REMEDIES. Notwithstanding any damages that Licensee might incur for any reason whatsoever (including, without limitation, all damages referenced above and all direct or general damages), the entire liability of Licensor and any of its suppliers under any provision of this Agreement and Licensee's exclusive remedy for all of the foregoing shall be limited to the greater of the amount actually paid by Licensee for the Software or U.S.$5.00. The foregoing limitations, exclusions and disclaimers shall apply to the maximum extent permitted by applicable law, even if any remedy fails its essential purpose.

9. INDEMNITY. Licensee agrees that Licensor shall have no liability whatsoever for any use Licensee makes of the Software. Licensee shall indemnify and hold harmless Licensor from any claims, damages, liabilities, costs and fees (including reasonable attorney fees) arising from Licensee's use of the Software as well as from Licensee's failure to comply with any term of this Agreement.
10. FAULT TOLERANCE. The Software is not fault-tolerant and is not designed, manufactured or intended for use or resale in on-line control equipment in hazardous environments requiring fail-safe performance, such as, but not limited to, the operation of nuclear facilities, aircraft navigation or communication systems, air traffic control, life support machines, or weapons systems, in which the failure of the Software could lead directly or indirectly to death, personal injury, or physical or environmental damage ("High Risk Activities"). Licensor and its suppliers specifically disclaim any express or implied warranty of fitness for High Risk Activities.
11. U.S. GOVERNMENT LICENSE RIGHTS. Software provided to the U.S. Government pursuant to solicitations issued on or after December 1, 1995 is provided with the commercial license rights and restrictions described elsewhere herein. Software provided to the U.S. Government pursuant to solicitations issued prior to December 1, 1995 is provided with "Restricted Rights" as provided for in FAR, 48 CFR 52.227-14 (JUNE 1987) or DFAR, 48 CFR 252.227- 7013 (OCT 1988), as applicable. The "Manufacturer" for purposes of these regulations is Motorola, Inc., One Symbol Plaza, Holtsville, NY 11742.
12. EXPORT RESTRICTIONS. Licensee shall comply with all export laws and restrictions and regulations of the Department of Commerce, the United States Department of Treasury Office of Foreign Assets Control ("OFAC"), or other United States or foreign agency or authority, and Licensee shall not export, or allow the export or re-export of the Software in violation of any such restrictions, laws or regulations. By downloading or using the Software, Licensee agrees to the foregoing and represents and warrants that Licensee is not located in, under the control of, or a national or resident of any restricted country.
13. MISCELLANEOUS. Licensee may not sublicense, assign, or transfer this Agreement, or its rights or obligations hereunder, without the prior written consent of Licensor. Any attempt to otherwise sublicense, assign, or transfer any of the rights, duties, or obligations hereunder is null and void. Licensor may assign this Agreement in its sole discretion. In the event that any of the provisions of this Agreement shall be held by a court or other tribunal of competent jurisdiction to be illegal, invalid or unenforceable, such provisions shall be limited or eliminated to the minimum extent necessary so that this Agreement shall otherwise remain in full force and effect. No waiver or modification of this Agreement will be binding upon a party unless made in writing and signed by a duly authorized representative of such party and no failure or delay in enforcing any right will be deemed a

waiver. This Agreement shall be governed by the laws of the State of New York without regard to the conflicts of law provisions thereof. The application the United Nations Convention of Contracts for the International Sale of Goods is expressly excluded. Unless waived by Licensor for a particular instance, any action or proceeding arising out of this Agreement must be brought exclusively in the state or federal courts of New York and Licensee hereby consents to the jurisdiction of such courts for any such action or proceeding. This Agreement supersedes all prior discussions and writings and constitutes the entire agreement between the parties with respect to the subject matter hereof. The prevailing party in any action arising out of this Agreement shall be entitled to costs and attorneys' fees.

Contents

Chapter 1. Introduction

Chapter 2. Common Commands

Chapter 3. User Exec Commands

Chapter 4. Privileged Exec Commands

Chapter 5. Global Configuration Commands

Chapter 7. crypto-group

Chapter 8. crypto-peer

Chapter 9. crypto-ipsec

Chapter 10. crypto-map

Chapter 11. crypto-trustpoint Instance

Chapter 12. interface Instance

Chapter 13. spanning tree-mst Instance

Chapter 14. Extended ACL Instance

Chapter 15. Standard ACL Instance

Chapter 16. Extended MAC ACL Instance

Chapter 17. DHCP Server Instance

Chapter 18. DHCP Class Instance

Chapter 19. Radius Server Instance

Chapter 20. Wireless Instance

Chapter 21. SOLE Instance

1

Introduction

This chapter describes the commands defined by the switch *Command Line Interface* (CLI). Access the CLI by running a terminal emulation program on a computer connected to the serial port on the front of the switch, or by using a Telnet session via *secure shell* (SSH) to access the switch over the network.

The default CLI user designation is **cli**. The default username and password are *admin* and *superuser*.

1.1 CLI Overview

The CLI is used for configuring, monitoring, and maintaining the switch managed network. The user interface allows you to execute commands, whether using a serial console or using a remote access method.

This chapter describes the basic features of the CLI. Topics covered include an introduction to command modes, navigation and editing features, help features, and command history features.

The CLI is segregated into different command modes. Each mode has its own set of commands for configuration, maintenance and monitoring. The commands available at any given time depend on the mode you are in. Enter a question mark (**?**) at the system prompt to view a list of commands available for each command mode/instance.

Use specific commands to navigate from one command mode to another. The standard order is: USER EXEC mode, PRIV EXEC mode and GLOBAL CONFIG mode.

A session generally begins in USER EXEC mode (one of the two access levels of the EXEC mode). For security, only a limited subset of EXEC commands are available in the USER EXEC mode. This level is reserved for tasks that do not change the configuration of the switch (such as determining the current switch configuration).

To access commands, enter the PRIV EXEC mode (the second access level for the EXEC mode). In PRIV EXEC mode, enter any EXEC command. The PRIV EXEC mode is a superset of the USER EXEC mode.

Most of the USER EXEC mode commands are one-time commands and are not saved across reboots of the switch. For example, the show command displays the current configuration and the clear command clears the interface.

Access the GLOBAL CONFIG mode from the PRIV EXEC mode. In the GLOBAL CONFIG mode, enter commands that set general system characteristics. Configuration modes, allow you to change the running configuration. If you save the configuration later, these commands are stored across switch reboots.

Access a variety of protocol-specific (or feature-specific) modes from the global configuration mode. The CLI hierarchy requires you access specific configuration modes only through the global configuration mode.

You can also access sub-modes from the global configuration mode. Configuration sub-modes define specific features within the context of a configuration mode.

Table 1.1 summarizes the commands available from the switch.

Table 1.1 WS5100 CLI Hierarchy

User Exec Mode	***Priv Exec Mode***	***Global Configuration Mode***
clear	acknowledge	aaa
clrscr	archive	access-list
cluster-cli	cd	autoinstall
debug	change-passwd	banner
disable	clear	bridge
enable	clock	country-code
exit	clrscr	crypto

User Exec Mode	***Priv Exec Mode***	***Global Configuration Mode***
help	cluster-cli	errdisable
logout	configure	fallback
no	copy	ftp
page	debug	hostname
ping	delete	interface
quit	diff	ip
service	dir	line
show	disable	local
telnet	edit	logging
terminal	enable	mac
traceroute	erase	mac-address-table
	exit	management
	halt	ntp
	help	prompt
	kill	radius-server
	logout	redundancy
	mkdir	service
	more	snmp-server
	no	spanning-tree
	page	timezone
	ping	username
	pwd	vpn

User Exec Mode	*Priv Exec Mode*	*Global Configuration Mode*
	quit	wlan-acl
	reload	
	rename	
	rmdir	
	service	
	show	
	telnet	
	terminal	
	traceroute	
	upgrade	
	upgrade-abort	
	write	

1.2 Getting Context Sensitive Help

Enter a question mark (**?**) at the system prompt to display a list of commands available for each mode. Optionally obtain a list of arguments and keywords for any command using the switch CLI context-sensitive help.

Use the following commands to obtain help specific to a command mode, command name, keyword or argument:

Command	*Description*
(prompt)# **help**	Displays a brief description of the help system.
*(prompt)# abbreviated-command-entry***?**	Lists commands in the current mode that begin with a particular character string.

Command	***Description***
(prompt)# abbreviated-command-entry<**Tab**>	Completes a partial command name.
(prompt)# **?**	Lists all commands available in the command mode.
prompt)# command ?	Lists the available syntax options (arguments and keywords) for the command.
(prompt)# command keyword ?	Lists the next available syntax option for the command.

NOTE: The system prompt varies depending on which configuration mode you are in.

When using context-sensitive help, the space (or lack of a space) before the question mark (?) is significant. To obtain a list of commands that begin with a particular sequence, enter the characters followed by a question mark (?). Do not include a space. This form of help is called **word help**, because it completes a word.

```
WS5100#service?
  service  Service Commands

WS5100#service
```

Enter a question mark (?) (in place of a keyword or argument) to list keywords or arguments. Include a space before the **?**. This kind of help is called **command syntax help.** It shows keywords or arguments are available based on the command/keyword and argument already entered.

```
WS5100>service ?
  diag      Diagnostics
  encrypt   Encrypt password or key with secret
  save-cli  Save CLI tree for all modes in html format
  show      Show running system information

WS5100>service
```

It's possible to abbreviate commands and keywords to allow a unique abbreviation. For example, "configure terminal" can be abbreviated as `config t`. Since the abbreviated command is unique, the switch accepts the abbreviation and executes the command.

Enter the help command (available in any command mode) to provide the following description:

```
WS5100>help
CLI provides advanced help feature.  When you need help,
anytime at the command line please press '?'.

If nothing matches, the help list will be empty and you must backup
until entering a '?' shows the available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each possible
   argument.
2. Partial help is provided when an abbreviated argument is entered
   and you want to know what arguments match the input
   (e.g. 'show ve?'.)

WS5100>
```

1.3 Using the no and default Forms of Commands

Almost every command has a `no` form. Use the no form to disable a feature or function. Use the command without the no keyword to re-enable a disabled feature or enable a feature disabled by default.

1.3.1 Basic Conventions

Keep the following conventions in mind while working within the CLI:

- Always use **?** at the end of a command to view sub-modes that can be used. If yes, type the first few characters of the sub-mode and press the tab key to add the sub-mode. Continue using **?** until you reach the final sub-mode you would like to use.
- Pre-defined CLI commands and keywords are case-insensitive: `cfg = Cfg = CFG`. However (for clarity), CLI commands and keywords are displayed in this guide using mixed case. For example, `apPolicy`, `trapHosts`, `channelInfo`.
- Enter commands in uppercase, lowercase, or mixed case. Only passwords are case sensitive.

- If an instance name (or other parameter) contains whitespace, the name must be enclosed in quotes:

```
WS5100.(Cfg)> spol "Default Switch Policy"
WS5100.(Cfg).SPolicy.[Default Switch Policy]>
```

NOTE: CLI commands starting with `#`, at the `WS5100#` prompt, is ignored and is not executed.
Any leading space before a CLI command is ignored in execution

1.4 Using CLI Editing Features and Shortcuts

A variety of shortcuts and editing features are available. The following describe these features:

- *Moving the Cursor on the Command Line*
- *Completing a Partial Command Name*
- *Deleting Entries*
- *Re-displaying the Current Command Line*
- *Transposing Mistyped Characters*
- *Controlling Capitalization*

1.4.1 Moving the Cursor on the Command Line

Table 1.2 shows the key combinations or sequences you can use to move the cursor around on the command line. **Ctrl** defines the Control key, which must be pressed simultaneously with its associated letter key.

Esc supports the Escape key (which must be pressed first), followed by its associated letter key. Keys are not case sensitive. Specific letters were chosen to provide an easy way of remembering their functions. In Table 1.2, characters in bold (inside the "***Function Summary***" column) indicate the relation between a letter and its function.

Table 1.2 Key Combinations Used to Move the Cursor

Keystrokes	***Function Summary***	***Function Details***
Left Arrow or **Ctrl-B**	Back character	Moves the cursor one character to the left. When entering a command that extends beyond a single line, press the Left Arrow or Ctrl-B keys repeatedly to scroll back to the system prompt and verify the beginning of the command entry. You can press the Ctrl-A key combination.
Right Arrow or **Ctrl-F**	Forward character	Moves the cursor one character to the right.
Esc, B	Back word	Moves the cursor back one word.
Esc, F	Forward word	Moves the cursor forward one word.
Ctrl-A	Beginning of line	Moves the cursor to the beginning of the line.
Ctrl-E	End of line	Moves the cursor to the end of the command line.
Ctrl-d		Deletes the current character
Ctrl-U		Deletes text up to cursor
Ctrl-K		Deletes from cursor to end of the line
Ctrl-P		Obtains the prior command from memory
Ctrl-N		Obtains the next command from memory
Esc-C		Converts the rest of a word to uppercase
Esc-L		Converts the rest of a word to lowercase
Esc-D		Deletes the remainder of a word
Ctrl-W		Deletes the word up to the cursor

Keystrokes	***Function Summary***	***Function Details***
Ctrl-Z		Enters the command and returns to the root promp
Ctrl-L		Refresh input line

1.4.2 Completing a Partial Command Name

If you cannot remember a complete command name, or if you want to reduce the amount of typing you have to perform, enter the first few letters of a command, then press the **Tab** key. The command line parser completes the command if the string entered is unique to the command mode. If your keyboard does not have a Tab key, press Ctrl-I.

The CLI recognizes a command once you have entered enough characters to make the command unique. If you enter "conf" within the privileged EXEC mode, the CLI associates the entry with the configure command, since only the configure command begins with `conf`.

In the following example, the CLI recognizes a unique string in the privileged EXEC mode when the Tab key is pressed:

```
WLAN Module# conf<Tab>
WLAN Module# configure
```

When you use the command completion feature, the CLI displays the full command name. The command is not executed until you use the **Return** or **Enter** key. This way you can modify the command if the full command was not what you intended in the abbreviation. If entering a set of characters (indicating more than one command), the system lists all commands that begin with that set of characters.

Alternatively, enter a question mark (?) to obtain a list of commands that begin with that set of characters. Do not leave a space between the last letter and the question mark (?).

For example, entering `co?` lists all commands available in the current command mode:

```
WLAN Module# co?
copy? commit
WLAN Module# co
```

NOTE: The characters you enter before the question mark are reprinted to the screen to allow you to complete the command entry.

1.4.3 Deleting Entries

Use any of the following keys (or key combinations) to delete command entries:

Keystrokes	Purpose
Backspace	Deletes the character to the left of the cursor.
Ctrl-D	Deletes the character at the cursor.
Ctrl-K	Deletes all characters from the cursor to the end of the command line.
Ctrl-W	Deletes a word up to the cursor.
Esc, D	Deletes from the cursor to the end of the word.

1.4.4 Re-displaying the Current Command Line

If you are entering a command and the system suddenly sends a message to your screen, you can easily recall your current command entry. To redisplay the current command line (refresh the screen), use the following key combination:

Keystrokes	Purpose
Ctrl-L	Re-displays the current command line.

1.4.5 Command Output pagination

Output often extends beyond the visible screen length. For cases where output continues beyond the screen, the output is paused and a `Press Any Key to Continue (Q to Quit)` prompt displays at the bottom of the screen. To resume the output, press the Return key to scroll down one line or press the Spacebar to display the next full screen of output.

1.4.6 Transposing Mistyped Characters

If you have mistyped a command entry, you can transpose the mistyped characters. To transpose characters, use the following key combination:

Keystrokes	Purpose
Ctrl-T	Transposes the character to the left of the cursor with the character located at the cursor.

1.4.7 Controlling Capitalization

Capitalize or lowercase words with a few simple key sequences. The switch's CLI commands are generally case-insensitive, and all in lowercase. To change the capitalization of commands, use one of the following k sequences:

Keystrokes	***Purpose***
Esc, C	Capitalizes the letters to the right of cursor.
Esc, L	Changes the letters at the right of cursor to lowercase.

2

Common Commands

This chapter describes the CLI commands used in the USER EXEC and PRIV EXEC modes.

The PRIV EXEC command set contains those commands available within the USER EXEC mode. Some commands can be entered in either mode. Commands entered in either USER EXEC mode or PRIV EXEC mode are referred to as EXEC mode commands. If a user or privilege is not specified, the referenced command can be entered in either mode.

2.1 Common Commands

Table 2.1 summarizes available common commands:

Table 2.1 Common Commands in WS5100

Command	Description	Ref.
clrscr	Clears the display screen	*page 2-2*
exit	Ends the current mode and moves to the previous mode	*page 2-2*
help	Displays the interactive help system	*page 2-2*
no	Negates a command or sets its defaults	*page 2-4*
service	Services or debugs the switch	*page 2-5*
show	Shows running system information	*page 2-23*

2.1.1 clrscr

Common Commands

Clears the screen and refreshes the prompt (**#**)

Syntax

```
clrscr
```

Parameters

None

Example

```
WS5100#clrscr
```

2.1.2 exit

Common Commands

Ends the current mode and moves to the previous mode

Syntax

```
exit
```

Parameters

None

Example

```
WS5100(config)#exit
```

2.1.3 help

Common Commands

Use this command to access the advanced help feature. Use "**?**" anytime at the command prompt to access the help topic.

Two kinds of help are provided:

1. Full help is available when ready to enter a command argument.
2. Partial help is provided when an abbreviated argument is entered and you want to know what arguments match the input (for example 'show ve?'.)

Syntax

```
help
```

or

```
?
```

Parameters

None

Example

```
WS5100>show ?
  autoinstall          autoinstall configuration
  banner               Display Message of the Day Login banner
  commands             Show command lists
  crypto               encryption module
  environment          show environmental information
  history              Display the session command history
  interfaces           Interface status and configuration
  ip                   Internet Protocol (IP)
  ldap                 LDAP server
  licenses             Show any installed licenses
  logging              Show logging configuration and buffer
  mac                  MAC access-list assignment
  management           Display L3 Managment Interface name
  mobility             Display Mobility Parameters
  ntp                  Network time protocol
  privilege            Show current privilege level
  radius               RADIUS configuration commands
  redundancy-group     Display redundancy group parameters
  redundancy-history   Display state transition history of the
                       switch.
  redundancy-members   Display redundancy group members in detail
  snmp                 Display SNMP engine parameters
  snmp-server          Display SNMP engine parameters
  terminal             Display terminal configuration parameters
  timezone             Display timezone
  users                Display information about terminal lines
  version              Display software & hardware version
  wireless             Wireless configuration commands
  wlan-acl             wlan based acl
WS5100>show
```

2.1.4 no

▸ *Common Commands*

Negates a command or sets its defaults

Syntax

```
no
```

Parameters

None

Example (User Exec)

```
WS5100>no ?
  cluster-cli  Cluster context
  debug        Debugging functions
  page         Toggle paging
  service      Service Commands
WS5100>no
```

Example (Priv Exec)

```
WS5100#no ?
  cluster-cli  Cluster context
  debug        Debugging functions
  page         Toggle paging
  service      Service Commands
  upgrade      Name of the patch to remove
WS5100#no
```

Example (Global Config)

```
WS5100(config)#no ?
  aaa                 VPN AAA authentication settings
  access-list         Configure access-lists
  autoinstall         autoinstall configuration command
  banner              Reset login banner to nothing
  bridge              Bridge group commands
  country-code        Clear the currently configured country code.
                      All existing configurations will be erased
  crypto              encryption module
  errdisable          errdisable
  fallback            Configures software fallback feature
  ftp                 Configure FTP Server
  hostname            Reset system's network name to default
  interface           Delete a virtual interface
  ip                  Internet Protocol (IP)
  line                Configure a terminal line
```

```
  local               Local user authentication database for VPN
  logging             Modify message logging facilities
  mac                 MAC configuration
  mac-address-table   Configure MAC address table
  management          sets properties of the management interface
  ntp                 Configure NTP
  prompt              Reset system's prompt
  radius-server       RADIUS server configuration commands
  redundancy          Configure redundancy group parameters
  service             Service Commands
  snmp-server         Modify SNMP engine parameters
  spanning-tree       Spanning tree
  timezone            Revert the timezone to default (UTC)
  username            Establish User Name Authentication
  vpn                 vpn
  wlan-acl            Remove an ACL from WLAN

WS5100(config)#no
```

2.1.5 service

▸ *Common Commands*

Services or debugs the switch

Syntax (User Exec)

```
service [diag|encrypt|save-cli|show|wireless]

service (diag)[enable|fanduty <40-100>|identify|limit|period]

service (diag)(limit)[buffer|fan|filesys|inodes|load|maxFDs|
pkbuffers|procRAM|ram|routecache|temperature]

service (diag)(limit)(buffer)[128|128k|16k|1k|256|2k|32|32k|4k|512|
64|64k|8k]
service (diag)(limit)(fan)<1|2> (low)
service (diag)(limit)(filesys)[etc2|flash|ram]
service (diag)(limit)(inodes)[etc2|flash|ram]
service (diag)(limit)(load)[1|15|5]
service (diag)(limit)(maxFDs)<0-32767>
service (diag)(limit)(pkbuffers)<0-65535>
service (diag)(limit)(procRAM)
service (diag)(limit)(ram)
service (diag)(limit)(routecache)<0-65535>
service (diag)(limit)(temperature)<1-8>
service (diag)(period) <100-30000>
```

```
service (encrypt)(secret)(2)(PASSPHRASE)(plaintext)(keyword)

service (save-cli)
service (show) [cli|command-history|crash-info|diag|info|memory|
process|reboot-history|startup-log|upgrade-history|watchdog]

service (show)(crash-info)(PANIC_FILENAME)
service (show)(diag)(hardware|led-status|limits|period|stats|top)

service (wireless)
```

Parameters (User Exec)

diag	Diagnostics
	• enable – Enables in service diagnostics
	• fanduty <40-100> – Sets the CPU fan PWM duty cycle. Define a value between 40-100%. Setting a value below 60 is considered unreliable
	• identify – Identifies a switch by flashing its LEDs
	• limit –Sets the diagnostic limit command
	  ◦ buffer [] – Configures the buffer usage warning limit. The warning limit can be set to a buffer limit size [128|128k|16k|1k|256|2k|32|32k|4k|512|64|64k|8k]
	  ◦ fan <1|2> (low) – Sets the fan speed limit. Configure the fan speed limit for both, Fan 1 and Fan 2
	  ◦ filesys [etc2|flash|ram] – Sets the file system freespace limit

	• inodes[etc2|flash|ram] – File system inode limit • load [1|15|5] – Aggregate processor load • maxFDs <0-32767> – Configures the maximum number of file descriptors. Set between 0 to 32767 • pkbuffers <0-65535>– Configures the packet buffer head cache limit. Set between 0 and 65535 • procRAM – Defines the RAM space used by a process. Set he percentage of RAM space used by the processor between 0.0 and 100.0 percent • ram – Configures free space for the RAM. Configures the free space to anything between 0.0 to 100.0 percent • routecache <0-65535> – Configures IP route cache usage. Set with a value between 0 and 65553 • tempreature <1-8> – Sets the temperature sensor for the switch. Set as many as 8 temperature sensors • period <100-30000> – Configures the diagnostics period. Set a value between 100-30000 milliseconds. The default value is 1000 milliseconds.

encrypt	Encrypts a password or key with a secret passphrase • secret – Encrypts passwords/keys with a secret phrase • 2 – Type of encryption SHA256-AES256 • PASSPHRASE – Defines the passphrase used for encryption • ENCRYPT_KEY – Defines the plain text password or key to encrypt
save-cli	Saves the CLI tree for all modes inHTML

show	Displays running system information
	• cli – Shows the CLI tree of the current mode
	• command-history – Displays the command (except show commands) history
	• crash-info – Displays information about core, panic and AP dump files
	  • PANIC_FILENAME – Shows contents of a specified kernel panic file
	• diag – Sets or displays switch diagnostics
	  • hardware – Shows the system hardware configuration
	  • led-status – Show LED state variables and current state
	  • limits – Show limit values
	  • period – Shows the period (ms) for in-service diagnostics
	  • stats – Shows curent diagnostics statistics
	  • top – Shows the top processes (sorted by memory usage)
	• info – Shows a snapshot of available support information
	• memory – Shows memory statistics
	• process – Shows processes (sorted by memory usage)
	• reboot-history – Shows a reboot history

	• startup-log – Shows the startup log • upgrade-history – Shows an upgrade history • watchdog – Shows watchdog status
wireless	Displays current wireless parameters

Syntax (Priv Exec)

```
service [clear|copy|diag|diag-shell|encrypt|pktcap|pm|save-cli|
securitymgr|show|start-shell|test|watchdog|wireless]

service clear
[all|aplogs|clitree|cores|dumps|panics|securitymgr(flows)
{<0-349>|WORD|all|eth <1-2>|vlan <1-4094>}]

service copy (tech-support) (URL)[tftp|ftp|sftp]

service diag [enable|fanduty|identify|limit|period]

service diag-shell <Cr>

service encrypt

service pktcap (on) [bridge|interface|router]
service pktcap (on) (bridge) [count <1-99999>|filter|verbose|write]
service pktcap (on) (bridge) (filter)
        [LINE|arp|capwap|dst|ether|host|icmp|ip|ip6|l2|l3|l4|net|
          not|port|src|tcp|udp|vlan|wlan]
service pktcap (on) (bridge) (filter) (arp)[LINE|and|or]
service pktcap (on) (bridge) (filter)
         (capwap)[LINE|and|ctrl|data|or]
service pktcap (on) (bridge) (filter) (dst) [A.B.C.D|net]
service pktcap (on) (bridge) (filter) (ether)
        [broadcast|dst|host|multicast|proto|src]
service pktcap (on) (bridge) (filter) (host) <IP address>
service pktcap (on) (bridge) (filter) (icmp) [LINE|and|or]
service pktcap (on) (bridge) (filter) (ip)
        [LINE|and|multicast|or|proto]
service pktcap (on) (bridge) (filter) (ip6) [LINE|and|or]
service pktcap (on) (bridge) (filter) (l2|l3|l4) [u16|u32|u8]
service pktcap (on) (bridge) (filter) (net) <IP subnet>
service pktcap (on) (bridge) (filter) (not)
        [arp|capwap|dst|ether|host|icmp|ip|ip6|l2|l3|l4|net|not|
          port|src|tcp|udp|vlan|wlan]
service pktcap (on) (bridge) (filter) (port) <0-65535>
service pktcap (on) (bridge) (filter) (src) [<IP address>|net]
service pktcap (on) (bridge) (filter) (tcp) [LINE|and|or|syn]
service pktcap (on) (bridge) (filter) (udp) [LINE|and|or]
service pktcap (on) (bridge) (filter) (vlan) <1-4095>
service pktcap (on) (bridge) (filter) (wlan) <1-2>

service pm (stop)

service save-cli
```

```
service securitymgr [disable|disable-flow-rate-limit|dump-core|
         enable-http-stats]

service (show) [cli|command-history|crash-info|diag|info|last-
passwd|memory|pm (history)[name|all]|process|reboot-
history|securitymgr|startup-log|upgrade-history|watchdog|wireless]

service (show) (securitymgr)
               (flows)[details|source][A.B.C.D|any](destination)
               [A.B.C.D|any](protocol) [any|icmp|tcp|udp]

service start-shell

service test

service watchdog

service wireless [ap-history|buffer-counters|clear-ap-log|
dump-core|enhanced-beacon-table|enhanced-probe-table|
idle-radio-send-multicast|legacy-load-balance|radio-misc-cfg|
rate-scale|request-ap-log|save-ap-log|snmp-trap-throttle|
vlan-cache]
```

Parameters (Priv Exec)

clear	Performs a variety of reset functions • all – Removes all core, dump and panic files • aplogs – Removes all AP log files • clitree – Removes clitree.html (created by the save-cli command) • cores – Removes all core files • dumps – Removes all dump files • panics – Removes all kernel panic files • securitymgr – Securitymgr parameters • flows – Sessions established • <0-349> – Flow Index • WORD – Interface name • all – All established sessions • eth – Ethernet interface • vlan – VLAN
copy	Copies from one file to another • tech-support – Copies extensive system information useful to technical support for troubleshooting • URL [] – Target URLfrom which to copy • tftp://<hostname:port or IP>/path/file • ftp://<user>:<passwd>@ <hostname:port or IP>/path/file • sftp://<user>@<hostname:port or IP>/ path/file

diag	Sets or displays switch diagnostic values
	• enable – Enables in-service diagnostics
	• fanduty <40-100> – CPU fan PWM duty cycle. Set a value between 40-100%. Setting a value below 60 is considered unreliable
	• identify – Identifies a switch by flashing the LEDs
	• limit – Diagnostic limit commands
	  • buffer [] – Configures the buffer usage warning limit. The warning limit can be set to the buffer limit size of [128|128k|16k|1k|256|2k|32|32k|4k|512|64|64k|
	  8k]
	  • fan <1|2> (low) – Sets the fan speed limit. Configure the fan speed limit for both, Fan 1 and Fan 2
	  • filesys [etc2|flash|ram] – Sets the file system freespace limit
	  • inodes[etc2|flash|ram] – Sets the file system inode limit
	  • load [1|15|5] – Aggregate processor load
	  • maxFDs <0-32767> – Configures the maximum number of file descriptors. Set between 0 to 32767 file descriptors
	  • pkbuffers <0-65535>– Sets the packet buffer head cache limit. Set between 0 to 65535 as the buffer cache limit

	• procRAM – Configures the RAM space used by a process. Set the percentage of RAM space between 0.0 and 100.0 percent. • ram – Configures the free space for the RAM. Configure the free space between 0.0 and 100.0 percent. • routecache <0-65535> – Configures IP route cache usage. Set between 0 and 65553 • tempreature <1-8> – Sets the temperature sensor for the switch. Set as many as 8 temperature sensors. • period <100-30000> – Configures the diagnostics period. Set a value between 100-30000 milli seconds. The default value is 1000 milliseconds
diag-shell	Provides diag shell access
encrypt	Encrypt password or key with secret • secret – Encrypt passwords/keys with secret phrase • 2 – Type of encryption SHA256-AES256. • PASSPHRASE – Passphrase for encryption. • ENCRYPT_KEY – Plaintext password or key to encrypt

pktcap (on) [bridge|interface|router|vpn] [count|filter|verbose|write]	Packet capture
	• on – Defines the Capture location
	• bridge – Captures at the bridge
	  • count – Limits the capture packet count
	  • filter – Captures the filter
	  • verbose – Displays full packet body
	  • write – Captures to a file
	• interface – Captures at an interface
	  • WORD – Interface name
	  • ge – GigabitEthernet interface
	  • me1 – FastEthernet interface
	  • sa – StaticAggregate interface
	  • vlan – VLAN
	• router – Capture at the router.
	  • count – Limits capture packet count
	  • filter – Captures filter
	  • verbose – Displays the full packet body
	  • write – Captures to a file
	• vpn – Capture at the VPN
	  • count – Limits capture packet count
	  • filter – Captures the filter
	  • inbound – Captures ingress direction only
	  • outbound – Captures egress direction only
	  • verbose – Displays full packet body
	  • write – Captures to a file

pm	Process Monitor • stop – Stops the PM from monitoring all daemons
save-cli	Saves the CLI tree for all modes in HTML
securitymgr	Securitymgr parameterss • disable – Disables securitymgr • disable-flow-rate-limit – Disables flow rate limitings • dump-core – Creates a core file of the securitymgr processs • enable-http-stats – Enables the securitymgr HTTP statistics interface

show	Displays running system information
	• cli – Shows the CLI tree of the current mode
	• command-history – Displays a command (except show commands) history
	• crash-info – Displays information about core, panic and AP dump files
	• diag – Displays diagnostics
	• info – Shows a snapshot of available support information
	• last-passwd – Displays the last password used to enter shell
	• memory – Shows memory statistics
	• pm – Process Monitor
	  • history – State changes for a process, the time they happened and events
	  • WORD – Process name
	  • all – All processes
	• process – Shows processes (sorted by memory usage)
	• reboot-history – Shows a reboot history
	• securitymgr – Security manager information displays
	• startup-log – Shows the startup log
	• upgrade-history – Shows an upgrade history
	• watchdog – Show the watchdog status
	• wireless – Wireless parameters display

show securitymgr ()	Service Security Manager parameters
	• flows – Sessions established
	  • details|source – Shows detailed flow statistics or source IP address
	  • [A.B.C.D|any] – Flows where source address is A.B.C.D or flows with any source address
	  • destination – Destination IP address
	  • [A.B.C.D|any] – Flows where the destination address is A.B.C.D or flows with any destination address
	  • protocol – Protocol type.
	  • [any|icmp|tcp|udp] – Flows having any or icmp or tcp or udp protocol

start-shell	Provides shell access.
test	Provides test parameters
watchdog	Enables the switch watchdog.
wireless	Wireless parameters. • ap-history – Access-port history. • buffer-counters – Allocation counts for various buffers. • clear-ap-log – Clears the AP logs. • dump-core – Creates a core file of the ccsrvr process. • enhanced-beacon-table – Enhanced beacon table for AP locationing. • enhanced-probe-table – Enhanced probe table for MU locationing. • idle-radio-send-multicast – Forwards multicast packets to radios without associated MUs.

	• legacy-load-balance – Invokes legacy load balance algorithms with the switch • radio-misc-cfg – Radio specific configuration U16 for all radios • rate-scale – Enables wireless rate scaling (default) • request-ap-log – Requests an AP log • save-ap-log – Saves debug/error logs sent by the access-port • snmp-trap-throttle – Limits the number of SNMP traps generated from the wireless module • vlan-cache – VLAN-cache mode

Syntax (GLOBAL Config)

```
service [advanced-vty|dhcp|diag|password-encryption|
pm (sys-restart)|prompt (crash-info)|radius (restart)|
set (command-history|reboot-history|upgrade-history)<10-300>|
show (cli)|terminal-length <0-512>|watchdog]
```

Parameters (GL)BAL Config)

advanced-vty	Enables advanced mode vty interface
dhcp	Enables the DHCP server
diag	• enable – Enables in-service diagnostics • limit – Diagnostic limit command • period – Sets the diagnostics period
password-encryption	Encrypts passwords • secret – Encrypts passwords/keys with a secret phrase • 2 – Type of encryption SHA256-AES256 • PASSPHRASE – Passphrase for encryption • ENCRYPT_KEY – Plaintext password or key to encrypt

pm	Process Monitor • sys-restart – Enables the PM to restart the system when a processes fails
prompt	Enable crash-info prompt • crash-info – Enables a crash-info prompt
radius	Enable radius server • restart – Restarts the radius server with updated configuration
set	Set service parameters. • command-history <10-300> – Sets the size of the command history (default is 200) • reboot-history <10-300> – Sets the size of the reboot history (default is 50) • upgrade-history <10-300> – Sets the size of upgrade history (default is 50)
show	Shows running system information • cli – Shows the CLI tree of the current mode
terminal-length	System wide terminal length configuration • <0-512> – Number of lines of VTY (0 means no line control).
watchdog	Enables the watchdog

Example

```
WS5100#service diag ?
  enable  Enable in service diagnostics
  led     LED control
  limit   diagnostic limit command
  period  Set diagnostics period

WS5100#service diag enable
```

```
WS5100#service diag led ?
  1  1 - upper LED
  2  2 - lower LED

WS5100#service diag led 1 ?
  amber  amber
  blue   blue
  red    red

WS5100#service diag led 1 amber ?
  flashing  LED Flashing
  off       LED off
  on        LED on

WS5100#service diag led 1 amber flashing
WS5100#service diag led 1 amber flashing
WS5100#service diag led 1 blue on
WS5100#service diag led 1 red off
WS5100#service diag led 2 amber flashing

WS5100#service diag limit ?
  buffer       buffer usage warning limit
  fan          Fan speed limit
  filesys      file system freespace limit
  load         agregate processor load
  maxFDs       maximum number of file descriptors
  pkbuffers    packet buffer head cache
  procRAM      percent RAM used by a process
  ram          percent free RAM
  routecache   IP route cache usage
  temperature  temperature limit
WS5100#service diag limit buffer ?
  128   128 byte buffer limit
  128k  128k byte buffer limit
  16k   16k byte buffer limit
  1k    1k byte buffer limit
  256   256 byte buffer limit
  2k    2k byte buffer limit
  32    32 byte buffer limit
  32k   32k byte buffer limit
  4k    4k byte buffer limit
  512   512 byte buffer limit
  64    64 byte buffer limit
  64k   64k byte buffer limit
  8k    8k byte buffer limit
```

```
WS5100>service show command-history
WS5100>service show command-history
Configured size of command history is 200

  Date & Time          User  Location   Command
=========================================================================
==
May 31 21:57:44 2007   admin     vty 130     exit
May 31 20:30:11 2007   admin     vty 130     configure terminal
May 31 20:27:08 2007   admin     vty 130     enable
May 31 20:18:03 2007   admin     vty 130     exit
May 31 20:17:32 2007   admin     vty 130     configure terminal
May 31 20:17:26 2007   admin     vty 130     enable
May 31 18:32:42 2007   admin     con 0     ip address 10.10.10.2/24
May 31 18:32:29 2007   admin     con 0     interface vlan 1
May 31 18:31:48 2007   admin     con 0     configure terminal
May 31 18:31:45 2007   admin     con 0     enable
May 29 15:40:04 2007   admin     vty 131     enable
May 29 15:23:43 2007   admin     con 0     exit
May 29 15:23:36 2007   admin     con 0     ip address 10.10.10.2/24
May 29 15:23:19 2007   admin     con 0     exit
May 29 15:23:19 2007   admin     con 0     exit
May 29 15:23:03 2007   admin     con 0     interface vlan 1
May 29 15:22:48 2007   admin     con 0     configure terminal
May 29 15:22:45 2007   admin     con 0     enable
May 25 21:32:27 2007   admin     vty 131     configure terminal
May 25 21:32:21 2007   admin     vty 131     enable
May 24 18:34:36 2007   admin     vty 131     configure terminal
May 24 18:34:21 2007   admin     vty 131     enable
May 23 19:07:35 2007   admin     vty 131     configure  terminal
May 23 19:06:59 2007   admin     vty 131     enable
May 23 14:36:09 2007   admin     vty 130     enable
May 21 16:37:13 2007   admin     vty 130     enable
May 21 16:34:36 2007   admin     con 0     enable

WS5100>service show reboot-history
Configured size of reboot history is 50

  Date & Time             Event
=====================================================
May 31 18:29:42 2007     startup
- - -                   shutdown (ungraceful:unexpected cold
restart)
May 31 15:42:23 2007     startup
- - -                   shutdown (ungraceful:unexpected cold
restart)
May 31 12:35:18 2007     startup
```

```
- - -                    shutdown (ungraceful:unexpected cold
restart)
May 30 17:15:13 2007     startup
- - -                    shutdown (ungraceful:unexpected cold
restart)
May 29 15:10:51 2007     startup
- - -                    shutdown (ungraceful:unexpected cold
restart)
May 28 20:06:31 2007     startup
- - -                    shutdown (ungraceful:unexpected cold
restart)
May 25 14:21:35 2007     startup
- - -                    shutdown (ungraceful:unexpected cold
restart)
May 24 14:20:09 2007     startup
- - -                    shutdown (ungraceful:unexpected cold
restart)
May 23 14:07:21 2007     startup
- - -                    shutdown (ungraceful:unexpected cold
```

2.2 show

▸ *Common Commands*

Displays the settings for the specified system component. There are a number of ways to invoke the show command:

- When invoked without any arguments, it displays information about the current context. If the current context contains instances, the show command (usually) displays a list of these instances
- When invoked with the display_parameter, it displays information about that component

Syntax

```
show [display_parameter]
```

Parameters

Display Parameters	Description	Mode	Example
autoinstall	Displays the autoinstall configuration	Common	page 27
banner	Displays the message of the day login banner	Common	page 27
commands	Displays command lists	Common	page 28
crypto	Displays current encryption details	Common	page 29
environment	Displays environmental information	Common	page 32
history	Displays the session command history	Common	page 32
interfaces	Displays the current interface status and configuration	Common	page 32
ip	Displays the internet protocol	Common	page 34
ldap	Displays LDAP server configuration parameters	Common	page 40
licenses	Displays the installed licenses, if any	Common	page 41
logging	Displays the logging configuration and buffer	Common	page 41
mac	Displays the media access control IP configuration	Common	page 42
mac-address-table	Displays the MAC address table	Common	page 42
management	Displays L3 management interface name	Common	page 43
mobility	Displays mobility parameters	Common	page 43
ntp	Displays network time protocol information	Common	page 46
port-channel	Displays port channel commands	Common	page 47
privilege	Displays the current privilege level	Common	page 47

Display Parameters	***Description***	***Mode***	***Example***
radius	Displays RADIUS configuration commands	Common	*page 48*
redundancy-group	Displays redundancy group parameters	Common	*page 49*
redundancy-history	Displays the state transition history of the switch	Common	*page 51*
redundancy-members	Displays redundancy group members in detail	Common	*page 52*
snmp	Displays SNMP engine parameters	Common	*page 52*
snmp-server	Displays SNMP engine parameters	Common	*page 53*
sole	Displays the *Smart Opportunistic Location Engine* (SOLE) configuration	Common	*page 55*
spanning-tree	Displays the spanning tree information	Common	*page 57*
static-channel-group	Displays static channel group membership information	Common	*page 58*
terminal	Displays terminal configuration parameters	Common	*page 59*
timezone	Displays the timezone.	Common	*page 59*
users	Displays information about terminal lines	Common	*page 60*
version	Displays software and hardware version information	Common	*page 60*
wireless	Displays wireless configuration commands	Common	*page 62*
wlan-acl	Displays WLAN ACL information	Common	*page 70*

Display Parameters	***Description***	***Mode***	***Example***
access-list	Displays the access list *Internet Protocol* (IP) configuration	Privilege /Global Config	*page 71*
aclstats	Displays ACL statistics	Privilege /Global Config	*page 72*
alarm-log	Displays all the alarms currently in the system	Privilege /Global Config	*page 72*
boot	Displays the boot configuration	Privilege /Global Config	*page 73*
clock	Displays the system clock	Privilege /Global Config	*page 73*
debugging	Displays the current debugging settings	Privilege /Global Config	*page 74*
dhcp	Displays DHCP server configurations	Privilege /Global Config	*page 74*
file	Displays filesystem information.	Privilege /Global Config	*page 75*
ftp	Displays the FTP server configuration	Privilege /Global Config	*page 75*
password-encryption	Displays password encryption data	Privilege /Global Config	*page 76*

Display Parameters	*Description*	*Mode*	*Example*
running-config	Displays the current operating configuration	Privilege /Global Config	*page 76*
securitymgr	Displays debug information for ACL, VPN and NAT	Privilege /Global Config	*page 80*
sessions	Displays currently open and active connections	Privilege /Global Config	*page 80*
startup-config	Displays the content of the startup configuration	Privilege /Global Config	*page 80*
upgrade-status	Displays the status of the last image upgrade	Privilege /Global Config	*page 82*

2.2.1 autoinstall

▸ *Common to all modes*

Syntax

```
show autoinstall
```

Parameters

None

Example

```
WS5100>show autoinstall
WS5100>
```

2.2.2 banner

▸ *Common to all modes*

Syntax

```
show banner
```

Parameters

motd	Defines the *Message of the Day* banner

Example

```
WS5100>show banner motd
Welcome to CLI
WS5100>
```

2.2.3 commands

- *Common to all modes*

Syntax

```
WS5100>show commands
```

Parameters

None

Example

```
WS5100#show commands
  acknowledge alarm-log (all|<1-65535>)
  acknowledge alarm-log (all|<1-65535>)
  archive tar /create (FILE|URL) .FILE
  archive tar /create (FILE|URL) .FILE
  archive tar /table (FILE|URL)
  archive tar /table (FILE|URL)
  archive tar /xtract (FILE|URL) DIR
  archive tar /xtract (FILE|URL) DIR
  cd (DIR|)
  cd (DIR|)
  change-passwd
  clear aclstats
  clear alarm-log (new|all|acknowledged|<1-65535>)
  clear alarm-log (new|all|acknowledged|<1-65535>)
  clear alarm-log (new|all|acknowledged|<1-65535>)
  clear alarm-log (new|all|acknowledged|<1-65535>)
  clear arp-cache
  clear crypto ipsec sa (A.B.C.D |)
  clear crypto ipsec sa (A.B.C.D |)
  clear crypto isakmp sa ( A.B.C.D |)
  clear crypto isakmp sa ( A.B.C.D |)
  clear ip dhcp binding (*|A.B.C.D)
.................................................(contd)
WS5100#
```

2.2.4 crypto

- *Common to all modes*

Syntax

```
show crypto(ipsec|isakmp|key|map|pki)

show crypto ipsec(sa|security-association(lifetime)|transformset)
show crypto isakmp(policy(<1-10000>)|sa)
show crypto key(mypubkey)
show crypto map(interface|tag)
show crypto pki(request|trustpoints)
```

Parameters

ipsec [sa|securityassociation (lifetime)|transformset (name)]	Displays the IPSEC policy • sa – IPSec security association • security-association – Security association • lifetime – Defines the lifetime • transformset – Transformset • name – Defines the transform set name or all transform sets
isakmp [policy <1-10000>|sa]	Displays ISAKMP policies • policy <1-10000> – Displays the priority allthe isakmp policies • sa – All crypto ISAKMP security associations
key (mypubkey) (rsa)	Displays authentication key management • mypubkey – Shows the public keys assoicated with the switch • rsa – Displays the RSA public keys
map [interface|tag] (name)	Displays crypto maps • interface (name) – Sets crypto maps for an interface • tag (name) – Sets crypto maps with a given tag
pki [request|trustpoints] (name)	Displays Public Key Infrastructure (PKI) commands • request (name) – Displays the certificate requests • trustpoints (name) – Displays the trustpoints and their configuration

Usage Guidelines

The security engine periodically updates the IPSec and Isakamp statistics (every 60 seconds)

Example

```
WS5100(config)#show crypto pki request tptest
-----BEGIN CERTIFICATE REQUEST-----
MIIB2zCCAUQCAQAwaDELMAkGA1UEBhMCaW4xEjAQBgNVBAgTCWthcm5hdGFrYTES
MBAGA1UEBxMJYmFuZ2Fsb3JlMQ8wDQYDVQQKEwZzeW1ib2wxDDAKBgNVBAsTA3dp
ZDESMBAGA1UEAxMJdGVzdC1jZXJ0MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKB
gQC3qisZdTn7rKzv5TrGtKt7fwMwaYpgehyl52I4fDLZYY/WTTTJFyKwW6s+Pq2R
mM9oiqX8mCZeSEIJIATpAVT2M5Ukb4Br9YQDcWHs84oXRJxKPeZ3WscBld2soPvK
ui1LoizZH9iqawmkXED1TFMBbDWiOcfnqQKn8Tddeax/JQIDAQABoDMwMQYJKoZI
hvcNAQkOMSQwIjALBgNVHQ8EBAMCBLAwEwYDVR0lBAwwCgYIKwYBBQUHAwEwDQYJ
KoZIhvcNAQEEBQADgYEAoJMylm3aaY1CnkOO5TbxB+qL4F4MKL6+o/m0yRPqy/2S
gkk/OwxHvc3TbA9WjbKkFWIDyqU7X0d+c8f9KogwxDwWHll2IBiTCtBAq6hpgKOv
Um9GFvMFps9XVkKtYttN3fer9tA+6xY9CKlr12mNGOYFHyVjMc3Pic0ODFiPHAU=
-----END CERTIFICATE REQUEST-----

WS5100(config)#show crypto pki trustpoints

Trustpoint :default-trustpoint
------------------------------------------------
  Server certificate configured
    Subject Name:
      Common Name:          Symbol Technologies
    Issuer Name:
      Common Name:          Symbol Technologies
  Valid From:   Sep 13 16:14:49 2006 GMT
  Valid Until:  Sep 13 16:14:49 2007 GMT

Trustpoint :tptest
------------------------------------------------
  CA certificate configured
    Subject Name:
      Common Name:          monarch
      Organizational Unit: wid
      Organization:         symbol
      Location:             bangalore
      State:                karnataka
      Country:              in
      email:                testuser@domain.com
    Issuer Name:
      Common Name:          monarch
      Organizational Unit: wid
      Organization:         symbol
      Location:             bangalore
      State:                karnataka
      Country:              in
      email:                testuser@domain.com
  Valid From:   Sep 11 05:48:52 2006 GMT
  Valid Until:  Sep 11 05:48:52 2007 GMT
```

2.2.5 environment

- *Common to all modes*

Syntax

```
show environment
```

Parameters

None

Example

```
WS5100>show environment
       CPU temperature :  33.0 C
       system temperature :  33.0 C
       CPU fan         :  4354 rpm
       case fan         :  8766 rpm
WS5100>
```

2.2.6 history

- *Common to all modes*

Syntax

```
show history
```

Parameters

None

Example

```
WS5100>show history
   1 show
   2 clrscr
   3 enable
   4 clrscr
   5 configure terminal
   6 exit
   7 clrscr
   8 show history
WS5100>
```

2.2.7 interfaces

- *Common to all modes*

Syntax

```
show interfaces(IFNAME|eth <1-2>|switchport|vlan)
```

Parameters

IFNAME	Displays the interface name
eth	Displays ethernet interface information
switchport	Displays native VLAN(s) and allowed VLAN information on switch ports
vlan	Displays VLAN interface details

Usage Guidelines

Use the `show interface` command to display the administrative and operational status of all the interfaces or a specified interface

Example

```
WS5100#show interfaces eth 1
Interface eth1
  Hardware Type Ethernet, Interface Mode Layer 2, address is 00-a0-
f8-65-ea-8e
  index=2001, metric=1, mtu=1500, (HAL-IF)
<UP,BROADCAST,RUNNING,MULTICAST>
  Speed: Admin Auto, Operational 10M, Maximum 1G
  Duplex: Admin Auto, Operational Half
  Switchport Settings: Mode: Access, Access Vlan: 2100
    input packets 0, bytes 0, dropped 0, multicast packets 0
    input errors 0, length 0, overrun 0, CRC 0, frame 0, fifo 0,
missed 0
    output packets 0, bytes 0, dropped 0
    output errors 0, aborted 0, carrier 0, fifo 0, heartbeat 0,
window 0
WS5100#

WS5100(config)#show interfaces switchport eth1
Interface eth1
  Switchport Settings: Mode: Access, Access Vlan: 2100

WS5100(config)#show interfaces switchport vlan1
Interface vlan1
  Switchport Settings: Mode: Access, Access Vlan: 0
```

2.2.8 ip

- *Common to all modes*

Syntax

```
show ip (access-group (IFNAME | eth <1-2> | vlan <1-4094>) | arp |
ddns(binding)|dhcp(binding|class|pool|sharednetwork)|
dhcp-vendor-options | domain-name | http(secure-server|server)|
interface(IFNAME|brief|vlan) | name-server |
route(A.B.C.D|A.B.C.D/M|detail) | routing | ssh | telnet )

show ip access-group (IFNAME|eth <1-2> |vlan <1-4094>)
Show ip access-group <interface-name>

show ip arp

show ip ddns(binding)

show ip dhcp(binding|class|pool|sharednetwork)

show ip dhcp-vendor-options

show ip domain-name

show ip http(secure-server|server)

show ip interface(IFNAME|brief|eth|vlan)

show ip name-server

show ip route(A.B.C.D|<IP-prefix-len>|detail)

show ip routing

show ip ssh

show ip telnet
```

Parameters

access-group	Displays the ACLs attached to an interface • IFNAME – Enter the name of the interface to which the ACL is associated. access-group lists the details of the ACLs configured on the particular Layer 3 or Layer 2 interface • eth – Enter the name of the ethernet interface to which the ACL is associated • vlan – Enter the name of the VLAN interface to which the ACL is associated
arp	Displays existing entries in the *Address Resolution Protocol* (ARP) table
ddns	Displays the DDNS configuration • binding – DNS address bindings
dhcp	Displays the DHCP server configuration • binding – DNS address bindings • class – Configures the DHCP Server class • pool – DHCP Pool designation • sharednetwork – Shared network information
dhcp-vendor-options	DHCP Option 43 parameters received from DHCP server
domain-name	Displays domain name information
http	*Hyper Text Transfer Protocol* (HTTP) • secure-server – Secure HTTP server • server – HTTP server

interface	Use the show ip interface command to display the administrative and operational status of all Layer-3 interfaces or a specified Layer-3 interface • IF NAME – Interface name. • brief – Brief summary of the IP status and its configuration • eth – Ethernet interface. • vlan – VLAN Interface
name-server	Displays static and dynamic name-server entries
route	Display IP routing table entries • A.B.C.D – Network in the IP routing table • A.B.C.D/M – Number of valid bits in the network prefix IP prefix <network>/<length>, e.g., 35.0.0.0/8 • detail – IP routing table in detail
routing	IP routing status
ssh	*Secured Shell* (SSH) server
telnet	Telnet server

Usage Guidelines

1. The interface and VLAN status is displayed as UP regardless of a disconnection. In such a case, shutdown the VLAN. Follow the steps below:

   a. Check the status of an interface and VLAN using:

```
WS5100(config)#show ip interface brief
Interface          IP-Address         Status            Protocol
vlan1               157.235.208.69(DHCP)   up                up
vlan3               unassigned           up                up
WS5100(config)#
```

   b. If the stauts of the VLAN is UP (even if eth1/eth2 is diconnected), shutdown the VLAN associated with eth1 using:

```
WS5100(config-if)#show ip interface vlan 3 brief
Interface          IP-Address         Status            Protocol
```

```
vlan3                unassigned            up                    up
WS5100(config-if)#shutdown
```

c. Check the stauts. Note that the VLAN has now been disassociated and the status is DOWN.

```
WS5100(config)#show ip interface brief
Interface          IP-Address          Status             Protocol
vlan1               157.235.208.69(DHCP)   up                  up
vlan3              unassigned           administratively down down
WS5100(config)#
```

2. The above example could also occur when a DHCP interface is disconnected. DHCP is not effected though, because it runs on a virtual interface and not on a physical interface. In this case, it is the physical interface that is disconnected not the virtual interface. When the ethernet interface comes back up, it will restart the dDHCP client on any virtual interfaces (SVIs) of which the physical interface is a member port. This ensures if the interface was disconnected and reconnected to a different interface it will obtain a new IP address, route, name server, domain name etc. corresponding to the new DHCP server configuration.

Example

```
WS5100(config)#show ip access-group eth 1
Interface eth1
  Inbound IP Access List :
  Inbound MAC Access List :
WS5100(config)#show ip access-group vlan 1
Interface vlan1
  Inbound IP Access List :
WS5100(config)#show ip access-group eth2
Interface eth2
  Inbound IP Access List :
  Inbound MAC Access List :

WS5100#show ip dhcp binding
IP              MAC/Client-Id      Type       Expiry Time
--              -------------      ----       -----------

WS5100(config)#show ip dhcp class
!
ip dhcp class TestClass2
 option user-class MC900
!
ip dhcp class BlahBlahBlah
!
ip dhcp class ClassNameTest
```

```
 option user-class UserClassTest
!
ip dhcp class TestDHCPclass
!
ip dhcp class Add-DHCP-class1
!
ip dhcp class MonarchDHCPclas
 option user-class MC9000
!
ip dhcp class WS5100DHCPclass
 option user-class MC800
WS5100(config)#
WS5100#show ip dhcp pool
!
ip dhcp pool pl
!
ip dhcp pool pool1
 domain-name test.com
 bootfile 123
 network 10.10.10.0/24
 address range 10.10.10.2 10.10.10.30
!
ip dhcp pool poo110
 next-server 1.1.1.1
 netbios-node-type b-node

WS5100#show ip dhcp-vendor-options
Server Info:
Firmware Image File:
Config File:
Cluster Config File:

WS5100#show ip domain-name
 IP domain-lookup : Enable
 Domain Name   : symbol.com
WS5100#show ip http server
HTTP server: Running
Config status: Enabled


WS5100#show ip http secure-server
HTTP secure server: Running
Config status: Enabled
Trustpoint: default-trustpoint

WS5100#show ip interface brief
Interface     IP-Address        Status     Protocol
vlan1         157.235.208.233   (DHCP)up   up
tunnel1       unassigned        up         up
```

```
WS5100#show ip interface tunnel 1 ?
  brief  Brief summary of IP status and configuration

WS5100#show ip interface tunnel 1 brief
Interface     IP-Address        Status      Protocol
tunnel1       unassigned        up          up

WS5100#show ip interface vlan 1 brief
Interface     IP-Address        Status      Protocol
vlan1         157.235.208.233   (DHCP)up    up

WS5100#show ip name-server
157.235.3.195            dynamic
157.235.3.196            dynamic

WS5100#show ip routing
IP routing is on

WS5100(config)#show ip route detail
Codes: K - kernel/icmp, C - connected, S - static, D - DHCP
       > - Active route,  - Next-hop in FIB, p - stale info

S       1.1.0.0/16 [1/0] via 1.1.1.1 inactive
S       1.1.1.0/24 [1/0] via 1.1.1.2 inactive
S       10.0.0.0/8 [1/0] via 10.10.10.10 inactive
S       157.235.208.0/24 [1/0] via 157.235.208.246 inactive

WS5100#show ip ssh
SSH server: enabled
Status: running
Keypair name: default_ssh_rsa_key
Port: 22

WS5100#show ip telnet
Telnet server: enabled
Status: running
Port: 23
```

2.2.9 ldap

- *Common to all modes*

Syntax

```
show ldap(configuration(primary|secondary))
```

Parameters

ldap	Defines the LDAP server
configuration	Sets the LDAP server
primary	Defines the Primary LDAP server
secondary	Defines the Secondary LDAP server

Example

```
WS5100(config-radsrv)#show ldap configuration
LDAP Server Config Details

_____________________________

Primary LDAP Server configuration

        IP Address              : 10.10.10.1
        Port                    : 369
        Login                   :
(sAMAccountName=%{Stripped-User-Name:-%{User-Name}})
        Bind DN                 :
cn=kumar,ou=symbol,dc=activedirectory,dc=com
        Base DN                 :
ou=symbol,dc=activedirectory,dc=com
        Password                : 0 symbol@123
        Password Attribute      : UserPassword
        Group Name              : cn
        Group Membership Filter:
(&(objectClass=group)(member=%{Ldap-UserDn}))
        Group Member Attr       : radiusGroupName
        Net timeout             : 1 second(s)

Secondary LDAP

        IP Address              : 10.10.10.5
        Port                    : 369
        Login                   :
(sAMAccountName=%{Stripped-User-Name:-%{User-Name}})
```

```
        Bind DN                 :
cn=kumar,ou=symbol,dc=activedirectory,dc=com
        Base DN                 :
ou=symbol,dc=activedirectory,dc=com
        Password                : 0 symbol@123
        Password Attribute      : UserPassword
        Group Name              : cn
        Group Membership Filter:
(&(objectClass=group)(member=%{Ldap-UserDn}))
        Group Member Attr       : radiusGroupName
        Net timeout             : 1 second(s)
```

2.2.10 licenses

- *Common to all modes*

Syntax

```
show licenses
```

Parameters

None

Example

```
WS5100(config)#show licenses
feature usage  license string              license value    usage
AP             2FFD7fE9 CD016155 14A92C70  48               1
```

2.2.11 logging

- *Common to all modes*

Syntax

```
show logging
```

Parameters

None

Example

```
WS5100(config)#show logging

Logging module: enabled
    Aggregation time: disabled
    Console logging: level debugging
    Buffered logging: level informational
    Syslog logging: level debugging
        Facility: local7
        Logging to: 157.235.203.37
```

```
        Logging to: 10.0.0.2

Log Buffer (6520 bytes):

Sep 14 19:11:59 2006: %DAEMON-6-INFO: radiusd[4643]: Ready to
process requests.

Sep 14 19:11:58 2006: %PM-5-PROCSTOP: Process "radiusd" has been
stopped

Sep 14 18:51:14 2006: %CC-5-RADIOADOPTED: 11a radio on AP 00-A0-F8-
BF-8A-A2 adopted

Sep 14 18:51:14 2006: %CC-5-RADIOADOPTED: 11bg radio on AP 00-A0-
F8-BF-8A-A2 adopted
```

2.2.12 mac

- *Common to all modes*

Syntax

`show mac(access-list)`

Parameters

access-list	Displays existing MAC access lists

Example

```
WS5100(config)#show mac access-list
WS5100(config)#
```

2.2.13 mac-address-table

- *Common to all modes*

Syntax

`show mac-address-table`

Parameters

None

Example

```
WS5100(config)#show mac-address-table
WS5100(config)#
```

2.2.14 management

- *Common to all modes*

Syntax

```
show management
```

Parameters

None

Example

```
WS5100>show management
Mgmt Interface: vlan1
Management access permitted via any vlan interface
WS5100>
```

2.2.15 mobility

- *Common to all modes*

Syntax

```
show mobility [event-log|forwarding|global|mobile-
unit|peer|statistics]
show mobility event-log [mobile-unit|peer]
show mobility forwarding (AA-BB-CC-DD-EE-FF)
show mobility mobile-unit [<AA-BB-CC-DD-EE-FF>|detail]
show mobility peer [<A.B.C.D>|detail]
show mobility statistics <AA-BB-CC-DD-EE-FF>
```

Parameters

event-log	Displays the mobility event logs • mobile-unit – MU event logs • peer – Peer event logs
forwarding	Displays and defines Mobile units in the forwarding plane • AA-BB-CC-DD-EE-FF – MAC address of the mobile unit
global	Displays and defines global mobility parameters
mobile-unit	Mobile units in the mobility database • AA-BB-CC-DD-EE-FF – MAC address of the mobile unit • detail – Displays detailed information
peer	Mobility peers • A.B.C.D – IP address of Peer • detail – Displays detailed peer information
statistics	Mobility statistics. • AA-BB-CC-DD-EE-FF – MAC address of the mobile unit

Example

```
WS5100(config)#show mobility ?
  event-log    Event Log
  forwarding   Mobile-unit information in the forwarding plane
  global       Global Mobility parameters
  mobile-unit  Mobile-units in the Mobility Database
  peer         Mobility peers
  statistics   Mobile-unit Statistics

WS5100(config)#show mobility event-log mobile-unit
Time             Event        Evt-Src-IP      MU-Mac             MU-
IP
HS-IP            CS-IP
09/14 19:17:52  IP-UPD-MU    n/a             00-0f-3d-e9-a6-54
157.235.208.134 157.235.208.16  157.235.208.16
09/14 19:17:51  ADD-MU       n/a             00-0f-3d-e9-a6-54
0.0.0.0
157.235.208.16  157.235.208.16
09/14 19:17:51  DEL-MU       n/a             00-0f-3d-e9-a6-54
0.0.0.0
```

```
157.235.208.16  157.235.208.16
09/14 19:17:50  ADD-MU       n/a             00-0f-3d-e9-a6-54
0.0.0.0
157.235.208.16  157.235.208.16
```

WS5100>show mobility forwarding

```
Mobility Forwarding-plane Information
  State: HS : Home-switch        CS : Current-switch
         !HS: Not Home-switch    !CS: Not Current-switch
Mac-Address        IP-Address      State   HS-Vlan    Tunnel
WS5100>
```

WS5100>show mobility global

```
Mobility Global Parameters
Admin Status                      : DISABLED
Operational-Status                : DISABLED (Admin-status is
DISABLED)
Local Address                     : 10.10.10.2 (mgmt-vlan)
Port Number                       : 58788
Max Roam Period                   : 5 sec
Number of Peers                   : 0 (established=0)
Number of MUs                     : 0 (Home=0, Foreign=0, Delete-
pend=0)
L3-Mobility enabled WLANs         : NONE
WS5100>
```

WS5100(config)#show mobility mobile-unit detail

```
HOME MU Database: Total=1
MU MAC-Address: 00-0f-3d-e9-a6-54, IP-Address: 157.235.208.134,
SSID=wios_rad_test1
  Home-Switch: 157.235.208.16, Current-Switch: 157.235.208.16, HS-
VLAN=1
Foreign MU Database: Total=0
```

WS5100(config)#show mobility peer detail

```
Mobility Peers: Total=1, Established=0
Peer: 1.1.1.1, State: PASSIVE-CONNECTING
  Join-Sent  : 0      Join-Rcvd  : 0      Leave-Sent : 0
Leave-Rcvd : 0
  Rehome-Sent: 0      Rehome-Rcvd: 0      L3roam-Sent: 0
L3roam-Rcvd: 0
  Num-flaps  : 0      Connect-retries: 0    Peer-Uptime: 0 days,
00:00:00
```

```
WS5100(config)#show mobility statistics

MU <00-0f-3d-e9-a6-54> Mob-State HS_AND_CS
-----------------------------------------------
Inter-          |Rx                                          |Tx
face            |unicast    MC         BC         Error
|unicast    MC
BC         Error
wlan_port       0          0          0          0          0
0
0          0
```

2.2.16 ntp

- *Common to all modes*

Syntax

```
show ntp (association (detail)|status)
```

Parameters

ntp	Displays the *Network Time Protocol* (NTP) configuration
association	Displays existing NTP associations
detail	Displays NTP association details
status	Displays NTP status

Example

```
WS5100>show ntp associations
  address         ref clock       st  when  poll  reach  delay
offset    disp
 * master (synced), # master (unsynced), + selected, - candidate, ~
configured
WS5100>

WS5100>show ntp status
Clock is synchronized, stratum 0, actual frequency is 0.0000 Hz,
precision is 2**0
reference time is 00000000.00000000 (Feb 07 06:28:16 UTC 2036)
clock offset is 0.000 msec, root delay is 0.000 msec
root dispersion is 0.000 msec,
WS5100>
```

```
WS5100(config)#show ntp associations detail
157.235.208.105 configured, sane, valid, leap_sub, stratum 16
ref ID INIT, time 00000000.00000000 (Feb 07 06:28:16 UTC 2036)
our mode client, peer mode unspec, our poll intvl 6, peer poll
intvl 10
root delay 0.00 msec, root disp 0.00, reach 000,
delay 0.00 msec, offset 0.0000 msec, dispersion 0.00
precision 2**-20,
org time 00000000.00000000 (Feb 07 06:28:16 UTC 2036)
rcv time 00000000.00000000 (Feb 07 06:28:16 UTC 2036)
xmt time c8b42a7e.6eb04252 (Sep 14 19:22:38 UTC 2006)
filtdelay =  0.00  0.00  0.00  0.00  0.00  0.00  0.00  0.00

WS5100>show ntp status
Clock is synchronized, stratum 0, actual frequency is 0.0000 Hz,
precision is 2^0
reference time is 00000000.00000000 (Feb 07 06:28:16 UTC 2036)
clock offset is 0.000 msec, root delay is 0.000 msec
root dispersion is 0.000 msec,
WS5100>
```

2.2.17 port-channel

- *Common to all modes*

Syntax

```
show port-channel (load-balance)
```

Parameters

load-balance	Displays the existing load balancing configuration

Example

```
WS5100>show port-channel load-balance
WS5100>
```

2.2.18 privilege

- *Common to all modes*

Syntax

```
show privilege
```

Parameters

None

Example

```
WS5100>show privilege
Current user privilege: superuser
WS5100>
```

2.2.19 radius

- *Common to all modes*

Syntax

```
show radius (configuration | eap (configuration)| group | nas (
A.B.C.D/M)| proxy | rad-user | trust-point)
```

Parameters

radius	Displays RADIUS configuration commands
configuration	RADIUS server configuration parameters
eap (configuration)	Displays and defines the EAP configuration
group	Displays the RADIUS group configuration
nas (A.B.C.D/M)	Defines a client IP address and mask
proxy	Lists proxy information
rad-user	Displays RADIUS user information
trust-point	Defines the RADIUS trust-point configuration

Example

```
WS5100(config)#show radius proxy
Proxy Details

_______________
Proxy retry delay : 6  seconds
Proxy retry count : 4

Proxy Realm Details

_____________________
Realm   : symbol.com
        IP Address    : 10.10.10.5
        Port          : 1812
        Shared secret : 0 secret123
```

2.2.20 redundancy-group

- *Common to all modes*

This command displays the switch's IP address, number of active neighbors, group license, installed license, cluster AP adoption count, switch adoption count, hold time, discovery time, heartbeat interval, cluster id and switch mode.

In a cluster, this command displays the redundancy runtime and configuration of the "self-switch". Use `config` to view only configuration information and/or `runtime` parameters.

Syntax

```
show redundancy-group (config | runtime)
```

Parameters

config	Displays configured redundancy group information
runtime	Displays runtime redundancy group information

Example

```
WS5100(config)#show redundancy-group

Redundancy Group Configuration Detail
Redundancy Feature                  : Disabled
Redundancy group ID                 : 1
Redundancy Mode                     : Primary
Redundancy Interface IP             : 0.0.0.0
Number of configured peer(s)        : 0
Heartbeat-period                    : 5 Seconds
Hold-period                         : 15 Seconds
Discovery-period                    : 30 Seconds
Handle STP                          : Disabled
Switch Installed License            : 48
Switch running image version        : 3.1.0.0-008D
Auto-revert-period                  : 5 mins
Auto-revert Feature                 : Disabled
DHCP-Server Redundancy              : Disabled

Redundancy Group Runtime Information
Redundancy Protocol Version          : 2.0
Redundancy Group License             : 0
Cluster AP Adoption Count            : Not Applicable
Switch AP Adoption Count             : Not Applicable
Redundancy State                     : Disabled
```

```
Radio Portals adopted by Group       : Not Applicable
Radio Portals adopted by this Switch : Not Applicable
Rogue APs detected in this Group     : Not Applicable
Rogue APs detected by this Switch    : Not Applicable
MUs associated in this Group         : Not Applicable
MUs associated in this Switch        : Not Applicable
Selfhealing RPs in this Group        : Not Applicable
Selfhealing APs in this Switch       : Not Applicable
Group maximum AP adoption capacity   : Not Applicable
Switch Adoption capacity             : Not Applicable
Established Peer(s) Count            : Not Applicable
Redundancy Group Connectivity status : Not Applicable
DHCP Server in group                 : Not Applicable

WS5100(config)#
```

```
WS5100(config)#show redundancy-group config

Redundancy Group Configuration Detail
Redundancy Feature                 : Disabled
Redundancy group ID                : 1
Redundancy Mode                    : Primary
Redundancy Interface IP            : 0.0.0.0
Number of configured peer(s)       : 0
Heartbeat-period                   : 5 Seconds
Hold-period                        : 15 Seconds
Discovery-period                   : 30 Seconds
Handle STP                         : Disabled
Switch Installed License           : 48
Switch running image version       : 3.1.0.0-008D
Auto-revert-period                 : 5 mins
Auto-revert Feature                : Disabled
DHCP-Server Redundancy             : Disabled

WS5100(config)#
```

```
WS5100(config)#show redundancy-group runtime

Redundancy Group Runtime Information
Redundancy Protocol Version          : 2.0
Redundancy Group License             : 0
Cluster AP Adoption Count            : Not Applicable
Switch AP Adoption Count             : Not Applicable
Redundancy State                     : Disabled
Radio Portals adopted by Group       : Not Applicable
Radio Portals adopted by this Switch : Not Applicable
Rogue APs detected in this Group     : Not Applicable
Rogue APs detected by this Switch    : Not Applicable
```

```
MUs associated in this Group         : Not Applicable
MUs associated in this Switch        : Not Applicable
Selfhealing RPs in this Group        : Not Applicable
Selfhealing APs in this Switch       : Not Applicable
Group maximum AP adoption capacity   : Not Applicable
Switch Adoption capacity             : Not Applicable
Established Peer(s) Count            : Not Applicable
Redundancy Group Connectivity status : Not Applicable
DHCP Server in group                 : Not Applicable

WS5100(config)#
```

2.2.21 redundancy-history

- *Common to all modes*

Displays the switch state transition history

Syntax

```
show redundancy-history
```

Parameters

None

Example

```
WS5100>show redundancy-history
State Transition History

Time                   Event Triggered         state
------------------------------------------------------------
Sat Oct 06 12:07:55    Redundancy Enabled      Startup
Sat Oct 06 12.07.56    Startup Done            Discovery
Sat Oct 06 12:08:26    Discovery Done          Active
Sat Oct 06 22:10:10    Redundancy Disabled     Startup

WS5100>show
```

2.2.22 redundancy-members

- *Common to all modes*

Displays the member switches in the cluster. The user can provide the `IP address` of the switch in cluster whose information alone is needed.

Syntax

```
show redundancy-members (A.B.C.D)
```

Parameters

A.B.C.D	Displays the IP addresses of member switches

Example

```
WS5100(config)#show redundancy-members brief

Member ID (Self)              : 10.10.10.10
Member State                  : Not Applicable

Member ID                     : 10.10.10.1
Member State                  : Peer Configured
```

2.2.23 snmp

- *Common to all modes*

Syntax

```
show snmp [user(snmpmanager|snmpoperator|snmptrap)]
```

Parameters

user	Displays SNMP user information
snmpmanager	Shows SNMP manager information
snmpoperator	Shows SNMP operator information
snmptrap	Shows SNMP trap information

Example

```
WS5100>show snmp user snmpmanager
userName      access   engineId                    Authentication
Encryption
snmpmanager   rw       800001848067458b6bd7157745  MD5
DES
WS5100>

WS5100>show snmp user snmpoperator
userName      access   engineId                    Authentication
Encryption
snmpoperator  ro       800001848067458b6bd7157745  MD5
DES
WS5100>

WS5100>show snmp user snmptrap
userName      access   engineId                    Authentication
Encryption
snmptrap      rw       800001848067458b6bd7157745  MD5
DES
WS5100>
```

2.2.24 snmp-server

- *Common to all modes*

Syntax

```
show snmp-server(traps(wireless-statistics( mobile-unit | radio |
wireless-switch | wlan)))
```

Parameters

traps	Displays trap enabled flags
wireless-statistics	Displays existing wireless-stats rate traps
mobile-unit	Displays existing mobile unit rate traps
radio	Displays existing radio rate traps
wireless-switch	Displays existing wireless switch rate traps
wlan	Displays existing WLAN rate traps

Example

```
WS5100>show snmp-server traps
-------------------------------------------------------------------------
Global enable flag for Traps                                          N
-------------------------------------------------------------------------
Enable flag status for Individual Traps
-------------------------------------------------------------------------
Module Type               Trap Type                  Enabled?[Y/N]
-------------------------------------------------------------------------
snmp                      coldstart                                   N
snmp                      linkdown                                    N
snmp                      linkup                                      N
snmp                      authenticationFail                          N
nsm                       dhcpIPChanged                               N
redundancy                memberUp                                    N
redundancy                memberDown                                  N
redundancy                memberMisConfigured                         N
redundancy                adoptionExceeded                            N
redundancy                grpAuthLevelChanged                         N
misc                      lowFsSpace                                  N
misc                      processMaxRestartsReached                   N
wireless station          associated                                  N
wireless station          disassociated                               N
wireless station          deniedAssociationOnCapability               N
wireless station          deniedAssociationOnShortPream               N
wireless station          deniedAssociationOnSpectrum                 N
wireless station          deniedAssociationOnErr                      N
wireless station          deniedAssociationOnSSID                     N
wireless station          deniedAssociationOnRates                    N
wireless station          deniedAssociationOnInvalidWPAWPA2IE         N
wireless station          deniedAssociationAsPortCapacityReached      N
wireless station          tkipCounterMeasures                         N
wireless station          deniedAuthentication                        N
wireless station          radiusAuthFailed                            N
wireless radio            adopted                                     N
wireless radio            unadopted                                   N
wireless radio            detectedRadar                               N
wireless ap-detection     externalAPDetected                          N
wireless self-healing     activated                                   N
wireless ids              excessiveAuthAssociation                    N
wireless ids              excessiveProbes                             N
misc                      savedConfigModified                         N
WS5100>

WS5100>show snmp-server traps wireless-statistics mobile-unit
     pktsps-greater-than                    disabled
     tput-greater-than                      disabled
     avg-bit-speed-less-than                disabled
     avg-signal-less-than                   disabled
```

```
     nu-percent-greater-than                  disabled
     gave-up-percent-greater-than             disabled
     avg-retry-greater-than                   disabled
     undecrypt-percent-greater-than           disabled
WS5100>

WS5100>show snmp-server traps wireless-statistics radio
     pktsps-greater-than                      disabled
     tput-greater-than                        disabled
     avg-bit-speed-less-than                  disabled
     avg-signal-less-than                     disabled
     nu-percent-greater-than                  disabled
     gave-up-percent-greater-than             disabled
     avg-retry-greater-than                   disabled
     undecrypt-percent-greater-than           disabled
     num-stations-greater-than                disabled
WS5100>

WS5100>show snmp-server traps wireless-statistics wireless-switch
     pktsps-greater-than                      disabled
     tput-greater-than                        disabled
     num-stations-greater-than                disabled
WS5100>

WS5100>show snmp-server traps wireless-statistics wlan
     pktsps-greater-than                      disabled
     tput-greater-than                        disabled
     avg-bit-speed-less-than                  disabled
     avg-signal-less-than                     disabled
     nu-percent-greater-than                  disabled
     gave-up-percent-greater-than             disabled
     avg-retry-greater-than                   disabled
     undecrypt-percent-greater-than           disabled
     num-stations-greater-than                disabled
WS5100>
```

2.2.25 sole

- *Common to all modes*

Syntax

```
show sole (config|stats|status)

show sole (config|stats)(adapter)(ADAPTER NAME)
show sole (status)[adapter|engine (ADAPTER)]
```

Parameters

config (adapter) (ADAPTER NAME)	Shows the switch SOLE adapter configuration • adapter – Show the existing configuration of the SOLE adapters
stats (adapter) (ADAPTER NAME)	Displays SOLE adapter statstics • adapter – Displays SOLE adapter statstics
status [adapter|engine (ADAPTER)]	Displays the current SOLE adapter status • adapter – Displays the current SOLE adapter status • engine (ADAPTER) – Show the external location engine status for SOLE adapter.

Example

```
WS5100#show sole config adapter

SOLE Adapter
 Adapter Type: AeroScout
 Adapter Version: 2.01
 Configured Status: enabled Operational Status: enabled
 Adapter Build Time: Thu Sep 13 21:44:45 2007
WS5100#

WS5100#show sole status adapter
#     Type     Status
-----------------------------
1  AeroScout  enabled
WS5100#

WS5100#show sole stats adapter
Adapter Type: AeroScout Adapter Status: enabled
Number of messages received from engine             : 0
Number of messages sent to engine                   : 0
Number of tag reports sent to engine                : 0
Time at which last message was received from engine : -
Time at which last message was sent to engine       : -
WS5100#

WS5100#show sole status engine
Type          Engine         State
-----------------------------------------
AeroScout   0.0.0.0          Idle
WS5100#
```

2.2.26 spanning-tree

- *Common to all modes*

Syntax

```
show spanning-tree (mst)[config|
detail(interface){IF Name|eth <1-2>|vlan <1-4094>}|
instance <1-15> (interface){IF NAME|eth <1-2>|vlan <1-4094>}]
```

Parameters

config	Displays MSTP configuration information
detail(interface) {IF Name|eth <1-2>|vlan <1-4094>}	Displays detailed interface information • IF Name – Displays the interface name • eth <1-2> – Defines the Ethernet interface • vlan (1-4094> – Defines the VLAN interface
instance <1-15> (interface) {IF NAME|eth <1-2>|vlan <1-4094>}	Displays instance information • IF Name – Displays the interface name • eth <1-2> – Defines the Ethernet interface • vlan (1-4094> – Defines the VLAN interface

Example

```
WS5100(config)#show spanning-tree mst config
%
%  MSTP Configuration Information for bridge 1 :
%-----------------------------------------------------------
%  Format Id       : 0
%  Name            : My Name
%  Revision Level  : 0
%  Digest          : 0xAC36177F50283CD4B83821D8AB26DE62
%-----------------------------------------------------------
WS5100(config)#

WS5100(config)#show spanning-tree mst detail interface eth 1
% Bridge up - Spanning Tree Disabled
% CIST Root Path Cost 0 - CIST Root Port 0 - CIST Bridge Priority
32768
% Forward Delay 15 - Hello Time 2 - Max Age 20 - Max-hops 20
% 1: CIST Root Id 8000000000000000
% 1: CIST Reg Root Id 8000000000000000
% 1: CST Bridge Id 800000a0f865ea8e
% portfast bpdu-filter disabled
```

```
% portfast bpdu-guard disabled
% portfast errdisable timeout disabled
% portfast errdisable timeout interval 300 sec
% cisco interoperability not configured - Current cisco
interoperability off
%   eth1: Port 2001 - Id 87d1 - Role Disabled - State Forwarding
%   eth1: Designated External Path Cost 0 -Internal Path Cost 0
%   eth1: Configured Path Cost 2000000  - Add type Explicit ref
count 1
%   eth1: Designated Port Id 0 - CST Priority 128  -
%   eth1: CIST Root 000000a0f865ea8e
%   eth1: Regional Root 000000a0f865ea8e
%   eth1: Designated Bridge 000000a0f865ea8e
%   eth1: Message Age 0 - Max Age 0
%   eth1: CIST Hello Time 0 - Forward Delay 0
%   eth1: CIST Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0
%   eth1: Version Multiple Spanning Tree Protocol - Received None -
Send STP
%   eth1: No portfast configured - Current  portfast off
%   eth1: portfast bpdu-guard  default  - Current portfast bpdu-
guard off
%   eth1: portfast bpdu-filter default  - Current portfast bpdu-
filter off
%   eth1: no root guard configured     - Current root guard off
%   eth1: Configured Link Type point-to-point - Current  shared
%
WS5100(config)#
```

2.2.27 static-channel-group

- *Common to all modes*

Syntax

```
show static-channel-group
```

Parameters

None

Example

```
WS5100(config)#show static-channel-group
WS5100(config)#
```

2.2.28 terminal

- *Common to all modes*

Syntax

```
show terminal
```

Parameters

None

Example

```
WS5100>show terminal
Terminal Type: vt102
Length: 44     Width: 125
WS5100>
```

2.2.29 timezone

- *Common to all modes*

Syntax

```
show timezone
```

Parameters

None

Example

```
WS5100>show timezone
Timezone is Etc/UTC
WS5100>
```

2.2.30 users

- *Common to all modes*

Syntax

```
show users
```

Parameters

None

Example

```
WS5100>show users
   Line      PID   User         Uptime       Location
   0 con 0   316   admin        06:08:11     ttyS0
 130 vty 0   2308    admin       00:35:18      0
WS5100>
```

2.2.31 version

- *Common to all modes*

Syntax

```
show version (verbose)
```

Parameters

verbose	Displays software and hardware version information

Example

```
WS5100>show version
WS5100 version 3.0.2.0-003B
Copyright (c) 2006 Symbol Technologies, Inc.
Booted from primary.

Switch uptime is 0 days, 6 hours 10 minutes
CPU is Intel(R) Pentium(R) 4 CPU 2.00GHz
256208 kB of on-board RAM
ide device hda disk model Kouwell DOM capacity 501760 blocks, cache
0
WS5100>

WS5100>show version verbose
WS5100 version 3.0.2.0-003B
Copyright (c) 2006 Symbol Technologies, Inc.
Booted from primary.
```

```
Switch uptime is 0 days, 6 hours 10 minutes
CPU is Intel(R) Pentium(R) 4 CPU 2.00GHz
PCI bus 3 device 8 function 1
    Ethernet controller
    Intel Corporation
    82546EB Gigabit Ethernet Controller (Copper)
PCI bus 3 device 8 function 0
    Ethernet controller
    Intel Corporation
    82546EB Gigabit Ethernet Controller (Copper)
PCI bus 1 device 3 function 0
    PIC
    VIA Technologies, Inc.
    VPX/VPX2 I/O APIC Interrupt Controller
PCI bus 0 device 17 function 0
    ISA bridge
    VIA Technologies, Inc.
    VT8237 ISA bridge [KT600/K8T800/K8T890 South]
PCI bus 0 device 15 function 0
    IDE interface
    VIA Technologies, Inc.
    VT82C586A/B/VT82C686/A/B/VT823x/A/C PIPC Bus Master IDE
256208 kB of on-board RAM
ide device hda disk model Kouwell DOM capacity 501760 blocks, cache
0
WS5100>
```

2.2.32 wireless

- Common to all modes

Syntax

```
show wireless [(aap-version|
ap (<1-48>|<AA-BB-CC-DD-EE-FF>)|
ap-detection-config |
ap-images |
ap-unadopted |
approved-aps |
channel-power (11a (indoor | outdoor))| 11b (indoor | outdoor)| 11bg
(indoor | outdoor))|
client(exclude-list|include-list)|
config |
country-code-list|
default-ap|
hotspot-config <1-32>|
ids (filter-list)|
known (ap) (statistics)<1-256>|
mac-auth-local <1-1000> |
mesh (statistics)<-32> (detail) |
mobile-unit(<1-4096> | AA-BB-CC-DD-EE-FF | association-history| probe-
           history|radio|statistics|wlan) |
multicast-packet-limit|
phrase-to-key (wep128 | wep64)|
qos-mapping (wired-to-wireless | wireless-to-wired)|
radio ( <1-1000> | beacon-table | config ( <1-1000> |default-11a
      |default-11b | default-11bg)| monitor-table | statistics)
       <1-1000>|
regulatory (country codes)|
self-heal-config <1-1000>|
sensor (<1-48>|default-config)|
unapproved-aps |
wireless-switch-statistics (detail)|
wlan [config( <1-32> | all | enabled)| statistics <1-32>)]
```

Parameters

aap-version	Displays the minimum adaptive firmware version string
ap	Status of the adopted access port • <1-48> – Defines the index of the access port • AA-BB-CC-DD-EE-FF – Sets the MAC address of a access port
ap-detection-config	Detected AP configuration parameters
ap-images	Displays the access port images on the switch
ap-unadopted	Lists unadopted access ports
approved-aps	Dispalys approved APs detected by access port scans
channel-power	Lists the channels and power levels available for a radio • 11a – Defines the radio as 802.11a • 11b – Defines the radio as 802.11b . • 11bg – Defines the radio as 802.11bg • indoor – Radio is placed indoor • outdoor – Radio is placed outdoor
client [exclude-list|include-list]	Wireless client configuration • exclude-list – Sets the exclude list configuration • include-list – Sets the include list configuration
config	Wireless configuration parameters
country-code-list	Displays the list of supported country names and 2 letter IS0 3166 codes
default-ap	Displays default access-port information
hotspot-config <1-32>	WLAN hotspot configuration for specified index

ids	Displays intrusion detection configuration parameters • configured-bad-essids – Displays a list of bad essids. This parameter sets the number of seconds a MU is filtered • filter-list – Displays the list of currently filtered mobile units
known (ap) (statistics) <1-256>	Displays known AP parameters • ap – Defines a known AP index <1-256> • statistics – Displays known adaptive AP stats • <1-256> – Displays adaptive ap statistics for known adaptive APs between 1-256.
mac-auth-local <1-1000>	Displays mac-auth-local entries
mesh (statistics) <1-32> (detail)	Displays mesh related parameters • statistics – Dispalys mesh statistics • <1-32> – Defines the mesh index • detail – Detailed mesh statistics
mobile-unit	Displays the paramters of associated mobile units • <1-4096> – Index of mobile unit • AA-BB-CC-DD-EE-FF – MAC address of mobile unit • association-history – Displays the mobile unit history • probe-history – Displays the MU probe-history • <1-200> – Defines index to display probe-logging • config-list – Lists probe history MAC addresses • radio – Displays mobile units associated to this radio • statistics – Displays mobile unit RF statistics • wlan – Displays mobile units associated to this WLAN
multicast-packet-limit	Displays multicast-packet-limit

phrase-to-key	Displays the WEP keys generated by a passphrase • wep128 – Displays WEP128 keys • wep64 – Displays WEP64 keys
qos-mapping	Quality of service mappings used for mapping WMM access categories and 802.1p/DSCP tags • wired-to-wireless – Mappings used when traffic is switched from wired to the wireless side • wireless-to-wired – Mappings used when traffic is switched from wireless to the wired side
radio	Radio related commands • <1-1000> – Defines a single radio's index • beacon-table – Displays the radio-to-radio beacon table • config <1-1000> – Numerical index for the radio's configuration • default-11a – Default 11a configuration template • default-11b – Default 11b configuration template • default-11bg – Default 11bg configuration template • monitor-table – Displays the radio-to-radio monitoring table • statistics – Radio statistics
regulatory	Regulatory (allowed channel/power) information for a particular country
self-heal-config [*<1-1000>*|all]	Sets self healing configuration parameters • <1-1000> – Defines a single radio's index • all – Defines the self-healing configuration for all radios
sensor	Wireless Intrusion Protection System parameters • <1-48> – Specifies the index of a particular sensor to view detailed information about that sensor • default-config – Default configuration parameters for sensors

unapproved-aps	Defines unapproved APs seen by an access port or a mobile unit's scan
wireless-switch-statistics	Wireless-switch statistics • detail – Displays detailed wireless-switch statistics
wlan	Displays wireless LAN parameters
config	WLAN configuration
<1-32>	A WLAN index <1-32> • all – All WLAN in configuration • enabled – Only currently enabled WLANs • statistics – WLAN statistics • <1-32> – Defines a WLAN's index <1-32>

Example

```
WS5100>show wireless ap
Number of access-ports adopted   : 0
Available licenses               : 0
Clustering enabled               : N
Clustering mode                  : primary
WS5100>

WS5100>show wireless ap-detection-config
Rogue    AP timeout      : 300 seconds
Approved AP timeout      : 300 seconds
mu-assisted scan         : enabled
mu-assisted scan refresh : 300 seconds
configured approved-aps  :
Index | Bss Mac           | Ssid
-------------------------------------------------------

Adaptive minimum adoption version: 2.0.0.0-000R
WS5100>

WS5100>show wireless ap-images
  Idx   ap-type      Image-Name          Size (bytes)  Version
   1    ap300     WISP-AP300               293516      00.02-29
   2    ap300     WIAP-300                 244076      01.00-1635b
   3    ap300     AP300-IDS-Sensor         295064      00.00-04
   4    ap100     AP100                    31034       02.05-00
   5    ap4131    AP4131                   191440      07.00-01
```

```
   6    ap4131    Revert-AP4131           665704      00.00-00
WS5100>

WS5100>show wireless ap-unadopted
WS5100>

WS5100>show wireless approved-aps
access-port detection is disabled
WS5100>

WS5100>show wireless channel-power 11a indoor
% Error: No valid channels or power levels
WS5100>

WS5100>show wireless config
country-code            : None
adoption-pref-id        : 1
proxy-arp               : enabled
adopt-unconf-radio      : enabled
dot11-shared-key-auth   : disabled
ap-detection            : disabled
oversized-frames        : disabled
manual-wlan-mapping     : disabled
dhcp sniff state        : disabled
dhcp fix windows        : disabled
broadcast-tx-speed      : optimize-for-throughput
smart-scan 11a channels :
smart-scan 11bg channels:
WS5100>

WS5100>show wireless hotspot-config

WLAN: 1 status: disabled description: WLAN1 ssid: 101
 Page-Location: simple
 Internal Pages
  Page-type : login
   Title : Login Page
   Header : Network Login
   Description : Please enter your username and password
   Footer : Contact the network administrator if you do not have an
account
  Image URL main:
  Image URL small:

  Page-type : welcome
   Title : Authentication success.
   Header : Authentication Success.
   Description : You now have network access.<BR>Click the
disconnect link below to end this session.
```

```
   Footer :
  Image URL main:
  Image URL small:

  Page-type : fail
   Title : Unable to authenticate
   Header : Authentication Failed.
   Description : Either the username and password are invalid, or
service is unavailable at this time
   Footer : Contact the network administrator if you do not have an
account
  Image URL main:
  Image URL small:

 External Pages
  Page-Type : login
   URL :
  Page-Type : welcome
   URL :
  Page-Type : fail
   URL :
Allow-list IP addresses

WLAN: 2 status: disabled description: WLAN2 ssid: 102
 Page-Location: simple
 Internal Pages
  Page-type : login
   Title : Login Page
 -- MORE --, next page: Space, next line: Enter, quit: Control-C
.....................................................

WS5100>show wireless ids
 detect-window               : 10 seconds

 Excessive Operations::  Threshold(mu radio switch)   Filter-Ageout
  probe-requests       :       0      0      0             60 Sec
  association-requests :       0      0      0             60 Sec
  disassociations      :       0      0      0             60 Sec
  authentication-fails :       0      0      0             60 Sec
  crypto-replay-fails  :       0      0      0             60 Sec
  80211-replay-fails   :       0      0      0             60 Sec
  decryption-fails     :       0      0      0             60 Sec
  unassoc-frames       :       0      0      0             60 Sec
  eap-starts           :       0      0      0             60 Sec


 Anomaly Detection::             Status     Filter-Ageout
  probe-requests          :   disabled      60 Sec
  association-requests    :   disabled      60 Sec
```

```
  disassociations          :   disabled      60 Sec
  authentication-fails     :   disabled      60 Sec
  crypto-replay-fails      :   disabled      60 Sec
  80211-replay-fails       :   disabled      60 Sec
  decryption-fails         :   disabled      60 Sec
  unassoc-frames           :   disabled      60 Sec
  eap-starts               :   disabled      60 Sec
  null-destination         :   disabled      60 Sec
  same-source-destination  :   disabled      60 Sec
  multicast-source         :   disabled      60 Sec
  weak-wep-iv              :   disabled      60 Sec
  tkip-countermeasures     :   disabled      60 Sec
  invalid-frame-length     :   disabled      60 Sec
WS5100>

WS5100>show wireless mac-auth-local 50
WS5100>

WS5100>show wireless mobile-unit statistics
% Error: None of the mobile-units are associated!!

WS5100(config)#show wireless mobile-unit
index   MAC-address       radio type wlan vlan/tunnel  ready  IP-
address    last active Posture Status
  2     00-0E-9B-98-F9-34  1     11g  1      vlan 1    Y
192.168.2.45    0 Sec
Number of mobile-units associated: 1
WS5100(config)#

WS5100(config)#show wireless mobile-unit association-history
MU MAC             Radio  WLAN  Timestamp          Event
============================================================
00-0E-9B-98-F9-34  1      1     1116316            Association
00-0E-9B-98-F9-34  1      1     12248923           Unassociation
00-0E-9B-98-F9-34  1      1     12250053           Association
00-0E-9B-98-F9-34  1      1     4280690527         Unassociation
00-0E-9B-98-F9-34  1      1     4280691647         Association
00-0E-9B-98-F9-34  1      1     4280716777         Unassociation
00-0E-9B-98-F9-34  1      1     4280717937         Association
WS5100(config)#

WS5100(config)#show wireless mobile-unit radio 1
index   MAC-address       radio type wlan vlan/tunnel  ready  IP-
address    last active Posture Status
  2     00-0E-9B-98-F9-34  1     11g  1      vlan 1    Y
192.168.2.45    0 Sec
Listed 1 of a total of 1 mobile-units
WS5100(config)#
```

```
WS5100(config)#show wireless wlan config 1

WLAN: 1, status: enabled, description: WLAN1, ssid: sardarjee
 auth: none, encr: none, inactivity-timeout: 1800 seconds
 vlan 1: unlimited users
 mu-mu-disallow: disabled, secure-beacon: disabled, answer-bcast-
ess: enabled,
 weight: 1, prioritize-voice: disabled, spectralink-voice-protocol:
disabled
 multicast mask1: 00-00-00-00-00-00, mask2: 00-00-00-00-00-00
 traffic-classification : normal, wmm-mapping: 8021p, L3-mobility:
disabled
 Client Bridge Backhaul is disabled on this WLAN
 NAC Mode: bypass-nac-except-include-list

Exclude list(s): NotMe
WS5100(config)#
```

2.2.33 wlan-acl

- *Common to all modes*

Syntax

```
show wlan-acl [<1-32>|all]
```

Parameters

<1-32>	Displays ACLs attached to the specified WLAN ID
all	Displays all ACLs attached to a WLAN port

Example

```
WS5100>show wlan-acl 20
WLAN port: 20
  Inbound IP Access List   :
  Inbound MAC Access List  :
  Outbound IP Access List  :
  Outbound MAC Access List :
WS5100>

WS5100>show wlan-acl all
WLAN port: 1
  Inbound IP Access List   :78
  Inbound MAC Access List  :200
  Outbound IP Access List  :78
  Outbound MAC Access List :200
WS5100>
```

2.2.34 access-list

▸ *Priviledge / Global Config*

Displays the access lists (numbered and named) configured on the switch. The numbered access list displays numbered ACLs. The named access list displays named ACL details.

Syntax

```
show access-list
show access-list ( <1-99> | <100-199> | <1300-1999> | <2000-2699> |
WORD )
Show access-list <acl-name>
```

Parameters

<1-99>	IP standard access list
<100-199>	IP extended access list
<1300-1999>	IP standard access list (expanded range)
<2000-2699>	IP extended access list (expanded range)
WORD	Name of ACL

Example

```
WS5100(config)#show access-list
Extended IP access list 110
    permit ip 192.168.1.0/24 192.168.100.0/24 rule-precedence 5
    permit ip 192.168.63.0/24 192.168.100.0/24 rule-precedence 63
    permit ip 192.168.157.0/24 192.168.100.0/24 rule-precedence 157
WS5100(config)#

WS5100(config)#show access-list 110
Extended IP access list 110
    permit ip 192.168.1.0/24 192.168.100.0/24 rule-precedence 5
    permit ip 192.168.63.0/24 192.168.100.0/24 rule-precedence 63
    permit ip 192.168.157.0/24 192.168.100.0/24 rule-precedence 157
WS5100(config)#
```

2.2.35 aclstats

Priviledge / Global Config

Displays the statisitcs of configured access lists

Syntax

```
aclstats [<name>|vlan <1-4094>]
```

Parameters

IFNAME	Displays the interface name.
vlan <1-4092>	Defines the VLAN interface. Select from an index value between 1- 4092

Example

```
WS5100(config)#interface vlan 400
WS5100(config-if)#
```

2.2.36 alarm-log

Priviledge / Global Config

Syntax

```
show alarm-log ( <1-65535>| acknowledged | all | count | new |
severity-to-limit( critical |informational | major | normal |
warning))
```

Parameters

<1-65535>	Displays the details of a specific alarm ID
acknowledged	Displays information for acknowledged alarms currently in the system
all	Displays all the alarms currently in the system
count	Displays the number (count) of the alarms currently in the system
new	Displays those new alarms currently in the system

severity-to-limit	Displays the alarms having specified a severity, as well as those alarms with a severity higher than the specified value
critical	Displays all critical alarms
informational	Displays all informational or higher severity alarms
major	Displays all major or higher severity alarms
normal	Displays all normal or higher severity alarms
warning	Displays all warning or higher severity alarms

2.2.37 boot

Priviledge / Global Config

Syntax

```
show boot
```

Parameters

None

Example

```
WS5100#show boot

Image     Build Date             Install Date           Version
Primary May 17 21:34:52 2007  May 21 16:27:40 2007     3.0.2.0-003B
Secondary May 10 23:21:58 2007 May 17 20:09:23 2007    3.0.2.0-002D

Current Boot       : Primary
Next Boot          : Primary
Software Fallback  : Enabled
WS5100#
```

2.2.38 clock

Priviledge / Global Config

Syntax

```
show clock
```

Parameters

None

Example

```
WS5100#show clock
Jun 01 00:51:34 UTC 2007
WS5100#
```

2.2.39 debugging

Priviledge / Global Config

Syntax

```
show debugging (mstp)
```

Parameters

mstp	Displays the current MSTP configuration

Example

```
WS5100(config)#show debugging mstp
MSTP debugging status:
WS5100(config)#
```

2.2.40 dhcp

Privilege / Global Config

Displays existing DHCP server configurations

Syntax

```
show dhcp [config|status]
```

Parameters

config	Displays the current DHCP server configuration
status	Displays whether the DHCP server is running

Example

```
WS5100#show dhcp config

service dhcp
!
ip dhcp pool vlan6
 default-router xxx.xxx.xxx.2
 network xxx.xxx.xx.0/24
```

```
 address range xxx.xxx.xx.xx aaa.aaa.aa.aa

WS5100#
```

2.2.41 file

▸ *Privilege / Global Config*

Syntax

```
show file (information (FILE)| systems)
```

Parameters

information	Displays file information
FILE	Displays the information on file
systems	Lists existing filesystems

Example

```
WS5100#show file systems
File Systems:

     Size(b)      Free(b)      Type  Prefix
           -            -    opaque  system:
    13704192     11904000     flash  nvram:
    19524608     16866304     flash  flash:
           -            -   network  sftp:
           -            -   network  http:
           -            -   network  ftp:
           -            -   network  tftp:
WS5100#
```

2.2.42 ftp

▸ *Privilege / Global Config*

Syntax

```
show ftp
```

Parameters

None

Example

```
WS5100#show ftp
```

```
FTP Server: Disabled
User Name:  anonymous or ftpuser
Password:   ********
Root dir:   flash:/
WS5100#
```

2.2.43 password-encryption

Priviledge / Global Config

Syntax

```
show password-encryption (status)
```

Parameters

status	Displays the existing password-encryption status

Example

```
WS5100#show password-encryption status
Password encryption is disabled
WS5100#
```

2.2.44 running-config

Privilege / Global Config

Displays the contents of those configuration files wherein all configured MAC and IP access lists are applied to an interface

Syntax

```
show running-config(full|include-factory)
```

Parameters

full	Displays the file's full (complpete) configuration
include-factory	Includes factory defaults

Example

```
WS5100(config)#show running-config
!
! configuration of WS5100 version 3.1.0.0-008D
!
version 1.0
!
service prompt crash-info
!
username admin password 1 8e67bb26b358e2ed20fe552ed6fb832f397a507d
username admin privilege  superuser
username operator password 1
fe96dd39756ac41b74283a9292652d366d73931f
!
!
!
spanning-tree mst config
 name My Name
!
country-code us
logging buffered 4
logging console 4
snmp-server sysname WS5100
snmp-server manager v2
snmp-server manager v3
snmp-server user snmptrap v3 encrypted auth md5
0x7be2cb56f6060226f15974c936e2739b
snmp-server user snmpmanager v3 encrypted auth md5
0x7be2cb56f6060226f15974c936e2739b
snmp-server user snmpoperator v3 encrypted auth md5
0x49c451c7c6893ffcede0491bbd0a12c4
crypto isakmp keepalive 10
crypto ipsec security-association lifetime kilobytes 4608000
fallback enable
ip http server
ip http secure-trustpoint default-trustpoint
ip http secure-server
ip ssh
ip telnet
no service pm sys-restart
!
wireless
 wlan 1 enable
 wlan 1 ssid sardarjee
 radio add 1 00-A0-F8-BF-8A-4B 11bg ap300
 radio add 2 00-A0-F8-BF-8A-4B 11a ap300
 enhanced-beacon-table enable
 enhanced-beacon-table channel-set a 36 44 149
 enhanced-beacon-table channel-set bg 1 2 4 5
```

```
!
radius-server local
!
interface eth1
 switchport access vlan 2100
!
interface eth2
 switchport access vlan 1
!
interface vlan1
 ip address 192.168.2.1/24
!
sole
!
!
aaa authentication login default local none
line con 0
line vty 0 24
!
end

WS5100(config)#
```

```
WS5100(config)#show running-config include-factory
!
! configuration of WS5100 version 3.1.0.0-008D
!
version 1.0
!
service prompt crash-info
no service set command-history
no service set reboot-history
no service set upgrade-history
!
hostname WS5100
!
banner motd Welcome to CLI!
username admin password 1 8e67bb26b358e2ed20fe552ed6fb832f397a507d
username admin access  console web ssh telnet
username admin privilege  superuser
username operator password 1
fe96dd39756ac41b74283a9292652d366d73931f
username operator access  console web ssh telnet
username operator privilege  monitor
!
!
!
!
spanning-tree mst config
```

```
 name My Name
!
no management secure
ip domain-lookup
service diag period 1000
service diag enable
country-code us
redundancy group-id 1
redundancy interface-ip 0.0.0.0
redundancy mode primary
redundancy hold-period 15
redundancy heartbeat-period 5
redundancy discovery-period 30
no redundancy handle-stp enable
no redundancy dhcp-server enable
no redundancy enable
.............................................
.............................................
.............................................
.............................................
no radio default-11b enhanced-beacon-table
no radio default-11b enhanced-probe-table
no radio 1 neighbor-smart-scan
no radio 2 neighbor-smart-scan
no ap-detection enable
.............................................
.............................................
.............................................
.............................................
ip address 123.111.2.1/24
 no ip helper-address
!
sole
 no adapter AeroScout enable
!
radius-server retransmit 3
radius-server timeout 5
radius-server key
!
aaa authentication login default local none
line con 0
line vty 0 24
!
end

WS5100(config)#
```

2.2.45 securitymgr

Privilege / Global Config

Syntax

```
show securitymgr(debug-logs)
```

Parameters

event-logs	Display securitymgr event logs

2.2.46 sessions

Privilege / Global Config

Syntax

```
show sessions
```

Parameters

None

Example

```
WS5100#show sessions
SESSION   USER       LOCATION        IDLE         START TIME
   1       cli    Console           06:24m      May 31 18:31:36
2007
** 2       cli    10.10.10.1        00:00m      Jun  1 00:04:30
2007
WS5100#
```

2.2.47 startup-config

Privilege / Global Config

Syntax

```
show startup-config
```

Parameters

None

Example

```
WS5100#show startup-config
!
! configuration of WS5100 version 3.1.0.0-008D
!
version 1.0
!
service prompt crash-info
!
username admin password 1 8e67bb26b358e2ed20fe552ed6fb832f397a507d
username admin privilege  superuser
username operator password 1
fe96dd39756ac41b74283a9292652d366d73931f
!
!
!
spanning-tree mst config
 name My Name
!
country-code us
logging buffered 4
logging console 4
snmp-server sysname WS5100
snmp-server manager v2
snmp-server manager v3
snmp-server user snmptrap v3 encrypted auth md5
0x7be2cb56f6060226f15974c936e2739b
snmp-server user snmpmanager v3 encrypted auth md5
0x7be2cb56f6060226f15974c936e2739b
snmp-server user snmpoperator v3 encrypted auth md5
0x49c451c7c6893ffcede0491bbd0a12c4
crypto isakmp keepalive 10
crypto ipsec security-association lifetime kilobytes 4608000
fallback enable
ip http server
ip http secure-trustpoint default-trustpoint
ip http secure-server
ip ssh
ip telnet
no service pm sys-restart
!
wireless
 wlan 1 enable
 wlan 1 ssid sardarjee
 radio add 1 00-A0-F8-BF-8A-4B 11bg ap300
 radio 1 enhanced-beacon-table
 radio 1 enhanced-probe-table
 radio add 2 00-A0-F8-BF-8A-4B 11a ap300
 ap-detection approved add 1 any any
```

```
 enhanced-beacon-table enable
 enhanced-beacon-table channel-set a 36 44 149
 enhanced-beacon-table channel-set bg 1 2 4 5
!
radius-server local
!
interface eth1
 switchport access vlan 2100
!
interface eth2
 switchport access vlan 1
!
interface vlan1
 ip address 192.168.2.1/24
!
sole
!
!
aaa authentication login default local none
line con 0
line vty 0 24
!
end

WS5100#
```

2.2.48 upgrade-status

- *Privilege / Global Config*

Syntax

```
show upgrade-status(detail)
```

Parameters

detail	Displays the image's last upgrade log

Example

```
WS5100#show upgrade-status
Last Image Upgrade Status : Successful
Last Image Upgrade Time   : Mon May 21 16:27:40 2007
WS5100#
```

3

User Exec Commands

Logging in to the switch places you within the USER EXEC command mode. Typically, a login requires a user name and password. You have three login attempts before a connection attempt is refused. USER EXEC commands (available at the user level) are a subset of the commands available at the privileged level. In general, USER EXEC commands allow you to connect to remote devices, perform basic tests and list system information.

To list available USER EXEC commands, use **?** at the command prompt. The USER EXEC prompt consists of the device host name followed by an angle bracket (**>**). The default host name is generally "WLAN Module". Use the GLOBAL CONFIG command to change the hostname.

3.1 User Exec Commands

Table 3.1 summarizes USER EXEC commands:

Table 3.1 User Exec Mode Command Summary

Command	Description	Ref.
clear	Resets the command to the previous configuration	*page 3-2*
clrscr	Clears the display screen	*page 2-2*
cluster-cli	Displays the cluster context	*page 3-4*
debug	Displays debugging functions	*page 3-4*
disable	Turns off (disables) the privileged mode command set	*page 3-6*

Table 3.1 User Exec Mode Command Summary

Command	Description	Ref.
enable	Turns on (enables) the privileged mode command set	*page 3-6*
exit	Ends the current mode and moves down to the previous mode	*page 2-2*
help	Describes the interactive help system	*page 2-2*
logout	Exits the EXEC mode	*page 3-7*
no	Negates a command or sets its defaults.	*page 2-4*
page	Toggles the paging functionality	*page 3-7*
ping	Sends ICMP echo messages	*page 3-7*
quit	Exits the current mode and moves to the previous mode	*page 3-8*
service	Displays service commands	*page 2-5*
show	Shows the running system information. Refer to *Common Commands* on *page 2-23*	*page 2-23*
telnet	Opens a telnet session.	*page 3-8*
terminal	Sets terminal line parameters	*page 3-9*
traceroute	Traces the route to a destination	*page 3-9*

3.1.1 clear

User Exec Commands

Resets the previous (last saved) command

Syntax

```
clear [crypto (ipsec|isakmp (sa)<A.B.C.D>|mobility(event-log|
mobile-unit|peer-statistics)|
spanning-tree (spanning-tree)(interface)<NAME>]
```

Parameters

crypto	Clears IPSec/ISAKMP SAs for a given peer
	• ipsec – Clears IPSec SA's
	• isakmp – Clears ISAKMP SA's
	  • sa – Clears all IPSec/ISAKMP SA's
	  • Peer IP – Peer IP address.

mobility	Clears mobility attributes
	• event-log – Clears event log
	  • mobile-unit – Clears MU event-logs
	  • peer – Clears peer event logs
	• mobile-unit – Clears MUs
	  • MU MAC address – Clears the MAC address of a MU
	  • all – Clears the MU MAC address, including the foreign and home database
	  • foreign-database – Clears MUs present in the foreign MU database
	  • home-database – Clears MUs present in the home MU database
	• peer-statistics – Clears Mobility Peer Statistics.
	  • Peer IP Address – IP address of Peer

spanning-tree	Clears the spanning tree protocols configured for the interface

Example

```
WS5100>clear crypto ike sa 111.222.333.01
WS5100>

WS5100>clear crypto ipsec sa
WS5100>
```

3.1.2 cluster-cli

User Exec Commands

Use this command to enter the cluster-cli context. The cluster-cli context provides centralized management to configure all cluster members from any one member. Any command executed under this context will be executed to all the switches in the cluster.

A new context (*redundancy*) supports the cluster-cli. Any commands executed under this context are executed to all members of the cluster.

Syntax

```
cluster-cli enable
```

Parameters

enable	Enables the cluster context.

Example

```
WS5100>cluster-cli enable
WS5100>
```

3.1.3 debug

User Exec Commands

Use this command to debug the switch

Syntax

```
debug (certmgr(all|err|info)|ip (https|ssh)|
mobility(cc|error|forwarding|mu|packet|peer|system))
```

Parameters

certmgr	Certificate Manager Debugging Messages • *all* – Traces error and informational messages from the certificate manager • error – Traces error messages from the certificate manager • *info* – Traces informational messages from the certificate manager

ip ()	Internet Protocol (IP) • https – Secure HTTP (HTTPS) server • ssh – Secured Shell (SSH) server
mobility ()	L3 mobility. • cc – ccserver events • error – Error events • forwarding – Dataplane forwarding • mu – MU events and state changes • packet – Control packets events • peer – Peer establishments • system – System events

Examples

```
WS5100>debug certmgr all
WS5100>

WS5100>debug certmgr error
WS5100>

WS5100>debug certmgr info
WS5100>

WS5100>debug ip ssh
WS5100>


WS5100>debug mobility cc
WS5100>

WS5100>debug mobility error
WS5100>
WS5100>debug mobility forwarding
WS5100>

WS5100>debug mobility mu
WS5100>

WS5100>debug mobility packet
WS5100>
```

```
WS5100>debug mobility peer
WS5100>

WS5100>debug mobility system
WS5100>
```

3.1.4 disable

User Exec Commands

Enables the PRIV mode in order to use the disable command. Use the `disable` command to exit the PRIV mode.

Syntax

`disable`

Parameters

None

Example

```
WS5100>disable
WS5100>
```

3.1.5 enable

User Exec Commands

Use the enable command to enter the PRIV mode

Syntax

`enable`

Parameters

None

Example

```
WS5100>enable
```

3.1.6 logout

▸ User Exec Commands

Use this command instead of the `exit` command to exit the EXEC mode

Syntax

```
logout
```

Parameters

None

Example

```
The WS5100 Series Switch logs off on execution of this command.
```

3.1.7 page

▸ User Exec Commands

Use the page command to toggle the switch paging function. Enabling this command displays the CLI command output page by page, instead of running the entire output at once.

Syntax

```
page
```

Parameters

None

3.1.8 ping

▸ User Exec Commands

Sends ICMP echo messages to a user-specified location

Syntax

```
ping [IP address|hostname]
```

Parameters

[IP address|hostname]	Pings the specified destination address or hostname

Example

```
WS5100>ping 192.168.2.100
PING 192.168.2.100 (192.168.2.100): 100 data bytes
```

```
128 bytes from 192.168.2.100: icmp_seq=0 ttl=128 time=2.7 ms
128 bytes from 192.168.2.100: icmp_seq=1 ttl=128 time=38.4 ms
128 bytes from 192.168.2.100: icmp_seq=2 ttl=128 time=4.6 ms

--- 192.168.2.100 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 2.7/15.2/38.4 ms
WS5100>
```

3.1.9 quit

User Exec Commands

Use this command to exit the current mode and move to the previous mode

Syntax

```
quit
```

Parameters

None

Example

The switch logs off upon execution of the command

3.1.10 telnet

User Exec Commands

Opens a telnet session

Syntax

```
telnet [IP address|hostname]
```

Parameters

[IP address|hostname]	Defines the IP address or hostname of a remote system

Example

```
WS5100#telnet 157.111.222.33
Entering character mode
Escape character is '^]'.
Red Hat Linux release 9 (Shrike)
Kernel 2.4.20-6bigmem on an i686
login: cli
Password:
```

3.1.11 terminal

▸ User Exec Commands

Sets the length/number of lines displayed within the terminal window

Syntax

```
terminal[length <0-512>|no(length <0-512>|width)|width <0-512> ]
```

Parameters

length	Sets the number of lines on a screen
no	Negates a command or sets its defaults
width	Sets the width/number of characters on a screen line

Example

```
WS5100>terminal length 100
WS5100>

WS5100>terminal width 200
WS5100>
```

3.1.12 traceroute

▸ User Exec Commands

Traces the route to its defined destination

Syntax

```
traceroute (WORD | ip WORD)
```

Parameters

WORD	Traces the route to a destination address or hostname
IP Address	IP trace

Example

```
WS5100#traceroute 157.222.333.33
traceroute to 157.235.208.39 (157.235.208.39), 30 hops max, 38 byte
packets
1 157.235.208.39 (157.235.208.39) 0.466 ms 0.363 ms 0.226 ms
WS5100#
```

4

Privileged Exec Commands

Most PRIV EXEC commands set operating parameters. Privileged-level access should be password protected to prevent unauthorized use. The PRIV EXEC command set includes commands contained within the USER EXEC mode. The PRIV EXEC mode also provides access to configuration modes, and includes advanced testing commands.

The PRIV EXEC mode prompt consists of the host name of the device followed by a pound sign (**#**). To access the PRIV EXEC mode, enter the following at the prompt:

```
WS5100#enable
```

The PRIV EXEC mode is often referred to as the **enable mode**, because the `enable` command is used to enter the mode.

If a password has been configured, you are prompted to enter it before you can access the PRIV EXEC mode. The password is not displayed and is case sensitive. If an enable password has not been set, the PRIV EXEC mode can be accessed only from the router console (terminal connected to the console port).

4.1 Priv Exec Command

Table 4.1 summarizes the switch PRIV EXEC commands:.

Table 4.1 Priv Exec Mode Command Summary

Command	Description	Ref.
acknowledge	Acknowledges alarms	*page 4-4*
archive	Manages archive files	*page 4-4*

Table 4.1 Priv Exec Mode Command Summary

Command	Description	Ref.
cd	Changes current directory	*page 4-6*
change-passwd	Changes the password of the logged user	*page 4-6*
clear	Resets functions to last saved configuration	*page 4-7*
clock	Configures the software system clock	*page 4-10*
clrscr	Clears the displayed screen	*page 2-2*
cluster-cli	Displays the cluster context	*page 4-10*
configure	Enters the configuration mode	*page 4-11*
copy	Copies content from one file to another	*page 4-11*
debug	Displays debugging functions	*page 4-12*
delete	Deletes a specified file from the system	*page 4-14*
diff	Displays differences between two files	*page 4-15*
dir	Lists the files on a filesystem	*page 4-16*
disable	Turns off privileged mode command	*page 4-17*
edit	Edits a text file	*page 4-17*
enable	Turns on the privileged mode command	*page 4-18*
erase	Erases a filesystem	*page 4-18*
exit	Ends the current mode and moves to the previous mode	*page 2-2*
halt	Halts the switch	*page 4-19*
help	Displays a description of the interactive help system	*page 2-2*
kill	Kills (terminates) a specified session	*page 4-19*
logout	Exits the EXEC mode	*page 4-20*

Table 4.1 Priv Exec Mode Command Summary

Command	Description	Ref.
mkdir	Creates a directory	*page 4-21*
more	Displays the contents of a file	*page 4-21*
no	Negates a command or sets its defaults	*page 2-4*
page	Toggles the paging function	*page 4-23*
ping	Sends ICMP echo messages to a specified location	*page 4-23*
pwd	Displays the current directory	*page 4-24*
quit	Exits the current mode and moves to the previous mode	*page 4-24*
reload	Halts the switch and performs a warm reboot	*page 4-24*
rename	Renames a file	*page 4-25*
rmdir	Deletes a directory	*page 4-26*
service	Displays service commands	*page 2-5*
show	Shows running system information. Refer to *Common Commands* on *page 2-23*	*page 2-23*
telnet	Opens a telnet session	*page 4-26*
terminal	Sets terminal line parameters	*page 4-27*
traceroute	Traces a route to a destination	*page 4-28*
upgrade	Upgrades the switch software image	*page 4-28*
upgradeabort	Aborts an ongoing upgrade operation	*page 4-30*
write	Writes the running configuration to memory or a terminal	*page 4-30*

4.1.1 acknowledge

Priv Exec Command

Acknowledges alarms

Syntax

```
acknowledge alarm-log [<1-65535> | all]
```

Parameters

alarm-log	Acknowledges alarms • <1-65535> – Acknowledges the specific alarm ID • all – Acknowledges all alarms

Example

```
WS5100#acknowledge alarm-log all
No corresponding record found in the Alarm Log.

WS5100#acknowledge alarm-log 200
No corresponding record found in the Alarm Log.
WS5100#
```

4.1.2 archive

Priv Exec Command

Manages file archive operations

Syntax

```
archive tar /table [FILE|URL]
archive tar /create [FILE|URL] .FILE
archive tar /xtract [FILE|URL] DIR
```

Parameters

tar	Manipulates (creates, lists or extracts) a tar file
/table	Lists the files in a tar file
/create	Creates a tar file
/xtract	Extracts content from a tar file

FILE	Defines a Tar filename
URL	Tar file URL

Example

How to zip the folder flash:/log/?

```
WS5100#archive tar /create flash:/out.tar flash:/log/
tar: Removing leading '/' from member names
flash/log/
flash/log/snmpd.log
flash/log/messages.log
flash/log/startup.log
flash/log/radius/
WS5100#dir flash:/
```

Viewing the output tar file?

```
Directory of flash:/
  drwx   1024      Thu Apr 17 08:25:50 2007   hotspot
  drwx   120       Fri Apr  8 12:27:20 2007   log
  drwx   1024      Thu Apr  7 16:23:34 2007   crashinfo
  drwx   1024      Wed May 23 15:30:19 2007   backup
  -rw-   173056    Fri May  8 14:39:48 2007   out.tar
```

Which files are tared?

```
WS5100#archive tar /table flash:/out.tar
drwxrwxrwt 0/600  0 2007-05-08 12:27:20 flash/log
-rw-r--r-- 0/0    381 2007-05-08 12:27:28 flash/log/snmpd.log
-rw-r--r-- 0/0    151327 2007-05-08 14:37:26 flash/log/messages.log
-rw-r--r-- 0/0    17318 2007-05-08 12:27:29 flash/log/startup.log
drwxrwxrwt 0/600  0 2007-05-08 12:27:14 flash/log/radius
```

Untar fails..?

```
WS5100#archive tar /xtract flash:/out.tar flash:/out/
tar: flash:/out.tar: No such file or directory
```

4.1.3 cd

Priv Exec Command

Changes the current directory

Syntax

```
cd [DIR|]
```

Parameters

DIR	Changes current directory to DIR.

Example

```
WS5100#cd
nvram:/   system:/  flash:/
WS5100#cd flash:/?
  DIR  Change current directory to DIR
WS5100#cd flash:/
flash:/backup/     flash:/crashinfo/  flash:/hotspot/    flash:/
log/
flash:/out/
WS5100#cd flash:/log/?
  DIR  Change current directory to DIR
WS5100#cd flash:/log/
WS5100#pwd
flash:/log/
WS5100#
```

4.1.4 change-passwd

Changes the password of a logged in user

Priv Exec Command

Syntax

```
change-passwd
```

Parameters

None

Usage Guidelines

A password must be between 8 to 32 characters in length. For security, the console does not display user entered key words or the old password and new password fields.

Verify the console displays a “password successfully changed” message.

NOTE: The console (by default), does not display a user entered keyword for an old password and new password.

Leaving the old password and new password fields empty displays the following error message:

```
Error: Invalid password length. It should be between 8 -
32characters.
```

Example

```
WS5100#change-passwd
Enter old password:
Enter new password:
Password for user 'admin' changed successfully
WS5100#
```

4.1.5 clear

Priv Exec Command

Resets the current context

Syntax

```
clear [aclstats|alarm-log|arp-cache|counters|crypto|
ip|logging|mac-address-table|mobility|spanning-tree]

clear alarm-log (<1-65535>|acknowledge|all|new)
clear counters [all|bridge|interface(<NAME>|all|eth <1-2>|vlan <1-
               4094>)|router|thread]
clear crypto(ike|ipsec)sa(remote peer)
clear ip(dhcp(binding)[*|A.B.C.D]|nat(translation)*)
clear  mac-address-table [dynamic|multicast|static]
                         (address|bridge|interface|vlan)
clear mobility(mu|mu-log|peer-log|peer-statistics)
clear mobility mu(<MAC Address>|all|foreign-database|home-database)
clear spanning-tree (detected-protocols)(interface)<INTF Name>
```

Parameters

aclstats	Clears ACl statistics
alarm-log	Clears alarm-log • <1-65535> – Clears the specific alarm ID • acknowledge – Clears acknowledged alarms • all – Clear all alarms • new – Clear new alarms
arp-cache	Clears the ARP cache.
counters [all|bridge|interface|router| thread]	Clears counters • all – Clears all counters • bridge – Clears bridge counters • interface [<INTF name>|all|eth <1-2>|vlan <1-4094>] – Clears interface counters. • router – Clears router counters • thread – Clear sper-thread counters
crypto	crypto • ike – Clears the IKE • ipsec – Clears ipsec • sa – Displays the security association. • remote-peer – Remote Peer IP address
ip	Clears Internet Protocol (IP) DHCP/NAT. • dhcp – DHCP server configuration • binding – DHCP address bindings For more details see *DHCP Server Instance on page 17-1* • * – Clears all bindings. • A.B.C.D – Clears a specific binding • nat – *Network Address Translation (*NAT) • translation – Clears a specified translation
logging	Modifies message logging facilities

mac-address-table	Clears entries in the forwarding database
	• dynamic – Clears all dynamic entries
	• multicast – Clears all multicast entries
	• static – Clears all management configured entries
	  • address – Clears a specified MAC address
	  • bridge <1-32> – Clears bridge group commands
	  • interface – Clears all MAC addresses for the specified interface
	  • vlan <1-4094> – Clears all MAD addresses for the specified VLAN

mobility	Clears Mobility Attributes • mu – Clears the MU • MAC Address – MAC address of the MU • all – All MUs (Home and Foreign). • foreign-database – Displays MUs present in the foreign MU database. • home-database – Displays MUs present in the home MU database • mu-log – Clears the mobility MU event log • peer-log – Clears the mobility PEER event log • peer-statisitcs – Clears mobility peer statistcs
spanning-tree (detected-protocols) (interface) <NAME>	Clears existing spanning-tree commands

Example

```
WS5100#clear alarm-log new
WS5100#

WS5100#clear alarm-log acknowledged
WS5100#
```

```
WS5100#clear arp-cache
WS5100#

WS5100#clear logging
WS5100#

WS5100#clear mobility event-log peer
WS5100#

WS5100#clear ip dhcp binding *
WS5100#
```

4.1.6 clock

▸ *Priv Exec Command*

Configures the software system clock

Syntax

`clock set HH:MM:SS [1-31] MONTH [1993-2035]`

Parameters

set	Sets system date and time

Example

```
WS5100#clock set 15:10:30 25 May 2007

WS5100#show clock
May 25 15:10:31 UTC 2007
```

4.1.7 cluster-cli

▸ *Priv Exec Command*

Use this command to access the cluster-cli context. The cluster-cli context provides centralized management to configure all members of cluster from one member. Any command executed under this context is executed to all switches in the cluster.

A new context (*redundancy*) is available to support the cluster-cli. Any commands executed under this context are executed on each cluster member.

Use `no cluster-cli` to exit the cluster-cli context.

Syntax

`cluster-cli enable`

Parameters

enable	Enables the switch cluster context

Example

4.1.8 configure

▸ *Priv Exec Command*

Enters into the configuration mode

Syntax

```
configure terminal
```

Parameters

terminal	Configure from the terminal

Example

```
WS5100#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
WS5100(config)#
```

4.1.9 copy

▸ *Priv Exec Command*

Use this command to copy any file (config,log,txt ...etc) from any location to the switch and vice-versa.

NOTE: Copying a new config file onto an existing running-config file merges it with the existing running-config on the switch. Both, the existing running-config and the new config file are applied as the current running-config.

Copying a new config file onto a start-up config files replaces the existing start-up config file with the parameters of the new file. It is better to erase the existing start-up config file from and then copy the new config file to the startup config.

Syntax

```
copy (FILE|URL) (FILE|URL)
```

Parameters

FILE	Target file from which to copy
URL	Target URL from which to copy

Example

Transferring file snmpd.log to remote tftp server?

```
WS5100#copy flash:/log/snmpd.log
tftp://157.235.208.105:/snmpd.log
```

Accessing running-config file from remote tftp server into switchrunning-config?

```
WS5100#copy tftp://157.235.208.105:/running-
config running-config
```

4.1.10 debug

Priv Exec Command

Use this command for debugging. This command is also used for debugging

Syntax

```
debug all
debug cc [access-port|all|alt|ap-detect|capwap|cluster|
          config|dot11|eap|ids|kerberos|l3-mob|loc-ap|
          loc-mu|media|mobile-unit|radio|radius|self-
          heal|snmp|system|wips|wisp|wlan]
debug ccstats <CCStats Module>
debug certmgr [all|error|info]
debug dhcpsvr [all|error|info]
debug imi [all|cli-client|cli-server|errors|init|ntp]
debug ip [https|ssh]
debug logging [all|errors|monitor|subagent]
debug mgmt [all|cgi|err|sys]
debug mobility [all|cc|error|forwarding|mu|packet|peer|system]
debug mstp [all|cli|packet|protocol|timer]
debug nsm [all|events|kernel|packet]
debug pktdrvr [rate-limit|skip-packet-filter]
debug radius [all|err|info|warn]
debug redundancy [all|ccmsg|config|errors|general|heartbeats|
                  init|packets|proc|shutdown|states|subagent|timer|
                  warnings]
debug securitymgr [all|debug|error|ikeerror|pmdebug|pmerror]
debug sole [adapters|algo|all|errors|init]
```

Parameters

all	Enables debugging
cc	Cellcontroller (wireless) debugging messages
ccstats	Cellcontroller statistics (wireless) debugging messages
certmgr	Certificate manager debugging messages
dhcpsvr	DHCP Conf Server debugging messages
imi	Integrated management interface debugging messages
ip	Internet protocol debugging messages
logging	Modify message logging facilities debugging messages
mgmt	Management daemon debugging messages
mobility	L3 mobility debugging messages.
mstp	*Multiple Spanning Tree Protocol* (MSTP) debugging message .
nsm	*Network Service Module* (NSM) debugging messages
pktdrvr	Pktdrvr (kernel wireless) debugging messages
radius	RADIUS server debugging messages
redundancy	Redundancy protocol debugging messages
securitymgr	Security manager debugging messages
sole	Location engine debugging messages

Example

```
WS5100#debug ?
  all           Enable all debugging
  cc            Cellcontroller (wireless) debugging messages
  ccstats       Cellcontroller (wireless) debugging messages
  certmgr       Certificate Manager Debugging Messages
  dhcpsvr       DHCP Conf Server Debugging Messages
  imi           Integrated Management Interface
```

```
  ip            Internet Protocol (IP)
  logging       Modify message logging facilities
  mgmt          Mgmt daemon
  mobility      L3 Mobility
  mstp          Multiple Spanning Tree Protocol (MSTP)
  nsm           Network Service Module (NSM)
  pktdrvr       Pktdrvr (kernel wireless) debugging messages
  radius        RADIUS server debugging messages
  redundancy    Redundancy Protocol debugging messages
  securitymgr   Security Manager Debugging Messages
  sole          Location engine debugging messages

WS5100#debug
```

4.1.11 delete

Priv Exec Command

Deletes a specified file from the system

Syntax

```
delete ({/force|/recursive}|) .FILE
```

Parameters

/force	Forces deletion without a prompt
/recursive	Performs a recursive delete
FILE	Specifies the filename(s) to be deleted

Example

```
WS5100#delete flash:/out.tar flash:/out.tar.gz
Delete flash:/out.tar [y/n]? y
Delete flash:/out.tar.gz [y/n]? y

WS5100#delete /force flash:/tmp.txt
WS5100#

WS5100#delete /recursive flash:/backup/
Delete flash:/backup//fileMgmt_350_180B.core

[y/n]? y
Delete

flash:/backup//fileMgmt_350_18212X.core_bk
```

```
[y/n]? n
Delete flash:/backup//imish_1087_18381X.core.gz

[y/n]? n
WS5100#
```

4.1.12 diff

▸ *Priv Exec Command*

View the differences between 2 files

Syntax

```
diff (FILE|URL) (FILE|URL)
```

Parameters

FILE	Displays the differences between a FILE
URL	Displays the differences between a URL

Example

```
WS5100#diff startup-config running-config
--- startup-config
+++ running-config
@@ -89,7 +89,7 @@
  mobility peer 157.235.208.16
  wlan 1 enable
  wlan 1 ssid wlan123
- wlan 1 encryption-type wep128
+ wlan 1 encryption-type tkip
  wlan 1 authentication-type eap
  wlan 1 mobility enable
  wlan 1 radius server primary 127.0.0.1
@@ -184,10 +184,12 @@
  rad-user adam password 0 mypassword
  rad-user eve password 0 mypassword123
  rad-user sumi password 0 mypassword
+ rad-user test password 0 mypassword123
  rad-user vasavi password 0 mypassword123
  group kumar2
   rad-user sumi
-  policy wlan 2
+  policy vlan 44
+  policy wlan 10
  !
  group kumar3
```

4.1.13 dir

Priv Exec Command

View the list of files on a filesystem

Syntax

```
dir ({/all|/recursive}|) (DIR|all-filesystems|)
```

Parameters

/all	Lists all files
/recursive	Lists files recursively
DIR	Lists files in the named file path
all-filesystems	Lists the files on all filesystems

Example

```
WS5100#dir
Directory of flash:/

  drwx   1024      Wed Jul 19 19:14:05 2006   hotspot
  drwx   120       Wed Aug 30 15:32:44 2006   log
  drwx   1024      Thu Aug 31 23:50:09 2006   crashinfo
  -rw-   14271     Tue Jul 25 15:16:41 2006   Radius-config
  -rw-   14271     Wed Jul 26 15:42:08 2006   flash:
  drwx   1024      Wed Aug  9 17:35:08 2006   radius
  -rw-   3426      Wed Jul 26 16:08:02 2006   running-config-new
  -rw-   13163     Wed Jul 26 16:08:42 2006   radius-config
  -rw-   80898     Thu Aug 17 14:59:39 2006   cli_commands.txt
  -rw-   65015     Fri Aug 11 19:57:37 2006
cli_commands.txtli_commands.txt
  -rw-   65154     Thu Aug 17 15:11:23 2006   cli_commands_180B.txt

WS5100#
```

4.1.14 disable

Priv Exec Command

Turns off the privileged mode command

Syntax

```
disable
```

Parameters

None

Example

```
WS5100#disable
WS5100>
```

4.1.15 edit

Priv Exec Command

Edits a text file

Syntax

```
edit FILE
```

Parameters

FILE	Name of the file to be modified

Example

```
WS5100#edit startup-config
  GNU nano 1.2.4                                        File:
startup-config

!
! configuration of WS5100 version 3.1.0.0-038R
!
version 1.1
!
!
aaa authentication login default local none
service prompt crash-info
!
username admin password 1 8e67bb26b358e2ed20fe552ed6fb832f397a507d
username admin privilege  superuser
```

```
username operator password 1
fe96dd39756ac41b74283a9292652d366d73931f
!
!
!
spanning-tree mst configuration
 name My Name
!
no bridge multiple-spanning-tree enable bridge-forward
```

4.1.16 enable

Priv Exec Command

Turns on the privileged mode command

Syntax

```
enable
```

Parameters

None

Example

```
WS5100#enable
WS5100#
```

4.1.17 erase

Priv Exec Command

Erases a target filesystem

Syntax

```
erase (nvram:|flash:|startup-config)
```

Parameters

nvram	Erases everything in nvram
flash	Erases everything in flash
startup-config	Resets the configuration to factory default

Example

```
WS5100#erase flash:
% Error: path is a directory
WS5100#erase ne
WS5100#erase nvram:
% Error: no user deleteable files in nvram:
WS5100#erase startup-config
WS5100#
```

4.1.18 halt

Priv Exec Command

Stops (halts) the switch

Syntax

```
halt
```

Parameters

None

Example

```
WS5100#halt
Wireless switch will be halted, do you want to continue? (y/n): y
.........
```

4.1.19 kill

Priv Exec Command

Kills (terminates) a specified session.

Syntax

```
kill session <1-16>
```

Parameters

session	Active session. There are 16 active sessions which can be terminated.

Example

```
Telnet to switch
[xyz@xyz xyz]$ telnet

157.235.208.93
Trying 157.235.208.93...
Connected to 157.235.208.93 (157.235.208.93).
Escape character is '^]'.

WS5100 release 3.0.0.0-19193X
Login as 'cli' to access CLI.
WS5100 login: root
~ #
WS5100#show sessions
SESSION   USER       LOCATION        IDLE

  START TIME
** 1       root   Console           00:00m

Jan  1 00:00:00 1970
   2       root   157.235.208.105   00:38m

Jan  1 00:00:00 1970
   3       root   157.235.208.105   00:00m

Jan  1 00:00:00 1970

WS5100#kill session 9
% Error: Invalid session number
WS5100#kill session 3

~ # Connection closed by foreign host.
[xyz@xyz xyz]$
```

4.1.20 logout

Priv Exec Command

Exits from the EXEC mode.

Syntax

```
logout
```

Parameters

None

Example

```
WS5100#logout

WS5100 release 3.0.0.0-200B
Login as 'cli' to access CLI.
WS5100 login:
```

4.1.21 mkdir

Priv Exec Command

Creates a new directory in the filesystem.

Syntax

```
mkdir DIR
```

Parameters

DIR	Directory name

Example

```
WS5100#mkdir TestDIR
WS5100#
```

4.1.22 more

Priv Exec Command

View the contents of a file

Syntax

```
more FILE
```

Parameters

FILE	Displays the contents of the file

Example

```
WS5100#more flash:/log/messages.log
Sep 08 12:27:30 2006: %PM-5-PROCSTOP: Process

"radiusd" has been stopped
Sep 08 12:27:31 2006: %LICMGR-6-NEWLICENSE:
```

```
Licensed AP count changed to 48
Sep 08 12:27:31 2006: %CC-5-COUNTRYCODE:

config: setting country code to [in:
India]
Sep 08 12:27:31 2006: %DAEMON-6-INFO: radiusd

[460]: Ready to process requests.
Sep 08 12:27:35 2006: %DAEMON-6-INFO: init:

Starting pid 328, console
/dev/ttyS0
Sep 08 12:27:37 2006: %AUTH-6-INFO: login[328]:

root login  on `ttyS0' from
`Console'
Sep 08 12:27:47 2006: %IMI-5-USERAUTHSUCCESS:

User 'admin' logged in with role
of ' superuser' from auth source 'local'
Sep 08 12:28:01 2006: %NSM-6-DHCPDEFRT: Default

route with gateway
157.235.208.246 learnt via DHCP
Sep 08 12:28:01 2006: %NSM-6-DHCPIP: Interface

vlan1 acquired IP address
157.235.208.93/24 via DHCP
Sep 08 12:29:07 2006: %CC-5-RADIOADOPTED: 11bg

radio on AP 00-A0-F8-BF-8A-A2
adopted
Sep 08 12:29:07 2006: %CC-5-RADIOADOPTED: 11a

radio on AP 00-A0-F8-BF-8A-A2
adopted
Sep 08 12:29:12 2006: %MOB-6-MUADD: Station 00

-0F-3D-E9-A6-54: Added to
Mobility Database
Sep 08 12:29:12 2006: %CC-6-STATIONASSOC:

Station 00-0F-3D-E9-A6-54 associated
to radio 3 wlan 1
 -- MORE --, next page: Space, next line:

Enter, quit: Control-C
```

4.1.23 page

Priv Exec Command

Toggles switch paging. Enabling this command displays the command output page by page instead of running the entire output at once

Syntax

```
page
```

Parameters

None

Example

```
WS5100#page
WS5100#
```

4.1.24 ping

Priv Exec Command

Send (transmits) ICMP echo messages.

Syntax

```
ping WORD
```

Parameters

WORD	Ping destination address or hostname.

Example

```
WS5100#ping 157.235.208.39
PING 157.235.208.39 (157.235.208.39): 100 data bytes
128 bytes from 157.235.208.39: icmp_seq=0 ttl=64 time=2.3 ms
128 bytes from 157.235.208.39: icmp_seq=1 ttl=64 time=0.2 ms
128 bytes from 157.235.208.39: icmp_seq=2 ttl=64 time=0.3 ms
128 bytes from 157.235.208.39: icmp_seq=3 ttl=64 time=0.2 ms
128 bytes from 157.235.208.39: icmp_seq=4 ttl=64 time=0.1 ms

--- 157.235.208.39 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.1/0.6/2.3 ms
WS5100#
```

4.1.25 pwd

▸ *Priv Exec Command*

View the contents of the current directory.

Syntax

```
pwd
```

Parameters

None

Example

```
WS5100#pwd
flash:/
WS5100#
```

4.1.26 quit

▸ *Priv Exec Command*

Exits the current mode and moves to the previous mode

Syntax

```
quit
```

Parameters

None

Example

```
WS5100#quit

WS5100 release 3.0.0.0-200B
Login as 'cli' to access CLI.
WS5100 login:
```

4.1.27 reload

▸ *Priv Exec Command*

Halts the switch and performs a warm reboot

Syntax

```
reload
```

Parameters

None

Example

```
WS5100#reload
```

4.1.28 rename

Priv Exec Command

Renames a file in the existing filesystem

Syntax

```
rename FILE FILE
```

Parameters

FILE	Specifies the file to rename

Example

```
WS5100#rename flash:/TestDIR/ NewTestDir
WS5100#DIR
Directory of flash:/

  drwx   1024      Wed Jul 19 19:14:05 2006   hotspot
  drwx   120       Wed Aug 30 15:32:44 2006   log
  drwx   1024      Thu Aug 31 23:50:09 2006   crashinfo
  -rw-   14271     Tue Jul 25 15:16:41 2006   Radius-config
  -rw-   14271     Wed Jul 26 15:42:08 2006   flash:
  drwx   1024      Wed Aug  9 17:35:08 2006   radius
  -rw-   3426      Wed Jul 26 16:08:02 2006   running-config-new
  -rw-   13163     Wed Jul 26 16:08:42 2006   radius-config
  -rw-   80898     Thu Aug 17 14:59:39 2006   cli_commands.txt
  -rw-   65015     Fri Aug 11 19:57:37 2006
cli_commands.txtli_commands.txt
  -rw-   65154     Thu Aug 17 15:11:23 2006   cli_commands_180B.txt
  -rw-   32        Sat Sep  2 00:15:38 2006   cli_commands.save
  drwx   1024      Sat Sep  2 00:31:24 2006   NewTestDir

WS5100#
```

4.1.29 rmdir

Priv Exec Command

Deletes an existing file from the file system

Syntax

```
rmdir DIR
```

Parameters

DIR	Name of the directory to delete

Example

```
WS5100#rmdir flash:/NewTestDir/
WS5100#DIR
Directory of flash:/

  drwx   1024      Wed Jul 19 19:14:05 2006   hotspot
  drwx   120       Wed Aug 30 15:32:44 2006   log
  drwx   1024      Thu Aug 31 23:50:09 2006   crashinfo
  -rw-   14271     Tue Jul 25 15:16:41 2006   Radius-config
  -rw-   14271     Wed Jul 26 15:42:08 2006   flash:
  drwx   1024      Wed Aug  9 17:35:08 2006   radius
  -rw-   3426      Wed Jul 26 16:08:02 2006   running-config-new
  -rw-   13163     Wed Jul 26 16:08:42 2006   radius-config
  -rw-   80898     Thu Aug 17 14:59:39 2006   cli_commands.txt
  -rw-   65015     Fri Aug 11 19:57:37 2006
cli_commands.txtli_commands.txt
  -rw-   65154     Thu Aug 17 15:11:23 2006   cli_commands_180B.txt
  -rw-   32        Sat Sep  2 00:15:38 2006   cli_commands.save
```

4.1.30 telnet

Priv Exec Command

Opens a telnet session

Syntax

```
telnet WORD (PORT|)
```

Parameters

WORD	IP address or hostname of the remote system

Example

```
WS5100#telnet 157.111.222.33

Entering character mode
Escape character is '^]'.

Red Hat Linux release 9 (Shrike)
Kernel 2.4.20-6bigmem on an i686
login: cli
Password:
```

4.1.31 terminal

Priv Exec Command

Sets the length/number of lines displayed on the terminal

Syntax

```
terminal[length <0-512>|no(length <0-512>|width)|width <0-512> ]
```

Parameters

length	Sets the number of lines on a screen
no	Negates a command or sets its defaults
width	Sets the width/number of characters on a screen line

Example

```
WS5100>terminal length 100
WS5100>

WS5100>terminal width 200
WS5100>
```

4.1.32 traceroute

Priv Exec Command

Traces a route to a destination

Syntax

```
traceroute (WORD | ip WORD)
```

Parameters

WORD	Traces a route to a destination address or hostname
ip	IP trace

Example

```
WS5100#traceroute 157.222.333.33
traceroute to 157.235.208.39 (157.235.208.39), 30 hops max, 38 byte
packets
 1  157.235.208.39 (157.235.208.39)  0.466 ms  0.363 ms  0.226 ms
WS5100#
```

4.1.33 upgrade

Priv Exec Command

Upgrades the software image.

Syntax

```
upgrade URL (background|)
```

Parameters

URL	Location of target firmware image to be used in upgrade

Example

```
WS5100#upgrade tftp://157.235.208.105:/img
var2 is 10 percent full
/tmp is 2 percent full
Free Memory 161896 kB
FWU invoked via Linux shell
Running from partition /dev/hda5, partition to

update is /dev/hda6
Reading image file header
```

```
Removing other partition
Sep 08 15:57:18 2006: %KERN-6-INFO: EXT3 FS on

hda1, internal journal.
Making file system
Extracting files (this can take some time).Sep

08 15:57:23 2006: %KERN-6-INFO:
kjournald starting.  Commit interval 5 seconds.
Sep 08 15:57:23 2006: %KERN-6-INFO: EXT3 FS on

hda6, internal journal.
Sep 08 15:57:23 2006: %KERN-6-INFO: EXT3-fs:

mounted filesystem with ordered
data mode..
.......................
Sep 08 15:58:17 2006: %DIAG-4-CPULOAD: One

minute average load limit exceeded,
value is 100.00% limit is 99.90% (top process
kernel/ISR 100.00%)
Sep 08 15:58:44 2006: %PM-4-PROCNORESP: Process

"logd" is not responding
Sep 08 15:58:44 2006: %PM-4-PROCNORESP: Process

"logd" is not responding
Sep 08 15:58:44 2006: %PM-4-PROCNORESP: Process

"logd" is not responding
Sep 08 15:58:44 2006: %PM-4-PROCNORESP: Process

"logd" is not responding
Version of firmware update file is 3.0.0.0-

19193X
Sep 08 15:58:44 2006: %KERN-6-INFO: EXT3 FS on

hda1, internal journal.
Creating LILO files
Running LILO
Successful
Sep 08 15:58:46 2006: %FWU-6-FWUDONE: Firmware

update successful, new version
is 3.0.0.0-19193X
WS5100#
```

4.1.34 upgradeabort

Priv Exec Command

Aborts an ongoing upgrade process

Syntax

```
upgrade-abort
```

Parameters

None

Example

```
WS5100#
```

4.1.35 write

Priv Exec Command

Writes the running configuration to memory or a terminal

Syntax

```
write [memory | terminal]
```

Parameters

memory	Writes to NV memory
terminal	Writes to terminal

Example

```
WS5100#write terminal
!
! configuration of WS5100 version 3.0.0.0-200B!
version 1.0
!
service prompt crash-info
!
username admin password 1 8e67bb26b358e2ed20fe552ed6fb832f397a507d
username admin privilege  superuser
username operator password 1
fe96dd39756ac41b74283a9292652d366d73931f
username manager password 1
45b27d6483fc630981ad5096ff26a7956ce0c038
username manager privilege  superuser
```

```
!
!no country-code
logging console 7
no logging on
fallback enable
ftp password 1 810a25d76c31e495cc070bdf42e076f7c9b0a1cd
ip http server
ip http secure-trustpoint local
ip http secure-server
ip ssh
ip telnet
snmp-server manager v2
snmp-server manager v3
crypto isakmp identity address
crypto isakmp keepalive 10
crypto ipsec security-association lifetime kilobytes 4608000
!.....................................
```

5

Global Configuration Commands

The term global is used to indicate characteristics or features effecting the system as a whole. Use the Global configuration mode to configure the system globally, or enter specific configuration modes to configure specific elements (such as interfaces or protocols). Use the configure terminal command (under PRIV EXEC) to enter the global configuration mode.

The example below describes the process of entering global configuration mode from privileged EXEC mode:

```
WS5100# configure terminal

WS5100(config)#
```

NOTE: The system prompt changes to indicate you are now in global configuration mode. The prompt for global configuration mode consists of the device host name followed by (config) and the pound sign (#).

Commands entered in the global configuration mode update the running configuration file as soon as they are entered. However, these changes are not saved in the startup configuration file until a *copy running-config startup-config* EXEC command is issued.

5.1 Global Configuration Commands

Table 5.1 summarizes the Global Config commands

Table 5.1 Global Config Mode Command Summary

Command	Description	Ref.
aaa	Configures the current authentication, authorization and accounting (aaa) login settings	page 5-4
access-list	Adds an access list entry	page 5-5
autoinstall	Autoinstalls a configuration command	page 5-11
banner	Defines a login banner	page 5-12
boot	Reboots the switch	page 5-13
bridge	Displays bridge group commands	page 5-13
clrscr	Clears the display screen	page 2-2
country-code	Configures the country of operation. All existing radio configuration will be erased	page 5-14
crypto	Defines encryption parameters	page 5-16
do	Runs commands from the EXEC mode	page 5-23
end	Ends the current mode and moves to the EXEC mode.	page 5-23
errdisable	errdisable	page 5-24
exit	Ends the current mode and moves to the previous mode	page 2-2
fallback	Configures the software fallback feature	page 5-25
ftp	Configures FTP server parameters	page 5-25
help	Describes the interactive help system	page 2-2
hostname	Sets the system's network name	page 5-26
interface	Defines an interface to configure	page 5-26

Table 5.1 Global Config Mode Command Summary

Command	Description	Ref.
ip	Internet Protocol (IP)	*page 5-27*
license	Sets license management commands	*page 5-32*
line	Configures a terminal line	*page 5-33*
local	Sets the username and password for local user authentication.	*page 5-33*
logging	Modifies message logging facilities	*page 5-34*
mac	Configures MAC access-lists	*page 5-35*
mac-address-table	Configures MAC address table	*page 5-36*
management	Sets properties of the management interface	*page 5-37*
no	Negates a command or set its defaults	*page 2-4*
ntp	Configures NTP parameters	*page 5-37*
prompt	Sets the system prompt	*page 5-41*
radius-server	Enters the RADIUS server mode	*page 5-41*
redundancy	Configures redundancy group parameters	*page 5-42*
service	Service commands	*page 5-44*
snmp-server	Modifies SNMP engine parameters	*page 5-45*
sole	Configures location engine parameters	*page 5-55*
spanning-tree	Configures spanning tree commands	*page 5-56*
timezone	Configures the timezone	*page 5-60*
username	Establishes user name authentication	*page 5-60*
vpn	Defines the VPN configuration	*page 5-61*

Table 5.1 Global Config Mode Command Summary

Command	Description	Ref.
wireless	Configures wireless parameters	*page 5-61*
wlan-acl	Apply an ACL on WLAN	*page 5-62*

5.1.1 aaa

Global Configuration Commands

Configures the current authentication, authorization and accounting (aaa) login settings.

Syntax

```
aaa [authentication(login(default(local|none|radius)))|nas|
vpn-authentication(primary(A.B.C.D))|secondary(A.B.C.D))]

aaa authentication login default {none|{local|radius}}
aaa nas WORD
aaa vpn-authentication (primary|secondary) A.B.C.D key  WORD
(authport PORT_RANGE |)
```

Parameters

authentication	Authentication configuration parameters
login	Sets the authentication lists for login
default	Defines the default authentication list
local	Sets the local user database
none	No authentication
radius	Defines an external RADIUS server
nas	NAS identifier. This parameter accepts a string of 64 characters
vpn-authentication	VPN authentication using RADIUS
primary	Defines the primary address
secondary	Defines the secondary address

A.B.C.D	IP address

Usage Guidelines

Use an AAA login to determine whether management user authentication must be performed against a local user database or an external RADIUS server

5.1.2 access-list

Global Configuration Commands

Adds an access list entry. Use the access list command (under global configuration) to configure the access list mechanism for filtering frames by protocol type or vendor code

Syntax

```
access-list
```

For Standard IP ACL's:

```
access-list (<1-99>|<1300-1999>) (deny|permit|mark (8021p <0-7> | tos
<0-255>))(A.B.C.D/M | host A.B.C.D | any)(log) (rule-precedence <1-
5000>)
```

For Extended IP ACL's:

```
access-list (<100-199>|<2000-2699>) {deny | permit | mark {dot1p <0-
7> | tos <0-255>}} {ip} {source/source-mask | host source | any }
{destination/destination-mask  | host destination | any } [log] [rule-
precedence access-list-entry precedence]
```

```
access-list (<100-199>|<2000-2699>) {deny | permit | mark {dot1p <0-
7> | tos <0-255>}} {icmp} {source/source-mask | host source | any}
{destination/ destination-mask | host destination | any} [icmp-type |
[icmp-type icmp-code]] [log] [rule-precedence access-list-entry
precedence]
```

```
access-list (<100-199>|<2000-2699>) {deny | permit | mark {dot1p <0-
7> | tos <0-255>}} {tcp|udp} {source/source-mask | host source | any}
[operator source-port] {destination/destination-mask | host
destination | any} [operator destination-port] [log]
[rule-precedence |access-list-entry precedence]
```

NOTE Using `access-list [<100-199>|<2000-2699>]` moves you to the **`(config-ext-nacl)`** instance. For additional information, see *Extended ACL Instance on page 14-1*.

Using `access-list [<1-99>|<1300-1999>]` moves you to the **`(config-std-nacl)`** instance. For additional information, see *Standard ACL Instance on page 15-1*.

To create a named ACL, use `ip access-lsit` (Standard/Extended). For more information, check *ip on page 5-27*.

Parameters

access-list (<1-99>|<1300-1999>) (deny|permit|mark (8021p <0-7> | tos <0-255>)) (A.B.C.D/M | host A.B.C.D | any)(log) (rule-precedence <1-5000>)	Adds a standard access list entry. • (<1-99>|<1300-1999>) – Defines access numbers from 1 to 99 or 1300 to 1999 • (deny|permit|mark) – Defines action types on an ACL. The action type `mark` is functional only over a Port ACL • 8021p <0-7> – Used only with the action type `mark` to specify 8021p priority values • tos <0-255> – Used only with the action type `mark` to specify *type of service* (tos) values • (A.B.C.D/M | host A.B.C.D | any) – Source is the source address of the network or host in dotted decimal. Source-mask is the network mask. For example, 10.1.1.10/24 indicates the first 24 bits of the source IP are used for matching • The keyword **any** is an abbreviation for a source IP of 0.0.0.0 and source-mask bits equal to 0 • The keyword **host** is an abbreviation for exact source (A.B.C.D) and source-mask bits equal to 32 • log – Generates log messages when the packet coming from the interface matches the ACL entry. Log messages are generated only for router ACL's • (rule-precedence <1-5000>) – Define an Integer value between 1-5000. This value sets the rule precedence in the ACL

access-list (<100-199>|<2000-2699>) {deny | permit | mark {dot1p <0-7> | tos <0-255>}} {**ip**} {source/source-mask | host source | any } {destination/destination-mask | host destination | any } [log] [rule-precedence access-list-entry precedence]	Adds an extended IP access list entry using **IP** keyword • <100-199>|<2000-2699> – For IP type of extended ACL, the ACL number must be between 100-199 • {deny | permit | mark {dot1p <0-7> | tos <0-255>}} – Defines the action type for an ACL. The action type `mark` is functional only over a Port ACL • 8021p <0-7> – Use only with the action type `mark` to specify 8021p priority values • tos <0-255> – Use only with action type `mark` to specify *type Of service* (tos) values • {**ip**} – Specif an IP (to match any protocol) • {source/source-mask | host source | any } – The source is the address of the network or host in dotted decimal. Source-mask is the network mask. For example, 10.1.1.10/24 indicates the first 24 bits of the source IP are used for matching • The keyword **any** is an abbreviation for source IP of 0.0.0.0 and source-mask bits equal to 0 • The keyword **host** is an abbreviation for exact source (A.B.C.D) and source-mask bits equal to 32 • {destination/destination-mask | host destination | any } – Sets the destination host IP address or destination network address • [log] – Generates log messages when the packet coming from the interface matches the ACL entry. Log messages are generated only for router ACL's • [rule-precedence access-list-entry precedence] – Define an integer value between 1-5000. This value sets the rule precedence in the ACL

access-list (<100-199>|<2000-2699>) {deny | permit | mark {dot1p <0-7> | tos <0-255>}} {**icmp**} {source/source-mask | host source | any} {destination/ destination-mask | host destination | any} [icmp-type | [icmp-type icmp-code]] [log] [rule-precedence access-list-entry precedence]	Adds an Extended IP access list entry using an **icmp** keyword. • (<100-199>|<2000-2699>) – For ICMP extended ACLs, the ACL must be between 2000-2699 • {deny | permit | mark {dot1p <0-7> | tos <0-255>}} – Defines the action on an ACL. The action type `mark` is functional only over a Port ACL • {**icmp**} – Specifies ICMP as the protocol • {source/source-mask | host source | any} – Source is the source address of the network or host in dotted decimal. Source-mask is the network mask. For example, 10.1.1.10/24 indicates the first 24 bits of the source IP are used for matching • The keyword **any** is an abbreviation for source an IP of 0.0.0.0 and source-mask bits equal to 0 • The keyword **host** is an abbreviation for exact source (A.B.C.D) and source-mask bits equal to 32 • {destination/ destination-mask | host destination | any} – Sets the destination host IP address or destination network address • [icmp-type |icmp-type icmp-code] – **ICMP type** value from 0 - 255. Valid only for protocol type icmp. **ICMP code** value from 0 - 255. Valid only for a protocol type of ICMP • [log] – Generates log messages when the packet coming from the interface matches the ACL entry. Log messages are generated only for router ACL's • [rule-precedence access-list-entry precedence] – Define an integer value between 1-5000. This value sets the rule precedence in the ACL

Use an access list command under the global configuration to create an access list. The switch supports port, router and WLAN ACL's.

- When the access list is applied on an Ethernet port, it becomes a port ACL
- When the access list is applied on a VLAN interface, it becomes a router ACL
- When the access list is applied on a WLAN index, it becomes a WLAN ACL

A MAC access list (to allow arp), is mandatory for both port and WLAN ACL's. For more information on how to configure a MAC access list, see *permit on page 16-9*.

Example

The example below creates a standard access list (ACL) to permit any traffic coming to the interface:

```
WS5100(config)#access-list 1 permit any
WS5100(config)#
```

The example below creates a extended IP access list to permit IP traffic between two networks:

```
WS5100(config)#access-list 101 permit ip 192.168.1.0/24
192.168.2.0/24

WS5100(config)#
```

The example below creates a extended access list to permit tcp traffic, between two networks, with destination port range between 20 and 23:

```
WS5100(config)#access-list 101 permit tcp 192.168.1.0/24
192.168.2.0/24 range 20 23
WS5100(config)#
```

The example below denies icmp traffic from any source to any destination:

```
WS5100(config)#access-list 115 deny icmp any any
WS5100(config)#access-list 115 permit ip any any
WS5100(config)#
```

5.1.3 autoinstall

Global Configuration Commands

Autoinstalls the switch image.

Syntax

```
autoinstall [clear-config-history|cluster-
config|config|image|start]
autoinstall (cluster-config|config|image) (URL[tftp|ftp|http|cf])

autoinstall image version <number>
```

Parameters

clear-config-history	Autoinstalls a clear configuration history, resulting in a reversion
cluster-config	Autoinstalls a cluster-config setup
config	Autoinstalls a config setup
image <*version number*>	Autoinstalls the image setup. • Version number – The version number cannot be the same as the currently installed version number. Attempting to install the same version results in an unsuccessful download
start	Starts the autoinstall sequence

Example

```
WS5100(config)#autoinstall clear-config-history
WS5100(config)#
```

5.1.4 banner

Global Configuration Commands

Defines a login banner for the switch

Syntax

```
banner(motd(LINE|default))
```

Parameters

motd	Sets the message of the day banner
LINE	Defrine a custom MOTD string
default	Sets a default MOTD string

Example

```
WS5100(config)#banner motd Welcome to my WS5100 CLI
WS5100(config)

WS5100 release 3.0.2.0-003B
Login as 'cli' to access CLI.
WS5100 login: cli
Welcome to my WS5100 CLI
Welcome to my WS5100 CLI
WS5100>

WS5100(config)#banner motd default
WS5100(config)#

WS5100 release 3.0.2.0-003B
Login as 'cli' to access CLI.
WS5100 login: cli
Welcome to CLI
Welcome to CLI

WS5100>
```

5.1.5 boot

Global Configuration Commands

Reboots the switch with an image in the mentioned partition (either the primary or secondary partition)

Syntax

```
boot(system) [primary|secondary]
```

Parameters

system	Specifies the boot image used after reboot
primary	Specifies the primary image
secondary	Specifies the secondary image

Example

```
WS5100(config)#boot system primary
Wireless switch will be rebooted, do you want to continue? (y/n):y
Do you want to save the configuration? (y/n):y

The system is going down NOW !!

% Connection is closed by administrator!
Please stand by while rebooting the system.
```

5.1.6 bridge

Global Configuration Commands

Configures bridge specific commands

Syntax

```
bridge(multiple-spanning-tree)(enable)
```

Parameters

multiple-spanning-tree (enable)	Enables *Multiple Spanning Tree Protocol* (MSTP) commands

Usage Guidelines

Enables or disables MSTP globally. Use a `no` command with the bridge-forward parameter to disable MSTP and change all ports to a forwarding state

Example

```
WS5100(config)#bridge multiple-spanning-tree enable
WS5100(config)#
```

5.1.7 country-code

Global Configuration Commands

Sets the country of operation.

Syntax

```
country-code
```

Parameters

None.

Usage Guidelines

Erases all existing radio configuration.

Example

```
WS5100(config)#country-code ?
  ae  United Arab Emirates
  ar  Argentina
  at  Austria
  au  Australia
  ba  Bosnia Herzegovina
  be  Belgium
  bg  Bulgaria
  bh  Bahrain
  bm  Bermuda
  br  Brazil
  bs  Bahamas
  by  Belarus
  ca  Canada
  ch  Switzerland
  cl  Chile
  cn  China
  co  Colombia
  cr  Costa Rica
  cy  Cyprus
  cz  Czech Republic
  de  Germany
```

```
dk  Denmark
do  Dominican Republic
ec  Ecuador
ee  Estonia
eg  Egypt
es  Spain
fi  Finland
fr  France
gb  United Kingdom
gr  Greece
gt  Guatemala
gu  Guam
hk  Hong Kong
hn  Honduras
hr  Croatia
ht  Haiti
hu  Hungary
id  Indonesia
ie  Ireland
il  Israel
in  India
is  Iceland
it  Italy
jo  Jordan
jp  Japan
kr  South Korea
kw  Kuwait
kz  Kazakhstan
li  Liechtenstein
lk  Sri Lanka
lt  Lithuania
lu  Luxembourg
lv  Latvia
ma  Morocco
mt  Malta
mx  Mexico
my  Malaysia
nl  Netherlands
no  Norway
nz  New Zealand
om  Oman
pe  Peru
ph  Philippines
pk  Pakistan
pl  Poland
pt  Portugal
qa  Qatar
ro  Romania
ru  Russia
```

```
  sa  Saudi Arabia
  se  Sweden
  sg  Singapore
  si  Slovenia
  sk  Slovak Republic
  th  Thailand
  tr  Turkey
  tw  Taiwan
  ua  Ukraine
  us  United States
  uy  Uruguay
  ve  Venezuela
  vn  Vietnam
  za  South Africa
WS5100(config)#country-code
```

5.1.8 crypto

- *Global Configuration Commands*

NOTE: `crypto isakmp(policy)Priority` moves you to the `config-crypto-isakmp` instance. For more information, see *crypto-isakmp on page 6-1*.

`crypto isakmp(`*`client`*`)` **`configuration group default`** moves you to the `config-crypto-group` instance. For more details see *crypto-group on page 7-1*.

`crypto isakmp(`*`peer`*`)` **`IP Address`** moves you to the `config-crypto-peer` instance. For more details see *crypto-peer on page 8-1*.

`crypto ipsec` **`transformset`** `(name) <value>` leads you to config-`crypto-ipsec`. Use the crypto ipsec transform-set command to define the transform configuration for securing data (for example, esp-3des, esp-sha-hmac, etc.). The transform-set is assigned to a crypto map using the map's set transform-set command. For more details see *crypto-ipsec on page 9-1*.

`crypto pki trustpoint` mode leads to the `config-trustpoint)` instance. For more details see *crypto-trustpoint Instance on page 11-1*.

Syntax

```
crypto(ipsec|isakmp|key|map|pki)

crypto ipsec(security-association|transform-set)
crypto ipsec security-association lifetime(kilobyte|Seconds)WORD
crypto ipsec transform-set(ah-md5-hmac|ah-sha-hmac|esp-3des|
esp-aes|esp-aes-192|esp-aes-256|esp-des|esp-md5-hmac|esp-sha-hmac)

crypto isakmp(client|identity|keepalive|key|peer|policy)
crypto isakmp client (configuration)(group)(default)
crypto isakmp(identity|keepalive|key|peer|policy)


crypto key(export|generate|import|zeroize)
crypto key (export|import)rsa<indentifier>(URL)(password)
crypto key generate(rsa <indentifier>)<key pair> <key pair>
crypto key zeroize (rsa <identifier>)

crypto map (map name)<sequence number> (isakmp|manual)dynamic

crypto pki(authenticate|enroll|export|import|trustpoint)
crypto pki authenticate <name> (terminal|URL)
crypto pki enroll<name> (request|self-signed)
crypto pki [import|export] <name> (request|trustpoint)(URL)
```

Parameters

ipsec (security-association| transform-set)	Configures IPSEC policies
	• security-association – Defines the security association parameter used to define its lifetime
	  • lifetime (kilobyte | seconds) – The lifetime of IPSEC security association. It can be defined in either:
	  kilobytes – Volume-based key duration. Minimum is 500 KB and maximum is 2147483646 KB
	  seconds – Time-based key duration. Minimum is 90 seconds and maximum is 2147483646 seconds
	• transform-set [set name] – Uses the crypto ipsec transform-set command to define the transform configuration for securing data
	  • ah-md5-hmac
	  • ah-sha-hmac
	  • esp-3des
	  • esp-aes
	  • esp-aes-192
	  • esp-aes-256
	  • esp-des
	  • esp-md5-hmac
	  • esp-sha-hmac
	The transform-set is then assigned to a crypto map using the map's set transform-set command. See *crypto-map on page 10-1*

isakmp [client|keepalive|key| peer|policy]	Configures the *Internet Security Association and Key Management Protocol* (ISAKMP) policy
	• client configuration (group) (default) – Leads to the config-cryptogroup instance
	For more details see *crypto-group on page 7-1*.
	• keepalive <10-3600> – Sets a keepalive interval for use with remote peers. It defines the number of seconds between DPD messages
	• key [0|2|word] [address|hostname] – Sets a pre-shared key for remote peer
	  • 0 – Password is specified UNENCRYPTED
	  • 2 – Password is encrypted with password-encryption secret
	  • WORD – User provided password
	  • address – Defines a shared key with an IP address.
	  • hostname – Defines the shared key with a hostname
	• peer [address|dn|hostname] – Sets the remote peer
	  • address – The IP address acts as an identity of the remote peer
	  • dn – The identity of the remote peer is the Distinguished Name
	  • hostname – The identity of the remote peer is the hostname.
	• policy <1-10000> – Sets a policy for an ISAKMP protection suite

key
[export|generate|import|
zeroize]
	Authentication key management functions
	• export rsa<name> URL [tftp|ftp] – Exports a keypair related configuration
	• generate rsa<name> <1024-2048> – Generates a keypair
	  • <1024-2048> – Size of keypair in bit
	• import rsa<name> URL [tftp|ftp] – Imports keypair related configuration
	• zeroize rsa<name> – Deletes a keypair
	• rsa<identifier> – RSA keypair identifier associated with keypair
	• URL – URL for sending the key to. It can be one of the following:
	  • tftp://<IP>/path/file (or)
	  • ftp://<user>:<passwd>@<IP>/path/file

map <name>
<sequence> [ipsec-
isakmp|
ipsec-manual] (dynamic)
	Enter a crypto map. For more details see *crypto-map on page 10-1*.
	• name <name> – Names the crypto map entry (not to exceed 32 characters)
	• <1-1000> – Sequence to insert into crypto map entry
	  • ipsec-isakmp – IPSEC w/ISAKMP
	  • ipsec-manual – IPSEC w/manual keying
	  • dynamic – Dynamic map entry (remote VPN configuration) for XAUTH with mode-config or ipsec-l2tp configuration

pki [authenticate|enroll| export|import|trustpoint]	Configures certificate parameters. The public key infrastructure is a protocol that creates encrypted public keys using digital certificates from certificate authorities. PKI ensures each online party is who they claim to be
	• authenticate <name> (terminal|tftp|ftp) – Defines the authenticate and import CA certificate
	• enroll <name> (request|self-signed) – Generates a certificate request or selfsigned certificate for the trustpoint
	• export <name> (request|trustpoint) (tftp|ftp) – Exports the trustpoint related configuraiton
	• import – Imports a trustpoint related configuration
	• trustpoint – Creates and configures a trustpoint.
	  • terminal – Copies and pastes enrollment mode.
	  • request – Certificate request mode of enrollment
	  • self-signed – Selfsigned mode of enrollment
	  • trustpoint – Trustpoint configuration

Usage Guidelines

Currently a peer address can be deleted with wrong isakmp value. Crypto currently matches only the IP address when a **no** command is issued

```
WS5100(config)#crypto isakmp key 12345678 address 4.4.4.4
```

```
WS5100(config)#show running-config
configuration of WS5100 version 3.0.0.0-200B!
version 1.0
!
service prompt crash-info
!
username admin password 1 8e67bb26b358e2ed20fe552ed6fb832f397a507d
username admin privilege  superuser
username operator password 1
fe96dd39756ac41b74283a9292652d366d73931f
username manager password 1
45b27d6483fc630981ad5096ff26a7956ce0c038
```

```
.........................................
.............................
crypto isakmp key 12345678 address 4.4.4.4
crypto ipsec security-association lifetime kilobytes 4608000
WS5100(config)#

WS5100(config)#no crypto isakmp key 12348 address 4.4.4.4
WS5100(config)#
```

In the example above, **key 12345678** is associated with IP **address 4.4.4.4**. Currently you can delete this key by using the no command and a wrong key number

Example

```
WS5100(config)#crypto pki ?
  authenticate  Authenticate and import CA Certificate
  enroll        Enroll
  export        Export
  import        Import
  trustpoint    Define a CA trustpoint

WS5100(config)#crypto pki trustpoint ?
  WORD  Trustpoint Name

WS5100(config)#crypto pki trustpoint Test
WS5100(config-trustpoint)#?
Trustpoint Config commands:
  clrscr        Clears the display screen
  company-name  Company Name(Applicable only for request)
  email         email
  end           End current mode and change to EXEC mode
  exit          End current mode and down to previous mode
  fqdn          Domain Name Configuration
  help          Description of the interactive help system
  ip-address    Internet Protocol (IP)
  no            Negate a command or set its defaults
  password      Challenge Password(Applicable only for request)
  rsakeypair    Rsa Keypair to associate with the trustpoint
  service       Service Commands
  show          Show running system information
  subject-name  Subject Name is a collection of required parameters
                to configure a trustpoint.

WS5100(config-trustpoint)#
```

5.1.9 do

Global Configuration Commands

Runs commands from either the User Exec or Priv Exec mode

Syntax

```
do (command of other mode)
```

Parameters

None.

Example

```
WS5100(config)#do ping 157.235.208.69
PING 157.235.208.69 (157.235.208.69): 100 data bytes
128 bytes from 157.235.208.69: icmp_seq=0 ttl=64 time=0.1 ms
128 bytes from 157.235.208.69: icmp_seq=1 ttl=64 time=0.0 ms
128 bytes from 157.235.208.69: icmp_seq=2 ttl=64 time=0.0 ms
128 bytes from 157.235.208.69: icmp_seq=3 ttl=64 time=0.0 ms
128 bytes from 157.235.208.69: icmp_seq=4 ttl=64 time=0.0 ms

--- 157.235.208.69 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.0/0.0/0.1 ms
WS5100(config)#
```

NOTE: In the example above, `ping` is a PRIV EXEC command.

5.1.10 end

Global Configuration Commands

Ends the current mode and changes to the EXEC mode.

Syntax

```
end
```

Parameters

None.

Example

```
WS5100(config)#end

WS5100#?
```

```
Priv Exec commands:
  acknowledge     Acknowledge alarms
  archive         Manage archive files
  autoinstall     autoinstall configuration command
  cd              Change current directory
  ........................................
  ........................................
```

5.1.11 errdisable

Global Configuration Commands

Enables the timeout mechanism for the por

Syntax

```
errdisable (recovery)[cause (bpduguard)|interval <10-1000000>]
```

Parameters

recovery	Enables the timeout mechanism for the port to be enabled back
cause (bpduguard)	Reason for errdisable • bpduguard – Recovers from errdisable due to bpduguard
interval <10-1000000>	Interval after which the port is enabled • <10-1000000> – Errdisable-timeout interval in seconds

Usage Guidelines

Use `no` command with `errdisable` parameter to the disable bridge timeout mechanism for the port

Example

```
WS5100(config)#errdisable recovery interval 100
WS5100(config)#

WS5100(config)#errdisable recovery cause bpduguard
WS5100(config)#

WS5100(config)#no errdisable recovery cause bpduguard
WS5100(config)#
```

5.1.12 fallback

Global Configuration Commands

Enables and configures the software fallback feature. Failure to boot with configured "use on boot" image allows booting with other image

Syntax

```
fallback(enable)
```

Parameters

enable	Enables the software fallback feature

Example

```
WS5100(config)#fallback enable
WS5100(config)#
```

5.1.13 ftp

Global Configuration Commands

Configures the switch as an FTP server

Syntax

```
ftp enable
ftp password(0|1|LINE)
ftp rootdir(DIR)
```

Parameters

enable	Enables FTP server
password	Configures the FTP password. Set the password using one of the following options: • 0 — Password is specified UNENCRYPTED. • 1 — Password is encrypted with SHA1 algorithm. • LINE — Password.
rootdir	Configures the FTP root dir. Set the ROOT directory location of the FTP server using: • DIR — Used to set root dir of the ftp server

Example

```
WS5100(config)#ftp enable
WS5100(config)#
```

5.1.14 hostname

Global Configuration Commands

Changes the system's network name

Syntax

`hostname(WORD)`

Parameters

WORD	Provide the name for the systems network

Example

```
WS5100(config)#hostname Eldorado
Eldorado(config)#
```

5.1.15 interface

Global Configuration Commands

Configures a selected interface. This command is used to enter the interface configuration mode for the specified physical *Switch Virtual Interface* (SVI) interface. If the VLANx (SVI) interface does not exist, it is automatically created

NOTE: The interface mode leads to the `config-if` instance. For more details see *interface Instance on page 12-1*. The prompt changes from `ws5100(config) #` to `ws5100(config-if)`

Syntax

`interface(IFNAME|eth <1-2>|vlan <1-4094>)`

Parameters

IFNAME	Defines the interface name
eth <1-2>	Defines the Ethernet interface

vlan <1-4094>	Defines the VLAN interface

Usage Guidelines

Use the `[no] interface {<interface-name>}` to delete the specified SVI. Valid interfaces include all VLANx interfaces.

Example

```
WS5100(config)#interface eth 2
WS5100(config-if)#

WS5100(config)#interface vlan 2
WS5100(config-if)#
```

5.1.16 ip

▸ *Global Configuration Commands*

Configures a selected Internet Protocol

NOTE: Using `access-list extended` moves you to the **`(config-ext-nacl)`** instance. For more information, see *Extended ACL Instance on page 14-1*.

Using `access-list extended` moves you to the **`(config-std-nacl)`** instance. For more information, see *Standard ACL Instance on page 15-1*.

Use an `ip dhcp pool (pool name)` command to move to the **`(config-dhcp)`** instance. For additional information, see *DHCP Server Instance on page 17-1*.

Syntax

```
ip(access-list|default-gateway|dhcp|domain-lookup|domain-
name|http|local|name-server|nat|route|routing|ssh|telnet)

ip(access-list(extended(<100-199|<2000-2699>|WORD)|standard(<1-
99>|<1300-1999>|WORD))

ip default-gateway(A.B.C.D)

ip dhcp(bootp|class|excluded-address|option|ping|pool|restart)
ip dhcp bootp(ignore)
```

```
ip dhcp class (class name)
ip dhcp excluded-address(A.B.C.D)
ip dhcp option(option name)
ip dhcp ping(timeout(<1-10>))
ip dhcp pool(pool name)

ip domain-lookup

ip domain-name(WORD)

ip http(secure-server|secure-trustpoint(WORD)|server(localhost))

ip local[pool(default{low-ip-address(A.B.C.D)})]

#ip name-server(A.B.C.D)

ip nat (inside|outside) [destination|source] static <A.B.C.D>
[<1-65535> (tcp|udp)|<A.B.C.D>]

ip route(A.B.C.D|A.B.C.D/M)<next-hop>

ip routing

ip ssh(port|rsa)
ip ssh(port(<0-65536>))
ip ssh(rsa(keypair-name(WORD)))

ip telnet(port(<0-65535>))
```

Parameters

access-list	Using the access list parameter options to enter the **`ext-nacl`** context and the **`std-nacl`** context. The prompt changes to the context entered • For more information, see *Extended ACL Instance on page 14-1* • For an extended ACL and *Standard ACL Instance on page 15-1* for standard ACL
default-gateway (A.B.C.D)	Configures the IP address of the default gateway • (A.B.C.D) – IP address of the next-hop router

dhcp	DHCP server configuration
	• bootp – Defines the BOOTP specific configuration
	  • ignore – Configures the DHCP server to ignore BOOTP requests
	• class – Defines a DHCP class and enters the DHCP class configuration mode
	  • WORD – DHCP class name
	• *excluded-address* – Prevents DHCP server from assigning certain addresses
	  • *A.B.C.D* – Low IP address
	• *option <name>* – Defines the DHCP servers' option name
	• *ping (timeout <1-10>)* – Specifies HDHCP servers' ping timeout in seconds
	• *pool <name>* – Configures the DHCP server's address pool
	For more information, see
	DHCP Server Instance on page 17-1

domain-lookup	Enables the DNS based name to address translation on the switch
domain-name	Sets the domain name for the switch.
http	*Hyper Text Transfer Protocol* (HTTP) • *secure-server – Sets* the *Secure HTTP Server* (HTTPS) • *secure-trustpoint* – Enter the name of the trustpoint used for secure connection • *server (localhost)* – HTTP server used only to serve requests from localhost
local	VPN local IP pool configuration • pool (default) – Specifies the address range for the default group tag • *low-ip-address (A.B.C.D)* – Specifies the Lowest range for IP address

name-server (A.B.C.D)	Specifies the DNS server for the DHCP client. A maximum of 6 name servers can be configured. Servers are tried in the order entered • *A.B.C.D* – IP address of DNS server.
nat	Defines *Network Address Translation* (NAT) values
(inside|outside) [destination|source] static <A.B.C.D> [<1-65535> (tcp|udp)|<A.B.C.D>]	• (inside|outside) – Specifies the inside/outside address translation • [destination|source] – Destination/source address translation. • static <A.B.C.D> – Specifies the static local (global mapping) for the inside local IP address • <1-65535> (tcp|udp) – Inside local Port. Select tcp or udp
route (<A.B.C.D>|< A.B.C.D/M >) <next-hop>	Adds a static route entry in the routing table • *A.B.C.D* – IP destination prefix. • *A.B.C.D/M* – IP destination prefix. • <next-hop> – IP address of the next hop used to reach the destination
routing	Turns on IP routing.
ssh	Secured Shell (SSH) server. • port <0-65535> – Listening port. Set between 0-65536 • rsa (keypair-name) – RSA encryption key used for confiuring RSA keypair
telnet (port) <0-65535>	Telnet server. • port <0-65535> – Defines the listening port ID. The value can be anything between 0-65535

Usage Guidelines 1

1. Use the `no` command along with ip to undo any IP based configuration.

   ```
   [no] ip(access-list|default-gateway|dhcp|domain-lookup|
   domain-name|http|local|name-server|nat|route|routing|ssh|telnet)
   ```

2. When using the `ip access-list` parameter, enter the following contexts:

   - ext-nacl – extended ACL. For more information, see *Extended ACL Instance on page 14-1*
   - std-nacl – Standard ACL. For more information, see *Standard ACL Instance on page 15-1*
   - dhcp – DHCP Server instance. For more information, see *DHCP Server Instance on page 17-1*
   - dhcpclass – DHCP User Class instance. For more information, see *DHCP Class Instance on page 18-1*
   - Clear the ip dhcp binding using the *clear* command

NOTE: To delete Standard/Extended and MAC ACL use **`no access-list <access-list name>`** under the Global Config mode.

Usage Guidelines 2

Follow the steps below to create a DHCP User Class:

1. Create a DHCP class named **`WS5100DHCPclass`**. WS5100 supports a maximum of 32 DHCP classes

   ```
   WS5100(config)#ip dhcp class WS5100DHCPclass
   WS5100(config-dhcpclass)#
   ```

2. Create a USER class named **`MC800`**. The privilege mode changes to `(config-dhcpclass)`. WS5100 supports a maximum of 8 Users classes per DHCP class

   ```
   WS5100(config)#ip dhcp class WS5100DHCPclass
   WS5100(config-dhcpclass)#
   ```

3. Create a Pool named **`WID`**, using `(config)#` mode

   ```
   WS5100(config)#ip dhcp pool WID
   WS5100(config-dhcp)#
   ```

4. Associate the DHCP class, created in Step 1 with the pool created in Step 3. The switch supports the association of only 8 CDHCP classes with a pool.

```
WS5100(config-dhcp)#class WS5100DHCPclass

WS5100(config-dhcp-class)#
```

5. The switch leads you to a new mode (config-dhcp-class). Use this mode to add address range to be used for the DHCP class, associated with the pool.

```
WS5100(config-dhcp-class)#address range 11.22.33.44
```

Example

```
WS5100(config)#ip access-list extended TestACL
WS5100(config-ext-nacl)#

WS5100(config)#ip access-list standard TestStdACL
WS5100(config-std-nacl)#

WS5100(config)#ip dhcp pool TestPool
WS5100(config-dhcp)#

WS5100(config)#ip dhcp class TestDHCPclass
WS5100(config-dhcpclass)#
```

5.1.17 license

▸ *Global Configuration Commands*

Display the details of the license

Syntax

```
license
```

Parameters

WORD	Enter the name of the feature for which you wish to add license

Example

```
WS5100(config)#show licenses
Serial Number 6283529900020
feature          license string                 license value  usage
  AP                                               48             4

WS5100(config)#
```

5.1.18 line

Global Configuration Commands

Configures the terminal line

Syntax

`line(console|vty)`

Parameters

console	Primary terminal line. Configure a value between 0-0
vty	Virtual terminal. Set a value between 0-871

5.1.19 local

Global Configuration Commands

Sets the username and password for local user authentication

Syntax

`local(username,password)`

Parameters

username	Define the local user name. The username can be a string of upto 64 characters
password	Define the local user password. The password can be a string of up to 21 characters

Example

```
WS5100(config)#local username "Noble Man" password "Noble Soul"
```

5.1.20 logging

Global Configuration Commands

Modifies message logging facilities

Syntax

```
logging(aggregation-
time|buffered|console|facility|host|monitor|on|syslog)

logging aggregation-time(<1-20>)

logging buffered(<0-
7>|alerts|critical|debugging|emergencies|errors|informational|
notifications|warnings)
```

Parameters

aggregation-time	Sets the number of seconds for aggregating repeated messages. The value can be configured between 1-60 seconds
buffered	Sets the buffered logging level
console	Sets the console logging level
monitor	Sets the terminal lines logging level
syslog	Sets the syslog servers logging level
<0-7>	Enter the Logging severity level. Can be between 0-7
alerts	Immediate action needed, (severity=1).
critical	Critical conditions, (severity=2)
debugging	Debugging messages, (severity=7)
emergencies	System is unusable, (severity=0)
errors	Error conditions, (severity=3)
informational	Informational messages, (severity=6)
notifications	Normal but significant conditions, (severity=5)
warnings	Warning conditions, (severity=4)

facility	Syslog facility in which log messages are sent
local0	Syslog facility local0
local1	Syslog facility local1
local2	Syslog facility local2
local3	Syslog facility local3
local4	Syslog facility local4
local5	Syslog facility local5
local6	Syslog facility local6
local7	Syslog facility local7
host	Configure remote host to receive log messages
A.B.C.D	Remote host's IP address
on	Enables the logging of system messages

Example

```
WS5100(config)#logging aggregation-time 20
WS5100(config)#
```

5.1.21 mac

▸ *Global Configuration Commands*

Configures MAC access lists

Syntax

```
mac(access-list(extended(WORD)))
```

Parameters

access-list	Defrines the ACL config for the MAC address
extended	MAC Extended ACL
WORD	Define the name of the ACL

Usage Guidelines

To delete Standard/Extended and MAC ACL, use **`no access-list <access-list name>`** under the Global Config mode.

Example

```
WS5100(config)#mac access-list extended Test1
WS5100(config-ext-macl)#
```

NOTE: By using the `ip access-list` parameter, enter the following contexts:

- .ext-macl — extended MAC ACL. For more details see *.Extended MAC ACL Instance on page 16-1*

5.1.22 mac-address-table

Global Configuration Commands

Configures the MAC address table.

Syntax

```
mac-address-table(aging-time)[0| <10-1000000>]
```

Parameters

aging-time [0|<10-1000000>]	The duration for which a learned mac address persists after the last update • 0 – Disables aging. • <10-1000000> – Sets the aging time in seconds.

Example

```
WS5100(config)#mac-address-table aging-time 100
WS5100(config)#
```

5.1.23 management

Global Configuration Commands

Sets management interface properties

Syntax

```
management(secure)
```

Parameters

secure	Limits local access (Web/Telnet etc.) to the management interface

Example

```
WS5100(config)#management secure
WS5100(config)#
```

5.1.24 ntp

Global Configuration Commands

Configure NTP values

Syntax

```
ntp(access-group|authenticate|authentication-key|autokey|
broadcast|broadcastdelay|master|peer|server|trusted-key)

ntp access-group(peer|query-only|serve|serve-only)
ntp access-group peer(<1-99>|<1300-1999>)
ntp access-group query-only(<1-99>|<1300-1999>)
ntp access-group serve(<1-99>|<1300-1999>)
ntp access-group serve-only(<1-99>|<1300-1999>)

ntp authenticate

ntp authentication-key(md5(WORD))

ntp autokey(client-only|host)

ntp broadcast(client|destination)
ntp broadcast destination(WORD(key|version))
ntp broadcast destination WORD key <1-65534>
ntp broadcast destination WORD version <1-4>

ntp broadcastdelay <1-999999>
```

```
ntp master <1-15>

ntp peer(WORD)
ntp peer WORD(autokey|key|prefer|version)
ntp peer WORD autokey(prefer|version<1-4>)
ntp peer WORD key(<1-65534>(prefer|version(<1-4>)))
ntp peer WORD prefer (version<1-4>)
ntp peer TestPeer version<1-4>

ntp server(WORD)
ntp server WORD(autokey|key|prefer|version)
ntp server WORD autokey(prefer|version<1-4>)
ntp server WORD key(<1-65534>(prefer|version(<1-4>)))
ntp server WORD prefer (version<1-4>)
ntp server TestPeer version<1-4>

ntp trusted-key <1-65534>
```

Parameters

access-group	Controls NTP access
peer	Provides full access
query-only	Allows only control queries
serve	Provides server and query access
serve-only	Provides only server access
<1-99>	Defines the standard IP access list
<1300-1999>	Standard IP access list (expanded range)
authenticate	Authenticates time sources
authentication-key	Defines the authentication key for trusted time sources.
md5	Sets MD5 authentication
WORD	Authentication key.
autokey	Enables the NTP autokey authentication scheme.
client-only	The switch is a client to other trusted-hosts in the autokey group

host	Configures the switch as a trusted host
broadcast	Configures the NTP broadcast service
client	Listens to NTP broadcasts
destination	Configures broadcast destination address
WORD	Define the destination broadcast IP address
key	Sets the broadcast key
<1-65534>	Defines the Key ID
version	Sets the NTP version
<1-4>	Sets the NTP Version number
broadcastdelay	Defines the estimated round-trip delay
<1-999999>	Sets the round-trip delay in microseconds
master	Acts as a NTP master clock
<1-15>	Sets teh stratum number for the NTP master clock
peer	Configures the NTP peer
server	Configures the NTP server
<Peer IP>	Sets the IP address of the peer only
autokey	Configures an autokey peer authentication scheme
key	Configures the peer authentication key
<1-65534>	Sets the peer key number
prefer	Prefer this peer when possible
version	Configures the NTP version
<1-4>	Sets the NTP version number
trusted-key	Key numbers for trusted time sources

<1-65534>	Define the Key number

Example

```
WS5100(config)#ntp peer ?
  WORD  Name/IP address of peer

WS5100(config)#ntp peer TestPeer ?
  autokey  Configure autokey peer authentication scheme
  key      Configure peer authentication key
  prefer   Prefer this peer when possible
  version  Configure NTP version
  <cr>

WS5100(config)#ntp peer TestPeer autokey ?
  prefer   Prefer this peer when possible
  version  Configure NTP version
  <cr>

WS5100(config)#ntp peer TestPeer autokey prefer ?
  version  Configure NTP version
  <cr>

WS5100(config)#ntp peer TestPeer autokey prefer version ?
  <1-4>  NTP version number

WS5100(config)#ntp peer TestPeer autokey prefer version 3
WS5100(config)#

WS5100(config)#ntp peer TestPeer key ?
  <1-65534>  Peer key number

WS5100(config)#ntp peer TestPeer key 20 ?
  prefer   Prefer this peer when possible
  version  Configure NTP version
  <cr>

WS5100(config)#ntp peer TestPeer key 20 prefer ?
  version  Configure NTP version
  <cr>

WS5100(config)#ntp peer TestPeer key 20 prefer version ?
  <1-4>  NTP version number

WS5100(config)#ntp peer TestPeer key 20 prefer version 2
Invalid server name "TestPeer" provided. Please enter a valid name
WS5100(config)#
```

5.1.25 prompt

Global Configuration Commands

Configures and sets the systems prompt

Syntax

```
prompt(LINE)
```

Parameters

LINE	Enter the new prompt displayed by the system

Example

```
WS5100(config)#prompt NobleMan
NobleMan
```

5.1.26 radius-server

Global Configuration Commands

Enters the RADIUS server mode. The system prompt changes from the default config mode to RADIUS server mode

NOTE: `radius-server` **`local`** mode moves you to the RADIUS server context. For more details see

Syntax

```
radius-server(host|key|local|retransmit|timeout)
radius-server host (A.B.C.D)
radius-server key(0|2| LINE)
radius-server local
radius-server retransmit <0-100>
radius-server timeout<1-1000>
```

Parameters

host	Specifies a RADIUS server
A.B.C.D	Defines the IP address of RADIUS server
key	Sets the Encryption key shared with the RADIUS servers

0	Password is specified UNENCRYPTED
2	Password is encrypted with password-encryption secret
LINE	Text of shared key, upto 127 characters
local	Configures local RADIUS server parameters.This takes you to a new **`config-radius-server`** context. Refer *Radius Server Instance* for more details
retransmit	Specifies the number of retries to active server
<0-100>	Number of retries for a transaction (default is 3)
timeout	Time to wait for a RADIUS server to reply
<1-1000>	Wait time (default 5 seconds)

Usage Guidelines

The RADIUS server host is used to configure RADIUS server details. These details are required for management user authentication if AAA authentication has been defined as RADIUS

Example

```
WS5100(config)#radius-server local
WS5100(config-radsrv)#
```

5.1.27 redundancy

▸ *Global Configuration Commands*

Configures redundancy group parameters

Syntax

```
redundancy [auto-revert (enable)|auto-revert-period <1-1800>|dhcp-
server (enable)|discovery-period <10-60>|enable|
group-id <1-65535>|handle-stp (enable)|heartbeat-period <1-255>|
hold-period <10-255>|interface-ip <IP Address>|
manual-revert|member-ip <IP address>|mode (primary|standby)]
```

Parameters

auto-revert (enable)	Enables auto-revert

auto-revert-period <1-1800>	Sets the redundancy auto-revert delay interval in minutes. The default is 5 minutes
dhcp-server (enable)	Enables the DHCP Redundancy protocol
discovery-period <10-60>	Sets the redundancy discovery interval in seconds. The default is 30 seconds
enable	Enables the redundancy protocol
group-id <1-65535>	Sets the cluster ID. The default cluster ID is 1
handle-stp (enable)	Delays the redundancy protocol state machine exec, considering STP
heartbeat-period <1-255>	Sets the redundancy heartbeat interval
hold-period <10-255>	Sets the redundancy hold interval
interface-ip <Switch IP>	Sets the redundancy interface IP address
manual-revert	Reverts standby to non-active mode
member-ip <Member IP>	Adds a member to this redundancy group
mode [primary|standby]	Sets the mode to either primary or standby

Example

```
WS5100(config)#redundancy discovery-period 20
WS5100(config)#

WS5100(config)#redundancy handle-stp enable
WS5100(config)#

WS5100(config)#redundancy heartbeat-period 20
WS5100(config)#

WS5100(config)#redundancy hold-period 25
WS5100(config)#

WS5100(config)#redundancy mode primary
WS5100(config)#
```

5.1.28 service

Global Configuration Commands

Use this command to retrieve system data (tables, log files, configuration, status and operation) for use in debugging and problem resolution. To view the `service` command of User Exec and Priv Exec Mode, refer to *service on page 2-5*.

Syntax

```
service(advanced-vty|dhcp|diag|password-encryption|
pm|prompt|radius|set|show|terminal-length|watchdog)
```

Parameters

advanced-vty	Enables advanced mode vty interface
dhcp	Enables the DHCP server service
diag	Services diag.
password-encryption	Encrypts passwords in configuration.
pm(max-sys-restarts| sys-restart)	Process Monitor. • max-sys-restarts – Maximum number of times PM will restart the system because of a failed processes. • sys-restart – Enable PM to restart the system when a processes fails. **Note:** The process restart is one count less than what is configured
prompt	Enables crash-info prompt
radius	Enables RADIUS server
set	Sets service parameters
show	Shows running system information
terminal-length	System wide terminal length configuration
watchdog	Enables service for watchdog

Example

```
WS5100(config)#service dhcp
WS5100(config)#

WS5100(config)#service radius restart
WS5100(config)#
```

5.1.29 snmp-server

▸ *Global Configuration Commands*

Modifies SNMP engine parameters

Syntax

```
snmp-
server(community|contact|enable|host|location|manager|sysname|user)
snmp-server community(WORD(ro|rw))
snmp-server contact LINE
snmp-server enable traps(all|dhcp-server|
diagnostics|miscellaneous|mobility|nsm|radius-server|
redundancy|snmp|wireless|wireless-statistics)

snmp-server enable traps all

snmp-server enable traps dhcp-server []

snmp-server enable traps disgnostics []

snmp-server enable traps miscellaneous
(caCertExpired|lowFsSpace|processMaxRestartsReached|savedConfigModi
fied|serverCertExpired)

snmp-server enable traps mobility []

snmp-server enable traps nsm dhcpIPChanged

snmp-server enable traps radius-server []

snmp-server enable traps redundancy
(adoptionExceeded|grpAuthLevelChanged|memberDown|memberMisConfigure
d| memberUp)

snmp-server enable traps snmp
(authenticationFail|coldstart|linkdown|linkup)

snmp-server enable traps wireless (ap-detection|ids|radio|
self-healing|station|wlan)
snmp-server enable traps wireless (ap-detection)
                              [externalAPDetected|externalAPRemoved]
```

```
snmp-server enable traps wireless (ids)
     [muExcessiveEvents|radioExcessiveEvents|switchExcessiveEvents]
snmp-server enable traps wireless (radio)
                          [adopted|detectedRadar|unadopted]
snmp-server enable traps wireless self-healing activated
snmp-server enable traps wireless station
           [associated|deniedAssociationAsPortCapacityReached|
            deniedAssociationOnCapability|deniedAssociationOnErr|
             deniedAssociationOnInvalidWPAWPA2IE|deniedAssociationO
             nRates|deniedAssociationOnSSID|deniedAssociationOnShor
             tPream|deniedAssociationOnSpectrum|deniedAuthenticatio
             n|disassociated|radiusAuthFailed|tkipCounterMeasures]
snmp-server enable traps wireless wlan [vlanUserLimitReached]

snmp-server enable traps wireless-statistics(mesh|min-packets|
mobile-unit|radio|wireless-switch|wlan)
snmp-server enable traps wireless-statistics mesh [avg-bit-speed-
less-than|avg-retry-greater-than|avg-signal-less-than|
gave-up-percent-greater-than|nu-percent-greater-than|
num-mobile-units-greater-than|pktsps-greater-than|
tput-greater-than|undecrypt-percent-greater-than]

snmp-server enable traps wireless-statistics min-packets <1-65535>

snmp-server enable traps wireless-statistics mobile-unit
(avg-bit-speed-less-than|avg-retry-greater-than|avg-signal-less-
than|gave-up-percent-greater-than|nu-percent-greater-than|
pktsps-greater-than|tput-greater-than|undecrypt-percent-greater-
than)

snmp-server enable traps wireless-statistics radio
(avg-bit-speed-less-than|avg-retry-greater-than|avg-noise-level-
threshold|avg-signal-less-than|gave-up-percent-greater-than|nu-
percent-greater-than|
num-mobile-units-greater-than|pktsps-greater-than|tput-greater-
than|undecrypt-percent-greater-than)
snmp-server enable traps wireless-statistics wireless-switch(num-
mobile-units-greater-than|pktsps-greater-than|tput-greater-than)

snmp-server enable traps wireless-statistics wlan
(avg-bit-speed-less-than|avg-retry-greater-than|avg-signal-less-
than|gave-up-percent-greater-than|nu-percent-greater-than|num-
mobile-units-greater-than|pktsps-greater-than|tput-greater-
than|undecrypt-percent-greater-than)

snmp-server host(A.B.C.D)
snmp-server location (LINE)
snmp-server manager(all|v2|v3)
snmp-server sysname

snmp-server user(snmpmanager|snmpoperator|snmptrap)
```

Parameters

community	Sets the community string and access privileges • *ro* – Read-only access with this community string. • *rw* – Read-write access with this community string.
contact	Text for mib object sysContact. • LINE – Sets the contact person for this managed node.
enable ( )	traps – Enables SNMP traps • all – Enables all traps • dhcp-server – Enables dhcp-server traps • diagnostics – Enables diagnostics traps • miscellaneous – Enables miscellaneous traps • mobility – Enables mobility traps • nsm – Enables nsm traps • radius-server – Enables radius-server traps • redundancy – Enables redundancy traps • snmp – Enables SNMP traps • wireless – Enables wireless traps • wireless-statistics – Modifies wireless-stats rate traps
enable (traps) dhcp-server ( )	Enables dhcp-server traps • dhcpServerDown – DHCP Server down • dhcpServerUp – DHCP Server up

enable (traps) diagnostics ( )	Enables diagnostics traps • cpuLoad15Min – Average CPU load for last 15 minutes exceeds limit • cpuLoad1Min • cpuLoad5Min • fanSpeedLow • fileDescriptors • ipRouteCache • packetBuffers • processMemoryUsage • ramFree • tempHigh • tempOver • usedKernelBuffer
enable (traps) miscellaneous ( )	Enables miscellaneous traps • caCertExpired – CA certificate has expired • lowFsSpace – Available file system space is lower than the limit • processMaxRestartsReached – Process has reached max restart • savedConfigModified – Saved configuration has been modified • serverCertExpired – Server certificate has expired
enable (traps) mobility ( )	Enable mobility traps. • operationallyDown – Mobility down • operationallyUp – Mobility up • peerDown – Mobility peer down • peerUp – Mobility peer up
enable (traps) nsm ()	Enables nsm traps. • dhcpIPChanged – DHCP IP changed

enable (traps) radius-server ()	Enables radius-server traps. • radiusServerDown – RADIUS server down • radiusServerUp – RADIUS server up
enable (traps) redundancy ( )	Enables redundancy traps • adoptionExceeded – Redundancy port adoption exceeded • grpAuthLevelChanged – Redundancy group Authorization Level changed • memberDown – Redundancy member down • memberMisConfigured – Redundancy member mis-configuration • memberUp – Defrines redundancy member as up
enable (traps) snmp ( )	Enables SNMP traps • authenticationFail – Enables authentication failure trap • coldstart – Enables coldStart trap • linkdown – Enables linkDown trap • linkup – Enables linkUp trap

enable (traps) wireless ( )	Enables wireless traps
	• ap-detection – Enables wireless AP detection traps
	  • externalAPDetected – External AP detected
	  • externalAPRemoved – External AP detected
	• ids – Enables wireless IDS traps.
	  • muExcessiveEvents – Excessive MU events
	  • radioExcessiveEvents – Excessive radio events
	  • switchExcessiveEvents – Excessive switch events
	• radio – Enables wireless radio traps
	  • adopted – Radio adopted
	  • detectedRadar – Radio detected radar
	  • unadopted – Radio detected radar
	• self-healing – Enables self healing traps
	  • activated – Self healing activated
	• station – Enables wireless station traps
	  • associated– Wireless station associated
	  • deniedAssociationAsPortCapacityReached – Wireless station denied association - port capacity reached
	  • deniedAssociationOnCapability – Wireless station denied association due to unsupported capability

	• deniedAssociationOnErr – Wireless station denied association due to internal error • deniedAssociationOnInvalidWPAWPA2 IE – Wireless station denied association due to invalid/absent WPA/WPA2 IE • deniedAssociationOnRates – Wireless station denied association due to incompatible Transmission rates • deniedAssociationOnSSID – Wireless station denied association due to invalid SSID • deniedAssociationOnShortPream – Wireless station denied association due to lack of short preamble support • deniedAssociationOnSpectrum – Wireless station denied association due to lack of spectrum management capability • deniedAuthentication – Wireless station denied 802.11 authentication • disassociated – Wireless station disassociated • tkipCounterMeasures – TKIP counter measures invoked • wlan – Enables wireless wlan traps. • vlanUserLimitReached – WALN/VLAN user limit reached

enable (traps) wireless-statistics ( )	Modifies wireless-stats rate traps • mesh – Modifies mesh rate traps • avg-bit-speed-less-than – Average bit speed in Mbps between <0.00> and <54.00> • avg-retry-greater-than – Average retry is greater than 0.00 and less than or equal to 16.00 • avg-signal-less-than – Average signal in dBm is less than -0.00 and greater than or equal to -120.00 • gave-up-percent-greater-than – Percentage of pkts dropped is greater than 0.00 and less than or equal to 100.00 • nu-percent-greater-than – Percentage of non-unicast pkts is greater than 0.00 and less than or equal to 100.00 • num-mobile-units-greater-than – Number of associated mobile-unit is <1-4096> • pktsps-greater-than – Packets per sec is greather than 0.00 and less than or equal to 100000.00 • tput-greater-than – Throughput in Mbps is greather than 0.00 and less than or equal to 100000.00 • undecrypt-percent-greater-than – Percentage of undecryptable pkts is geater than 0.00 and less than or equal to 100.00

	• min-packets – Minimum packets required for sending the trap
	  • <1-65535> – Defines the minimum packets for sending the trap. This can be set with a decimal number in the range of <1-65535>.
	• mobile-unit – Modifies mobile-unit rate traps.
	  • avg-bit-speed-less-than – Average bit speed in Mbps is between <0.00> and <54.00>
	  • avg-retry-greater-than – Average retry is greater than 0.00 and less than or equal to 16.00
	  • avg-signal-less-than – Average signal in dBm is less than -0.00 and greater than or equal to -120.00
	  • gave-up-percent-greater-than – Percentage of pkts dropped is greater than 0.00 and less than or equal to 100.00
	  • nu-percent-greater-than – Percentage of non-unicast pkts is greater than 0.00 and less than or equal to 100.00
	  • pktsps-greater-than – Packets per sec is greather than 0.00 and less than or equal to 100000.00
	  • tput-greater-than – Throughput in Mbps is greather than 0.00 and less than or equal to 100000.00
	  • undecrypt-percent-greater-than – Percentage of undecryptable pkts is geater than 0.00 and less than or equal to 100.00

	• tput-greater-than – Throughput in Mbps is greather than 0.00 and less than or equal to 100000.00 • undecrypt-percent-greater-than – Percentage of undecryptable pkts is geater than 0.00 and less than or equal to 100.00
host	SNMP server host. • A.B.C.D – SNMP server host IP-address
location	Text for mib object sysLocation.
manager	Enables the SNMP manager • all – Enables SNMP version v2 and v3 • v2 – Enables SNMP version v2 • v3 – Enables SNMP version v3
sysname	SNMP system name
user	Defines a user who can access SNMP engine • snmpmanager – Manager user • snmpoperator – Operator user • snmptrap – Trap user

Example

```
WS5100(config)#snmp-server community TestCommunity ro
WS5100(config)#

WS5100(config)#snmp-server contact TestManager
WS5100(config)#

WS5100(config)#snmp-server enable traps all
WS5100(config)#

WS5100(config)#snmp-server enable traps miscellaneous lowFsSpace
WS5100(config)#
WS5100(config)#snmp-server enable traps redundancy memberUp
```

```
WS5100(config)#

WS5100(config)#snmp-server enable traps snmp linkup
WS5100(config)#

WS5100(config)#snmp-server enable traps wireless  ap-detection
externalAPDetected
WS5100(config)#

WS5100(config)#snmp-server enable traps wireless  ids
excessiveProbes
WS5100(config)#

WS5100(config)#snmp-server enable traps wireless radio adopted
WS5100(config)#

WS5100(config)#snmp-server enable traps wireless self-healing
activated
WS5100(config)#

WS5100(config)#snmp-server enable traps wireless station
tkipCounterMeasures
WS5100(config)#

WS5100(config)#snmp-server enable traps wireless-statistics min-
packets 120
WS5100(config)#

WS5100(config)#snmp-server location "Located at thh 5th FLoor"
WS5100(config)#

WS5100(config)#snmp-server sysname "Gold Mine"
WS5100(config)#
```

5.1.30 sole

▸ Global Configuration Commands

Sets SOLE related configuration commands. This command leads you to the `(config-sole)#` instance. For more information on SOLE parameters, refer to *SOLE Instance on page 21-1*

Syntax

`sole`

Parameters

None.

Usage Guidelines

The SOLE command is used to enter the `config-sole` instance. The prompt changes from the regular `WS5100(config)#` to `WS5100(config-wireless)#`.

Example

```
WS5100(config)#sole
WS5100(config-sole)#
```

5.1.31 spanning-tree

▸ *Global Configuration Commands*

Configures spanning-tree commands

Syntax

```
spanning-tree [mst|portfast]

spanning-tree mst [<0-15> (priority <0-61440>)|
cisco-interoperability (enale|disable)|configuration|
forward-time <4-30>|hello-time <1-10>|max-age <6-40>|
max-hops <7-127>]

spanning-tree portfast [bpdufilter|bpduguard](default)
```

Parameters

mst [<0-15> (priority <0-61440>)| cisco-interoperability (enale|disable)| configuration| forward-time <4-30>| hello-time <1-10>| max-age <6-40>| max-hops <7-127>]	Enables the Multiple Spanning Tree Protocol on a bridge
	• <0-15> (priority <0-61440>) – Set the bridge priority for an MST instance to the value specified. Use the no parameter with this command to restore the default bridge priority value
	  • priority – Sets the bridge priority for the common instance
	  • <0-61440> – Define the bridge priority in increments of 4096 (Lower priority indicates greater likelihood of becoming root). The default value of the priority for each instance is 32768.
	• cisco-interoperability (enale|disable) – Enables/disables interoperability with Cisco's version of MSTP (incompatible with standard MSTP).
	  • enable – Enables CISCO Interoperability.
	  • disable – Disables CISCO Interoperability.
	• configuration – Multiple spanning tree configuration. This command moves to the *spanning tree-mst Instance on page 13-1*.
	• forward-time <4-30> – Sets the time (in seconds) after which (if this bridge is the root bridge) each port changes states to learning and forwarding. This value is used by all instances. The default value is 15 seconds
	• hello-time <1-10> – Sets the hello-time. The hello-time is the time (in seconds) after which (if this bridge is the root bridge) all the bridges in a bridged LAN exchange Bridge Protocol Data Units (BPDUs). A very low value leads to excessive traffic on the network, while a higher value delays the detection of a topology change. This value is used by all instances. The default value is 2 seconds.

	• max-age <6-40> – Max-age is the maximum time in seconds for which (if a bridge is the root bridge) a message is considered valid. This prevents the frames from looping indefinitely. The value of max-age must be greater than twice the value of hello time plus one, but less than twice the value of forward delay minus one The allowable range for max-age is 6-40 seconds. Configure this value sufficiently high, so a frame generated by root can be propagated to the leaf nodes without exceeding the max-age. Use this command to set the max-age for a bridge. This value is used by all instances.The default value of bridge max-age is `20` seconds. • max-hops <7-127> – Specifies the maximum allowed hops for a BPDU in an MST region. This parameter is used by all MST instances. To restore the default value, use the no parameter with this command. The default maxhops in a MST region is `20`.

portfast [bpdufilter|bpduguard] (default)	Enables the portfast feature on a bridge. It has the following options: • bpdufilter (default) – Use the `bpdu-filter` command to set the portfast BPDU filter for the port. Use the `no` parameter with this command to revert the port BPDU filter value to default The Spanning Tree Protocol sends BPDUs from all ports. Enabling the BPDU Filter feature ensures PortFastenabled ports do not transmit or receive BPDUs. • bpduguard (default) – Use the `bpdu-guard` command to enable the BPDU (Bridge Protocol Data Unit) Guard feature on a bridge. Use the `no` parameter with this command to disable BPDU Guard. When the BPDU Guard is set for a bridge, all portfast-enabled ports of the bridge that have BPDU guard set to default shut down the port on receiving a BPDU. In this case, the BPDU is not processed. The port can be brought back up manually (using the no shutdown command), or by configuring a errdisable-timeout to enable the port after the specified interval.

Usage Guidelines

The `mst > configuration` command moves you to the *spanning tree-mst Instance on page 13-1* Instance instance.

If a bridge does not hear bridge protocol data units (BPDUs) from the root bridge within the specified interval, defined in the max-age (seconds) parameter, assume the network has changed and recomputed the spanning-tree topology.

Generally, spanning tree configuration settings in config mode performs the configuration for bridge and bridge instances (for the switch).

Example

```
WS5100(config)#spanning-tree portfast bpduguard default
WS5100(config)#

WS5100(config)#spanning-tree mst configuration
WS5100(config-mst)#
```

5.1.32 timezone

Global Configuration Commands

Configure switch timezone settings

Syntax

```
timezone
```

Parameters

TIMEZONE	Press <tab> to traverse a list of files. This displays a list of files containing timezone information

Example

```
WS5100(config)#timezone
America/    Asia/      Atlantic/   Australia/  Etc/       Europe/
Pacific/    Africa/

WS5100(config)#timezone America/
America/Anchorage     America/Bogota        America/Buenos_Aires
America/Caracas       America/Chicago
America/Costa_Rica    America/Denver        America/Los_Angeles
America/Mexico_City   America/Montreal
America/New_York      America/Phoenix       America/Santiago
America/Sao_Paulo     America/St_Johns
America/Tegucigalpa   America/Thule         America/Winnipeg
America/Indianapolis

WS5100(config)#timezone America/Chicago
WS5100(config)#
```

5.1.33 username

Global Configuration Commands

Establishes user name authentication

Syntax

```
username
```

Parameters

WORD	Enter a name to authenticate the switch. The username should be between 1 and 28 characters

Example

```
WS5100(config)#username GoldenSwitch
WS5100(config)#
```

5.1.34 vpn

Global Configuration Commands

Configure VPN settings

Syntax

`vpn` **`authentication-method`**`(local|radius)`

Parameters

authentication-method	Selects the authenication scheme
local	Use this for user based authentication
radius	Use this for RADIUS server authentication

Usage Guidelines

Virtual Private Network (VPN) enables IP traffic to travel securely over a public TCP/IP network by encrypting all traffic from one network to another. A VPN uses "tunneling" to encrypt all information at the IP level

Example

5.1.35 wireless

Global Configuration Commands

Configures switch wireless parameters. This command moves you to the `config-wireless` instance. For more information, see *Wireless Instance on page 20-1*.

Syntax

`wireless`

Parameters

None

Usage Guidelines

The wireless command is used to enter the config-wireless instance wherein you can configure the WS5100 wireless parameters. You can confirm that you have entrered the wireless instance as the prompt changes from the the regular `WS5100(config)#` to `WS5100(config-wireless)#.`

Example

```
WS5100(config)#wireless
WS5100(config-wireless)#
```

5.1.36 wlan-acl

Global Configuration Commands

Use this command to apply an ACL on a WLAN index.

Syntax

```
wlan-acl [<1-32>{<1-99>|<100-199>|
<1300|1999>|<2000|2699>|word}][in|out]
```

Parameters

<1-32>[]	WLAN number. • <1-99> — IP standard access list. • <100-199> — IP extended access list. • <1300-1999> — IP standard access list (expanded range). • <2000-2699> — IP extended access list (expanded range). • WORD — Access list name.

Usage Guidelines 1

Every WLAN created is mapped to an index. When an ACL is applied on a WLAN index it becomes a WLAN ACL. The following type of ACL's can be applied on a WLAN:

- IP Standard ACL
- IP Extended ACL
- MAC Extended ACL

When a packet is send from a client to a WLAN index of an access port, it becomes an inbound traffic to the wireless LAN.

When a packet goes out of a access port, it becomes a outbound traffic to the wireless LAN index. Apply an ACL to a WLAN index in outbound direction to filter traffic from both wired and wireless interfaces.

`wlan-acl` can be attached both in the inbound and outbound directions.

NOTE: Most of the Wireless LAN related configuration are performed using the *Wireless Instance on page 20-1*.

Use `wlan-acl` (in the global configuration mode) to apply an ACL on a wireless LAN index .

The last ACE in the access list is an implict deny statement. Whenever the interface receives the packet, its content is checked against all the ACE's in the ACL. It is allowed/ denied based on the ACL configuration.

Usage Guidelines 2

Follow the procedure mentioned below to upgrade Wireless LAN ACL from 3.0/3.0.1 to 3.0.2 :

WLAN index in ACL rules are configurable in WS5100 3.0/3.0.1. In WS5100 3.0.2, WLAN is treated as a virtual port and the user has to create ACL rules without WLAN index and attach ACLs to WLAN port.

While upgrading from WS5100 3.0/3.0.1 to 3.0.2, the ACLs having WLAN index as selectors are replaced with ACLs without having any WLAN index selectors. After the completion of the upgrade, user has to apply those ACLs to WLAN port manually.

A sample ACL configuration in 3.0/3.0.1

- Standard IP access list 10

```
permit host 1.2.3.4 wlan 3 log rule-precedence 10
```

- Extended IP access list 110

```
deny icmp host 5.6.7.8 host 5.6.7.9 wlan 4 rule-precedence 10
deny icmp host 5.6.7.8 host 5.6.7.9 rule-precedence 20
```

- Extended IP access list extacl

```
permit icmp host 192.172.0.10 any wlan 12 rule-precedence 23
deny icmp any any rule-precedence 33
```

- Extended MAC access list macacl

```
permit any host 00:01:02:03:04:05 type ip wlan 14 rule-
precedence 11
permit host 00:01:03:04:07:08 any wlan 14 rule-precedence 21
permit any any wlan 14 rule-precedence 31
```

- Standard IP access list stdacl

```
permit any wlan 5 rule-precedence 34
permit host 10.0.0.10 wlan 6 rule-precedence 44
deny host 30.0.0.14 rule-precedence 54
```

After upgrade to 3.0.2 the configuration will look like

- Standard IP access list 10

```
permit host 1.2.3.4 log rule-precedence 10
```

- Extended IP access list 110

```
deny icmp host 5.6.7.8 host 5.6.7.9 rule-precedence 10
```

- Extended IP access list extacl

```
permit icmp host 192.172.0.10 any rule-precedence 23
deny icmp any any rule-precedence 33
```

- Extended MAC access list macacl

```
permit any host 00:01:02:03:04:05 type ip rule-precedence 11
permit host 00:01:03:04:07:08 any rule-precedence 21
permit any any rule-precedence 31
```

- Standard IP access list stdacl

```
permit any rule-precedence 34
permit host 10.0.0.10 rule-precedence 44
deny host 30.0.0.14 rule-precedence 54
```

NOTE: All ACLs which had WLAN index are now replaced with ones that don't have WLAN index.
In the above process, the acl "110" had two rules which got replaced by only one rule because after removal of WLAN index selector, both the rules look similar.

Follow the procedure mentioned below to manually upgrade the ACLs to the same configuration:

1. If all the rules in ACL have same WLAN index as **selector** and there are no other ACL rules then attach the ACL to the WLAN port.
   In the above example, the ACL "**macacl**" has two rules for WLAN 14 which can be attached to WLAN port as follows:

```
wlan-acl 14 macacl in
```

2. If ACL has mix of rules – with different WLAN indices and without an WLAN indices, then it should be grouped as follows.

   a. Create separate ACLs for all rules with a given WLAN index.

   b. Create separate ACLs for rules which do not have any WLAN index.

   To manually configure the Standard ACL, in the above example, it has to be split into 3 ACLs.

```
ip access-list standard stdacl1
permit any rule-precedence 34

ip access-list standard stdacl2
permit host 10.0.0.10 rule-precedence 44

ip access-list standard stdacl3
deny host 30.0.0.14 rule-precedence 54

no access-list stdacl

wlan-acl 5 stdacl1 in

wlan-acl 6 stdacl2 in
```

   The stdacl must be detached from the interface to which it was associated and stdacl3 must be attached to that interface.

When the user explicitly creates ACL rules with WLAN index as selector, the switch consumes that ACL without WLAN index selector. During this process a warning is raised to the user as mentioned in the example below.

```
WS5100(config)#access-list 14 permit any wlan 19 log
Warning : Acl rules with Wlan Index is deprecated. Wlan index
configured for the
rule will be ignored. Please use wlan-acl CLI to apply ACLs on WLAN
```

Example

The example below applies an ACL to WLAN index 200 in inbound direction from the global config mode.

```
WS5100(config)#wlan-acl 2 150 in
WS5100(config)#
```

NOTE: A MAC access list entry to allow `arp` is mandatory to apply an IP based ACL to an interface. MAC ACL always takes precedence over IP based ACL's.

The example below applies an ACL to WLAN index 200 in outbound direction from the global config mode.

```
WS5100(config)#wlan-acl 2 150 out
WS5100(config)#
```

6

crypto-isakmp

Use the `crypto isakmp policy(priority)` to initiate the `config-crypto-isakmp` instance.

6.1 Crypto ISAKMP Config Commands

Table 6.1 summarizes **`crypto-isakmp`** commands

Table 6.1 Crypto ISAKMP Command Summary

Command	*Description*	*Ref.*
authentication	Sets the authentication scheme	*page 6-2*
clrscr	Clears the display screen	*page 6-2*
encryption	Sets the encryption algorithm	*page 6-3*
end	Ends the current mode and moves to the EXEC mode	*page 6-3*
exit	Ends the current mode and moves to the previous mode	*page 6-4*
group	Sets the Diffie-Hellman group	*page 6-4*
hash	Sets the hash algorithm	*page 6-5*
help	Provides a desription of the interactive help system	*page 6-5*
lifetime	Sets the lifetime for the ISAKMP security association	*page 6-6*
no	Negates a command or sets its defaults	*page 6-6*

Table 6.1 Crypto ISAKMP Command Summary

Command	Description	Ref.
service	Defines the switch's service commands	*page 6-6*
show	Shows running system information	*page 6-7*

6.1.1 authentication

▸ *Crypto ISAKMP Config Commands*

Authenticates **rsa-sig** and **pre-share** keys

Syntax

```
authentication(pre-share|rsa-sig)
```

Parameters

pre-share	pre shared key
rsa-sig	rsa signature

Example

```
WS5100(config-crypto-isakmp)#authentication pre-share
WS5100(config-crypto-isakmp)#

WS5100(config-crypto-isakmp)#authentication rsa-sig
WS5100(config-crypto-isakmp)#
```

6.1.2 clrscr

▸ *Crypto ISAKMP Config Commands*

Clears the display screen

Syntax

```
clrscr
```

Parameters

None.

Example

```
WS5100(config-crypto-isakmp)#clr
WS5100(config-crypto-isakmp)#
```

6.1.3 encryption

Crypto ISAKMP Config Commands

Configures the encryption level of the data transmitted using using `crypto-isakmp` command

Syntax

`encryption(3des|aes|aes-192|aes-256|des)`

Parameters

3des	3des - Triple data encryption standard
aes	aes - advanced data encryption standard
aes-192	aes-192 - advanced data encryption standard
aes-256	aes-256 - advanced data encryption standard
des	des - data encryption standard

Example

```
WS5100(config-crypto-isakmp)#encryption 3des
WS5100(config-crypto-isakmp)#

WS5100(config-crypto-isakmp)#encryption aes-256
WS5100(config-crypto-isakmp)#
```

6.1.4 end

Crypto ISAKMP Config Commands

Ends and exits the current mode and changes to the PRIV EXEC mode. The prompt changes to `WS5100#`.

Syntax

`end`

Parameters

None.

Example

```
WS5100(config-crypto-isakmp))#end
WS5100#
```

6.1.5 exit

Crypto ISAKMP Config Commands

Ends the current mode and moves to the previous mode (GLOBAL-CONFIG). The prompt changes to `WS5100(config)#`.

Syntax

```
exit
```

Parameters

None.

Example

```
WS5100(config-crypto-isakmp)#exit
WS5100(config)#
```

6.1.6 group

Crypto ISAKMP Config Commands

Specifies the Diffie-Hellman group (1 or 2) used by this IKE policy to generate keys (which are then used to create the IPSec SA)

Syntax

```
group(1|2|5)
```

Parameters

1	768-bit mod P.
2	1024-bit mod P.
5	Diffie-Hellman group 5.

Usage Guidelines

The local IKE policy and the peer IKE policy must have matching group settings in order for negotiation to be successful.

Example

```
WS5100(config-crypto-isakmp)#group 5
WS5100(config-crypto-isakmp)#
```

6.1.7 hash

Crypto ISAKMP Config Commands

Specifies the hash algorithm used to authenticate data transmitted over the IKE SA

Syntax

`hash(md5|sha)`

Parameters

md5	Choose the md5 hash algorithm
sha	Choose the sha hash algorithm

Example

```
WS5100(config-crypto-isakmp)#hash sha
WS5100(config-crypto-isakmp)#
```

6.1.8 help

Crypto ISAKMP Config Commands

Accesses the system's interactive help system

Syntax

`help`

Parameters

None.

Example

```
WS5100(config-crypto-isakmp)#help
CLI provides advanced help feature.  When you need help,
anytime at the command line please press '?'.

If nothing matches, the help list will be empty and you must backup
until entering a '?' shows the available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each possible
   argument.
2. Partial help is provided when an abbreviated argument is entered
   and you want to know what arguments match the input
   (e.g. 'show ve?'.)
WS5100(config-crypto-isakmp)#
```

6.1.9 lifetime

▸ Crypto ISAKMP Config Commands

Specifies how long an IKE SA is valid before expiring

Syntax

```
lifetime <seconds>
```

Parameters

<seconds>	Specifies how many seconds an IKE SA lasts before expiring. A time stamp (in seconds) can be configured between 3600 and 2147483647.

Example

```
WS5100(config-crypto-isakmp)#lifetime 5200
WS5100(config-crypto-isakmp)#
```

6.1.10 no

▸ Crypto ISAKMP Config Commands

Negates a command or sets its defaults

Syntax

```
no [authentication|encryption|group|hash|lifetime]
```

Parameters

None.

Example

```
WS5100(config-crypto-isakmp)#no lifetime
WS5100(config-crypto-isakmp)#
```

6.1.11 service

▸ Crypto ISAKMP Config Commands

Invokes service commands to trobuleshoot or debug `(config-crypto-isakmp)` instance configurations

Syntax

```
service(show)(cli)
```

Parameters

cli	Displays the CLI tree of current mode

Example

```
WS5100(config-crypto-isakmp)#service show cli
Crypto Isakmp Config mode:
+-authentication
  +-pre-share [authentication ( rsa-sig | pre-share )]
  +-rsa-sig [authentication ( rsa-sig | pre-share )]
+-clrscr [clrscr]
+-do
  +-LINE [do LINE]
+-encryption
  +-3des [encryption ( des | 3des | aes | aes-192 | aes-256 )]
  +-aes [encryption ( des | 3des | aes | aes-192 | aes-256 )]
  +-aes-192 [encryption ( des | 3des | aes | aes-192 | aes-256 )]
  +-aes-256 [encryption ( des | 3des | aes | aes-192 | aes-256 )]
  +-des [encryption ( des | 3des | aes | aes-192 | aes-256 )]
+-end [end]
+-exit [exit]
+-group
  +-1 [group (1|2|5)]
  +-2 [group (1|2|5)]
  +-5 [group (1|2|5)]
+-hash
  +-md5 [hash (sha|md5)]
.................

WS5100(config-crypto-isakmp)#
```

6.1.12 show

▸ *Crypto ISAKMP Config Commands*

Use this command to view current system information running on the switch

Syntax

```
show <paramater>
```

Parameters

?	Displays all the parameters for which information can be viewed using the show command

Example

```
WS5100(config-crypto-isakmp)#show ?
  access-list           Internet Protocol (IP)
  aclstats              Show ACL Statistics information
  alarm-log             Display all alarms currently in the system
  autoinstall           autoinstall configuration
  banner                Display Message of the Day Login banner
  boot                  Display boot configuration.
  clock                 Display system clock
  commands              Show command lists
  crypto                encryption module
  debugging             Debugging information outputs
  dhcp                  DHCP Server Configuration
  environment           show environmental information
  file                  Display filesystem information
  ftp                   Display FTP Server configuration
  history               Display the session command history
  interfaces            Interface status
  ip                    Internet Protocol (IP)
  ldap                  LDAP server
  licenses              Show any installed licenses
  logging               Show logging configuration and buffer
  mac                   Internet Protocol (IP)
  mac-address-table     Display MAC address table
  management            Display L3 Managment Interface name
  mobility              Display Mobility parameters
  ntp                   Network time protocol
  password-encryption   password encryption
  port-channel          Portchannel commands
  privilege             Show current privilege level
  radius                RADIUS configuration commands
  redundancy-group      Display redundancy group parameters
  redundancy-history    Display state transition history of the
                        switch.
  redundancy-members    Display redundancy group members in detail
  running-config        Current Operating configuration
  securitymgr           Securitymgr parameters
  sessions              Display current active open connections
  snmp                  Display SNMP engine parameters
  snmp-server           Display SNMP engine parameters
  sole                  Smart Opportunistic Location Engine
                        Configuration
  spanning-tree         Display spanning tree information
  startup-config        Contents of startup configuration
  static-channel-group  static channel group membership
  terminal              Display terminal configuration parameters
  timezone              Display timezone
  upgrade-status        Display last image upgrade status
```

```
  users                 Display information about currently logged
                        in users
  version               Display software & hardware version
  wireless              Wireless configuration commands
  wlan-acl              wlan based acl

WS5100(config-crypto-isakmp)#show
```

7

crypto-group

Use the `crypto isakmp client (configuration)(group)(default)` to initiate the `config-crypto-group` instance.

7.1 Crypto Group Config Commands

Table 7.1 summarizes the switch **`config-crypto-group`** commands

Table 7.1 Crypto Group Command Summary

Command	Description	Ref.
clrscr	Clears the display screen	*page 7-2*
dns	Defines a primary and secondary *Domain Name Server* (DNS)	*page 7-2*
end	Ends the current mode and moves to the EXEC mode	*page 7-3*
exit	Ends the current mode and moves to the previous mode	*page 7-3*
help	Describe the interactive help system	*page 7-4*
service	Invokes service commands to trobuleshoot or debug the `(config-crypto-isakmp)` instance configuration	*page 7-5*
show	Shows running system information	*page 7-6*
wins	Defines a *Windows Name Server* (WINS)	*page 7-8*

7.1.1 clrscr

Crypto Group Config Commands

Clears the display screen.

Syntax

```
clrscr
```

Parameters

None

Example

```
WS5100(config-crypto-group)#clr
WS5100(config-crypto-group)#
```

7.1.2 dns

Crypto Group Config Commands

Specifies the DNS server address(es) to assign to a client

Syntax

```
dns <IP Address>
```

Parameters

<IP Address>	The first DNS server address to assign
<IP Address> optional	Assign a second (optional) DNS server address

Example

```
WS5100(config-crypto-group)#dns-server 172.1.17.1 172.1.17.3
WS5100(config-crypto-group)#
```

7.1.3 end

Crypto Group Config Commands

Ends and exits the current mode and changes to the PRIV EXEC mode. The prompt changes to `WS5100#`.

Syntax

```
end
```

Parameters

None

Example

```
WS5100(config-crypto-group)#end
WS5100#
```

7.1.4 exit

Crypto Group Config Commands

Ends the current mode and moves to theprevious mode (GLOBAL-CONFIG). The prompt changes to `WS5100(config)#`.

Syntax

```
exit
```

Parameters

None

Example

```
WS5100(config-crypto-group)#exit
WS5100(config)#
```

7.1.5 help

Crypto Group Config Commands

Accesses the system's interactive help system

Syntax

```
help
```

Parameters

None

Example

```
WS5100(config-crypto-group)#help
CLI provides advanced help feature.  When you need help,
anytime at the command line please press '?'.

If nothing matches, the help list will be empty and you must backup
until entering a '?' shows the available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each possible
   argument.
2. Partial help is provided when an abbreviated argument is entered
   and you want to know what arguments match the input
   (e.g. 'show ve?'.)

WS5100(config-crypto-group)#
```

7.1.6 service

Crypto Group Config Commands

Invokes the service commands used to trobuleshoot or debug the `(config-crypto-isakmp)` instance configurations

Syntax

`service(show)(cli)`

Parameters

cli	Displays the CLI tree of current mode

Example

```
WS5100(config-crypto-group)#service show cli
Crypto Client Config mode:
+-clrscr [clrscr]
+-dns
  +-A.B.C.D [dns A.B.C.D]
+-do
  +-LINE [do LINE]
+-end [end]
+-exit [exit]
+-help [help]
+-quit [quit]
+-s
  +-commands [show commands]
    +-WORD [show commands WORD]
  +-running-config [show running-config]
    +-full [show running-config full]
    +-include-factory [show running-config include-factory]
+-service
  +-show
    +-cli [service show cli]
+-show
  +-access-list [show access-list]
    +-<1-99> [show access-list (<1-99>|<100-199>|<1300-1999>|<2000-
2699>|WORD)]
.............................................
.............................................
WS5100(config-crypto-group)#
```

7.1.7 show

Crypto Group Config Commands

Displays the current system information running on the switch

Syntax

```
show <paramater>
```

Parameters

?	Displays the parameters for which information can be viewed using the show command

Example

```
WS5100(config-crypto-group)#show ?
  access-list           Internet Protocol (IP)
  aclstats              Show ACL Statistics information
  alarm-log             Display all alarms currently in the system
  autoinstall           autoinstall configuration
  banner                Display Message of the Day Login banner
  boot                  Display boot configuration.
  clock                 Display system clock
  commands              Show command lists
  crypto                encryption module
  debugging             Debugging information outputs
  dhcp                  DHCP Server Configuration
  environment           show environmental information
  file                  Display filesystem information
  ftp                   Display FTP Server configuration
  history               Display the session command history
  interfaces            Interface status
  ip                    Internet Protocol (IP)
  ldap                  LDAP server
  licenses              Show any installed licenses
  logging               Show logging configuration and buffer
  mac                   Internet Protocol (IP)
  mac-address-table     Display MAC address table
  management            Display L3 Managment Interface name
  mobility              Display Mobility parameters
  ntp                   Network time protocol
  password-encryption   password encryption
  port-channel          Portchannel commands
  privilege             Show current privilege level
  radius                RADIUS configuration commands
  redundancy-group      Display redundancy group parameters
```

```
  redundancy-history    Display state transition history of the
                        switch.
  redundancy-members    Display redundancy group members in detail
  running-config        Current Operating configuration
  securitymgr           Securitymgr parameters
  sessions              Display current active open connections
  snmp                  Display SNMP engine parameters
  snmp-server           Display SNMP engine parameters
  sole                  Smart Opportunistic Location Engine
                        Configuration
  spanning-tree         Display spanning tree information
  startup-config        Contents of startup configuration
  static-channel-group  static channel group membership
  terminal              Display terminal configuration parameters
  timezone              Display timezone
  upgrade-status        Display last image upgrade status
  users                 Display information about currently logged
                        in users
  version               Display software & hardware version
  wireless              Wireless configuration commands
  wlan-acl              wlan based acl

WS5100(config-crypto-group)#show
```

7.1.8 wins

Crypto Group Config Commands

Specifies the *Windows Internet Naming Service* (WINS) servers to assign to a client

Syntax

```
wins <IP Address> <IP Address>
```

Parameters

<IP Address>	The first WINS server address to assign
<IP Address> optional	Assign a second (optional) WINS server address

Example

```
WS5100(config-crypto-group)#wins 128.2.11.1 128.2.19.23
WS5100(config-crypto-group)#
```

8

crypto-peer

Use the `crypto isakmp peer [IP Address|dns|hostname]` command to initiate `config-crypto-peer` instance.

8.1 Crypto Peer Config Commands

Table 8.1 summarizes the **`config-crypto-peer`** commands

Table 8.1 Crypto Peer Command Summary

Command	Description	Ref.
clrscr	Clears the display screen	*page 8-2*
end	Ends the current mode and moves to the EXEC mode	*page 8-2*
exit	Ends the current mode and moves to the previous mode	*page 8-2*
help	Descrbes the interactive help system	*page 8-3*
no	Negates a command or sets its defaults	*page 8-3*
service	Invokes service commands to trobuleshoot or debug the `(config-crypto-peer)` instance configuration	*page 8-4*
set	Sets configuration parameters	*page 8-5*
show	Displays running system	*page 8-5*

8.1.1 clrscr

Crypto Peer Config Commands

Clears the display screen

Syntax

```
clrscr
```

Parameters

None

Example

```
WS5100(config-crypto-peer)#clr
WS5100(config-crypto-peer)
```

8.1.2 end

Crypto Peer Config Commands

Ends and exits the current mode and change to the PRIV EXEC mode. The prompt changes to `WS5100#`.

Syntax

```
end
```

Parameters

None

Example

```
WS5100(config-crypto-peer)#end
WS5100#
```

8.1.3 exit

Crypto Peer Config Commands

Ends the current mode and moves to the previous mode (GLOBAL-CONFIG). The prompt changes to `WS5100(config)#`

Syntax

```
exit
```

Parameters

None

Example

```
WS5100(config-crypto-peer)#exit
WS5100(config)#
```

8.1.4 help

▸ *Crypto Peer Config Commands*

Accesses the system's interactive help system

Syntax

```
help
```

Parameters

None

Example

```
WS5100(config-crypto-peer)#help
CLI provides advanced help feature.  When you need help,
anytime at the command line please press '?'.
If nothing matches, the help list will be empty and you must backup
until entering a '?' shows the available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each possible
   argument.
2. Partial help is provided when an abbreviated argument is entered
   and you want to know what arguments match the input
   (e.g. 'show ve?'.)
WS5100(config-crypto-peer)#
```

8.1.5 no

▸ *Crypto Peer Config Commands*

Negates a command or sets its defaults

Syntax

```
(no) set (aggressive-mode)(password)
```

Parameters

See *set* command for parameters details

Example

```
WS5100(config-crypto-peer)#no aggrerssive-mode
WS5100(config-crypto-peer)#
```

8.1.6 service

Crypto Peer Config Commands

Invokes service commands to trobuleshoot or debug the `(config-crypto-peer)` instance configuration

Syntax

```
service(show)(cli)
```

Parameters

cli	Show CLI tree of current mode

Example

```
WS5100(config-crypto-peer)#service show cli
Crypto Peer Config mode:
+-clrscr [clrscr]
+-do
  +-LINE [do LINE]
+-end [end]
+-exit [exit]
+-help [help]
+-no
  +-set
    +-aggressive-mode
      +-password [no set aggressive-mode password]
+-quit [quit]
+-s
  +-commands [show commands]
    +-WORD [show commands WORD]
  +-running-config [show running-config]
    +-full [show running-config full]
    +-include-factory [show running-config include-factory]
+-service
  +-show
    +-cli [service show cli]
+-set
  +-aggressive-mode
    +-password
.....................................
.....................................

WS5100(config-crypto-peer)#
```

8.1.7 set

Crypto Peer Config Commands

Configures the aggressive-mode of `crypto-peer`

Syntax

```
set aggressive-mode (password)
```

Parameters

aggressive-mode	Defines aggressive mode attributes • password – Specifies a tunnel-password attribute

Example

```
WS5100(config-crypto-peer)#set aggressive-mode password CheckMeIn
WS5100(config-crypto-peer)#
```

8.1.8 show

Crypto Peer Config Commands

Displays the current system information running on the switch

Syntax

```
show <paramater>
```

Parameters

?	Displays the parameters for which the information can be viewed using the show command

Example

```
WS5100(config-crypto-peer)#show ?
  access-list           Internet Protocol (IP)
  aclstats              Show ACL Statistics information
  alarm-log             Display all alarms currently in the system
  autoinstall           autoinstall configuration
  banner                Display Message of the Day Login banner
  boot                  Display boot configuration.
  clock                 Display system clock
  commands              Show command lists
  crypto                encryption module
  debugging             Debugging information outputs
```

```
  dhcp                    DHCP Server Configuration
  environment             show environmental information
  file                    Display filesystem information
  ftp                     Display FTP Server configuration
  history                 Display the session command history
  interfaces              Interface status
  ip                      Internet Protocol (IP)
  ldap                    LDAP server
  licenses                Show any installed licenses
  logging                 Show logging configuration and buffer
  mac                     Internet Protocol (IP)
  mac-address-table       Display MAC address table
  management              Display L3 Managment Interface name
  mobility                Display Mobility parameters
  ntp                     Network time protocol
  password-encryption     password encryption
  port-channel            Portchannel commands
  privilege               Show current privilege level
  radius                  RADIUS configuration commands
  redundancy-group        Display redundancy group parameters
  redundancy-history      Display state transition history of the
                          switch.
  redundancy-members      Display redundancy group members in detail
  running-config          Current Operating configuration
  securitymgr             Securitymgr parameters
  sessions                Display current active open connections
  snmp                    Display SNMP engine parameters
  snmp-server             Display SNMP engine parameters
  sole                    Smart Opportunistic Location Engine
                          Configuration
  spanning-tree           Display spanning tree information
  startup-config          Contents of startup configuration
  static-channel-group    static channel group membership
  terminal                Display terminal configuration parameters
  timezone                Display timezone
  upgrade-status          Display last image upgrade status
  users                   Display information about currently logged
                          in users
  version                 Display software & hardware version
  wireless                Wireless configuration commands
  wlan-acl                wlan based acl

WS5100(config-crypto-peer)#show
```

9

crypto-ipsec

Use the `(config-crypto ipsec)` instance to define the transform configuration for securing data(e.g., esp-3des, esp-sha-hmac, etc.). The transform set is assigned to a crypto map using the map's transform-set command. For more details, see crypto-map transform set on *page 10-7*.

9.1 Crypto IPsec Config Commands

Table summarizes the **`config-crypto-ipsec`** commands .

Table 9.1 Crypto IPsec Command Summary

Command	Description	Ref.
clrscr	Clears the display screen.	*page 6-2*
end	Ends the current mode and moves to the EXEC mode	*page 6-3*
exit	Ends the current mode and moves to the previous mode	*page 6-4*
help	Describes the interactive help system	*page 6-5*
mode	Configures the IP Sec transportation mode	*page 9-2*
no	Negates a command or set its defaults	*page 6-6*
service	Invokes service commands to trobuleshoot or debug `(config-crypto-isakmp)` instance configurations	*page 6-6*
show	Displays running system information	*page 9-2*

9.1.1 mode

Crypto IPsec Config Commands

Use this command to configure IPSec mode of operation.

Syntax

```
mode(transport|tunnel)
```

Parameters

transport	Transport mode
tunnel	Tunnel mode

Example

```
WS5100(config-crypto-ipsec)#mode transport
WS5100(config-crypto-ipsec)#
```

9.1.2 show

Crypto IPsec Config Commands

Syntax

```
clrscr
```

Parameters

?	Displays the parameters for which information can be viewed using the show command

Example

```
WS5100(config-crypto-ipsec)#show ?
  access-list          Internet Protocol (IP)
  alarm-log            Display all alarms currently in the system
  autoinstall          autoinstall configuration
  banner               Display Message of the Day Login banner
  boot                 Display boot configuration.
  clock                Display system clock
  commands             Show command lists
  crypto               crypto
  debugging            Display debugging setting
  environment          show environmental information
  file                 Display filesystem information
  ftp                  Display FTP Server configuration
```

```
  history               Display the session command history
  interfaces            Interface status and configuration
  ip                    Internet Protocol (IP)
  ldap                  ldap server
  licenses              Show any installed licenses
  logging               Show logging configuration and buffer
  mac                   Media Access Control
  management            Display L3 Managment Interface name
  mobility              Display Mobility Parameters
  ntp                   Network time protocol
  password-encryption   password encryption
  privilege             Show current privilege level
  radius                Radius configuration commands
  redundancy-group      Display redundancy group parameters
  redundancy-history    Display state transition history of the
switch.
  redundancy-members    Display redundancy group members in detail
  running-config        Current Operating configuration
  securitymgr           Display debug info for ACL, VPN and NAT
  sessions              Display current active open connections
  snmp                  Display SNMP engine parameters
  snmp-server           Display SNMP engine parameters
  startup-config        Contents of startup configuration
  terminal              Display terminal configuration parameters
  timezone              Display timezone
  upgrade-status        Display last image upgrade status
  users                 Display information about terminal lines
  version               Display software & hardware version
  wireless              Wireless configuration commands

WS5100(config-crypto-ipsec)#show
```

10

crypto-map

The `config-crypto-map` commands define a *Certificate Authority* (CA) trustpoint. This is a seperate instance, but belongs to the `crypto pki trustpoint` mode under the `config` instance.

10.1 Crypto Map Config Commands

Table 10.1 summarizes **`config-crypto-map`** commands T

Table 10.1 Crypto Map Command Summary

Command	*Description*	*Ref.*
clrscr	Clears the display screen	*page 10-2*
end	Ends the current mode and moves to the EXEC mode	*page 10-2*
exit	Ends the current mode and moves to the previous mode	*page 10-2*
help	Describes the interactive help system	*page 10-3*
match	Assigns an IP access-list to a crypto map definition	*page 10-3*
no	Negates a command or set its defaults	*page 10-5*
service	Invoke the service commands to trobuleshoot or debug the instance configurations	*page 10-6*
set	Sets values for encryption/decryption parameters	*page 10-7*
show	Displays the running system information	*page 10-10*

10.1.1 clrscr

Crypto Map Config Commands

Clears the display screen

Syntax

```
clrscr
```

Parameters

None

Example

```
WS5100(config-crypto-map)#clr
WS5100(config-crypto-map)
```

10.1.2 end

Crypto Map Config Commands

Use this command to end and exit the current mode and move to the to PRIV EXEC mode. The prompt now changes to `WS5100#`

Syntax

```
end
```

Parameters

None

Example

```
WS5100(config-crypto-map)#end
WS5100#
```

10.1.3 exit

Crypto Map Config Commands

Ends the current mode and moves to the previous mode (GLOBAL-CONFIG). The prompt changes to `WS5100(config)#`

Syntax

```
exit
```

Parameters

None

Example

```
WS5100(config-crypto-map)#exit
WS5100(config)#
```

10.1.4 help

▸ *Crypto Map Config Commands*

Use this command to access the system's interactive help system

Syntax

```
help
```

Parameters

None

Example

```
WS5100(config-crypto-map)#help
CLI provides advanced help feature.  When you need help,
anytime at the command line please press '?'.

If nothing matches, the help list will be empty and you must backup
until entering a '?' shows the available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each possible
   argument.
2. Partial help is provided when an abbreviated argument is entered
   and you want to know what arguments match the input
   (e.g. 'show ve?'.)
WS5100(config-crypto-map)#
```

10.1.5 match

▸ *Crypto Map Config Commands*

Use this command to assign an IP access-list to a crypto map definition. The access-list designates the IP packets to be encrypted by this crypto map.

A crypto map entry is a single policy that describes how certain traffic is secured. There are two types of crypto map entries: ipsec-manual and ipsec-ike entries. Each entry is given an index (used to sort the ordered list).

When a non-secured packet arrives on an interface, the crypto map set associated with that interface is processed (in order). If a crypto map entry matches the non-secured traffic, the traffic is discarded.

When a packet is transmitted on an interface, the crypto map set associated with that interface is processed. The first crypto map entry that matches the packet is used to secure the packet. If a suitable SA exists, it is used for transmission. Otherwise, IKE is used to establish an SA with the peer. If no SA exists (and the crypto map entry is "respond only"), the packet is discarded.

When a secured packet arrives on an interface, its SPI is used to look up a SA. If a SA does not exist (or if the packet fails any of the security checks), it is discarded. If all checks pass, the packet is forwarded normally.

Syntax

```
match <list name>
```

Parameters

list name	Enter the name of the access list or ACL ID to assign to this crypto map

Usage Guidelines

Crypto map entries do not directly contain the selectors used to determine which data to secure. Instead, the crypto map entry refers to an access control list. An access control list (ACL) is assigned to the crypto map using the match address command. If no ACL is configured for a crypto map, the entry is incomplete and will have no effect on the system.

The entries of the ACL used in a crypto map should be created with respect to traffic sent by the OS. The source information must be the local OS, and the destination must be the peer.

Only extended access-lists can be used in crypto maps.

Example

The following shows setting up an ACL (called TestList) and assigning the new list to a crypto map (called TestMap):

```
WS5100(config)#ip access-list extended TestList
Configuring New Extended ACL "TestList"
(config-ext-nacl)#exit

WS5100(config)#crypto map TestMap 220 isakmp dynamic
WS5100(config-crypto-map)#

WS5100(config-crypto-map)#match address TestMap
WS5100(config-crypto-map)#
```

10.1.6 no

▸ *Crypto Map Config Commands*

Negates a command or sets its defaults

Syntax

```
no <previous command used>
```

Parameters

Use the commands configured under this instance

Example

```
WS5100(config-crypto-map)#no aggrerssive-mode
WS5100(config-crypto-map)#
```

10.1.7 service

Crypto Map Config Commands

Invokes service commands to trobuleshoot or debug `(config-crypto-isakmp)` instance configurations

Syntax

```
service(clear|diag-shell|save-cli|show|start-shell|tethereal)
```

Parameters

clear	Removes specified support information
diag-shell	Provides diag shell access
save-cli	Saves the CLI tree for all modes in HTML
show	Shows the running system information
start-shell	Provides shell access
tethereal	Dumps and analyzes network traffic

Example

```
WS5100(config-crypto-map)#service show ?
  cli              Show CLI tree of current mode
  command-history  Display command (except show commands) history.
  crash-info       Display information about core, panic and AP
dump files
  info             Show snapshot of available support information
  last-passwd      Display last password used to enter shell
  reboot-history   Show reboot history
  startup-log      Show startup log
  upgrade-history  Show upgrade history
WS5100(config-crypto-map)#service show

WS5100(config-crypto-map)#service show info
4.0M out of 4.0M available for logs.
9.7M out of 11.4M available for history.
16.4M out of 18.6M available for crashinfo.
List of Files:
 messages.log                    0       Oct 9  13:01
 snmpd.log                       316     Oct 9  13:01
 startup.log                     16.5k   Oct 9  13:01
 command.history                 8.5k    Oct 9  20:26
 reboot.history                  3.4k    Oct 9  13:01
```

```
 upgrade.history                  782     Aug 29 18:32
Please export these files or delete them for more space.
WS5100(config-crypto-map)#
```

10.1.8 set

▸ *Crypto Map Config Commands*

Use this command to set the various set parameters of the peer device.

Syntax

```
set (localid|mode|peer|pfs|remote-type[ipsec-l2tp|xauth]|
security-association|session-key|transformset)

set localid(dn|hostname)

set security-association
(level(perhost)|lifetime(kilobytes|seconds)<value>)

set session-key (inbound|outbound)(ah|esp)
set session-key (inbound|outbound) ah <hexkey data>
set session-key (inbound|outbound) esp <SPI> cipher <hexdata key>
authenticator <hexkey data>
```

Parameters

local id	Sets the local identity • *dn* – Defines the distinguished name • *hostname* – Sets the hostname
mode	Sets the mode of the tunnels for this Crypto Map • *aggressive* – Initiates aggressive mode • *main* – Initiates main mode
peer	Sets the IP address of the peer device. This can be set for multiple remote peers. The remote peer can be either an IP address or hostname **Note:** In manual mode, only one remote peer can be added for a crypto map • IP address – Enter the IP address of the peer device. If not configured, it implies responder only to any peer

pfs	Use the *set pfs* command to choose the type of perfect forward secrecy (if any) required during IPSec negotiation of SAs for this crypto map. Use the no form of this command to require no PFS • *group 1* – IPSec is required to use the Diffie-Hellman Group 1 (768-bit modulus) exchange during IPSec SA key generation • *group 2* – IPSec is required to use the Diffie-Hellman Group 2 (1024-bit modulus) exchange during IPSec SA key generation • *group 5* – IPSec is required to use Diffie-Hellman Group 5
remote-type	Sets the remote VPN client type. • ipsec-l2tp – Specify the remote VPN client as using IPSEC/L2TP • xauth – Specify the remote VPN client as using XAUTH with mode config
security-association	Defines the lifetime (in kilobytes and/or seconds) of the IPSec SAs created by this crypto map • *level(perhost)* – Specify a security association granularity level for identities • *lifetime(kilobyte|seconds)* – Security an association lifetime
session-key	Use the set session-key command to define the encryption and authentication keys for this crypto map • *inbound* – Defines encryption keys for inbound traffic • *outbound* – Defines encryption keys for outbound traffic

inbound/outbound (ah|esp)	Defines encryption keys for inbound/outbound traffic • *ah* – Authentication header protocol • <256-4294967295> – *Security Parameter Index* (SPI) for the security association • *esp* – Encapsulating security payload protocol • <256-4294967295> – Derfines the security parameter Index • cipher – Specify encryption/decryption key • *authenticator <hex key data>* – Specify an authentication key
transformset <name>	Use the set transform-set command to assign a transform-set to a crypto map.

Usage Guidelines

```
WS5100(config-crypto-map)#set peer (name)
```

If no peer IP address is configured, the manual crypto map is not valid and not complete. A peer IP address is required for manual crypto maps. To change the peer IP address, the no set peer command must be issued first; then the new peer IP address can be configured.

```
WS5100(config-crypto-map)#set pfs
```

If left at the default setting, no perfect forward secrecy (PFS) is used during IPSec SA key generation. If PFS is specified, the specified Diffie-Hellman Group exchange is used for the initial (and all subsequent) key generation. This means no data linkage between prior keys and future keys.

```
WS5100(config-crypto-map)#set security-association lifetime
(kilobytes|seconds)
```

Values can be entered in both kilobytes and seconds. Whichever limit is reached first, ends the security association.

```
WS5100(config-crypto-map)#set session-key
(inbound|outbound)(ah|esp)
WS5100(config-crypto-map)#set session-key (inbound|outbound) ah
<hexkey data>
WS5100(config-crypto-map)#set session-key (inbound|outbound) esp
<SPI> cipher <hexdata key> authenticator <hexkey data>
```

The inbound local SPI (security parameter index) must equal the outbound remote SPI. The outbound local SPI must equal the inbound remote SPI. The key values are the hexadecimal representations of the keys.

They are not true ASCII strings. Therefore, a key of 3031323334353637 represents "01234567".

```
WS5100(config-crypto-map)#set transformset (name)
```

Crypto map entries do not directly contain the transform configuration for securing data. Instead, the crypto map is associated with transform sets which contain specific security algorithms.

If a transform-set is not configured for a crypto map, the entry is incomplete and has no effect. For manual key crypto maps, only one transform set can be specified.

Example

```
WS5100(config-crypto-map)#set localid hostname TestMapHost
WS5100(config-crypto-map)#
```

10.1.9 show

- *Crypto Map Config Commands*

Displays the current system information running on the switch.

Syntax

```
show <paramater>
```

Parameters

?	Displays all the parameters for which information can be viewed using the show command

Example

```
WS5100(config-crypto-map)#show ?
  access-list          Internet Protocol (IP)
  alarm-log            Display all alarms currently in the system
  autoinstall          autoinstall configuration
  banner               Display Message of the Day Login banner
  boot                 Display boot configuration.
  clock                Display system clock
  commands             Show command lists
  crypto               crypto
  debugging            Display debugging setting
  environment          show environmental information
  file                 Display filesystem information
  ftp                  Display FTP Server configuration
  history              Display the session command history
  interfaces           Interface status and configuration
  ip                   Internet Protocol (IP)
  ldap                 ldap server
  licenses             Show any installed licenses
  logging              Show logging configuration and buffer
  mac                  Media Access Control
  management           Display L3 Managment Interface name
  mobility             Display Mobility Parameters
  ntp                  Network time protocol
  password-encryption  password encryption
  privilege            Show current privilege level
  radius               Radius configuration commands
  redundancy-group     Display redundancy group parameters
  redundancy-history   Display state transition history of the
switch.
  redundancy-members   Display redundancy group members in detail
  running-config       Current Operating configuration
  securitymgr          Display debug info for ACL, VPN and NAT
  sessions             Display current active open connections
  snmp                 Display SNMP engine parameters
  snmp-server          Display SNMP engine parameters
  startup-config       Contents of startup configuration
  terminal             Display terminal configuration parameters
  timezone             Display timezone
  upgrade-status       Display last image upgrade status
  users                Display information about terminal lines
  version              Display software & hardware version
  wireless             Wireless configuration commands

WS5100(config-crypto-map)#show
```

11

crypto-trustpoint Instance

`config-crypto-trustpoint` commands define a *Certificate Authority* (CA) trustpoint. This is a separate instance, but belongs to the `crypto pki trustpoint` mode under the `config` instance.

11.1 Trustpoint (PKI) Config Commands

Table 11.1 summarizes **`config-crypto-trustpoint`** commands:

Table 11.1 Trustpoint (PKI) Config Command Summary

Command	Description	Ref.
clrscr	Clears the display screen	*page 11-2*
company-name	Defines a company name for the trustpoint	*page 11-2*
email	Sets an e-mail ID for the trustpoint.	*page 11-3*
end	Ends the current mode and moves to the EXEC mode	*page 11-3*
exit	Ends the current mode and moves to the previous mode	*page 11-4*
fqdn	Sets the domain name of the trustpoint	*page 11-4*
help	Displays the interactive help system	*page 11-5*
ip-address	Sets an IP address for the trustpoint	*page 11-5*
no	Negates a command or sets its defaults	*page 11-6*

Table 11.1 Trustpoint (PKI) Config Command Summary

Command	Description	Ref.
password	Sets the challenge password (applicable only for requests), to access the trustpoint	*page 11-6*
rsakeypair	Defines a RSA Keypair to associate with the trustpoint	*page 11-7*
service	Invokes service commands to troubleshoot or debug the `crypto pki trustpoint` instance configuration	*page 11-7*
show	Displays running system information	*page 11-9*
subject-name	The subject name is a collection of required parameters to configure a trustpoint	*page 11-11*

11.1.1 clrscr

Trustpoint (PKI) Config Commands

Clears the display screen

Syntax

```
clrscr
```

Parameters

None

Example

```
WS5100(config-trustpoint)#clrscr
WS5100(config-trustpoint)#
```

11.1.2 company-name

Trustpoint (PKI) Config Commands

Sets the company name (Applicable only for request)

Syntax

```
company-name
```

Parameters

WORD	Company name (2 to 64 characters)

Example

```
WS5100(config-trustpoint)#company-name RetailKing
WS5100(config-trustpoint)#
```

11.1.3 email

Trustpoint (PKI) Config Commands

Sets the e-mail ID for the trustpoint

Syntax

```
email
```

Parameters

WORD	email address (2 to 64 characters)

Example

```
WS5100(config-trustpoint)#email abcTestemailID@symbol.com
WS5100(config-trustpoint)#
```

11.1.4 end

Trustpoint (PKI) Config Commands

Ends and exits the current mode and moves to the PRIV EXEC mode. The prompt changes to `WS5100#`

Syntax

```
end
```

Parameters

None

Example

```
WS5100(config-trustpoint)#end
WS5100#
```

11.1.5 exit

Trustpoint (PKI) Config Commands

Ends the current mode and moves to previous the mode (GLOBAL-CONFIG). The prompt changes to `WS5100(config)#`

Syntax

```
exit
```

Parameters

None

Example

```
WS5100(config-trustpoint)#exit
WS5100(config)#
```

11.1.6 fqdn

Trustpoint (PKI) Config Commands

Configures the domain name of the trustpoint

Syntax

```
fqdn
```

Parameters

None

NOTE: The length of domain name should be between 9 and 64 characters.

Example

```
WS5100(config-trustpoint)#fqdn RetailKing.com
WS5100(config-trustpoint)#
```

11.1.7 help

Trustpoint (PKI) Config Commands

Displays the systems interactive help system

Syntax

```
help
```

Parameters

None

Example

```
WS5100(config-trustpoint)#help
CLI provides advanced help feature. When you need help,
anytime at the command line please press '?'.

If nothing matches, the help list will be empty and you must backup
until entering a '?' shows the available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each possible
   argument.
2. Partial help is provided when an abbreviated argument is entered
   and you want to know what arguments match the input
   (e.g. 'show ve?'.)

WS5100(config-trustpoint)#
```

11.1.8 ip-address

Trustpoint (PKI) Config Commands

Sets an IP address for the trustpoint

Syntax

```
ip-address
```

Parameters

A.B.C.D	Enter the IP address for the trustpoint

Example

```
WS5100(config-trustpoint)#ip-address 157.200.200.02
WS5100(config-trustpoint)#
```

11.1.9 no

Trustpoint (PKI) Config Commands

Negates a command or sets its defaults

Syntax

```
no <previous command used>
```

Parameters

None.

Example

```
WS5100(config-trustpoint)#no ip-address
WS5100(config-trustpoint)#
```

11.1.10 password

Trustpoint (PKI) Config Commands

Sets the challenge password (applicable only for requests) to acces trustpoint.

Syntax

```
password(0|2|WORD)
```

Parameters

0	Password is specified as UNENCRYPTED. The password should be between 4 to 20 characters
2	Password is encrypted with password-encryption secret. The string length of encrypted password should be between 44 - 64 characters
WORD	Sets the password (4 to 20 characters)

Example

```
WS5100(config-trustpoint)#password 0 TestPassword
WS5100(config-trustpoint)#
```

11.1.11 rsakeypair

Trustpoint (PKI) Config Commands

Configures a RSA Keypair to associate with the trustpoint

Syntax

```
rsakeypair
```

Parameters

WORD	RSA Keypair Identifier.

Usage Guidelines

The RSA key pair configures the switch to have *Rivest, Shamir, and Adelman* (RSA) key pairs. Thus, the switch software can maintain a different key pair for each identity certificate

Example

```
WS5100(config-trustpoint)#rsakeypair were
WS5100(config-trustpoint)#
```

The rsakeypair name were in this example is an exisitng keypair value

11.1.12 service

Trustpoint (PKI) Config Commands

Invokes service commands to trobuleshoot or debug the `crypto pki trustpoint` instance configuration

Syntax

```
service(clear|diag-shell|save-cli|show|start-shell|tethereal)
```

Parameters

clear	Removes specified support information
diag-shell	Provides diagnostic shell access to debug and test the switch
save-cli	Saves the CLI tree for all modes in HTML
show	Displays the running system information

start-shell	Provides shell access
tethereal	Dumps and analyzes network traffic

Example

```
WS5100(config-trustpoint)#service diag-shell

Diagnostic shell started for testing
diag >
  boot            Reboots the switch
  delete          Deletes specified file from the system.
  exit            Exit from the CLI
  fallback        Configures firmware fallback feature
  help            Description of the interactive help system
  logout          Exit from the CLI
  no              Negate a command or set its defaults
  reload          Halt and perform a warm reboot
  service         Service Commands
  show            Show running system information
  upgrade         Upgrade firmware image

diag >

WS5100(config-trustpoint)#service save-cli
 CLI command tree is saved as clitree.html.
 This tree can be viewed via web at http://<ipaddr>/cli/
clitree.html
WS5100(config-trustpoint)#

WS5100(config-trustpoint)#service show ?
  cli              Show CLI tree of current mode
  command-history  Display command (except show commands) history.
  crash-info       Display information about core, panic and AP
dump files
  info             Show snapshot of available support information
  last-passwd      Display last password used to enter shell
  reboot-history   Show reboot history
  startup-log      Show startup log
  upgrade-history  Show upgrade history

WS5100(config-trustpoint)#service start-shell
Last password used: password with MAC 00:a0:f8:65:ea:8e
Password:

WS5100(config-trustpoint)#service tethereal ?
  LINE  tethereal options in the format
        [-V (print detailed packet)] [-x (hex dump of packet)]
```

```
        [-p (no promiscuous mode for interface)]
        [-n (disable name resolution)] [-c <count> ] [-h (detailed
help)]
        [-E (to capture ESPD) ][-e (capture nonEspd packets)]
        [-f <capture filter expression in format "xx xx xx"> ]
        [-i <interface on which to capture packets> ] [-W (wisp
packet only)]
        [-s <snaplen> ] [-r <filename> (read contents of specified
file)]
        [-w <savefile> (save capture in specified file) ]
        [-X (for examples on tethereal capture filter) ]
```

11.1.13 show

- *Trustpoint (PKI) Config Commands*

Displays current system information running on the switch

Syntax

```
show <parameter>
```

Parameters

?	Displays the parameters for which the information can be viewed using the show command

Example

```
WS5100(config-trustpoint)#show ?
  access-list          Internet Protocol (IP)
  alarm-log            Display all alarms currently in the system
  autoinstall          autoinstall configuration
  banner               Display Message of the Day Login banner
  boot                 Display boot configuration.
  clock                Display system clock
  commands             Show command lists
  crypto               crypto
  debugging            Display debugging setting
  environment          show environmental information
  file                 Display filesystem information
  ftp                  Display FTP Server configuration
  history              Display the session command history
  interfaces           Interface status and configuration
  ip                   Internet Protocol (IP)
  ldap                 ldap server
  licenses             Show any installed licenses
  logging              Show logging configuration and buffer
  mac                  Media Access Control
```

```
  management            Display L3 Managment Interface name
  mobility              Display Mobility Parameters
  ntp                   Network time protocol
  password-encryption   password encryption
  privilege             Show current privilege level
  radius                Radius configuration commands
  redundancy-group      Display redundancy group parameters
  redundancy-history    Display state transition history of the
switch.
  redundancy-members    Display redundancy group members in detail
  running-config        Current Operating configuration
  securitymgr           Display debug info for ACL, VPN and NAT
  sessions              Display current active open connections
  snmp                  Display SNMP engine parameters
  snmp-server           Display SNMP engine parameters
  startup-config        Contents of startup configuration
  terminal              Display terminal configuration parameters
  timezone              Display timezone
  upgrade-status        Display last image upgrade status
  users                 Display information about terminal lines
  version               Display software & hardware version
  wireless              Wireless configuration commands

WS5100(config)#show crypto pki trustpoints

Trustpoint :default-trustpoint
------------------------------------------------
  Server certificate configured
    Subject Name:
      Common Name:          Symbol Technologies
    Issuer Name:
      Common Name:          Symbol Technologies
  Valid From:   May 17 14:48:25 2007 GMT
  Valid Until:  May 16 14:48:25 2008 GMT

Trustpoint :test
------------------------------------------------
  Server certificate configured
    Subject Name:
      Common Name:          nn
      Organizational Unit: nn
      Organization:         nn
      Location:             nn
      State:                nn
      Country:              nn
    Issuer Name:
      Common Name:          nn
      Organizational Unit: nn
      Organization:         nn
```

```
      Location:            nn
      State:               nn
      Country:             nn
  Valid From:   Jun  8 19:21:55 2007 GMT
  Valid Until:  Jun  7 19:21:55 2008 GMT

Trustpoint :test1
------------------------------------------------
  Server certificate configured
    Subject Name:
      Common Name:         mm
      Organizational Unit: mm
      Organization:        mm
      Location:            mm
      State:               mm
      Country:             mm
    Issuer Name:
      Common Name:         mm
      Organizational Unit: mm
      Organization:        mm
      Location:            mm
      State:               mm
      Country:             mm
  Valid From:   Jun  8 19:24:38 2007 GMT
  Valid Until:  Jun  7 19:24:38 2008 GMT

WS5100(config)#
```

11.1.14 subject-name

- *Trustpoint (PKI) Config Commands*

Creates a subject name to configure a trustpoint. The subject name is a collection of required parameters to configure a trustpoint

Syntax

```
subject-name
```

Parameters

WORD	Enter brief descriptions when prompted

Example

```
WS5100(config-trustpoint)#subject-name TestPool ?
  WORD  Country ( 2 character ISO Code )

WS5100(config-trustpoint)#subject-name TestPool US ?
  WORD  State( 2 to 128 characters )

WS5100(config-trustpoint)#subject-name TestPool US OH ?
  WORD  City( 2 to 128 characters )

WS5100(config-trustpoint)#subject-name TestPool US OH PB ?
  WORD  Organization( 2 to 64 characters )

WS5100(config-trustpoint)#subject-name TestPool US OH PB SYMBOL ?
  WORD  Organization Unit( 2 to 64 characters )

WS5100(config-trustpoint)#subject-name TestPool US OH PB SYMBOL WID
?
  <cr>

WS5100(config-trustpoint)#subject-name TestPool US OH PB SYMBOL WID
WS5100(config-trustpoint)#
```

12

interface Instance

Use the **(config-if)** instance to configure the interfaces — Ethernet, VLAN and tunnel associated with the switch.

12.1 Interface Config Commands

Table 12.1 summarizes the **config-if** commands:

Table 12.1 Interface Config Command Summary

Command	Description	Ref.
clrscr	Clears the display screen	*page 12-2*
crypto	Defines the encryption module	*page 12-3*
description	Creates an interface specific description	*page 12-3*
duplex	Sets the duplex mode used by the interface	*page 12-4*
end	Ends the current mode and moves to the EXEC mode	*page 12-5*
exit	Ends the current mode and moves to the previous mode	*page 12-5*
help	Displays the interactive help system	*page 12-5*
ip	Sets the IP address for the assigned ethernet, VLAN or tunnel	*page 12-6*
mac	Applies a MAC access list to a gigabit ethernet interface	*page 12-8*

Table 12.1 Interface Config Command Summary (Continued)

Command	Description	Ref.
management	Sets the selected interface as management interface	*page 12-9*
no	Negates a command or sets its defaults	*page 12-9*
port-channel	Configures the load-balancing criteria of an aggregated port	*page 12-10*
service	Invokes service commands to troubleshoot or debug the `(config-if)` instance configurations	*page 12-11*
show	Displays running system information	*page 12-12*
shutdown	Shuts down a selected interface	*page 12-15*
spanning-tree	Disables the selected interface. The interface is administratively enabled unless explicitly disabled using this command	*page 12-15*
speed	Specifies the speed of a fast-ethernet (10/100) or a gigabit ethernet port (10/100/1000)	*page 12-17*
static-channel-group	Configures static channel commands	*page 12-18*
switchport	Sets switching mode characteristics	*page 12-19*

12.1.1 clrscr

▸ *Interface Config Commands*

Clears the display screen

Syntax

`clrscr`

Parameters

None

Example

```
WS5100(config-if)#clrscr
WS5100(config-if)#
```

12.1.2 crypto

Interface Config Commands

Syntax

```
crypto map(WORD)
```

Parameters

map <tag>	Assigns a Crypto Map • <tag> – Crypto Map tag

Usage Guidelines

At any given instance you can add one crypto mapset to a single interface. The switch does not allow the same cryptomap set to be attached to multiple interfaces

12.1.3 description

Interface Config Commands

Creates an interface specific desciption

Syntax

```
description
```

Parameters

LINE	Define the characters describing this interface

Example

```
WS5100(config-if)#description "interface for RetailKing"
WS5100(config-if)#
```

12.1.4 duplex

Interface Config Commands

Specifies the duplex mode of operation

NOTE:

- Duplexity can only be set for an Ethernet Interface. Enter the `(config-if)` instance using the `eth` parameter of the `interface` mode
- The duplex can not be set until the speed is set to a non-auto value

Syntax

```
duplex(auto|full|half)
```

Parameters

auto	The port automatically detects whether it should run in full or half-duplex mode
full	Sets the port in full-duplex mode
half	Sets the port in half-duplex mode

Usage Guidelines

The duplex defines the communication used by the port. The switch (by default) is set in the auto duplexmode. In auto mode, the duplex is selected based on connected network hardware

12.1.5 end

Interface Config Commands

Ends and exits the current mode and moves to the PRIV EXEC mode. The prompt changes to `WS5100#`

Syntax

```
end
```

Parameters

None

Example

```
WS5100(config-if)#end
WS5100#
```

12.1.6 exit

Interface Config Commands

Ends the current mode and moves to the previous mode (GLOBAL-CONFIG). The prompt changes to `WS5100(config)#`.

Syntax

```
exit
```

Parameters

None

Example

```
WS5100(config-if)#exit
WS5100(config)#
```

12.1.7 help

Interface Config Commands

Displays the system's interactive help

Syntax

```
help
```

Parameters

None

Example

```
WS5100(config-if)#help
CLI provides advanced help feature.  When you need help,
anytime at the command line please press '?'.

If nothing matches, the help list will be empty and you must backup
until entering a '?' shows the available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each possible
   argument.
2. Partial help is provided when an abbreviated argument is entered
   and you want to know what arguments match the input
   (e.g. 'show ve?'.)

WS5100(config-if)#
```

12.1.8 ip

Interface Config Commands

Sets the IP address for the assigned ethernet, VLAN or tunnel

Syntax

```
ip(access-group|address|helper-address|nat)
ip access-group(<1-99>|<100-199>|<1300-1999>|<2000-2699>)in
ip address(A.B.C.D/M|dhcp)(secondary)
ip helper-address A.B.C.D
ip nat(inside|outside)
```

Parameters

access-group	Defines the access group • (*<1-99>*|*<100-199>*) – Sets the IP extended access list • (*<1300-1999>*|*<2000-2699>*) – Sets the IP extended access list (expanded range) • word – Defines the access list name • in – Sets incoming packets

address	Sets a static IP address and network mask for a Layer 3 SVI (*Switch Virtual Interface*) • A.B.C.D/M – Sets the IP address (10.0.0.1/8) • secondary – Defines an optional secondary IP address • dhcp – Uses a DHCP Client to obtain an IP address for the interface. This enables DHCP on a Layer 3 SVI
helper-address	Forwards DHCP and BOOTP packets • *A.B.C.D – Defines the* IP to which DHCP and BOOTP packets are forwarded
nat	Sets *Network Address Translation* (NAT) parameters • *inside* – Inside interface • *outside* – Outside interface

Usage Guidelines

IPv4 commands are not allowed on a L2 interface. Use the `ip access-group` command to attach an access list to an interface. Use the `no ip access-group` command to remove the access list from the interface

Use `mac access-group` to attach a MAC access list to an interface

Use the `[no] ip [options]` command to undo IP based interface configurations

Example

```
WS5100(config-if)#ip access-group 110 in
WS5100(config-if)#

WS5100(config-if)#ip address 192.168.234.1/24
WS5100(config-if)#
```

Follow the steps below to create a helper address on VLAN 2000 for using a DHCP server on VLAN 1000:

```
WS5100(config)#interface vlan 1000
WS5100(config-if)#ip address 172.168.100.1/24

WS5100(config-if)#interface vlan 2000
WS5100(config-if)#ip address 172.168.200.1/24
```

```
WS5100(config-if)#ip helper-address 172.168.100.10 vlan 1000
WS5100(config-if)#
```

The example below displays static NAT source translation:

```
WS5100(config)#interface vlan 1000
WS5100(config-if)#ip nat inside

WS5100(config-if)#interface vlan 2000
WS5100(config-if)#ip nat outside

WS5100(config)#ip nat inside source static 172.168.200.10
157.235.205.57
WS5100(config)#
```

12.1.9 mac

Interface Config Commands

Applies a MAC access list to a gigabit ethernet interface

NOTE: The access list cannot be applied on a management interface (me1).

Syntax

```
mac (access-group <acl_name>) (in)
```

Parameters

access-group <acl_name>	Sets the MAC access groups ACL
in	Applies the ACL to ingress packets

Example

```
WS5100(config-if)#mac access-group Ark200 in
WS5100(config-if)#
```

12.1.10 management

▸ *Interface Config Commands*

Sets the selected interface as management interface. It can only be used on a VLANx interface. The TFTP/FTP server providing the switch its config file at startup must be accessible via this interface.

VLAN 1 is the default management interface for the switch

Syntax

`management`

Parameters

None

Usage Guidelines

The management privilege can be set only on a L3 interface. Use this command along with the `(config) management secure` in the config mode. This ensure management access is restricted to the management VLAN only

Refer *management on page 5-37* for `(config) management secure` configuration.

Example

```
WS5100(config)#interface vlan 1000
WS5100(config-if)#management
WS5100(config-if)#
```

12.1.11 no

▸ *Interface Config Commands*

Negates a command or sets its defaults

Syntax

```
no [crypto|description|duplex|ip|mac|port-channel|
shutdown|spanning-tree|speed|static-channel-group|switchport]
```

Parameters

The `no` command negates any command associated with it. Wherever required, use the same parameters associated with the command getting negated

Example

```
WS5100(config-if)#no duplex
WS5100(config-if)#
```

12.1.12 port-channel

Interface Config Commands

Selects the load-balance criteria of an aggregated port

Syntax

```
port-channel (load-balance) [src-dst-ip|src-dst-mac]
```

Parameters

load-balance [src-dst-ip|src-dst-mac]	Sets load-balancing for port channel • src-dst-ip – Defines the Source and Destination IP address based on the current load balancing • src-dst-mac – Sets the Source and Destination MAC address based on the load balancing

Usage Guidelines

Use this command to configure and set load balance on the aggregated port using `(config-if) static-channel-group`.

Example

The example below creates a channel group 1, with interface ge1 and ge 2.

```
WS5100(config)#interface ge1
WS5100(config-if)#static-channel-group 1

WS5100(config)#interface ge2
WS5100(config-if)#static-channel-group 1
```

The example below defines the load balance based on the IP or MAC address

```
WS5100(config)#interface sa1
WS5100(config-if)#port-channel load-balance src--dst-ip
WS5100(config-if)#
```

12.1.13 service

Interface Config Commands

Invokes service commands to troubleshoot or debug the `(config-if)` instance configuration

Syntax

`service(show)(cli)`

Parameters

cli	Shows the CLI tree of current mode

Example

```
WS5100(config-if)#service show cli
Interface Config mode:
+-clrscr [clrscr]
+-crypto
  +-map
    +-WORD [crypto map WORD]
+-description
  +-LINE [description LINE]
+-do
  +-LINE [do LINE]
+-duplex
  +-auto [duplex (half|full|auto)]
  +-full [duplex (half|full|auto)]
  +-half [duplex (half|full|auto)]
+-end [end]
+-exit [exit]
+-help [help]
+-ip
  +-access-group
    +-<1-99>
      +-in [ip access-group (<1-99>|<100-199>|<1300-1999>|<2000-
2699>|WORD) (in)]
    +-<100-199>
.............................
.............................
WS5100(config-if)#
```

12.1.14 show

Interface Config Commands

Displays current system information running on the switch

Syntax

```
show <parameter>
```

Parameters

?	Displays the parameters for which information can be viewed using the show command

Example

```
WS5100(config-if)#show ?
  access-list           Internet Protocol (IP)
  aclstats              Show ACL Statistics information
  alarm-log             Display all alarms currently in the system
  autoinstall           autoinstall configuration
  banner                Display Message of the Day Login banner
  boot                  Display boot configuration.
  clock                 Display system clock
  commands              Show command lists
  crypto                encryption module
  debugging             Debugging information outputs
  dhcp                  DHCP Server Configuration
  environment           show environmental information
  file                  Display filesystem information
  ftp                   Display FTP Server configuration
  history               Display the session command history
  interfaces            Interface status
  ip                    Internet Protocol (IP)
  ldap                  LDAP server
  licenses              Show any installed licenses
  logging               Show logging configuration and buffer
  mac                   Internet Protocol (IP)
  mac-address-table     Display MAC address table
  management            Display L3 Managment Interface name
  mobility              Display Mobility parameters
  ntp                   Network time protocol
  password-encryption   password encryption
  port-channel          Portchannel commands
  privilege             Show current privilege level
  radius                RADIUS configuration commands
  redundancy-group      Display redundancy group parameters
```

```
  redundancy-history    Display state transition history of the
                        switch.
  redundancy-members    Display redundancy group members in detail
  running-config        Current Operating configuration
  securitymgr           Securitymgr parameters
  sessions              Display current active open connections
  snmp                  Display SNMP engine parameters
  snmp-server           Display SNMP engine parameters
  sole                  Smart Opportunistic Location Engine
                        Configuration
  spanning-tree         Display spanning tree information
  startup-config        Contents of startup configuration
  static-channel-group  static channel group membership
  terminal              Display terminal configuration parameters
  timezone              Display timezone
  upgrade-status        Display last image upgrade status
  users                 Display information about currently logged
                        in users
  version               Display software & hardware version
  wireless              Wireless configuration commands
  wlan-acl              wlan based acl

WS5100(config-if)#show

WS5100(config-if)#show access-list
Standard IP access list 1
    deny any rule-precedence 1
WS5100(config-if)#

WS5100(config-if)#show boot

Image    Build Date Install    Date                    Version
-----    --------------------  --------------------    ------------
Primary   Aug 28 14:05:16 2006  Aug 29 18:32:17 2006    3.0.0.0-200B
Secondary Aug 14 06:18:03 2006  Aug 17 15:08:28 2006    3.0.0.0-180B

Current Boot       : Primary
Next Boot          : Primary
Software Fallback  : Enabled
WS5100(config-if)#

WS5100(config-if)#show wireless ?
  ap                          Status of adopted access-port
  ap-detection-config         Detected-AP Configuration Parameters
  ap-images                   List of access-port images on the
wireless
                              switch
  ap-unadopted                List of unadopted access-port
  approved-aps                Approved APs seen by access-port
scans
```

```
  channel-power               List of available channel and power
levels for
                              a radio
  config                      Wireless Configuration Parameters
  hotspot-config              Wlan hotspot configuration
  ids                         Intrusion detection parameters
  mac-auth-local              list out the mac-auth-local entries
  mobile-unit                 Details of associated mobile-units
  phrase-to-key               display the WEP keys generated by a
passphrase
  qos-mapping                 Quality of Service mappings used for
mapping
                              WMM access categories and 802.1p /
DSCP tags
  radio                       Radio related commands
  regulatory                  Regulatory (allowed channel/power)
information
                              for a particular country
  self-heal-config            Self-Healing Configuration Parameters
  sensor                      Wireless Intrusion Protection System
parameters
  unapproved-aps              Unapproved APs seen by access-port or
                              mobile-unit scans
  wireless-switch-statistics  wireless-switch  statistics
  wlan                        Wireless LAN related parameters

WS5100(config-if)#
WS5100(config-if)#show wireless config
country-code            : None
adoption-pref-id        : 1
proxy-arp               : enabled
adopt-unconf-radio      : enabled
dot11-shared-key-auth   : disabled
ap-detection            : disabled
oversized-frames        : disabled
manual-wlan-mapping     : disabled
dhcp sniff state        : disabled
dhcp fix windows        : disabled
broadcast-tx-speed      : optimize-for-throughput
smart-scan 11a channels :
smart-scan 11bg channels:
WS5100(config-if)#
```

12.1.15 shutdown

Interface Config Commands

Disables the selected interface. The interface is administratively enabled unless explicitly disabled using this command

Syntax

```
shutdown
```

Parameters

None

Example

```
WS5100(config-if)#shutdown
WS5100(config-if)#
```

12.1.16 spanning-tree

Interface Config Commands

Configures spanning tree parameters

Syntax

```
spanning-tree [bpdufilter(enable|disable)|
bpduguard(enable|disable)|edgeport|
force-version <0-3>|guard (root)|link-type(point-topoint|shared)|
mst(<0-15>|port-cisco-interoperability)|portfast]

spanning-tree mst [<0-15>(cost <1-200000000>|
port-priority <0-240>)|port-cisco-interoperability(disable|enable)]
```

Parameters

bpdufilter (disable|enable)	Use this command to set a portfast BPDU filter for the port. Use the `no` parameter with this command to revert the port BPDU filter to default. The spanning tree protocol sends BPDUs from all ports. Enabling the BPDU filter ensures PortFastenabled ports do not transmit or receive BPDUs.

bpduguard (disable|enable)	Use this command to enable or disable the BPDU guard feature on a port. Use the `no` parameter with this command to set the BPDU guard feature to default values. When the BPDU guard is set for a bridge, all portfast-enabled ports that have the BPDU-guard set to default shut down the port upon receiving a BPDU. If this occurs, the BPDU is not processed. The port can be brought back either manually (using the `no shutdown` command), or by configuring the errdisable-timeout to enable the port after the specified interval.
edgeport	Enables an interface as an edgeport.
force-version <0-3>	Specifies the spanning-tree force version. A version identifier of less than 2 enforces the spanning tree protocol. Select from the following versions: • *0 – STP* • *1 – Not supported.* • *2 – RSTP* • *3 – MSTP* The default value for forcing the version is MSTP
guard (root)	Enables the Root Guard feature for the port. The root guard disables the reception of superior BPDUs. The Root Guard ensures the enabled port is a designated port. If the Root Guard enabled port receives a superior BPDU, it moves to a discarding state. Use the `no` parameter with this command to disable the root guard feature.
link-type (point-to-point|shared)	Enables or disables point-to-point or shared link types. • point-to-point – Enables rapid transition • shared – Disables rapid transition

mst [<0-15> (cost <1-200000000>| port-priority <0-240>)| port-cisco-interoperability (disable|enable)]	Configures MST values on a spanning tree
	• <0-15> – Defines the Instance ID
	  • cost <1-200000000> – Defines the path cost for a port
	  • port-priority <0-240> – Defines the port priority for a bridge
	• port-cisco-interoperability (disable|enable) – Enables or disables interoperability with Cisco's version of MSTP (which is incompatible with standard MSTP)
	  • enable – Enables CISCO Interoperability
	  • disable – Disables CISCO Interoperability
	The default value for is `disabled`.

portfast	Enables rapid transitions

Example

```
WS5100(config-if)#spanning-tree edgeport
WS5100(config-if)#

WS5100(config-if)#spanning-tree guard root
WS5100(config-if)#

WS5100(config-if)#spanning-tree link-type point-to-point
WS5100(config-if)#

WS5100(config-if)#spanning-tree link-type shared
WS5100(config-if)#
```

12.1.17 speed

▸ *Interface Config Commands*

Specifies the speed of a fast-ethernet (10/100) or a gigabit-ethernet port (10/100/1000)

Syntax

```
speed(10|100|1000|auto)
```

Parameters

10	Forces 10 Mbps operation
100	Forces 100 Mbps operation
1000	Forces 1000 Mbps operation
auto	Port automatically detects the speed it should run based on the port at the other end of the link

Usage Guidelines

Set the interface speed to auto to detect and use the fastest speed available. Speed detection is based on connected network hardware

Example

```
WS5100(config-if)#speed auto
WS5100(config-if)#
```

12.1.18 static-channel-group

Interface Config Commands

Adds an interface to a static channel group

Syntax

```
static-channel-group <1-2>
```

Parameters

<1-2>	Sets a static channel group to associate the link with

Usage Guidelines

This command aggregates individual giga port's into a single aggregate link to provide a larger bandwidth. The static channel group is used to provide additional bandwidth in multiples of 1Gbps on the switch. All MAC layer and higher protocols see only the static channel group (aggregate link) rather than the individual ports that comprise it.

Example

```
WS5100(config-if)#static-channel-group 2
WS5100(config-if)#
```

12.1.19 switchport

Interface Config Commands

Sets switching mode characteristics for the selected interface

Syntax

```
switchport(access|mode|trunk)
switchport access vlan <1-4094>
switchport mode(access|trunk)
switchport trunk(allowed|native)
switchport trunk allowed vlan(add|none|remove)[VLAN_ID]
switchport trunk native(tagged|vlan<1-4094>)
```

Parameters

access	Configures the access VLAN of an access-mode port • vlan <1-4094> – Sets the VLAN when interface is in access mode
mode	Sets the mode of the interface to access or trunk mode. Can only be used on physical (layer2) interfaces • access – If `access` mode is selected, the access VLAN is automatically set to VLAN1. In this mode, only untagged packets in the access VLAN (vlan1) are accepted on this port. All tagged packets are discarded • trunk – If `trunk` mode is selected, tagged VLAN packets VLANs are accepted. The native VLAN is automatically set to VLAN1. Untagged packets are placed in the native VLAN by the switch. Outgoing packets in the native VLAN are sent untagged `trunk` is the default mode for both ports

trunk	Sets the trunking mode characteristics • allowed – Configures trunk characteristics when the port is in trunk-mode. • vlan – Sets allowed VLANs • add – Adds VLANs to the current list • none – Allows no VLANs to Xmit/Rx through the Layer2 interface • remove – Removes VLANs from the current lis . • VLAN_ID – VLAN_IDs added or removed. Can be either a range of VLANs (55-60) or a list of comma separated VLAN IDs (35, 41 etc.) • native – Configures the native VLAN ID of the trunk-mode port • tagged – Tags the native VLAN • vlan <1-4094> – Sets the native VLAN for classifying untagged traffic when interface is in trunking mode

Usage Guidelines

Interfaces ge1-ge4 can be configured as trunk or in access mode. An interface (when configured as trunk) allows packets (from the given list of VLANs) to be added to the trunk. An inerface configured as access allows packets only from native VLANs

Use the `[no] switchport (access|mode|trunk)` to undo switchport configurations

Example

```
WS5100(config-if)#switchport mode access
WS5100(config-if)#
```

13

spanning tree-mst Instance

Use the `(config-mst)` instance to configure the switch's *Multi Spanning Tree Protocol* (MSTP) configuration.

13.1 mst Config Commands

Table 13.1 summarizes the **`(config-mst)`** commands:

Table 13.1 MSTP Config Command Summary

Command	Description	Ref.
clrscr	Clears the display screen	*page 13-2*
end	Ends the current mode and moves to the EXEC mode	*page 13-2*
exit	Ends the current mode and moves to the previous mode	*page 13-3*
help	Displays the system's interactive help system	*page 13-3*
instance	Assigns a VLAN to the bridge instance	*page 13-4*
name	Sets a name for the MST region	*page 13-4*
no	Negates a command or sets defaults	*page 13-5*
revision	Configures the revision number of the MST bridge	*page 13-5*
service	Invokes the service commands needed to troubleshoot or debug `(config-if)` instance configurations	*page 13-6*

Table 13.1 MSTP Config Command Summary (Continued)

Command	Description	Ref.
show	Shows running system information	*page 13-7*

13.1.1 clrscr

mst Config Commands

Clears the display

Syntax

```
clrscr
```

Parameters

None

Example

```
WS5100(config-mst)#clrscr
WS5100(config-mst)#
```

13.1.2 end

mst Config Commands

Ends and exits the current mode and moves to the PRIV EXEC mode. The prompt changes to `WS5100#`.

Syntax

```
end
```

Parameters

None

Example

```
WS5100(config-mst)#end
WS5100#
```

13.1.3 exit

mst Config Commands

Ends the current mode and moves to the previous mode (GLOBAL-CONFIG). The prompt changes to `WS5100(config)#`

Syntax

```
exit
```

Parameters

None

Example

```
WS5100(config-mst)#exit
WS5100(config)#
```

13.1.4 help

mst Config Commands

Dispalys the system's interactive help system

Syntax

```
help
```

Parameters

None

Example

```
WS5100(config-mst)#help
CLI provides advanced help feature. When you need help,
anytime at the command line please press '?'.

If nothing matches, the help list will be empty and you must backup
until entering a '?' shows the available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each possible
   argument.
2. Partial help is provided when an abbreviated argument is entered
   and you want to know what arguments match the input
   (e.g. 'show ve?'.)

WS5100(config-mst)#
```

13.1.5 instance

mst Config Commands

Associates VLAN(s) with an instance

Syntax

```
instance <1-15> vlan <VLAN_ID>
```

Parameters

<1-15>	Defines the instance ID to which the VLAN is associated
vlan <VLAN_ID>	Sets the VLAN ID for its association with an instance

Usage Guidelines

MSTP works based instances. An instance is a group of VLANs with a common spanning tree. A single VLAN cannot be associated with multiple instances

Switches with the same instance, VLAN mapping, revision number and region names define a unique region. Switches in the same region exchange *bridge protocol data units* (BPDUs) with instance record information within it

Example

The example below sets an instance named 10 and maps VLAN 20 to it

```
WS5100(config-mst)#instance 10 vlan 20
WS5100(config-mst)#
```

13.1.6 name

mst Config Commands

Sets the name for the MST region

Syntax

```
name (region name)
```

Parameters

region name	MST region name

Example

```
WS5100(config-mst)#name MyRegion
WS5100(config-mst)#
```

13.1.7 no

mst Config Commands

Negates a command or sets its defaults

Syntax

```
no [instance|name|revision]
```

Parameters

instance	Sets the MST Instance
name	Assigns a name to the MST region
revision	Defines the revision number for configuration information

Usage Guidelines

The `no` command negates any command associated with it. Wherever required, use the same parameters associated with the command getting negated

Example

```
WS5100(config-mst)#no instance 10 vlan 20
WS5100(config-mst)#

WS5100(config-mst)#no name MyRegion
WS5100(config-mst)#

WS5100(config-mst)#no revision
WS5100(config-mst)#
```

13.1.8 revision

mst Config Commands

Sets the revision number of the MST bridge

Syntax

```
revision <0-255>
```

Parameters

0-255	Defines the revision number for configuration information

Example

```
WS5100(config-mst)#revision 20
WS5100(config-mst)#
```

13.1.9 service

mst Config Commands

Invokes the service commands needed to troubleshoot or debug `(config-if)` instance configurations

Syntax

```
service(show) (cli)
```

Parameters

None

Example

```
WS5100(config-mst)#service show cli
MSTI configuration mode:
+-clrscr [clrscr]
+-end [end]
+-exit [exit]
+-help [help]
+-instance
  +-<1-15> [instance <1-15>]
    +-vlan
      +-VLAN_ID [instance <1-15> vlan VLAN_ID]
+-name
  +-LINE [name LINE]
+-no
  +-instance
    +-<1-15> [no instance <1-15>]
      +-vlan
        +-VLAN_ID [no instance <1-15> vlan VLAN_ID]
  +-name [no name]
  +-revision [no revision]
+-quit [quit]
+-revision
  +-REVISION_NUM [revision REVISION_NUM]
+-s
  +-commands [show commands]
    +-WORD [show commands WORD]
  +-running-config [show running-config]
    +-full [show running-config full]
    +-include-factory [show running-config include-factory]
+-service
```

```
  +-show
    +-cli [service show cli]
+-show
  +-access-list [show access-list]
    +-<1-99> [show access-list (<1-99>|<100-199>|<1300-1999>|<2000-
2699>|WORD)]
    +-<100-199> [show access-list (<1-99>|<100-199>|<1300-
1999>|<2000-2699>|WORD)]
    +-<1300-1999> [show access-list (<1-99>|<100-199>|<1300-
1999>|<2000-2699>|WORD)]
    +-<2000-2699> [show access-list (<1-99>|<100-199>|<1300-
1999>|<2000-2699>|WORD)]
    +-WORD [show access-list (<1-99>|<100-199>|<1300-1999>|<2000-
2699>|WORD)]
  +-aclstats
    +-vlan
      +-<1-4094> [show aclstats ( vlan <1-4094> )].................
.................................................................
.................................................................

WS5100(config-mst)#
```

13.1.10 show

mst Config Commands

Displays current system information

Syntax

```
show <parameter>
```

Parameters

?	Displays the parameters for which information can be viewed using the show command

Example

```
WS5100(config-mst)#show ?
  access-list           Internet Protocol (IP)
  aclstats              Show ACL Statistics information
  alarm-log             Display all alarms currently in the system
  autoinstall           autoinstall configuration
  banner                Display Message of the Day Login banner
  boot                  Display boot configuration.
  clock                 Display system clock
  commands              Show command lists
  crypto                encryption module
```

```
  debugging              Debugging information outputs
  dhcp                   DHCP Server Configuration
  environment            show environmental information
  file                   Display filesystem information
  ftp                    Display FTP Server configuration
  history                Display the session command history
  interfaces             Interface status
  ip                     Internet Protocol (IP)
  ldap                   LDAP server
  licenses               Show any installed licenses
  logging                Show logging configuration and buffer
  mac                    Internet Protocol (IP)
  management             Display L3 Managment Interface name
  mobility               Display Mobility parameters
  ntp                    Network time protocol
  password-encryption    password encryption
  port-channel           Portchannel commands
  privilege              Show current privilege level
  radius                 RADIUS configuration commands
  redundancy-group       Display redundancy group parameters
  redundancy-history     Display state transition history of the
switch.
  redundancy-members     Display redundancy group members in detail
  running-config         Current Operating configuration
  securitymgr            Securitymgr parameters
  sessions               Display current active open connections
  snmp                   Display SNMP engine parameters
  snmp-server            Display SNMP engine parameters
  sole                   Smart Opportunistic Location Engine
Configuration
  spanning-tree          Display spanning tree information
  startup-config         Contents of startup configuration
  static-channel-group   static channel group membership
  terminal               Display terminal configuration parameters
  timezone               Display timezone
  upgrade-status         Display last image upgrade status
  users                  Display information about currently logged
in users
  version                Display software & hardware version
  wireless               Wireless configuration commands
  wlan-acl               wlan based acl

WS5100(config-mst)#show
```

14

Extended ACL Instance

Use the `(config-ext-nacl)` instance to configure the `ip access-list extended` ACLs associated with the switch

14.1 Extended ACL Config Commands

Table 14.1 summarizes `config-ext-nacl` commands:

Table 14.1 Extended ACL Config Command Summary

Command	Description	Ref.
clrscr	Clears the display screen	*page 14-2*
deny	Specifies packets to reject	*page 14-2*
end	Ends the current mode and moves to the EXEC mode	*page 14-7*
exit	Ends the current mode and moves to the previous mode	*page 14-7*
help	Displays the interactive help system	*page 14-8*
mark	Specifies packets to mark	*page 14-8*
no	Negates a command or sets its defaults	*page 14-12*
permit	Specifies packets to forward	*page 14-13*

Table 14.1 Extended ACL Config Command Summary (Continued)

Command	Description	Ref.
service	Invokes the service commands to troubleshoot or debug `(config-if)` instance configurations	*page 14-18*
show	Displays running system information	*page 14-20*
terminal	Sets terminal line parameters	*page 14-21*

14.1.1 clrscr

Extended ACL Config Commands

Clears the display screen

Syntax

```
clrscr
```

Parameters

None

Example

```
WS5100(config-ext-nacl)#clrscr
WS5100(config-ext-nacl)#
```

14.1.2 deny

Extended ACL Config Commands

Specifiesy packets to reject

Syntax

```
deny(icmp|ip|tcp|udp)

deny {ip} {source/source-mask | host source | any} {destination/
destination-mask  | host destination | any} [log] [rule-precedence
access-list-entry precedence]

deny {icmp} {source/source-mask | host source | any} {destination/
destination-mask | host destination | any} [icmp-type | [icmp-type
icmp-code]] [log] [rule-precedence access-list-entry precedence]
```

```
deny {tcp|udp} {source/source-mask | host source | any} [operator
source-port] {destination/destination-mask | host destination |
any} [operator destination-port] [log] [rule-precedence access-
list-entry precedence]
```

Parameters

deny {**ip**} {source/source-mask | host source | any} {destination/destination-mask | host destination | any} [log] [rule-precedence access-list-entry precedence]	Use with a `deny` command to reject IP packets
	• deny – Sets the action type on an ACL
	• {ip} – Specifies an IP (to match to a protocol)
	• {source/source-mask | host source | any} – The keyword source is the source IP address of the network or host in dotted decimal format. The source-mask is the network mask. For example, 10.1.1.10/24 indicates the first 24 bits of the source IP is used for matching
	  • *any* is an abbreviation for a source IP of 0.0.0.0 and source-mask bits equal to 0
	  • *host* is an abbreviation for the exact source (A.B.C.D) and source-mask bits equal to 32
	• {destination/destination-mask | host destination | any} – Defines the destination host IP address or destination network address
	• [log] – Generates log messages when the packet coming from the interface matches an ACL entry. Log messages are generated only for router ACLs
	• [rule-precedence access-list-entry precedence] – Defines an integer value between 1-5000. This value sets the rule precedence in the ACL

deny {**icmp**} {source/ source-mask | host source | any} {destination/ destination-mask | host destination | any} [icmp-type | [icmp-type icmp-code]] [log] [rule-precedence access-list-entry precedence]	Use with the `deny` command to reject ICMP packets
	• deny – Rejects ICMP packets
	• {icmp} – Specifies ICMP as the protocol
	• {source/source-mask | host source | any} – The source is the source IP address of the network or host (in dotted decimal format). The source-mask is the network mask. For example, 10.1.1.10/24 indicates the first 24 bits of the source IP is used for matching
	  • *any* is an abbreviation for a source IP of 0.0.0.0 and source-mask bits equal to 0
	  • *host* is an abbreviation for exact source (A.B.C.D) and source-mask bits equal to 32
	• {destination/ destination-mask | host destination | any} – Defines the destination host IP address or destination network address
	• [icmp-type |icmp-type icmp-code] – Sets the ICMP type value from 0 to 255, and is valid only for ICMP. The ICMP code value is from 0 to 255, and is valid only for protocol type icmp
	• [log] – Generates log messages when the packet coming from the interface matches the ACL entry. Log messages are generated only for router ACLs
	• [rule-precedence access-list-entry precedence] – Defines an integer value between 1-5000. This value sets the rule precedence in the ACL

deny {**tcp|udp**} {source/source-mask | host source | any} [operator source-port] {destination/destination-mask | host destination | any} [operator destination-port] [log] [rule-precedence access-list-entry precedence]	Use with the `deny` command to reject TCP or UDP packets
	• deny – Rejects TCP or UDP packets
	• {tcp|udp} – Specifies TCP or UDP as the protocol
	• {source/source-mask | host source | any} – The source is the source IP address of the network or host (in dotted decimal format). The source-mask is the network mask. For example, 10.1.1.10/24 indicates the first 24 bits of the source IP are used for matching
	  • *any* is an abbreviation for a source IP of 0.0.0.0, and the source-mask bits are equal to 0
	  • *host* is an abbreviation for exact source (A.B.C.D) and the source-mask bits equal to 32
	• [operator source-port] – Valid only for TCP or UDP protocols. Valid values are *eq* and *range*
	  • range – Specifies the protocol range (starting and ending protocol numbers)
	  • port – Sets the valid port number
	• {destination/destination-mask | host destination | any} – Defines the destination host IP address or destination network address
	• [operator destination-port] – Specifies the destination port
	• [log] – Generates log messages when the packet coming from the interface matches the ACL entry. Log messages are generated only for router ACLs
	• [rule-precedence access-list-entry precedence] – Defines an integer value between 1-5000. This value sets the rule precedence in the ACL

Usage Guidelines

Use this command to deny traffic between networks/hosts based on the protocol type selected in the access list configuration. The following protocol types are supported:

- *ip*
- *icmp*
- *tcp*
- *udp*

The last ACE in the access list is an implicit deny statement.

Whenever the interface receives the packet, its content is checked against the ACEs in the ACL. It is allowed/denied based on the ACL configuration.

- Filtering TCP/UDP allows the user to specify port numbers as filtering criteria
- Select the ICMP as the protocol to allow/deny ICMP packets. Selecting icmp provides the option of filtering icmp packets based on icmp type and code

NOTE: The log option is functional only for router ACL's. The log option displays an informational logging message about the packet that matches the entry sent to the console.

Example

The following example denies traffic between two subnets:

```
WS5100(config-ext-nacl)#deny ip 192.168.2.0/24 192.168.1.0/24
WS5100(config-ext-nacl)#permit ip any any
WS5100(config-ext-nacl)#
```

The following example denies TCP traffic with a source port range between 20 - 23 (from the source subnet to destination subnet):

```
WS5100(config-ext-nacl)#deny tcp 192.168.1.0/24 192.168.2.0/
24 range 20 23
WS5100(config-ext-nacl)#permit ip any any
WS5100(config-ext-nacl)#
```

The following example denies UDP traffic with a source port range between 20 - 23 (from the source subnet to destination subnet):

```
WS5100(config-ext-nacl)#deny udp 192.168.1.0/24 192.168.2.0/
24 range 20 23
WS5100(config-ext-nacl)#permit ip any any
WS5100(config-ext-nacl)#
```

The following example denies ICMP traffic from any source to any destination. The keyword *any* is used to match:

```
any source or destination IP address.
WS5100(config-ext-nacl)#deny icmp any any
WS5100(config-ext-nacl)#permit ip any any
WS5100(config-ext-nacl)#
```

14.1.3 end

Extended ACL Config Commands

Ends and exits the current mode and moves to the PRIV EXEC mode. The prompt changes to `WS5100#`

Syntax

```
end
```

Parameters

None

Example

```
WS5100(config-ext-nacl)#end
WS5100#
```

14.1.4 exit

Extended ACL Config Commands

Ends the current mode and moves to the previous mode (GLOBAL-CONFIG). The prompt changes to `WS5100(config)#`

Syntax

```
exit
```

Parameters

None

Example

```
WS5100(config-ext-nacl)#exit
WS5100(config)#
```

14.1.5 help

Extended ACL Config Commands

Displays the system's interactive help system

Syntax

```
help
```

Parameters

None

Example

```
WS5100(config-ext-nacl)#help
CLI provides advanced help feature.  When you need help,
anytime at the command line please press '?'.

If nothing matches, the help list will be empty and you must backup
until entering a '?' shows the available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each possible
   argument.
2. Partial help is provided when an abbreviated argument is entered
   and you want to know what arguments match the input
   (e.g. 'show ve?'.)

WS5100(config-ext-nacl)#
```

14.1.6 mark

Extended ACL Config Commands

Specifies packets to mark

Syntax

```
mark {dot1p <0-7> | tos <0-255>}} {ip} {source/source-mask | host
source | any} {destination/destination-mask  | host destination |
any} [log] [rule-precedence access-list-entry precedence]

mark {dot1p <0-7> | tos <0-255>}} {icmp} {source/source-mask | host
source | any} {destination/ destination-mask | host destination |
any} [icmp-type | [icmp-type icmp-code]] [log] [rule-precedence
access-list-entry precedence]

mark {dot1p <0-7> | tos <0-255>}} {tcp|udp} {source/source-mask |
host source | any} [operator source-port] {destination/destination-
mask | host destination | any} [operator destination-port] [log]
[rule-precedence access-list-entry precedence]
```

Parameters

mark {dot1p <0-7> | tos <0-255>}} {**ip**} {source/ source-mask | host source | any} {destination/ destination-mask | host destination | any} [log] [rule-precedence access-list-entry precedence]	Use with the `mark` command to specify IP packets as marked
	• mark {dot1p <0-7> | tos <0-255>} – Defines action types on an ACL. `mark` is functional only over a Port ACL
	  • dot1p <0-7> – Used only with the action type `mark` to specify 8021p priority values
	  • tos <0-255> – Used only with action the type `mark` to specify *Type Of Service* (tos) values
	• {ip} – Specifies an IP (to match any protocol)
	• {source/source-mask | host source | any} – The source is the source IP address of the network or host (in dotted decimal format). Source-mask is the network mask. For example, 10.1.1.10/24 indicates the first 24 bits of the source IP are used for matching
	  • *any* is an abbreviation for source IP of 0.0.0.0 and source-mask bits equal to 0
	  • *host* is an abbreviation for the exact source (A.B.C.D) and source-mask bits equal to 32
	• {destination/destination-mask | host destination | any} – Defines the destination host IP address or destination network address
	• [log] – Generates log messages when the packet coming from the interface matches the ACL entry. Log messages are generated only for router ACLs
	• [rule-precedence access-list-entry precedence] – Sets an integer value between 1-5000. This value sets the rule precedence in the ACL

mark {dot1p <0-7> | tos <0-255>}} {**icmp**} {source/source-mask | host source | any} {destination/ destination-mask | host destination | any} [icmp-type | [icmp-type icmp-code]] [log] [rule-precedence access-list-entry precedence]	Use with the `mark` command to specify ICMP packets as marked.
	• mark {dot1p <0-7> | tos <0-255>} – Action types on an ACL. The action type `mark` is functional only over a Port ACL
	• {icmp} – Specifies ICMP as the protocol
	• {source/source-mask | host source | any} – The source is the source IP address of the network or host (in dotted decimal format). The source-mask is the network mask. For example, 10.1.1.10/24 indicates the first 24 bits of the source IP is used for matching
	  • *any* is an abbreviation for source IP of 0.0.0.0 and source-mask bits equal to 0
	  • *host* is an abbreviation for exact source (A.B.C.D) and source-mask bits equal to 32
	• {destination/ destination-mask | host destination | any} – Sets the destination host IP address or destination network address
	• [icmp-type |icmp-type icmp-code] – Defines the ICMP value from 0 to 255. The value is valid only for ICMP. Define an ICMP code value from 0 to 255 (valid for ICMP only)
	• [log] – Generates log messages when the packet coming from the interface matches the ACL entry. Log messages are generated only for router ACLs
	• [rule-precedence access-list-entry precedence] – Sets an integer value between 1-5000. This value sets the rule precedence in the ACL

Usage Guidelines

This command marks traffic between networks/hosts based on the protocol type selected in the access list configuration

Use the mark option to specify the t*ype of service* (tos) and priority value. The tos value is marked in the IP header and the 802.1p priority value is marked in the dot1q frame.

- The following types of protocols are supported:
- *ip*
- *icmp*
- *tcp*
- *udp*

Whenever the interface receives the packet, its content is checked against all ACEs in the ACL. It is marked based on the ACL configuration

- Filtering protocol types TCP/UDP allows the user to specify port numbers as filtering criteria
- Select ICMP to allow/deny ICMP packets. Selecting ICMP allows you to filter packets based on the ICMP type and code

NOTE: The log option is functional only for router ACL's. The log option provides an informational logging message about the packet matching the entry sent to the console.

Example

The example below marks the dot1p priority value in the ethernet header to 5 on all TCP traffic coming from the source subnet:

```
WS5100(config-ext-nacl)#mark 8021p 5 tcp 192.168.2.0/24 any
WS5100(config-ext-nacl)#
```

The example below marks the tos value in the IP header to 245 on all tcp traffic coming from the source subnet:

```
WS5100(config-ext-nacl)#mark tos 245 tcp 192.168.2.0/24 any
WS5100(config-ext-nacl)#
```

14.1.7 no

Extended ACL Config Commands

Negates a command or sets its defaults

Syntax

```
no(deny|mark|permit)
```

Negates all the syntax combinations used in the *deny*, *mark* and *permit* designations to configure the Extended ACL

Parameters

deny	Specifies packets to reject
mark	Specifies packets to mark
permit	Specifies packets to forward

Usage Guidelines

Removes an access list control entry. Provide the rule-precedence value when using the no command

Example

```
WS5100(config-ext-nacl)#no mark 8021p 5 tcp 192.168.2.0/24 any
rule-precedence 10
WS5100(config-ext-nacl)#

WS5100(config-ext-nacl)#no permit ip any any rule-precedence 10
WS5100(config-ext-nacl)#

WS5100(config-ext-nacl)#no deny icmp any any rule-precedence 10
WS5100(config-ext-nacl)#
```

14.1.8 permit

Extended ACL Config Commands

Permits specific packets

NOTE: ACLs do not allow DHCP messages to flow by default. Configure an *Access Control Entry* (ACE) to allow DHCP messages to flow through.

```
WS5100(config-ext-nacl)#permit ip xxx.xxx.xxx.xxx/x
192.168.2.0/24

WS5100(config-ext-nacl)#permit ip any host
xxx.xxx.xxx.xxx

WS5100(config-ext-nacl)#
```

Syntax

```
permit {ip} {source/source-mask | host source | any} {destination/
destination-mask  | host destination | any} [log] [rule-precedence
access-list-entry precedence]

permit {icmp} {source/source-mask | host source | any}
{destination/ destination-mask | host destination | any} [icmp-type
| [icmp-type icmp-code]] [log] [rule-precedence access-list-entry
precedence]

permit{tcp|udp} {source/source-mask | host source | any} [operator
source-port] {destination/destination-mask | host destination |
any} [operator destination-port] [log] [rule-precedence access-
list-entry precedence]
```

Parameters

permit {**ip**} {source/source-mask | host source | any} {destination/destination-mask | host destination | any} [log] [rule-precedence access-list-entry precedence]	Use the `permit` command to allow IP packets
	• permit – Allows IP packets
	• {**ip**} – Specifies the IP (to match to any protocol)
	• {source/source-mask | host source | any} – The source is the source IP address of the network or host (in dotted decimal format). The source-mask is the network mask. For example, 10.1.1.10/24 indicates the first 24 bits of the source IP are used for matching
	  • *any* is an abbreviation for source IP of 0.0.0.0 and source-mask bits equal to 0
	  • *host* is an abbreviation for exact source (A.B.C.D) and source-mask bits equal to 32
	• {destination/destination-mask | host destination | any} – Sets the destination host IP address or destination network address
	• [log] – Generates log messages when the packet coming from the interface matches the ACL entry. Log messages are generated only for router ACLs
	• [rule-precedence access-list-entry precedence] – Sets an integer value between 1-5000. This value sets the rule precedence in the ACL

permit {**icmp**}
{source/source-mask | host source | any}
{destination/ destination-mask | host destination | any}
[icmp-type |
[icmp-type icmp-code]]
[log]
[rule-precedence access-list-entry precedence]
	Use with the `permit` command to allow ICMP packets
	• permit – Allows ICMP packets on an ACL.
	• {icmp} – Specifies ICMP as the protocol.
	• {source/source-mask | host source | any} – The keyword source is the source IP address of the network or host (in dotted decimal format). The source-mask is the network mask. For example, 10.1.1.10/24 indicates the first 24 bits of the source IP are used for matching
	  • *any* is an abbreviation for source IP of 0.0.0.0 and source-mask bits equal to 0.
	  • *host* is an abbreviation for exact source (A.B.C.D) and source-mask bits equal to 32.
	• {destination/ destination-mask | host destination | any} – Defines the destination host IP address or destination network address
	• [icmp-type |icmp-type icmp-code] – Sets the ICMP type value from 0 to 255 (valid only for ICMP). Set an ICMP code value from 0 to 255 (valid only for ICMP)
	• [log] – Generates log messages when the packet coming from the interface matches the ACL entry. Log messages are generated only for router ACLs
	• [rule-precedence access-list-entry precedence] – Set an integer value between 1-5000. This value sets the rule precedence in the ACL

permit{**tcp|udp**} {source/source-mask | host source | any} [operator source-port] {destination/destination-mask | host destination | any} [operator destination-port] [log] [rule-precedence access-list-entry precedence]	Use with the `permit` command to allow TCP or UDP packets
	• permit – Allows TCP or UDP packets
	• {tcp|udp} – Specifies TCP or UDP as the protocol.
	• {source/source-mask | host source | any} – The source is the source IP address of the network or host (in dotted decimal format). The source-mask is the network mask. For example, 10.1.1.10/24 indicates the first 24 bits of the source IP are used for matching
	  • *any* is an abbreviation for a source IP of 0.0.0.0 with the source-mask bits being equal to 0
	  • *host* is an abbreviation for exact source (A.B.C.D) with the source-mask bits being equal to 32
	• [operator source-port] – Valid only for TCP or UDP protocols. Valid values are *eq* and range
	  • range – Specifies the protocol range (starting and ending protocol numbers).
	  • port – Sets the valid port number
	• {destination/destination-mask | host destination | any} – Sets the destination host IP address or destination network address
	• [operator destination-port] – Specifies the destination port
	• [log] – Generates log messages when the packet coming from the interface matches the ACL entry. Log messages are generated only for router ACLs
	• [rule-precedence access-list-entry precedence] – Sets an integer value between 1-5000. This value sets the rule precedence in the ACL

Usage Guidelines

Use this command to permit traffic between networks/hosts based on the protocol type selected in the access list configuration. The following protocols are supported:

- *ip*
- *icmp*
- *tcp*
- *udp*

The last ACE in the access list is an implicit deny statement.

Whenever the interface receives the packet, its content is checked against all the ACEs in the ACL. It is allowed based on the ACL configuration.

- Filtering on TCP/UDP allows the user to specify port numbers as filtering criteria
- Select ICMP to allow/deny packets. Selecting ICMP allows to filter ICMP packets based on type and code

NOTE: The log option is functional only for router ACL's. The log option displays an informational logging message about the packet matching the entry sent to the console.

Example

The example below allows IP traffic from the source subnet to the destination subnet and denies all other traffic over an interface:

```
WS5100(config-ext-nacl)#permit ip 192.168.1.10/24 192.168.2.0/24
rule-precedence 40
WS5100(config-ext-nacl)#
```

The example below permits Telnet traffic from the source subnet and the destination subnet and denies all other traffic over an interface:

```
WS5100(config-ext-nacl)#permit tcp 192.168.4.0/24 192.168.5.0/24 eq
23 rule-pre
cedence 10
WS5100(config-ext-nacl)#
```

The example below permits ICMP traffic and denies all other traffic over an interface:

```
WS5100(config-ext-nacl)#permit icmp any any rule-precedence 30
WS5100(config-ext-nacl)#)#
```

14.1.9 service

Extended ACL Config Commands

Invokes service commands to troubleshoot or debug the `(config-if)` instance configurations

Syntax

```
service(clear|diag-shell|save-cli|show|start-shell|tethereal)
```

Parameters

clear	Removes the specified support information
diag-shell	Provides diagnostic shell access to debug and test the switch
save-cli	Saves CLI tree for all modes (in HTMLformat)
show	Displays the running system information
start-shell	Provides shell access
tethereal	Dumps and analyzes network traffic

Example

```
WS5100(config-ext-nacl)#service diag-shell

Diagnostic shell started for testing

diag >
  boot            Reboots the switch
  delete          Deletes specified file from the system.
  exit            Exit from the CLI
  fallback        Configures firmware fallback feature
  help            Description of the interactive help system
  logout          Exit from the CLI
  no              Negate a command or set its defaults
  reload          Halt and perform a warm reboot
  service         Service Commands
  show            Show running system information
  upgrade         Upgrade firmware image
```

```
diag >
WS5100(config-ext-nacl)#service save-cli
 CLI command tree is saved as clitree.html.
 This tree can be viewed via web at http://<ipaddr>/cli/
clitree.html
WS5100(config-ext-nacl)#

WS5100(config-ext-nacl)#service show ?
  cli              Show CLI tree of current mode
  command-history  Display command (except show commands) history.
  crash-info       Display information about core, panic and AP
dump files
  info             Show snapshot of available support information
  last-passwd      Display last password used to enter shell
  reboot-history   Show reboot history
  startup-log      Show startup log
  upgrade-history  Show upgrade history

WS5100(config-ext-nacl)#service show

WS5100(config-ext-nacl)#service start-shell
Last password used: password with MAC 00:a0:f8:65:ea:8e
Password:

WS5100(config-ext-nacl)#service tethereal ?
  LINE  tethereal options in the format
        [-V (print detailed packet)] [-x (hex dump of packet)]
        [-p (no promiscuous mode for interface)]
        [-n (disable name resolution)] [-c <count> ] [-h (detailed
help)]
        [-E (to capture ESPD) ][-e (capture nonEspd packets)]
        [-f <capture filter expression in format "xx xx xx"> ]
        [-i <interface on which to capture packets> ] [-W (wisp
packet only)]
        [-s <snaplen> ] [-r <filename> (read contents of specified
file)]
        [-w <savefile> (save capture in specified file) ]
        [-X (for examples on tethereal capture filter) ]

WS5100(config-ext-nacl)#service tethereal
```

14.1.10 show

Extended ACL Config Commands

Displays current system information running on the switch

Syntax

```
show<paramater>
```

Parameters

?	Displays the parameters for which information can be viewed using the show command

Example

```
WS5100(config-ext-nacl)#show ?
  access-list           Internet Protocol (IP)
  alarm-log             Display all alarms currently in the system
  autoinstall           autoinstall configuration
  banner                Display Message of the Day Login banner
  boot                  Display boot configuration.
  clock                 Display system clock
  commands              Show command lists
  crypto                crypto
  debugging             Display debugging setting
  environment           show environmental information
  file                  Display filesystem information
  ftp                   Display FTP Server configuration
  history               Display the session command history
  interfaces            Interface status and configuration
  ip                    Internet Protocol (IP)
  ldap                  ldap server
  licenses              Show any installed licenses
  logging               Show logging configuration and buffer
  mac                   Media Access Control
  management            Display L3 Managment Interface name
  mobility              Display Mobility Parameters
  ntp                   Network time protocol
  password-encryption   password encryption
  privilege             Show current privilege level
  radius                Radius configuration commands
  redundancy-group      Display redundancy group parameters
  redundancy-history    Display state transition history of the
switch.
  redundancy-members    Display redundancy group members in detail
  running-config        Current Operating configuration
  securitymgr           Display debug info for ACL, VPN and NAT
```

```
  sessions              Display current active open connections
  snmp                  Display SNMP engine parameters
  snmp-server           Display SNMP engine parameters
  startup-config        Contents of startup configuration
  terminal              Display terminal configuration parameters
  timezone              Display timezone
  upgrade-status        Display last image upgrade status
  users                 Display information about terminal lines
  version               Display software & hardware version
  wireless              Wireless configuration commands

WS5100(config-ext-nacl)#show
```

14.1.11 terminal

Extended ACL Config Commands

Sets the length (number of lines) displayed on the terminal window

Syntax

```
terminal(monitor|no)
terminal no(monitor)
```

Parameters

monitor	Copies debug output to the current terminal line
no	Negates a command or set its defaults. • monitor – Copies debug output to the current terminal line

Usage Guidelines

By default, log messages are generally not displayed using a Telnet session. Use the `terminal monitor` command to view Telnet log messages.

Example

```
WS5100(config-ext-nacl)#terminal monitor
WS5100(config-ext-nacl)#

WS5100(config-ext-nacl)#terminal no monitor
WS5100(config-ext-nacl)#
```

15

Standard ACL Instance

Use the `(config-std-nacl)` instance to configure `ip access-list standard` ACLs.

15.1 Standard ACL Config Commands

Table 15.1 summarizes the `config-std-nacl` commands:

Table 15.1 Standard ACL Config Command Summary

Command	Description	Ref.
clrscr	Clears the display screen	*page 15-2*
deny	Specifies packets to reject	*page 15-2*
end	Ends the current mode and moves to the EXEC mode	*page 15-3*
exit	Ends the current mode and moves to the previous mode	*page 15-4*
help	Displays the interactive help system	*page 15-4*
mark	Specifies packets to mark	*page 15-5*
no	Negates a command or sets its defaults	*page 15-6*
permit	Specifies packets to forward	*page 15-6*
service	Invokes service commands to troubleshoot or debug `(config-if)` instance configurations	*page 15-8*
show	Displays running system information	*page 15-9*

Table 15.1 Standard ACL Config Command Summary (Continued)

Command	Description	Ref.
terminal	Sets terminal line parameters	page 15-11

15.1.1 clrscr

Standard ACL Config Commands

Clears the display screen

Syntax

```
clrscr
```

Parameters

None

Example

```
WS5100(config-std-nacl)#clrscr
WS5100(config-std-nacl)#
```

15.1.2 deny

Standard ACL Config Commands

Specifies packets to reject

Syntax

```
deny(A.B.C.D/M|any|host)
deny any log(rule-precedence)<1-5000>
deny any rule-precedence<1-5000>
deny host A.B.C.D
```

Parameters

A.B.C.D/M	Sets the source IP address range to match
any	Any source IP address • log – The log matches against this entry • rule-precedence <1-5000> – Determines the access-list entry precedence

host	Single host address. • A.B.C.D – Exact source IP address to match.

Usage Guidelines

Use this command to deny traffic based on the source IP address or network address. The last ACE in the access list is an implicit deny statement.

Whenever the interface receives the packet, its content is checked against all the ACEs in the ACL. It is allowed/denied based on the ACL configuration.

NOTE: The log option is functional only for router ACL's. The log option results in an informational logging message for the packet matching the entry sent to the console.

Example

The example below denies all traffic entering the interface (a log message is generated whenever the interface receives a packet):

```
WS5100(config-std-nacl)#deny any log rule-precedence 50
WS5100(config-std-nacl)#
```

The example below denies traffic from the source network (xxx.xxx.1.0/24) and allows all other traffic to flow through the interface:

```
WS5100(config-std-nacl)#deny xxx.xxx.1.0/24 rule-precedence 60
WS5100(config-std-nacl)#permit any
```

15.1.3 end

Standard ACL Config Commands

Ends and exits from the current mode and moves to the PRIV EXEC mode. The prompt changes to `WS5100#`

Syntax

```
end
```

Parameters

None

Example

```
WS5100(config-std-nacl)#end
WS5100#
```

15.1.4 exit

Standard ACL Config Commands

Ends the current mode and moves to previous mode (GLOBAL-CONFIG). The prompt changes to `WS5100(config)#`

Syntax

```
exit
```

Parameters

None

Example

```
WS5100(config-std-nacl)#exit
WS5100(config)#
```

15.1.5 help

Standard ACL Config Commands

Displays the system's interactive help in HTML format

Syntax

```
help
```

Parameters

None

Example

```
WS5100(config-std-nacl)#help
CLI provides advanced help feature.  When you need help,
anytime at the command line please press '?'.

If nothing matches, the help list will be empty and you must backup
until entering a '?' shows the available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each possible
   argument.
2. Partial help is provided when an abbreviated argument is entered
   and you want to know what arguments match the input
   (e.g. 'show ve?'.)

WS5100(config-std-nacl)#
```

15.1.6 mark

▸ *Standard ACL Config Commands*

Specifies packets to mark

Syntax

```
mark(8021.1p<0-7>|tos<0-255>)(A.B.C.D/M|any|host)

mark(8021.1p<0-7>|tos<0-255>)any|host(log|rule-precedence<1-5000>|
|A.B>C.D)
```

Parameters

8021.1p<*0-7*>|tos<*0-255*>)	• Specifies .1p priority value between 0 and 7 • Specifies a *Type of Service* (tos) value between 0 and 255
(A.B.C.D/M|any|host)	*source* is the source IP address of the network or host in dotted decimal format. Source-mask is the network mask. For example, 10.1.1.10/24 indicates the first 24 bits of the source IP are used for matching
any	*any* is an abbreviation for source IP of 0.0.0.0 and source-mask bits equal to 0
host (log|rule-precedence<*1-5000*>||A.B>C.D)	*host* is an abbreviation for the exact source (A.B.C.D) and source-mask bits equal to 32

Usage Guidelines

Use this command to mark traffic from the source network/host. Use the mark option to specify the t*ype of service* (TOS) and priority value. The TOS value is marked in the IP header. The 802.1p priority value is marked in the frame.

When the interface receives the packet, its content is checked against the ACEs in the ACL. It is marked based on the ACL configuration.

NOTE: The log option is functional only for router ACLs. The log option results in an informational logging message about the packet matching the entry sent to the console.

Example

The example below marks the *type of service* (TOS) value to 254 for all traffic coming from the source network:

```
WS5100(config)#access-list 3 mark tos 254 xxx.xxx.3.0/24
WS5100 (config)#access-list 3 permit any
```

15.1.7 no

Standard ACL Config Commands

Negates a command or set its defaults

Syntax

```
no(deny|mark|permit)
```

Negates all the syntax combinatins used in *deny*, *mark* and *permit* designations.

Parameters

deny	Specifies packets to reject
mark	Specifies packets to mark
permit	Specifies packets to forward

Example

```
WS5100(config-std-nacl)#no permit any rule-precedence 10
WS5100(config-std-nacl)#

WS5100(config-std-nacl)#no deny any rule-precedence 20
WS5100(config-std-nacl)#

WS5100(config-std-nacl)#no mark tos 4 192.168.2.0/24 rule-
precedence 30
WS5100(config-std-nacl)#
```

15.1.8 permit

Standard ACL Config Commands

```
permit(A.B.C.D/M|any|host)
permit any(log|rule-precedence|wlan)
permit any log(rule-precedence)<1-500>
permit any rule-precedence<1-500>
permit any wlan<1-32>(log|rule-precedence)(rule-precedence)<1-500>
```

```
permit host A.B.C.D
```

Parameters

A.B.C.D/M	Defines the source IP address range to match
any	Any source IP address. • log – The log matches against this entry • rule-precedence*<1-500>* – Defines the access-list entry precedence
host	Single host address. • A.B.C.D – Defrines the exact source IP address to match

Usage Guidelines

Use this command to allow traffic based on the source IP address or network address. The last ACE in the access list is an implicit deny statement.

Whenever the interface receives the packet, its content is checked against all the ACEs in the ACL. It is allowed based on the ACL configuration.

NOTE: The log option is functional only for router ACLs. The log option displays an informational logging message about the packet matching the entry sent to the console.

Example

The example below permits all the traffic that comes to the interface:

```
WS5100(config-std-nacl)#permit any rule-precedence 50
WS5100(config-std-nacl)#
```

The example below permits traffic from the source network and provides a log message:

```
WS5100(config-std-nacl)#permit xxx.xxx.1.0/24 log rule-precedence
60
WS5100(config-std-nacl)#
```

15.1.9 service

Standard ACL Config Commands

Invokes service commands to troubleshoot or debug `(config-if)` instance configurations

Syntax

```
service(clear|diag-shell|save-cli|show|start-shell|tethereal)
```

Parameters

clear	Removes specified support information
diag-shell	Provides diagnostic shell access to debug and test the switch
save-cli	Saves the CLI tree for all modes (in HTML format)
show	Displays running system information
start-shell	Provides shell access
tethereal	Dumps and analyzes network traffic

Example

```
WS5100(config-std-nacl)#service diag-shell
Diagnostic shell started for testing
diag >

WS5100(config-std-nacl)#service save-cli
 CLI command tree is saved as clitree.html.
 This tree can be viewed via web at http://<ipaddr>/cli/
clitree.html
WS5100(config-std-nacl)#

WS5100(config-std-nacl)#service show ?
  cli              Show CLI tree of current mode
  command-history  Display command (except show commands) history.
  crash-info       Display information about core, panic and AP
dump files
  info             Show snapshot of available support information
  last-passwd      Display last password used to enter shell
  reboot-history   Show reboot history
  startup-log      Show startup log
  upgrade-history  Show upgrade history
WS5100(config-std-nacl)#service show
```

```
WS5100(config-std-nacl)#service start-shell
Last password used: password with MAC 00:a0:f8:65:ea:8e
Password:
WS5100(config-std-nacl)#

WS5100(config-std-nacl)#service tethereal ?
  LINE  tethereal options in the format
        [-V (print detailed packet)] [-x (hex dump of packet)]
        [-p (no promiscuous mode for interface)]
        [-n (disable name resolution)] [-c <count> ] [-h (detailed
help)]
        [-E (to capture ESPD) ][-e (capture nonEspd packets)]
        [-f <capture filter expression in format "xx xx xx"> ]
        [-i <interface on which to capture packets> ] [-W (wisp
packet only)]
        [-s <snaplen> ] [-r <filename> (read contents of specified
file)]
        [-w <savefile> (save capture in specified file) ]
        [-X (for examples on tethereal capture filter) ]

WS5100(config-std-nacl)#
```

15.1.10 show

▸ *Standard ACL Config Commands*

Displays current system information running on the switch

Syntax

`show<paramater>`

Parameters

?	Displays all the parameters for which the information can be viewed using the show command.

Example

```
WS5100(config-std-nacl)#show ?
  access-list           Internet Protocol (IP)
  alarm-log             Display all alarms currently in the system
  autoinstall           autoinstall configuration
  banner                Display Message of the Day Login banner
  boot                  Display boot configuration.
  clock                 Display system clock
  commands              Show command lists
  crypto                crypto
  debugging             Display debugging setting
  environment           show environmental information
  file                  Display filesystem information
  ftp                   Display FTP Server configuration
  history               Display the session command history
  interfaces            Interface status and configuration
  ip                    Internet Protocol (IP)
  ldap                  ldap server
  licenses              Show any installed licenses
  logging               Show logging configuration and buffer
  mac                   Media Access Control
  management            Display L3 Managment Interface name
  mobility              Display Mobility Parameters
  ntp                   Network time protocol
  password-encryption   password encryption
  privilege             Show current privilege level
  radius                Radius configuration commands
  redundancy-group      Display redundancy group parameters
  redundancy-history    Display state transition history of the
switch.
  redundancy-members    Display redundancy group members in detail
  running-config        Current Operating configuration
  securitymgr           Display debug info for ACL, VPN and NAT
  sessions              Display current active open connections
  snmp                  Display SNMP engine parameters
  snmp-server           Display SNMP engine parameters
  startup-config        Contents of startup configuration
  terminal              Display terminal configuration parameters
  timezone              Display timezone
  upgrade-status        Display last image upgrade status
  users                 Display information about terminal lines
  version               Display software & hardware version
  wireless              Wireless configuration commands

WS5100(config-std-nacl)#show
```

15.1.11 terminal

▸ *Standard ACL Config Commands*

Sets the number of lines displayed on the terminal window

Syntax

```
terminal(monitor|no)
terminal no(monitor)
```

Parameters

monitor	Copies debug output to the current terminal line
no	Negates a command or set its defaults
monitor	Copies debug output to the current terminal line

Usage Guidelines

By default, log messages are generally not displayed over a Telnet session. Use the `terminal monitor` command to view the log messages over a Telnet session

Example

```
WS5100(config-std-nacl)#terminal monitor
WS5100(config-std-nacl)#

WS5100(config-std-nacl)#terminal no monitor
WS5100(config-std-nacl)#
```

16

Extended MAC ACL Instance

Use the `(config-ext-macl)` instance to configure `mac access-list extended` ACLs.

16.1 MAC Extended ACL Config Commands

Table summarizes `config-ext-macl` commands:

Table 16.1 MAC Extended ACL Config Command Summary

Command	Description	Ref.
clrscr	Clears the display screen	*page 16-2*
deny	Specifies packets to reject	*page 16-2*
end	Ends the current mode and moves to the EXEC mode	*page 16-5*
exit	Ends the current mode and moves to the previous mode	*page 16-5*
help	Displays the interactive help system	*page 16-5*
mark	Specifies packets to mark	*page 16-6*
no	Negates a command or sets its defaults	*page 16-8*
permit	Specifies packets to forward	*page 16-9*
service	Invokes the service commands to troubleshoot or debug the `(config-if)` instance configurations	*page 16-11*
show	Shows running system information	*page 16-13*

Table 16.1 MAC Extended ACL Config Command Summary (Continued)

Command	Description	Ref.
terminal	Sets terminal line parameters	*page 16-14*

16.1.1 clrscr

MAC Extended ACL Config Commands

Clears the display screens

Syntax

```
clrscr
```

Parameters

None

Example

```
WS5100(config-ext-macl)#clrscr
WS5100(config-ext-macl)#
```

16.1.2 deny

MAC Extended ACL Config Commands

Specifies packets to reject

NOTE: Use a decimal value representation of ethertypes to implement a `permit/deny/mark` designation for a packet. The command set for Extended MAC ACLs provide the hexadecimal values for each listed ethertype. The switch supports all ethertypes. Use the decimal equvilant of the ethertype listed or for any other type of ethertype.

Syntax

```
{deny}{any|host source MAC address|source MAC/source MAC address
mask} {any|host destination MAC address|destination MAC/destination
MAC address mask}[vlan vlan-id] [dot1p dot1p-value] [type
value|ip|ipv6|arp|vlan|wisp | 0-65535] [log] [rule-precedence
access-list-entry precedence]
```

Parameters

Source Mask	Define a source mask specifying the bits to match. The source wildcard can be any one of the following: • `xx:xx:xx:xx:xx:xx/xx:xx:xx:xx:xx:xx`–Source MAC address and mask • *any* – Any source host • *host* – Exact source MAC address to match
Destination Mask	Define a destination mask specifying the bits to match. The destination wildcard can be any one of the following: • `xx:xx:xx:xx:xx:xx/xx:xx:xx:xx:xx:xx`–Destination MAC address and mask • *any* – Any destination host • *host* – Exact destination MAC address to match
dot1p*<0-7>*	Determine a 802.1p priority value to match
rule-precedence*<1-5000>*	Define an access-list entry precedence
type(*<1-65535>*|arp|ip|ipv6|vlan|wisp)	Set an ethertype value represented as an integer. Use keywords for well-known ethertypes (IP, IPv6, ARP etc.)
vlan*<1-4095>*	Set a VLAN tag ID to match

Usage Guidelines

The deny command disallows traffic based on layer 2 (data-link layer) data. The MAC access list denies traffic from a particular source MAC address or any MAC address. It can also disallow traffic from a list of MAC addresses based on the source mask

The MAC access list can disallow traffic based on the VLAN and ethertype

The most common ethertypes are:

- *arp*
- *wisp*
- *ip*
- *802.1q*

By default, the switch does not allow layer 2 traffic to pass through the interface. To adopt an access port through an interface, configure an access control list to allow an ethernet wisp.

NOTE: A MAC access list entry to allow arp is mandatory to apply an IP based ACL to an interface. MAC ACL always takes precedence over IP based ACL's.

The last ACE in the access list is an implict deny statement.

Whenever the interface receives the packet, its content is checked against all the ACEs in the ACL. It is allowed/denied based on the ACL configuration.

Example

The MAC AC (in the example below) denies traffic from any source MAC address to a particular host MAC address:

```
WS5100(config-ext-macl)#deny any host 00:01:ae:00:22:11
WS5100(config-ext-macl)#
```

The MAC ACL (in the example below) denies dot1q tagged traffic from VLAN interface 5:

```
WS5100(config-ext-macl)#deny any any vlan 5 type 8021q
WS5100(config-ext-macl)#
```

The example below denies traffic between two hosts based on MAC addresses:

```
WS5100(config-ext-macl)#deny host 01:02:fe:45:76:89 host
01:02:89:78:78:45
WS5100(config-ext-macl)#
```

16.1.3 end

MAC Extended ACL Config Commands

Ends and exits from the current mode and moves to the PRIV EXEC mode. The prompt changes to `WS5100#`

Syntax

```
end
```

Parameters

None

Example

```
WS5100(config-ext-macl)#end
WS5100#
```

16.1.4 exit

MAC Extended ACL Config Commands

Ends the current mode and moves to the previous mode (GLOBAL-CONFIG). The prompt changes to `WS5100(config)#`

Syntax

```
exit
```

Parameters

None

Example

```
WS5100(config-ext-macl)#exit
WS5100(config)#
```

16.1.5 help

MAC Extended ACL Config Commands

Displays the system's interactive help (in HTML format)

Syntax

```
help
```

Parameters

None

Example

```
WS5100(config-ext-macl)#help
CLI provides advanced help feature.  When you need help,
anytime at the command line please press '?'.

If nothing matches, the help list will be empty and you must backup
until entering a '?' shows the available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each possible
   argument.
2. Partial help is provided when an abbreviated argument is entered
   and you want to know what arguments match the input
   (e.g. 'show ve?'.)

WS5100(config-ext-macl)#
```

16.1.6 mark

MAC Extended ACL Config Commands

Specifies the packet to mark

NOTE: Use a decimal value representation of ethertypes to implement permit/deny/mark designations for a packet. An Extended MAC ACL provides the hexadecimal values for each listed ethertype. The switch supports all ethertypes. Use the decimal equvilant of the ethertype listed in the CLI or any other type of ethertype.

Syntax

```
{mark {dot1p <0-7>|tos <0-255>}}
{any|host source MAC address|source MAC source/MAC address mask}
{any|host destination MAC address|destination MAC/ destination MAC
address mask} [vlan vlan-id] [dot1p dot1p-value] [type
value|ip|ipv6|arp|vlan| wisp|0-65535] [log] [rule-precedence
access-list-entry precedence]
```

Parameters

8021p*<0-7>*	Modifies the 802.1p VLAN user priority
tos*<0-255>*	Modifies the TOS bits in an IP header

Source MAC Address	Specifies the bits to match. The source wildcard can be any one of the following: • `xx:xx:xx:xx:xx:xx/ xx:xx:xx:xx:xx:xx`–Source MAC address and mask • *any* – Any source host • *host* – Exact source MAC address to match
Destination MAC Address	Specifies the bits to match. The destination wildcard can be any one of the following: • `xx:xx:xx:xx:xx:xx/ xx:xx:xx:xx:xx:xx`–Destination MAC address and mask • *any* – Any destination host • *host* – Exact destination MAC address to match
dot1p*<0-7>*	Defines a VLAN 802.1p priority value to match
rule-precedence*<1-5000>*	Establishes an access-list entry precedence
type(*<1-65535>*|arp|ip|ipv6|vlan|wisp)	Defines an ethertype value represented as an integer or keyword for well-known ethertypes (like IP, IPv6, ARP etc.)
vlan*<1-4095>*	Defines the VLAN tag ID to match

Usage Guidelines

Use the mark option to specify the t*ype of service* (tos) and priority value. The tos value is marked in the IP header and the 802.1p priority value is marked in the dot1q frame.

Whenever the interface receives the packet, its content is checked against all the ACEs in the ACL. It is marked based on the ACL's configuration.

Example

The example below marks the dot1p priority value to 6 for all 802.1q tagged traffic from VLAN interface 5

```
WS5100(config-ext-macl)#mark 8021p 6 any any vlan 5 type 8021q
WS5100(config-ext-macl)#
```

The example below marks the tos field to 254 for IP traffic coming from the source MAC

```
WS5100(config-ext-macl)#mark tos 254 host 00:33:44:55:66:77 any
type ip
WS5100(config-ext-macl)#
```

16.1.7 no

MAC Extended ACL Config Commands

Negates a command or sets its defaults

Syntax

```
no(deny|mark|permit)
```

Negates all the syntax combinations used in *deny*, *mark* and *permit* designations to configure the Extended ACL

Parameters

deny	Specifies packets to reject
mark	Specifies packets to mark
permit	Specifies packets to forward

Example

```
WS5100(config-ext-macl)#no mark tos 254 host 00:33:44:55:66:77 any
type ip rule-precedence 50
WS5100(config-ext-macl)#

WS5100(config-ext-macl)#no deny any any vlan 5 type 8021q rule-
precedence 10
WS5100(config-ext-macl)#

WS5100(config-ext-macl)#no permit any any type wisp rule-precedence
50
WS5100(config-ext-macl)#
```

16.1.8 permit

MAC Extended ACL Config Commands

Specifies packets to forward

NOTE: Use a decimal value representation of ethertypes to implement permit/deny/mark designations for a packet. An Extended MAC ACL provides the hexadecimal values for each listed ethertype. The switch supports all ethertypes. Use the decimal equvilant of the ethertype listed in the CLI or any other type of ethertype.

Syntax

```
{permit} {any|host source MAC address|source MAC\source MAC address
mask} {any|host destination MAC address | destination
MAC\destination MAC address mask} [vlan vlan-id] [dot1p dot1p-
value] [type value|ip|ipv6|arp| vlan|wisp|0-65535] [log] [rule-
precedence access-list-entry precedence]
```

Parameters

Source MAC Address	Specifies the bits to match. The source wildcard can be any one of the following: • `xx:xx:xx:xx:xx:xx/xx:xx:xx:xx:xx:xx`–Source MAC address and mask • *any* – Uses any source host • *host* – Defines the exact source MAC address to match
Destination MAC Address	Bit mask specifying the bits to match. The destination wildcard can be any one of the following: • `xx:xx:xx:xx:xx:xx/xx:xx:xx:xx:xx:xx`–Destination MAC address and mask • *any* – Uses any available destination host • *host* – Defines the exact destination MAC address to match
dot1p<*0-7*>	Establishes the 802.1p priority

rule-precedence*<1-5000>*	Defines an access list entry precedence
type(*<1-65535>*|arp|ip|ipv6|vlan|wisp)	Sets an ethertype
vlan*<1-4095>*	Sets the VLAN ID

Usage Guidelines

When creating a Port ACL, the switch (by default) does not permit an ethertype WISP. Create a rule to allow WISP to adopt access ports. Use the following command to adopt access ports:

```
permit any any type wisp
```

NOTE: Use the following command to attach a MAC access list to a port on a layer 2 interface:

```
mac access-group <acl number/name> in
```

The permit command in the MAC ACL disallows traffic based on layer 2 (data-link layer) information. A MAC access list permits traffic from a source MAC address or any MAC address. It also has an option to allow traffic from a list of MAC addresses (based on the source mask).

The MAC access list can be configured to allow traffic based on VLAN information, ethernet type. Common types include:

- *arp*
- *wisp*
- *ip*
- *802.1q*

The switch (by default) does not allow layer 2 traffic to pass through the interface. To adopt an access port through an interface, configure an access control list to allow an ethernet wisp.

NOTE: To apply an IP based ACL to an interface, a MAC access list entry to allow ARP is mandatory. A MAC ACL always takes precedence over IP based ACLs.

The last ACE in the access list is an implicit deny statement.

Whenever the interface receives the packet, its content is checked against all the ACEs in the ACL. It is allowed/denied based on the ACL's configuration.

Example

The example below permits WISP traffic from any source MAC address to any destination MAC address:

```
WS5100(config-ext-macl)#permit any any type wisp
WS5100(config-ext-macl)#
```

The example below permits arp based traffic from any source MAC address to any destination MAC address:

```
WS5100(config-ext-macl)#permit any any type arp
WS5100(config-ext-macl)#
```

The example below permits IP based traffic from a source MAC address to any destination MAC address:

```
WS5100(config-ext-macl)#permit host 11:22:33:44:55:66 any type ip
WS5100(config-ext-macl)#
```

16.1.9 service

- *MAC Extended ACL Config Commands*

Invokes service commands to troubleshoot or debug `(config-if)` instance configurations

Syntax

```
service(clear|diag-shell|save-cli|show|start-shell|tethereal)
```

Parameters

show (cli)	Displays running system information

Example

```
WS5100(config-ext-macl)#service show cli
MAC Extended ACL Config mode:
+-clrscr [clrscr]
+-deny
  +-XX:XX:XX:XX:XX:XX/XX:XX:XX:XX:XX:XX
    +-XX:XX:XX:XX:XX:XX/XX:XX:XX:XX:XX:XX [(deny|permit|mark (8021p
<0-7> | tos
<0-255>))(XX:XX:XX:XX:XX:XX/XX:XX:XX:XX:XX:XX | host
XX:XX:XX:XX:XX:XX | any)(XX
:XX:XX:XX:XX:XX/XX:XX:XX:XX:XX:XX | host XX:XX:XX:XX:XX:XX |
any)(vlan <1-4095>
| dot1p <0-7> |) (type (<1-65535> | ip | ipv6          | arp | wisp
| 8021q | ra
rp | aarp | appletalk | ipx ) |)(rule-precedence <1-5000> |)]
      +-dot1p
        +-<0-7> [(deny|permit|mark (8021p <0-7> | tos <0-
255>))(XX:XX:XX:XX:XX:X
X/XX:XX:XX:XX:XX:XX | host XX:XX:XX:XX:XX:XX |
any)(XX:XX:XX:XX:XX:XX/XX:XX:XX:X
X:XX:XX | host XX:XX:XX:XX:XX:XX | any)(vlan <1-4095> | dot1p <0-7>
|) (type (<1
-65535> | ip | ipv6          | arp | wisp | 8021q | rarp | aarp |
appletalk | ip
x ) |)(rule-precedence <1-5000> |)]
          +-rule-precedence
            +-<1-5000> [(deny|permit|mark (8021p <0-7> | tos <0-
255>))(XX:XX:XX:
XX:XX:XX/XX:XX:XX:XX:XX:XX | host XX:XX:XX:XX:XX:XX |
any)(XX:XX:XX:XX:XX:XX/XX:
XX:XX:XX:XX:XX | host XX:XX:XX:XX:XX:XX | any)(vlan <1-4095> |
dot1p <0-7> |) (t
ype (<1-65535> | ip | ipv6          | arp | wisp | 8021q | rarp |
aarp | appleta
lk | ipx ) |)(rule-precedence <1-5000> |)]
          +-type
.....................................................................
.....................................................................
.....................................................................
WS5100(config-ext-macl)#
```

16.1.10 show

- *MAC Extended ACL Config Commands*

Displays current system information running on the switch

Syntax

`show<paramater>`

Parameters

?	Displays all the parameters for which information can be viewed using the show command

Usage Guidelines

The `show access-list` command displays the access lists configured for the switch. Provide the access list name or number to view specific ACL details

Example

```
WS5100(config-ext-macl)#show ?
  access-list           Internet Protocol (IP)
  alarm-log             Display all alarms currently in the system
  autoinstall           autoinstall configuration
  banner                Display Message of the Day Login banner
  boot                  Display boot configuration.
  clock                 Display system clock
  commands              Show command lists
  crypto                crypto
  debugging             Display debugging setting
  environment           show environmental information
  file                  Display filesystem information
  ftp                   Display FTP Server configuration
  history               Display the session command history
  interfaces            Interface status and configuration
  ip                    Internet Protocol (IP)
  ldap                  ldap server
  licenses              Show any installed licenses
  logging               Show logging configuration and buffer
  mac                   Media Access Control
  management            Display L3 Managment Interface name
  mobility              Display Mobility Parameters
  ntp                   Network time protocol
  password-encryption   password encryption
  privilege             Show current privilege level
  radius                Radius configuration commands
  redundancy-group      Display redundancy group parameters
  redundancy-history    Display switch state transition history
```

```
  redundancy-members   Display redundancy group members in detail
  running-config       Current Operating configuration
  securitymgr          Display debug info for ACL, VPN and NAT
  sessions             Display current active open connections
  snmp                 Display SNMP engine parameters
  snmp-server          Display SNMP engine parameters
  startup-config       Contents of startup configuration
  terminal             Display terminal configuration parameters
  timezone             Display timezone
  upgrade-status       Display last image upgrade status
  users                Display information about terminal lines
  version              Display software & hardware version
  wireless             Wireless configuration commands

WS5100(config-ext-macl)#show
```

16.1.11 terminal

▸ *MAC Extended ACL Config Commands*

Sets the length/number of lines displayed on the terminal window

Syntax

```
terminal(monitor|no)
terminal no(monitor)
```

Parameters

monitor	Copies debug output to the current terminal line
no	Negates a command or sets its defaults
monitor	Copies debug output to the current terminal line

Usage Guidelines

By default, log messages are generally not displayed over a telnet session. Use the `terminal monitor` command to view log messages using telnet

Example

```
WS5100(config-ext-macl)#terminal monitor
WS5100(config-ext-macl)#

WS5100(config-ext-macl)#terminal no monitor
WS5100(config-ext-macl)#
```

17

DHCP Server Instance

Use `(config)#ip dhcp pool <pool name>` to enter the `(config-dhcp)` instance. Use this instance to configure the DHCP server address pool associated the switch.

Also refer to *ip on page 12-6* for other DHCP related configurations.

17.1 DHCP Config Commands

Table 17.1 summarizes `config-dhcp` commands:

Table 17.1 DHCP Server Command Summary

Command	Description	Ref.
address	Defines the DHCP server include range	*page 17-3*
bootfile	Assigns a boot file name. The bootfile name can contain letters, numbers, dots and hyphens. Consecutive dots and hyphens are not permitted	*page 17-3*
class	Associates a class with a pool and moves to the DHCP pool class configuration mode	*page 17-4*
client-identifier	Uses an ASCII string as a client identifier	*page 17-7*
client-name	Assigns a client name	*page 17-7*
clrscr	Clears the display screen	*page 17-8*
ddns	Configures *Dynamic DNS* (DDNS) values	*page 17-8*

Table 17.1 DHCP Server Command Summary

Command	Description	Ref.
default-router	Configures a default router's IP address	*page 17-9*
dns-server	Sets the IP address of a DNS Server	*page 17-10*
domain-name	Sets the domain name	*page 17-10*
end	Ends the current mode and moves to the EXEC mode	*page 17-11*
exit	Ends the current mode and moves to the previous mode	*page 17-11*
hardware-address	Defines the hardware address using either a dashed or dotted hexadecimal string	*page 17-11*
help	Displays the interactive help system in HTML format	*page 17-12*
host	Configures an IP address for the host	*page 17-13*
lease	Assigns the lease time for a DHCP leased IP address	*page 17-13*
netbios-name-server	Configures NetBIOS (WINS) name servers	*page 17-15*
netbios-node-type	Defines the NetBIOS node type	*page 17-15*
network	Sets a network number and mask for the DHCP Server	*page 17-16*
next-server	Configures the next server in boot process	*page 17-16*
no	Negates a command or sets its defaults	*page 17-17*
option	Assigns a name for a DHCP option	*page 17-17*
service	Invokes service commands to trobuleshoot or debug `(config-dhcp)` instance configurations	*page 17-18*
show	Displays the running system information	*page 17-20*
update	Controls the usage of *Dynamic DNS* (DDNS)	*page 17-22*

17.1.1 address

DHCP Config Commands

Specifies a range of addresses for the DHCP network pool

Syntax

```
address (range) (low IP address) (high IP address)
```

Parameters

range (low IP address) (high IP address)	Adds an address range for the DHCP server • low IP address – Defines the first IP address in the address range • high IP address – Defines the last IP address in the address range

Usage Guidelines

Use the `address` comand to specify a range of addresses for the DHCP network pool. The DHCP server assigns IP address to DHCP clients from the address range. A high IP address is the upper limit for providing the IP address, and a low IP address is the lower limit for providing the IP address

Use the `no address (range)` command to remove the DHCP address range

Example

```
WS5100(config-dhcp)#address range 2.2.2.2 2.2.2.50
WS5100(config-dhcp)#
```

17.1.2 bootfile

DHCP Config Commands

Assigns a bootfile name for the DHCP configuration on the network pool

Syntax

```
bootfile <filename>
```

Parameters

bootfile <filename>	Sets the boot image for BOOTP clients. The file name can contain letters, numbers, dots and hyphens. Consecutive dots and hyphens are not permitted.

Usage Guidelines

Use the `bootfile` command to specify the boot image. The boot file contains the boot image name used for booting the bootp clients (DHCP clients). Only one boot file is allowed per pool.

Use `[no] bootfile` command to remove the bootfile. Do not use the <file name> with the bootfile command as only one bootfile exists per pool. The command `[no] bootfile` removes the exisitng command from the pool.

Example

```
WS5100(config-dhcp)#bootfile bootexample.txt
WS5100(config-dhcp)#
```

17.1.3 class

▸ *DHCP Config Commands*

Associates a DHCP class with a pool. This command is used in Step 4 in the usage guidelines that follow.

The CLI prompt moves to a sub-instance `(config-dhcp-class)`. The configuration mode changes from `(config-dhcp)# class` to `(config-dhcp-class)`.
Refer to *config-dhcp-class on page 17-5* for `(config-dhcp-class)` a command summary.

Syntax

```
class (class name)
```

Parameters

class (class name)	Associates a class with a pool and enters the DHCP pool class configuration mode

Usage Guidelines

Follow the steps mentioned below to create a DHCP User Class:

1. Create a DHCP class named **`WS5100DHCPclass`**. The switch supports a maximum of 32 DHCP classes.

   ```
   WS5100(config)#ip dhcp class WS5100DHCPclass
   WS5100(config-dhcpclass)#
   ```

2. Create a USER class named **`MC800`**. The privilege mode changes to `(config-dhcpclass)`. The switch supports a maximum of 8 users classes per DHCP class.

   ```
   WS5100(config-dhcpclass)#option user-class MC800
   WS5100(config-dhcpclass)#
   ```

3. Create a Pool named **`WID`**, using `(config)#` mode.

   ```
   WS5100(config)#ip dhcp pool WID
   WS5100(config-dhcp)#
   ```

4. Associate the DHCP class, created in Step 1 with the pool created in Step 3. The switch supports the association of only 8 DHCP classes with a pool.

   ```
   WS5100(config-dhcp)#class WS5100DHCPclass
   WS5100(config-dhcp-class)#
   ```

5. The switch moves to a new mode (config-dhcp-class). Use this mode to add an address range used for the DHCP class associated with the pool.

   ```
   WS5100(config-dhcp-class)#address range 11.22.33.44
   ```

Example

```
WS5100(config-dhcp)#class WS5100DHCPclass
```

17.1.3.1 config-dhcp-class

Use `(config-dhcp)# class` to enter the (`config-dhcp-class`) instance. Use this instance to set an address range for a DHCP user class within a DHCP server address pool.

Table 17.2 summarizes `config-dhcp-class` commands.

Table 17.2 DHCP Server Class Command Summary

Command	***Description***
address	Sets an address range for a DHCP class in a DHCP server address pool

Table 17.2 DHCP Server Class Command Summary

Command	Description
clrscr	Clears the display screen
end	Ends the current mode and moves to the EXEC mode
exit	Ends the current mode and moves to the previous mode
help	Displays the interactive help system in HTML format
no	Negates a command or sets its defaults
service	Assists in troubleshooting or debugging issues
show	Displays running system information

address

config-dhcp-class

Sets an address range for a DHCP class within a DHCP server address pool

Syntax

```
address (range) (low IP Address) (high IP Address)
```

Parameters

range (low IP Address) (High IP Address)	Assigns an address range for the DHCP class • A.B.C.D – Derfines the low IP address • A.B.C.D – Defines the high IP address

Example

```
WS5100(config-dhcp-class)#address range 11.22.13.14 11.22.33.56
WS5100(config-dhcp-class)#
```

17.1.4 client-identifier

DHCP Config Commands

Assigns a name to the client-identifier. A client identifier is used to reserve an IP address for DHCP client

Syntax

```
client-identifier <ascii string>
```

Parameters

client-identifier <ascii string>	Prepends a null character. Use `\\0` at beginning. A single `\` in the input is ignored

Example

```
WS5100(config-dhcp)#client-identifier testid
WS5100(config-dhcp)#
```

17.1.5 client-name

DHCP Config Commands

Adds name for DHCP clients

Syntax

```
client-name <name>
```

Parameters

client-name <name>	Use `client-name` to add a client name. The domain name must not be included

Example

```
WS5100(config-dhcp)#client-name testpc
WS5100(config-dhcp)#
```

17.1.6 clrscr

DHCP Config Commands

Clears the display screen

Syntax

```
clrscr
```

Parameters

None

Example

```
WS5100(config-dhcp)#clrscr
WS5100(config-dhcp)#
```

17.1.7 ddns

DHCP Config Commands

Sets dynamic DNS parameters

Syntax

```
ddns [domainname (name)|multiple-user-class|server (IP address)
(IP address)|ttl <1-864000>]
```

Parameters

domainname (name)	Sets the domain name used for DDNS updates
multiple-user-class	Enables the multiple user class option
server (IP address) (IP address)	Specifies the server to which DDNS updates have been sent • ip address – Defines an IP address in dotted decimal format
ttl <1-864000>	Sets a *Time To Live* (TTL) value for DDNS updates • <1-864000> – TTL value in seconds

Usage Guidelines

Use `update (dns) (override)` to enable an internal DHCP server to send DDNS updates for resource records (RRs) A, TXT and PTR. A DHCP server can always override the client even if the client is configured to perform the updates

In the DHCP server network pool, FQDN is defined as the DDNS domain name. This is used internally in DHCP packets between the DHCP server on the switch and the DNS server

Example

```
WS5100(config-dhcp)#ddns domainname TestDomain.com
WS5100(config-dhcp)#

WS5100(config-dhcp)#ddns multiple-user-class
WS5100(config-dhcp)#

WS5100(config-dhcp)#ddns ttl 1000
WS5100(config-dhcp)#

WS5100(config-dhcp)#ddns update-all
WS5100(config-dhcp)#
```

17.1.8 default-router

DHCP Config Commands

Configures the default router or gateway IP address for the network pool. To remove the default router list, use the `no default-router` command

```
default-router <Router IP address>
```

Parameters

default-router <router IP address>	Specifies the default router IP address for the network pool • <router IP address> – Sets the router's IP address

Usage Guidelines

The IP address of the router should be on the same subnet as the client subnet

Example

```
WS5100(config-dhcp)#default-router 2.2.2.1
WS5100(config-dhcp)#
```

17.1.9 dns-server

DHCP Config Commands

Sets the DNS server's IP address that's available to all DHCP clients connected to the pool. Use the `no dns-server` command to remove the DNS server list

Syntax

```
dns-server <ip address1> <ip address2> <ip address3> .....<ip
address8>
```

Parameters

dns-server <IP address>	Configures the DNS server's IP address. • <IP address> – Sets the server's IP address.

Usage Guidelines

For DHCP clients, the DNS server's IP address maps the host name to an IP address. DHCP clients use the DNS server's IP address based on the order (sequence) it is configured

Example

```
WS5100(config-dhcp)#dns-server 2.2.2.222
WS5100(config-dhcp)#
```

17.1.10 domain-name

DHCP Config Commands

Sets the domain name for the network pool. Use the `no domain-name` command to remove the domain name

Syntax

```
domain-name (name)
```

Parameters

domain-name (name)	Defines the domain name for the network pool

Usage Guidelines

The domain name cannot be more than 256 characters

Example

```
WS5100(config-dhcp)#domain-name Engineering
WS5100(config-dhcp)#
```

17.1.11 end

DHCP Config Commands

Exits the current mode and moves to the PRIV EXEC mode. The prompt changes to `WS5100#`

Syntax

```
end
```

Parameters

None

Example

```
WS5100(config-dhcp)#end
WS5100#
```

17.1.12 exit

DHCP Config Commands

Ends the current mode and moves to the previous mode (GLOBAL-CONFIG). The prompt changes to `WS5100#(config)#`

Syntax

```
exit
```

Parameters

None

Example

```
WS5100(config)#ip dhcp pool TestPool
WS5100(config-dhcp)#exit
WS5100(config)#
```

17.1.13 hardware-address

DHCP Config Commands

Reserves an IP address (manually) based on a DHCP client's hardware address. Use the `no hardware-address` command to remove this from the DHCP pool

Syntax

```
hardware-address [XX-XX-XX-XX-XX-XX | XX:XX:XX:XX:XX:XX]
```

Parameters

hardware-address [XX-XX-XX-XX-XX-XX | XX:XX:XX:XX:XX:XX]	Sets the client's hardware address • XX-XX-XX-XX-XX-XX – Defines a dashed hexadecimal string • XX:XX:XX:XX:XX:XX – Sets a dotted hexadecimal string

Usage Guidelines

Accepts only hexadecimal values

Example

```
WS5100(config-dhcp)#hardware-address 00:01:23:45:32:22
WS5100(config-dhcp)#
```

17.1.14 help

DHCP Config Commands

Displays the system's interactive help in HTML format

Syntax

```
help
```

Parameters

None

Example

```
WS5100(config-dhcp)#help
CLI provides advanced help feature.  When you need help,
anytime at the command line please press '?'.

If nothing matches, the help list will be empty and you must backup
until entering a '?' shows the available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each possible
   argument.
2. Partial help is provided when an abbreviated argument is entered
   and you want to know what arguments match the input
   (e.g. 'show ve?'.)

WS5100(config-dhcp)#
```

17.1.15 host

DHCP Config Commands

Defines a fixed IP address for the host in dotted decimal format. Use the `no host` command to remove the host from the DHCP pool

Syntax

```
host <IP address>
```

Parameters

host <IP address>	Sets a fixed address for the host • IP address – Sets an IP address in dotted decimal format

Usage Guidelines

The DHCP host pool (used to manually assign an IP address based on hardware address/ client identifier) configuration must contain a host IP address, client name and hardware address/client identifier.

The host IP address must belong to a subnet on the switch. There must be a DHCP network pool corresponding to that host IP address. There is no limit to the number of manual bindings. However, you can configure only one manual binding per host pool

Example

```
WS5100(config-dhcp)#host 2.2.2.111
WS5100(config-dhcp)#
```

17.1.16 lease

DHCP Config Commands

Sets a valid lease time for the IP address used by DHCP clients in the network pool

Syntax

```
lease [{<0-365> <0-23> <0-59>}|infinite]
```

Parameters

lease [{<0-365> <0-23> <0-59>} |infinite]	Sets the lease time for an IP address
	• <0-365> –Sets the lease period in days. Days can be made as 0 only when hours and/or mins are greater than 0
	  • <0-23> – Sets the hours for the lease period. Hours can be 0 only when days and/or minutes are configured with a value greater than 0
	  • <0-59> – Sets the minutes for the lease period. Minutes can be 0 only when days and/or hours are configured with a value greater than 0
	• infinite – Sets the lease period as infinite

Usage Guidelines

If lease parameter is not configured on the DHCP network pool, the default value is used. The default value of the lease is 24 hours

The lease vlaue for DHCP host pool is infinite

Example

```
WS5100(config-dhcp)#lease 20 12 30
WS5100(config-dhcp)#
```

17.1.17 netbios-name-server

DHCP Config Commands

Sets the netbios-name server's IP address

Syntax

```
netbios-name-server <IP address>
```

Parameters

netbios-name-server <IP address>	Defines the NetBIOS (WINS) name server • <IP address> – Sets the NetBIOS name server's IP address

Example

```
WS5100(config-dhcp)#netbios-name-server 2.2.2.222
WS5100(config-dhcp)#
```

17.1.18 netbios-node-type

DHCP Config Commands

Defines the netbios-node type

Syntax

```
netbios-node-type [b-node|h-node|m-node|p-node]
```

Parameters

netbios-node-type [b-node | h-node | m-node | p-node]	Defines the NetBIOS (WINS) name servers • *b-node* – Broadcast node. • *h-node* – Hybrid node. • *m-node* – Mixed node. • *p-node* – Peer-to-peer node.

Example

```
WS5100(config-dhcp)#netbios-node-type p-node
WS5100(config-dhcp)#
```

17.1.19 network

DHCP Config Commands

Sets the network pool's IP address. This address maps the current DHCP pool with a specific network

Syntax

```
network [A.B.C.D|A.B.C.D/M]
```

Parameters

network [A.B.C.D|A.B.C.D/M]	Sets the network number and mask • A.B.C.D – Network number in dotted decimal format. • A.B.C.D/M – Network number and mask.

Usage Guidelines

Ensure a VLAN interface (with specific network/subnet) exists on the switch before mapping a DHCP pool to a particular network

Example

```
WS5100(config-dhcp)#network  2.2.2.0/24
WS5100(config-dhcp)#
```

17.1.20 next-server

DHCP Config Commands

Sets the IP address of the next server in the boot process

Syntax

```
next-server <IP address>
```

Parameters

next-server <IP address>	Sets the next server in boot process • <IP address> – Defines the server's IP address

Example

```
WS5100(config-dhcp)#next-server 2.2.2.22
WS5100(config-dhcp)#
```

17.1.21 no

▸ *DHCP Config Commands*

Negates a command or sets itsdefaults.

Syntax

```
no [address|bootfile|client-identifier|client-name|ddns|default-
router|dns-server|domain-name|hardware-address|host|lease|netbios-
name-server|netbios-node-type|network|next-server|option|update]
```

Parameters

The `no` command negates any command associated with it. Wherever required, use the same parameters associated with the command getting negated

Example

```
WS5100(config)#no ip dhcp pool hotpool
WS5100(config)#

WS5100(config)#no ip dhcp pool test
WS5100(config)#

WS5100(config-dhcp)#no update dns
WS5100(config-dhcp)#
```

17.1.22 option

▸ *DHCP Config Commands*

Define the DHCP option used in DHCP pools

Syntax

```
option (name)
```

Parameters

option (name)	Sets raw DHCP options
	• (name) – Sets the name of the DHCP option
	  • IP Value – Sets the IP Value of the DHCP option
	  • ASCII Value – Sets the ASCII Value of the DHCP option

Usage Guidelines

Defines non standard DHCP option codes (0-254).

Example

```
WS5100(config)#ip dhcp option option189 189 ascii
WS5100(config)#
```

17.1.23 service

DHCP Config Commands

Invoke service commands to troubleshoot or debug `(config-dhcp)` instance configurations

Syntax

```
service(show) (cli)
```

Parameters

show	Shows running system information
cli	Shows the CLI tree of current mode

Example

```
WS5100(config-dhcp)#service show cli
DHCP Server Config mode:
+-address
  +-range
    +-A.B.C.D [address range A.B.C.D ( A.B.C.D |)]
      +-A.B.C.D [address range A.B.C.D ( A.B.C.D |)]
+-bootfile
  +-WORD [bootfile WORD]
+-client-identifier
  +-WORD [client-identifier WORD]
+-client-name
  +-WORD [client-name WORD]
+-clrscr [clrscr]
+-ddns
  +-domainname
    +-WORD [ddns domainname WORD]
  +-multiple-user-class [ddns multiple-user-class]
  +-server
    +-A.B.C.D [ddns server A.B.C.D (A.B.C.D|)]
      +-A.B.C.D [ddns server A.B.C.D (A.B.C.D|)]
  +-ttl
    +-<1-864000> [ddns ttl <1-864000>]
  +-update-all [ddns update-all]
+-default-router
  +-A.B.C.D [default-router .A.B.C.D]
+-dns-server
  +-A.B.C.D [dns-server .A.B.C.D]
+-do
  +-LINE [do LINE]
+-domain-name
  +-WORD [domain-name WORD]
+-end [end]
+-exit [exit]
+-hardware-address
  +-XX-XX-XX-XX-XX-XX [hardware-address (XX:XX:XX:XX:XX:XX|XX-XX-
XX-XX-XX-XX)(ethernet|token-ring|)]
    +-ethernet [hardware-address (XX:XX:XX:XX:XX:XX|XX-XX-XX-XX-XX-
XX)(ethernet|token-ring|)]
    +-token-ring [hardware-address (XX:XX:XX:XX:XX:XX|XX-XX-XX-XX-
XX-XX)(ethernet|token-ring|)]
  +-XX:XX:XX:XX:XX:XX [hardware-address (XX:XX:XX:XX:XX:XX|XX-XX-
XX-XX-XX-XX)(ethernet|token-ring|)]
    +-ethernet [hardware-address (XX:XX:XX:XX:XX:XX|XX-XX-XX-XX-XX-
XX)(ethernet|token-ring|)]
    +-token-ring [hardware-address (XX:XX:XX:XX:XX:XX|XX-XX-XX-XX-
XX-XX)(ethernet|token-ring|)].....................
..................................................
WS5100(config-dhcp)#
```

17.1.24 show

DHCP Config Commands

Displays current system information

Syntax

```
show <paramater>
```

Parameters

?	Displays parameters for which information can be viewed using the show command

Example

```
WS5100(config-dhcp)#show ?
  access-list           Internet Protocol (IP)
  aclstats              Show ACL Statistics information
  alarm-log             Display all alarms currently in the system
  autoinstall           autoinstall configuration
  banner                Display Message of the Day Login banner
  boot                  Display boot configuration.
  clock                 Display system clock
  commands              Show command lists
  crypto                encryption module
  debugging             Debugging information outputs
  dhcp                  DHCP Server Configuration
  environment           show environmental information
  file                  Display filesystem information
  ftp                   Display FTP Server configuration
  history               Display the session command history
  interfaces            Interface status
  ip                    Internet Protocol (IP)
  ldap                  LDAP server
  licenses              Show any installed licenses
  logging               Show logging configuration and buffer
  mac                   Internet Protocol (IP)
  mac-address-table     Display MAC address table
  management            Display L3 Managment Interface name
  mobility              Display Mobility parameters
  ntp                   Network time protocol
  password-encryption   password encryption
  port-channel          Portchannel commands
  privilege             Show current privilege level
  radius                RADIUS configuration commands
  redundancy-group      Display redundancy group parameters
```

```
  redundancy-history    Display state transition history of the
switch.
  redundancy-members    Display redundancy group members in detail
  running-config        Current Operating configuration
  securitymgr           Securitymgr parameters
  sessions              Display current active open connections
  snmp                  Display SNMP engine parameters
  snmp-server           Display SNMP engine parameters
  sole                  Smart Opportunistic Location Engine
Configuration
  spanning-tree         Display spanning tree information
  startup-config        Contents of startup configuration
  static-channel-group  static channel group membership
  terminal              Display terminal configuration parameters
  timezone              Display timezone
  upgrade-status        Display last image upgrade status
  users                 Display information about currently logged
in                        users
  version               Display software & hardware version
  wireless              Wireless configuration commands
  wlan-acl              wlan based acl

WS5100(config-dhcp)#show
WS5100(config)#show dhcp config

service dhcp
ip dhcp option option189 189 ascii
!
ip dhcp pool vlan4
 default-router 2.2.2.1
 network 4.4.4.0/24
 address range 4.4.4.100 4.4.4.200
!
ip dhcp pool vlan2
!
ip dhcp pool TestPool
 lease 200 12 30
 domain-name TestDomain
 bootfile DHCPbootfile
 netbios-node-type p-node
 ddns domainname TestDomain
 address range 1.2.3.2 2.3.2.1

WS5100(config)#show dhcp status

DHCP Server is Running on following interfaces

        vlan4
```

```
WS5100(config)#

WS5100(config)#show ip dhcp binding
IP              MAC/Client-Id      Type       Expiry Time
--              -------------      ----       -----------
WS5100(config)#
```

17.1.25 update

- *DHCP Config Commands*

Controls the usage of the DDNS service

Syntax

```
update (dns)(override)
```

Parameters

update (dns) (override)	Controls the usage of the DDNS service • (dns) – Dynamic DNS Configuration • (override) – Enable Dynamic Updates by onboard DHCP Server

Usage Guidelines

A DHCP client cannot perform updates for RR's A, TXT and PTR. Use `update (dns) (override)` to enable the internal DHCP Server to send DDNS updates for resource records (RR's) A, TXT and PTR. The DHCP Server can override the client, even if the client is configured to perform the updates.

In the network pool of DHCP Server, FQDN is configured as the DDNS domain name. This is used internally in DHCP packets between the switch's DHCP Server and the DNS server.

Example

```
WS5100(config-dhcp)#update dns override
WS5100(config-dhcp)#
```

17.2 Configuring the DHCP Server using Switch CLI

The switch DHCP configuration is conducted by creating pools and mapping them to L3 interfaces (SVI).

- A Network pool is the pool with "include" ranges. When the network pool is mapped to a L3 interface, DHCP clients requesting IPs from the L3 interface get an IP from the configured range
- A host pool is the pool used to assign static/fixed IP address to DHCP clients

17.2.1 Creating network pool

To create a network pool using the switch CLI:

1. Create a DHCP server dynamic address pool.

   ```
   WS5100(config)#ip dhcp pool test
   ```

2. Map the DHCP pool to the network pool.

   ```
   WS5100(config-dhcp)#network 192.168.0.0/24
   ```

3. Add the address range for the dynamic pool.

   ```
   WS5100(config-dhcp)#address range 192.168.0.30 192.168.0.60
   ```

4. Assign a domain name (as appropriate) to this dynamic pool.

   ```
   WS5100(config-dhcp)#domain-name test.com
   ```

5. Configure the DNS server's IP address.

   ```
   WS5100(config-dhcp)#dns-server 192.168.0.10 192.168.0.11
   ```

6. Configure the DHCP client's IP address lease period.

   ```
   WS5100(config-dhcp)#lease 10
   ```

7. Exit from the DHCP instance upon creation of the network pool.

   ```
   WS5100(config-dhcp)#exit
   ```

8. Start the DHCP Server to instantiate the network pool.

   ```
   WS5100(config)#service dhcp
   ```

17.2.2 Creating a Host Pool

To create a host pool:

1. Create a DHCP server host address pool.

   ```
   WS5100(config)#ip dhcp pool hostpool
   ```

2. Assign the client name of the host for which static allocation is required.

   ```
   WS5100(config-dhcp)#client-name linuxbox
   ```

3. Assign an IP address for the host.

   ```
   WS5100(config-dhcp)#host 192.168.0.50
   ```

4. Configure the hardware address of the host.

   ```
   WS5100(config-dhcp)#hardware 00:a0:f8:6f:6b:88
   ```

5. Exit from the DHCP instance upon creation of the network pool.

   ```
   WS5100(config-dhcp)#exit
   ```

6. Start the DHCP Server to instantiate the network pool.

   ```
   WS5100(config)#service dhcp
   ```

17.2.3 Troubleshooting DHCP Configuration

1. The DHCP Server is disabled by default. Use the following command to enable the DHCP Server.

   ```
   WS5100(config)#service dhcp
   ```

   This command administratively enables the DHCP server. If the DHCP configuration is incomplete, it is possible the DHCP server will be disabled even after the execution of this command.

2. Use the `network` command to map the network pool to interface.

   ```
   network 192.168.0.0/24
   ```

   In the above example, 192.168.0.0/24 represents the L3 interface. When you execute this command, no check is performed to endorse whether an interface (with the specified IP/Netmask) exists. The verification is not performed because you can create a pool and map it to non existing L3 interface.

   When you add a L3 interface and assign an IP address to it, the DHCP server gets enabled/started on this interface. If you have a pool for network 192.168.0.0/24, but

the L3 interface is 192.168.0.0/16, DHCP is not enabled on 192.168.0.0/16, since it is different from 192.168.0.0/24.

3. A network pool without any include range is as good as not having a pool. Add a include range using the `address range` command

   ```
   address range 192.168.0.30 192.168.0.30
   ```

4. To work properly, a host pool should have the following 3 items configured:

   - client-name (CLI is `client-name <name>`)
   - fixed-address CLI is `host <ip>`)
   - hardware-address/client-identifier

   The hardware address is `hardware-address <addr>`

   The client-identifier is `client-identifier <id>`

   If you use `client-identifier` instead of `hardware-address`, a DHCP client sends the client-identifier when it requests for IP address. The Client - identifier has to be configured in the DHCP Client as an ASCII value and the same has to be used in the DHCP server option (for example, the Client- identifier option).

5. A host pool should have its corresponding network pool configured, otherwise the host pool is useless. The fixed IP address configured in the host pool must be in the subnet of the corresponding network pool.

6. If you create a pool and map it to interface, it automatically gets enabled, provided DHCP is enabled at a global level. Use the `no network` command to disable DHCP on per pool/interface basis.

7. To set a newly created pool as a network pool, use one of the following CLI commands:

   - network (for example, network 192.168.0.0/24)
   - address range (for example, address range 192.168.0.30 192.168.0.50)

8. To set a newly created pool as a host pool, use one of the following CLI commands:

   - host (for example, host 192.168.0.1)
   - client-name (Eg client-name "kaveri")
   - client-identifier (Eg client-identifier "aabb:ccdd")
   - hardware-address (Eg hardware-address aa:bb:cc:dd:ee:ff)

9. A pool can be configured either as the host pool or network pool, but not both.

10. A host pool can have either `client-identifier` or `hardware-address` configured, but not both.
11. An excluded address range has a higher precedence than an included address range. Thus, if a range is part of both an excluded and included range, it will be excluded.
12. DHCP options are first defined at the global level using `ip dhcp option <name> <code> <type>`. The value for these options are defined using the `option` under the DHCP pool context.

17.2.4 Creating a DHCP Option

To create a DHCP option:

1. To create a non standard option named “tftp-server”.

```
WS5100(config)#ip dhcp option tftp-server 183 ip
```

2. Enter the DHCP pool —”test”.

```
WS5100(config)#ip dhcp pool test
```

3. Assign a value to the DHCP option configured above.

```
WS5100(config-dhcp)#option tftp-server 192.168.0.100
```

4. Exit the DHCP instance.

```
WS5100(config-dhcp)#exit
```

18

DHCP Class Instance

Use `(config)#ip dhcp class <class name>` to enter the `(config-dhcpclass)` instance. Use this instance to configure DHCP user classes. The switch supports a maximum of 8 user classes per DHCP class.

Refer to *ip on page 12-6* and *DHCP Class Instance on page 18-1*for other DHCP related configurations.

18.1 DHCP Server Class Config Commands

Table 18.1 summarizes `config-std-nacl` commands:

Table 18.1 DHCP Server Class Command Summary

Command	Description	Ref.
clrscr	Clears the display screen	*page 18-2*
end	Ends the current mode and moves to the EXEC mode	*page 18-2*
exit	Ends the current mode and moves to the previous mode	*page 18-3*
help	Displays the interactive help system in HTML format	*page 18-3*
multiple-user-class	Enables multiple user class options	*page 18-4*
no	Negates a command or sets its defaults	*page 18-4*

Table 18.1 DHCP Server Class Command Summary

Command	Description	Ref.
option	Defines DHCP Server options	page 18-5
service	Invokes service commands to troubleshoot or debug `(config-if)` instance configurations	page 18-6
show	Displays running system information	page 18-7

18.1.1 clrscr

▸ DHCP Server Class Config Commands

Clears the display screen

Syntax

```
clrscr
```

Parameters

None

Example

```
WS5100(config-dhcpclass)#clrscr
WS5100(config-dhcpclass)#
```

18.1.2 end

▸ DHCP Server Class Config Commands

Ends and exits the current mode and moves to the PRIV EXEC mode. The prompt changes to `WS5100#`

Syntax

```
end
```

Parameters

None

Example

```
WS5100(config-dhcpclass)#end
WS5100#
```

18.1.3 exit

DHCP Server Class Config Commands

Ends the current mode and moves to the previous mode (GLOBAL-CONFIG). The prompt changes to `WS5100(config)#`

Syntax

```
exit
```

Parameters

None

Example

```
WS5100(config-dhcpclass)#exit
WS5100(config)#
```

18.1.4 help

DHCP Server Class Config Commands

Displays the system's interactive help system in HTML format

Syntax

```
help
```

Parameters

None

Example

```
WS5100(config-dhcpclass)#help
CLI provides advanced help feature.  When you need help,
anytime at the command line please press '?'.

If nothing matches, the help list will be empty and you must backup
until entering a '?' shows the available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each possible
   argument.
2. Partial help is provided when an abbreviated argument is entered
   and you want to know what arguments match the input
   (e.g. 'show ve?'.)

WS5100(config-dhcpclass)#
```

18.1.5 multiple-user-class

DHCP Server Class Config Commands

Enables the multiple user class option. Once invoked, the client (MU) sends multiple user classes

Syntax

```
help
```

Parameters

None

Example

```
WS5100(config-dhcpclass)#multiple-user-class
WS5100(config-dhcpclass)#
```

18.1.6 no

DHCP Server Class Config Commands

Negates a command or sets its defaults.

Syntax

```
no [multiple-user-class|option]
```

Parameters

multiple-user-class	Disables the multiple user class option
option	Modifies the parameters of existing DHCP Server options.

Example

```
WS5100(config-dhcpclass)#no multiple-user-class
WS5100(config-dhcpclass)#
```

18.1.7 option

DHCP Server Class Config Commands

Specifies a value for DHCP user class options

Syntax

```
option (user-class)(user class name)
```

Parameters

user-class (user class name)	Creates/modifies DHCP Server user class options

Usage Guidelines

Follow the steps below to create a DHCP user class:

1. Creates a DHCP class named **`WS5100DHCPclass`**. The switch supports a maximum of 32 DHCP classes.

   ```
   WS5100(config)#ip dhcp class WS5100DHCPclass
   WS5100(config-dhcpclass)#
   ```

2. Create a USER class named **`MC800`**. The privilege mode changes to `(config-dhcpclass)`. The switch supports a maximum of 8 user classes per DHCP class.

   ```
   WS5100(config-dhcpclass)#option user-class MC800
   WS5100(config-dhcpclass)#
   ```

3. Create a Pool named **`WID`**, using `(config)#` mode.

   ```
   WS5100(config)#ip dhcp pool WID
   WS5100(config-dhcp)#
   ```

4. Associate the DHCP class, created in Step 1 with the pool created in Step 3. The switch supports the association of 8 DHCP classes with a pool.

   ```
   WS5100(config-dhcp)#class WS5100DHCPclass
   WS5100(config-dhcp-class)#
   ```

5. The switch moves to a new mode (config-dhcp-class). Use this mode to an add address range for the DHCP class associated with the pool.

   ```
   WS5100(config-dhcp-class)#address range 11.22.33.44
   ```

Example

```
WS5100(config-dhcpclass)#option user-class MC800
WS5100(config-dhcpclass)#
```

18.1.8 service

DHCP Server Class Config Commands

Invokes service commands to troubleshoot or debug `(config-if)` instance configurations

Syntax

```
service (show) (cli)
```

Parameters

show (cli)	Displays the CLI tree of the current mode

Example

```
WS5100(config-dhcpclass)#service show cli
DHCP Server Class Config mode:
+-clrscr [clrscr]
+-do
  +-LINE [do LINE]
+-end [end]
+-exit [exit]
+-help [help]
+-multiple-user-class [multiple-user-class_cmd]
+-no
  +-multiple-user-class [no multiple-user-class_cmd]
  +-option
    +-user-class
      +-WORD [no option user-class WORD]
+-option
  +-user-class
    +-WORD [option user-class WORD]
+-quit [quit]
+-s
  +-commands [show commands]
    +-WORD [show commands WORD]
  +-running-config [show running-config]
    +-full [show running-config full].............................
................................................................
................................................................
.................................................................
................................................................
WS5100(config-dhcpclass)#
```

18.1.9 show

DHCP Server Class Config Commands

Displays current system information

Syntax

```
show <parameters>

show dhcp [config|status]
show ip dhcp [binding|class|pool|sharednetwork]
```

?	Displays the parameters for which information can be viewed using the show command

Example

```
WS5100(config-dhcpclass)#show ?
  access-list            Internet Protocol (IP)
  aclstats               Show ACL Statistics information
  alarm-log              Display all alarms currently in the system
  autoinstall            autoinstall configuration
  banner                 Display Message of the Day Login banner
  boot                   Display boot configuration.
  clock                  Display system clock
  commands               Show command lists
  crypto                 encryption module
  debugging              Debugging information outputs
  dhcp                   DHCP Server Configuration
  environment            show environmental information
  file                   Display filesystem information
  ftp                    Display FTP Server configuration
  history                Display the session command history
  interfaces             Interface status
  ip                     Internet Protocol (IP)
  ldap                   LDAP server
  licenses               Show any installed licenses
  logging                Show logging configuration and buffer
  mac                    Internet Protocol (IP)
  management             Display L3 Managment Interface name
  mobility               Display Mobility parameters
  ntp                    Network time protocol
  password-encryption    password encryption
  port-channel           Portchannel commands
  privilege              Show current privilege level
  radius                 RADIUS configuration commands
  redundancy-group       Display redundancy group parameters
```

```
  redundancy-history    Display state transition history of the
switch.
  redundancy-members    Display redundancy group members in detail
  running-config        Current Operating configuration
  securitymgr           Securitymgr parameters
  sessions              Display current active open connections
  snmp                  Display SNMP engine parameters
  snmp-server           Display SNMP engine parameters
  sole                  Smart Opportunistic Location Engine
Configuration
  spanning-tree         Display spanning tree information
  startup-config        Contents of startup configuration
  static-channel-group  static channel group membership
  terminal              Display terminal configuration parameters
  timezone              Display timezone
  upgrade-status        Display last image upgrade status
  users                 Display information about currently logged
in users
  version               Display software & hardware version
  wireless              Wireless configuration commands
  wlan-acl              wlan based acl

WS5100(config-dhcpclass)#show

WS5100(config-dhcpclass)#show ip dhcp binding
IP               MAC/Client-Id       Expiry Time
--               -------------       -----------
WS5100(config-dhcpclass)#

WS5100(config-dhcpclass)#show ip dhcp class WS5100DHCPclass
!
ip dhcp class WS5100DHCPclass
 option user-class MC800
WS5100(config-dhcpclass)#

WS5100(config-dhcpclass)#show ip dhcp pool WID
!
ip dhcp pool WID
 class WS5100DHCPclass
  address range 11.22.33.44
WS5100(config-dhcpclass)#
```

19

Radius Server Instance

Use the `radius-server local` command to move to the RADIUS server mode. Local (Onboard) RADIUS server commands are listed under this mode. Use the `(config-radsrv)` instance to configure local RADIUS server parameters.

19.1 Radius Configuration Commands

Table 19.1 summarizes the Global Config command:

Table 19.1 RADIUS Server Command Summary

Command	Description	Ref.
authentication	Configure the authentication scheme used with the RADIUS server	*page 19-2*
ca	Defines CA parameters	*page 19-3*
clrscr	Clears the display screen	*page 19-4*
crl-check	Enables a *Certificate Revocation List* (CRL) check.	*page 19-4*
end	Ends the current mode and moves to the EXEC mode	*page 19-5*
exit	Ends the current mode and moves to the previous mode	*page 19-5*
group	Sets RADIUS user group parameters. **Note:** This command creates another sub-instance called **`config-radsrv-group`** with its own command summary	*page 19-6*

Table 19.1 RADIUS Server Command Summary

Command	Description	Ref.
help	Displays the interactive help system	page 19-16
ldap-server	Sets LDAP server parameters	page 19-17
nas	Sets RADIUS client parameters	page 19-19
no	Negates a command or sets its defaults	page 19-20
proxy	Defines the RADIUS proxy server configuration	page 19-21
rad-user	Sets the RADIUS user configuration	page 19-22
server	Configures server certificate parameters	page 19-23
service	Invokes service commands to troubleshoot or debug `(config-radsrv)` instance configurations	page 19-24
show	Displays running system information	page 19-25

19.1.1 authentication

▸ Radius Configuration Commands

Configures the authentication scheme used with the RADIUS server

Syntax

```
authentication(data-source|eap-auth-type)
authentication data-source(ldap|local)
authentication eap-auth-type(all|peap-gtc|peap-mschapv2|tls|ttls-
md5|ttls-mschapv2|ttls-pap)
```

Parameters

data-source	Sets the RADIUS data source for user authentication.
eap-auth-type	Defines RADIUS EAP and default authentication configurations
all	Enables TTLS and PEAP settings
peap-gtc	Defines the EAP and PEAP settings used with the default authentication configuration

peap-mschapv2	Sets the EAP/PEAP type used with mschapv2
tls	Defines an EAP/TLS configuration scheme
ttls-md5	Sets the EAP/TTLS configuration used with the default md5 authentication scheme
ttls-mschapv2	Sets the EAP/TTLS configuration used with the default mschapv2 authentication scheme
ttls-pap	Sets the EAP/TTLS configuration used with the default pap authentication scheme

Sets `eap-auth-type` to `all` to service RADIUS requests received from mobile units. Setting `eap-auth-type` to `peap-gtc/peap-mschapv2` ensures `peap-gtc/peap-mschapv2` service only

Similarly, setting `eap-auth-type` to `ttls-md5/ttls-mschapv2/ttls-pap` services all ttls authentication requests from mobile units

Setting `eap-auth-type` to `tls` ensures only tls authentication is serviced

Example

```
WS5100(config-radsrv)#authentication eap-auth-type peap-mschapv2
WS5100(config-radsrv)#

WS5100(config-radsrv)#authentication data-source ldap
WS5100(config-radsrv)#
```

19.1.2 ca

Radius Configuration Commands

Configures CA (*Certificate Authority*) parameters.

Syntax

```
ca trust-point(WORD)
```

Parameters

trust-point	Defines the trustpoint configuration
WORD	Displays the existing trustpoint name

Usage Guidelines

Configures the trustpoint used by the local RADIUS server. Create the `trustpoint` before it can be used by the `crypto pki trustpoint` command

The default trust point in use is – `default-trustpoint.`

Example

```
WS5100(config)#radius-server local
WS5100(config-radsrv)#ca trust-point tp1
WS5100(config-radsrv)#
```

19.1.3 clrscr

Radius Configuration Commands

Clears the display screen

Syntax

```
clrscr
```

Parameters

None

Example

```
WS5100(config-radsrv)#clrscr
WS5100(config-radsrv)#
```

19.1.4 crl-check

Radius Configuration Commands

Enables a *Certificate Revocation List* (CRL) check. To enable the certificate revocation list, ensure the `crl list` is loaded using a `crypto pki import <trustpoint-name> crl` command.

Syntax

```
crl-check
```

Parameters

enable	Enables the CRL check

Usage Guidelines

TLS uses certificates for authentication. CRL (updated with a trustpoint), contains index numbers of revoked certificates. The CRL checks for any revoked certificates used for `tls` authentication

Example

```
WS5100(config-radsrv)#crl-check enable
WS5100(config-radsrv)#
```

19.1.5 end

Radius Configuration Commands

Ends and exits the current mode and moves to the PRIV EXEC mode. The prompt changes to `WS5100#`.

Syntax

```
end
```

Parameters

None

Example

```
WS5100(config-radsrv)#end
WS5100#
```

19.1.6 exit

Radius Configuration Commands

Ends the current mode and moves to the previous mode (GLOBAL-CONFIG). The prompt changes to `WS5100(config)#`

Syntax

```
exit
```

Parameters

None

Example

```
WS5100(config-radsrv)#exit
WS5100(config)#
```

19.1.7 group

Radius Configuration Commands

Configures RADIUS user groups. The CLI moves to the `config-radsrv-group` sub-instance to create a new group

The prompt changes from `WS5100(config-radsrv)#` to `WS5100 (config-radsrv-group)#`

Table 19.2 summarizes the RADIUS user group commands within the (config-radsrv-group) sub-instance

Table 19.2 RADIUS User Group Command Summary

Command	Description	Ref.
clrscr	Clears the display screen	*page 19-7*
end	Ends the current mode and moves to the EXEC mode	*page 19-7*
exit	Ends the current mode and moves to the previous mode	*page 19-7*
group	Sets RADIUS user group parameters	*page 19-8*
guest-group	Defines guest group permissions	*page 19-8*
help	Displays the interactive help system in HTML format	*page 19-9*
no	Negates a command or sets its defaults	*page 19-9*
policy	Defines the RADIUS group access policy configuration	*page 19-11*
rad-user	Adds a RADIUS user to this group	*page 19-12*
service	Invokes RADIUS service commands if they have been stopped	*page 19-13*
show	Displays running system information	*page 19-13*

19.1.7.1 clrscr

Radius Configuration Commands

Clears the display screen

Syntax

```
clrscr
```

Parameters

None

Example

```
WS5100(config-radsrv-group)#clrscr
WS5100(config-radsrv-group)#
```

19.1.7.2 end

Radius Configuration Commands

Ends and exits the current mode and changes to the PRIV EXEC mode. The prompt changes to `WS5100#`

Syntax

```
end
```

Parameters

None

Example

```
WS5100(config-radsrv-group)#end
WS5100#
```

19.1.7.3 exit

Radius Configuration Commands

Ends the current mode and moves to the previous mode `(config-radsrv)`. The prompt changes to `WS5100(config)#`.

Syntax

```
exit
```

Parameters

None

Example

```
WS5100(config-radsrv-group)#exit
WS5100(config-radsrv)#group
```

19.1.7.4 group

Radius Configuration Commands

Establishes RADIUS user group parameters. This command creates a group within the existing RADIUS group

Syntax

```
group
```

Parameters

WORD	Defines the RADIUS group name

Example

```
WS5100(config-radsrv-group)#group TestGroup
WS5100(config-radsrv-group)#
```

19.1.7.5 guest-group

Radius Configuration Commands

Manages a guest user linked with a hotspot. Create a guest-user and associate it with the guest-group. The guest-user and the policies of the guest group are used for hotspot authentication/authorization

Syntax

```
guest-group
```

Parameters

enable	Defines this group as a guest group

Usage Guidelines

Creates a guest group. The guest user created using `rad-user` can only be part of the guest group

Example

```
WS5100(config-radsrv-group)#guest-group enable
WS5100(config-radsrv-group)#
```

19.1.7.6 help

Radius Configuration Commands

Displays the system's interactive help in HTML format

Syntax

```
help
```

Parameters

None

Example

```
WS5100(config-radsrv-group)#help
CLI provides advanced help feature. When you need help,
anytime at the command line please press '?'.

If nothing matches, the help list will be empty and you must backup
until entering a '?' shows the available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each possible
   argument.
2. Partial help is provided when an abbreviated argument is entered
   and you want to know what arguments match the input
   (e.g. 'show ve?'.)

WS5100(config-radsrv-group)#
```

19.1.7.7 no

Radius Configuration Commands

Use this command to negate a command or set its defaults.

Syntax

```
no(policy|rad-user|service)
no policy(day|time|vlan|wlan)
no policy wlan(<1-32>|all)<1-32>
```

Parameters

policy	Defines the RADIUS group access policy configuration
day	Resets the access policy (days of permitted access) for this group
time	Configures the group's hourly access permissions

vlan	Sets the VLAN ID for the group
wlan	Configures WLAN access policy for this group
<1-32>	Sets the WLAN range for the access policy
all	Removes all the WLAN allowed
rad-user	Removes a user from this group
WORD	Defines an existing user name in this group
all	Removes all users from this group
service	Invokes service commands for troubleshooting or debugging the parameters of the group
radius	Disables the RADIUS server

Example

```
WS5100(config-radsrv-group)#no policy day
WS5100(config-radsrv-group)#

WS5100(config-radsrv-group)#no policy time
WS5100(config-radsrv-group)#

WS5100(config-radsrv-group)#no policy vlan
WS5100(config-radsrv-group)#

WS5100(config-radsrv-group)#no policy wlan 2 5
WS5100(config-radsrv-group)#

WS5100(config-radsrv-group)#no rad-user all
WS5100(config-radsrv-group)#

WS5100(config-radsrv-group)#no service radius
%%Info: Radius service stopped...
WS5100(config-radsrv-group)#
```

19.1.7.8 policy

Radius Configuration Commands

Sets the authorization policies for a particular group (like day/time of access, WLANs allowed etc.)

NOTE: A user-based VLAN is effective only if dynamic VLAN authorization is enabled for the WLAN (as defined within the WLAN Configuration screen).

Syntax

```
policy(day|time|vlan|wlan)
policy day(all|fr|mo|sa|su|th|tu|we|weekdays)
ploicy time(start|end)<0-23><0-59>
policy vlan<1-4094>
```

Parameters

day	Day of access policy configuration
all	All days (from Sunday to Saturday)
fr	Friday
mo	Monday
sa	Saturday
su	Sunday
th	Thursday
tu	Tuesday
we	Wednesday
weekdays	Allows access only during weekdays (M-F)
time	Sets the access policy time for this group
start	Sets the start time
end	Defines the end time (must be greater than the start time)
<0-23>	Sets the hourly (hh) access limit

<0-59>	Sets the minute (mm) access limit
vlan	Sets the VLAN ID for this group
<1-4094>	Defines the VLAN range
wlan	Sets the WLAN access policy for this group
<1-32>	Sets the WLAN index

Example

```
WS5100(config-radsrv-group)#policy day weekdays
WS5100(config-radsrv-group)#

WS5100(config-radsrv-group)#policy time start 12 12 end 22 22
WS5100(config-radsrv-group)#

WS5100(config-radsrv-group)#policy vlan 20
WS5100(config-radsrv-group)#

WS5100(config-radsrv-group)#policy wlan 20 21 22 23
WS5100(config-radsrv-group)#
```

19.1.7.9 rad-user

Radius Configuration Commands

Adds an exisitng RADIUS user to this group. If the RADIUS user is not available in the Onboard RADIUS server's database, create a new RADIUS user using the `rad-user` command from within the `(config-radsrv)` mode. For more information, see *rad-user on page 19-22*

Syntax

```
rad-user
```

Parameters

WORD	Existing RADIUS user name

Example

```
WS5100(config-radsrv)#rad-user user1 password user1
WS5100(config-radsrv)#group group1
WS5100(config-radsrv-group)#rad-user user1

WS5100(config-radsrv-group)#
```

19.1.7.10 service

Radius Configuration Commands

Invokes RADIUS service commands (if they have been stopped). This command enables the RADIUS server. A RADIUS restart is executed only from the `config` mode.

Syntax

```
service(clear|diag-shell|radius|save-cli|show|start-
shell|tethereal)
service radius restart
```

Parameters

clear	Removes the specified support information
diag-shell	Provides diag shell access
radius	Enables a RADIUS server restart
save-cli	Saves the CLI tree for all modes in HTML
show	Displays running system information
start-shell	Provides shell access
tethereal	Dumps and analyzes network traffic

Example

```
WS5100(config-radsrv-group)#service radius restart
WS5100(config-radsrv-group)#
```

19.1.7.11 show

Radius Configuration Commands

Displays current system information running on the switch

Syntax

```
show<paramater>
```

Parameters

?	Displays the parameters for which information can be viewed using the show command

Example

```
WS5100(config-radsrv-group)#show ?
  access-list          Internet Protocol (IP)
  alarm-log            Display all alarms currently in the system
  autoinstall          autoinstall configuration
  banner               Display Message of the Day Login banner
  boot                 Display boot configuration.
  clock                Display system clock
  commands             Show command lists
  crypto               crypto
  debugging            Display debugging setting
  environment          show environmental information
  file                 Display filesystem information
  ftp                  Display FTP Server configuration
  history              Display the session command history
  interfaces           Interface status and configuration
  ip                   Internet Protocol (IP)
  ldap                 ldap server
  licenses             Show any installed licenses
  logging              Show logging configuration and buffer
  mac                  Media Access Control
  management           Display L3 Managment Interface name
  mobility             Display Mobility Parameters
  ntp                  Network time protocol
  password-encryption  password encryption
  privilege            Show current privilege level
  radius               Radius configuration commands
  redundancy-group     Display redundancy group parameters
  redundancy-history   Display state transition history of the
switch.
  redundancy-members   Display redundancy group members in detail
  running-config       Current Operating configuration
  securitymgr          Display debug info for ACL, VPN and NAT
  sessions             Display current active open connections
  snmp                 Display SNMP engine parameters
  snmp-server          Display SNMP engine parameters
  startup-config       Contents of startup configuration
  terminal             Display terminal configuration parameters
  timezone             Display timezone
  upgrade-status       Display last image upgrade status
  users                Display information about terminal lines
  version              Display software & hardware version
  wireless             Wireless configuration commands

WS5100(config-radsrv-group)#

WS5100(config-radsrv)#show radius trust-point

Trust-point Configured For Radius
```

```
_____________________________________
        Server Trust-point : default-trustpoint
        CA Trust-point     : default-trustpoint

WS5100(config-radsrv)#
```

19.1.7.12 Example–Creating a Group

The **(config-radsrv-group)** sub-instance is explained in the example below:

1. Create a group called **Sales** in the local RADIUS server database.
   WS5100(config-radsrv)#group sales
2. Check the RADIUS user group's configuration commands.

   WS5100(config-radsrv-group)#?

   RADIUS user group configuration commands:
3. Use a `policy` command to configure group policies for the group created in Step 1.

   ```
   WS5100(config-radsrv-group)#policy ?
   day   Day of access policy configuration
   time  Configure time of access policy for this group
   vlan  VLAN id for this group
   wlan  Configure wlan access policy for this group

   WS5100(config-radsrv-group)#policy day weekdays
   WS5100(config-radsrv-group)#policy time start 12 30 end 15 30
   ```
4. Use the **policy vlan** command to assign a VLAN ID of 10 to the Sales group

   ```
   WS5100(config-radsrv-group)#policy vlan 10
   ```
5. Use the **policy wlan** command to allow only authorized users to access this group's WLAN

   ```
   WS5100(config-radsrv-group)#policy wlan 1 2 5
   ```
6. Use `(config-radsrv)#rad-user` to create a user called **testuser** and add it to the group

   ```
   WS5100(config-radsrv)#rad-user testuser password testpassword group
   sales
   Sep 08 17:41:55 2006: RADCONF: Adding user "testuser" into local
   database
   Sep 08 17:41:55 2006: RADCONF: User "testuser" is added to group
   "sales"
   ```

7. Use `(config-radsrv)#nas` to add a NAS entry for the group

```
WS5100(config-radsrv)#nas ?
A.B.C.D/M  Radius client IP address

WS5100(config-radsrv)#nas 10.10.10.0/24 ?
key  Radius client shared secret

WS5100(config-radsrv)#nas 10.10.10.0/24 key ?
0     Password is specified UNENCRYPTED
2     Password is encrypted with password-encryption secret
LINE  The secret(client shared secret), upto 32 characters

WS5100(config-radsrv)#nas 10.10.10.0/24 key 0 very-secret!!
```

8. Use `(config-radsrv)#proxy` to add a realm name for the group

```
WS5100(config-radsrv)#proxy realm mydomain.com server 10.10.1.10 port
1812 secret 0 testing
```

9. Save the changes and restart the RADIUS server

```
WS5100(config-radsrv)#service radius restart
Sep 08 17:48:04 2006: %PM-5-PROCSTOP: Process "radiusd" has been
stopped
Sep 08 17:48:05 2006: RADCONF: radius config files generated
successfully
WS5100(config-radsrv)#Sep 08 17:48:05 2006: %DAEMON-6-INFO:
radiusd[8830]: Ready to process requests.
```

19.1.8 help

Radius Configuration Commands

Displays the system's interactive help in HTML format

Syntax

```
help
```

Parameters

None

Example

```
WS5100(config-radsrv)#help?
  help  Description of the interactive help system
```

```
WS5100(config-radsrv)#help
CLI provides advanced help feature.  When you need help,
anytime at the command line please press '?'.

If nothing matches, the help list will be empty and you must backup
until entering a '?' shows the available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each possible
   argument.
2. Partial help is provided when an abbreviated argument is entered
   and you want to know what arguments match the input
   (e.g. 'show ve?'.)

WS5100(config-radsrv)#
```

19.1.9 ldap-server

Radius Configuration Commands

Sets the LDAP server's configuration. It uses the exisitng external database (active directory with the onboard RADIUS server) instead of the local database on the switch

Syntax

`ldap-server(primary|secondary)host(A.B.C.D)`

Parameters

primary	Sets the primary LDAP server's configuration
secondary	Defines the secondary LDAP server's configuration
host <LDAP IP Address>	Sets the LDAP server's IP configuration • A.B.C.D – Defines the LDAP server IP address
port <number>	Enter the TCP/IP port number for the LDAP server acting as the data source
login	Use the following as the login: `(sAMAccountName=%{Stripped-User-Name:-%{User-Name}})`
bind-dn	Specifies the distinguished name to bind with the LDAP server

base-dn	Specifies a distinguished name that establishes the base object for the search. The base object is the point in the LDAP tree at which to start searching
passwd	Sets a valid password for the LDAP server
passwd-attr	Enter the password attribute used by the LDAP server for authentication
group-attr	Specifies the group attribute used by the LDAP server
group-filter	Specifies the group filters used by the LDAP server
group-membership	Specifies the Group Member Attribute sent to the LDAP server when authenticating users
net-timeout	Enter a timeout the system uses to terminate the connection to the RADIUS Server if no activity is detected

Usage Guidelines

Use the login filter and group filter values (described in the example below) for all LDAP configuration scenarios

Use `passwd` parameter to enter the password for active directory user mentioned in bind -dn. This is used for the initial login to the active directory

The `passwd-attr` and `group-membership` is retained as described in the following example:

Example

```
WS5100(config)#ldap-server primary host xxx.xxx.x.xx port 389 login
(sAMAccountName=%{Stripped-User-Name:-%{User-Name}}) bin
d-dn cn=admin,ou=wid,dc=symbolTech,dc=local base-dn
ou=wid,dc=symbolTech,dc=local passwd SYMBOL@123 passwd-attr
UserPassword
group-attr cn group-filter (|(&(objectClass=group)(member=%{Ldap-
UserDn}))(&(objectClass=GroupOfUniqueNames)(uniquemember=%{L
dap-UserDn}))) group-membership radiusGroupName net-timeout 1
WS5100(config)#
```

19.1.10 nas

Radius Configuration Commands

Sets the configuration of the RADIUS client

Syntax

`nas(A.B.C.D/M)key` *`(0|2|LINE)`*

Parameters

A.B.C.D/M	Sets the RADIUS client's IP address.
key	Sets the RADIUS client's shared key
0	Defines the Password as UNENCRYPTED
2	Password is encrypted with password-encryption secret
LINE	Defines the secret (client shared secret) up to 32 characters

Example

```
WS5100(config-radsrv)#nas ?
A.B.C.D/M  Radius client IP address

WS5100(config-radsrv)#nas 10.10.10.0/24 ?
key  Radius client shared secret

WS5100(config-radsrv)#nas 10.10.10.0/24 key ?
0     Password is specified UNENCRYPTED
2     Password is encrypted with password-encryption secret
LINE  The secret(client shared secret), upto 32 characters

WS5100(config-radsrv)#nas 10.10.10.0/24 key 0 very-secret!!
```

19.1.11 no

Radius Configuration Commands

Negates a command or sets its defaults.

Syntax

```
no(authentication|ca|crl-check|group|ldap-server|nas|proxy|rad-
user|server|service)
```

Parameters

authentication	Defines the RADIUS authentication
ca	Configures *Certificate Authority* (CA) parameters
crl-check	Enables a *Certificate Revocation List* (CRL) check
group	Sets the local RADIUS server's group configuration
ldap-server	Defines LDAP server parameters
nas	Sets the RADIUS client configuration
proxy	Defines the RADIUS proxy server
rad-user	Sets the RADIUS user configuration
server	Configures server certificate parameters
service	Invokes service commands for troubleshooting and debugging

Example

```
WS5100(config-radsrv)#no authentication data-source
WS5100(config-radsrv)#

WS5100(config-radsrv)#no ca trust-point
WS5100(config-radsrv)#
```

19.1.12 proxy

Radius Configuration Commands

Configures a proxy RADIUS server based on the realm/suffix

Syntax

```
proxy(realm|retry-count|retry-delay)
proxy relam(WORD)server(A.B.C.D)port(<1024-65535>)secret(0|2|WORD)
```

Parameters

realm WORD	The realm name is a string of up to 50 characters
	• server (A.B.C.D) – Sets the proxy server IP address
	• port <1024-65535> – Sets the proxy server port number
	• secret (0|2|WORD) – Sets the proxy server secret string
	  • 0 – Password is specified UNENCRYPTED
	  • 2 – Password is encrypted with a password encryption secret
	  • WORD – Sets the proxy server shared secret up to 32 characters

retry-count *<3-6>*	Defineds the proxy server retry count value
retry-delay*<5-10>*	Defines the proxy server retry delay time (in seconds)

Usage Guidelines

Only five RADIUS proxy servers can be configured. The proxy server attempts six retries before it times out. The retry count defines the number of times the switch transmits each RADIUS request before giving up. The timeout value defines the duration for which the switch waits for a reply to a RADIUS request before retransmitting the request

Example

```
WS5100(config-radsrv)#proxy realm Test server 10.10.10.1 port 2220
secret "Very Very Secret !!!"
WS5100(config-radsrv)#

WS5100(config-radsrv)#proxy retry-count 5
WS5100(config-radsrv)#

WS5100(config-radsrv)#proxy retry-delay 8
WS5100(config-radsrv)#
```

19.1.13 rad-user

Radius Configuration Commands

Sets RADIUS user parameters

Syntax

`rad-user(WORD)password` *`(0|2|WORD)`*

Parameters

WORD	Enter a user name up to 64 characters in length
password*(0|2|WORD)*	Sets the RADIUS user password
0	Defines the password as UNENCRYPTED
2	The password is encrypted with a password encryption secret
WORD	Sets a password up to 21 characters in length

Usage Guidelines

Use `group, guest, expiry-time expiry-date, start-time` and `start-date` parameters to create a RADIUS guest user.

The RADIUS user group specified while creating a guest user must be a *guest-group*

Example

```
WS5100(config-radsrv)#rad-user TestRadUser password "I SPY U"
WS5100(config-radsrv)#

WS5100(config-radsrv)#rad-user guest1 password 0 password1 group
guest-group
guest expiry-time 12:12 expiry-date 05:12:2007 start-time 12:12
start-date 05:11:2007
WS5100(config-radsrv)#
```

19.1.14 server

Radius Configuration Commands

Configures server certificate parameters used by a RADIUS server. The server certificate is a part of a trustpoint created using *crypto on page 5-16*

Syntax

```
server trust-point
```

Parameters

trust-point	Sets the trustpoint configuration
WORD	Existing trustpoint name

Usage Guidelines

Create a trustpoint using (crypto-pki-trustpoint) . The server certificate must be created under the trustpoint using crypto-pki commands. Refer to *crypto on page 5-16* for more information

Example

```
WS5100(config-radsrv)#server trust-point TestTP
WS5100(config-radsrv)#
```

19.1.15 service

Radius Configuration Commands

Invokes the service commands to trobuleshoot or debug the `(config-radsrv)` instance configuration. This command is also used to enable the RADIUS server

Syntax

```
service(clear|diag-shell|radius|save-cli|show|start-
shell|tethereal)
service radius restart
```

Parameters

clear	Removes the specified support information
diag-shell	Provides diag shell access
radius	Enables a RADIUS server restart
save-cli	Saves the CLI tree for all modes in HTML format
show	Displays running system information
start-shell	Provides shell access
tethereal	Dumps and analyzes network traffic

Example

```
WS5100(config-radsrv)#service show cli
Radius Configuration mode:
+-authentication
  +-data-source
    +-ldap [authentication data-source (local|ldap)]
    +-local [authentication data-source (local|ldap)]
  +-eap-auth-type
    +-all [authentication eap-auth-type (ttls-md5|ttls-pap|ttls-
mschapv2|peap-gt
c|peap-mschapv2|tls|all)]
    +-peap-gtc [authentication eap-auth-type (ttls-md5|ttls-
pap|ttls-mschapv2|pe
ap-gtc|peap-mschapv2|tls|all)]
    +-peap-mschapv2 [authentication eap-auth-type (ttls-md5|ttls-
pap|ttls-mschap
v2|peap-gtc|peap-mschapv2|tls|all)]
```

```
    +-tls [authentication eap-auth-type (ttls-md5|ttls-pap|ttls-
mschapv2|peap-gt
c|peap-mschapv2|tls|all)]
    +-ttls-md5 [authentication eap-auth-type (ttls-md5|ttls-
pap|ttls-mschapv2|pe
ap-gtc|peap-mschapv2|tls|all)]
    +-ttls-mschapv2 [authentication eap-auth-type (ttls-md5|ttls-
pap|ttls-mschap
v2|peap-gtc|peap-mschapv2|tls|all)]
    +-ttls-pap [authentication eap-auth-type (ttls-md5|ttls-
pap|ttls-mschapv2|pe
ap-gtc|peap-mschapv2|tls|all)]
+-ca
  +-trust-point
 -- MORE --, next page: Space, next line: Enter, quit: Control-C
```

19.1.16 show

▸ *Radius Configuration Commands*

Displays current system information running on the switch

Syntax

```
show<paramater>
```

Parameters

?	Displays the parameters for which information can be viewed using the show command

Example

```
WS5100(config-radsrv)#show ?
  access-list           Internet Protocol (IP)
  alarm-log             Display all alarms currently in the system
  autoinstall           autoinstall configuration
  banner                Display Message of the Day Login banner
  boot                  Display boot configuration.
  clock                 Display system clock
  commands              Show command lists
  crypto                crypto
  debugging             Display debugging setting
  environment           show environmental information
  file                  Display filesystem information
  ftp                   Display FTP Server configuration
  history               Display the session command history
  interfaces            Interface status and configuration
  ip                    Internet Protocol (IP)
  ldap                  ldap server
```

```
  licenses              Show any installed licenses
  logging               Show logging configuration and buffer
  mac                   Media Access Control
  management            Display L3 Managment Interface name
  mobility              Display Mobility Parameters
  ntp                   Network time protocol
  password-encryption   password encryption
  privilege             Show current privilege level
  radius                Radius configuration commands
  redundancy-group      Display redundancy group parameters
  redundancy-history    Display state transition history of the
switch.
  redundancy-members    Display redundancy group members in detail
  running-config        Current Operating configuration
  securitymgr           Display debug info for ACL, VPN and NAT
  sessions              Display current active open connections
  snmp                  Display SNMP engine parameters
  snmp-server           Display SNMP engine parameters
  startup-config        Contents of startup configuration
  terminal              Display terminal configuration parameters
  timezone              Display timezone
  upgrade-status        Display last image upgrade status
  users                 Display information about terminal lines
  version               Display software & hardware version
  wireless              Wireless configuration commands

WS5100(config-radsrv)#show
```

WS5100(config)#show radius trust-point

```
Trust-point Configured For Radius
_____________________________________
        Server Trust-point : default-trustpoint
        CA Trust-point     : default-trustpoint

WS5100(config)#
```

20

Wireless Instance

Use the `(config-wireless)` instance to configure local RADIUS server parameters associated with the switch.

20.1 Wireless Configuration Commands

Table 20.1 summarizes `(config-wireless)` commands:

Table 20.1 Wireless Config Command Summary

Command	Description	Ref.
aap	Sets *Adaptive AP* (AAP) related commands	*page 20-4*
adopt-unconf-radio	Adopts a radio even if its not yet configured. The default templates can be used for configuration	*page 20-4*
adoption-pref-id	Used as a preference identifier for this switch. All radios configured with this preference identifier are more likely to be adopted by this switch	*page 20-5*
ap	Displays access port related commands	*page 20-5*
ap-detection	Defines the AP detection configuration	*page 20-6*
ap-ip	Modifies static IP information for access ports	*page 20-7*

Table 20.1 Wireless Config Command Summary (Continued)

Command	Description	Ref.
ap-timeout	Changes the default inactivity timeout for access ports	*page 20-9*
ap-udp-port	Configures the UDP port for AP L3 adoption **NOTE:** Enable this option in the DHCP Server supporting this access-port	*page 20-9*
broadcast-tx-speed	Sets the rate at which broadcast and multicast traffic is transmitted	*page 20-10*
client	Defines the wireless client configuration	*page 20-10*
clrscr	Clears the display screen	*page 20-14*
convert-ap	Changes an AP's mode of operation	*page 20-14*
country-code	Configures the country of operation. All existing radio configurations are erased	*page 20-15*
dhcp-sniff-state	Records mobile unit DHCP state information	*page 20-17*
dot11-shared-key-auth	Enables support for 802.11 shared key authentication	*page 20-18*
end	Ends the current mode and moves to the EXEC mode	*page 20-18*
exit	Ends the current mode and moves to the previous mode	*page 20-19*
fix-broadcast-dhcp-rsp	Converts broadcast DHCP server responses to unicast responses	*page 20-19*
help	Displays the interactive help system	*page 20-19*
ids	Sets intrusion detection configuration commands	*page 20-20*

Table 20.1 Wireless Config Command Summary (Continued)

Command	Description	Ref.
mac-auth-local	Defines the local MAC authentication list	*page 20-23*
manual-wlan-mapping	Allows the manual mapping/un-mapping of WLANs to configured radios	*page 20-24*
mobile-unit	Configures mobile unit parameters	*page 20-24*
mobility	Configures mobility parameters	*page 20-25*
multicast-packet-limit	Sets a multicast packet limit (per second) for a VLAN	*page 20-26*
multicast-throttle-watermark	Configures watermarks for handling bursts of broadcast/multicast frames	*page 20-26*
no	Negates a command or sets its defaults	*page 20-27*
proxy-arp	Responds to ARP requests from the RON to a WLAN on behalf of MUs	*page 20-28*
qos-mapping	Defines the QoS mapping between wired and wireless domains	*page 20-28*
radio	Defines the radio's configuration	*page 20-29*
rate-limit	Sets the default rate limit (per user)	*page 20-38*
self-heal	Sets the self healing configuration	*page 20-38*
sensor	Defines the *Wireless Intrusion Protection System* (WIPS) configuration	*page 20-40*
service	Invokes service commands to troubleshoot or debug the `(config-wireless)` instance configuration	*page 20-41*
show	Displays running system information	*page 20-47*
wlan	Sets WLAN related parameters	*page 20-48*
wlan-bw-allocation	Allocates radio bandwidth (per WLAN)	*page 20-63*

20.1.1 aap

Wireless Configuration Commands

Defines the AAP configuration

Syntax

```
aap (config-aaply)[def-delay|mesh-delay]<3-10000>
```

Parameters

config-apply [def-delay|mesh-delay] <30-10000>	Applies AAP configuration settings • def-delay – Sets the default time to delay before applying AAP configuration • mesh-delay – Defines the interval to delay before applying AAP configuration to Mesh APs • <30-10000> – Set the delay time (in seconds)

Example

```
WS5100(config-wireless)#aap config-apply mesh-delay 300
WS5100(config-wireless)#
```

20.1.2 adopt-unconf-radio

Wireless Configuration Commands

Adopts a radio (even if not yet configured). Default templates are used for configuration

Syntax

```
adopt-unconf-radio
```

Parameters

enable	Enables the adoption of non-configured radios

Example

```
WS5100(config-wireless)#adopt-unconf-radio enable
WS5100(config-wireless)#
```

20.1.3 adoption-pref-id

Wireless Configuration Commands

Use as a preference identifier for the switch. All radios configured with this preference identifier are more likely to be adopted by this switch

Syntax

```
adoption-pref-id
```

Parameters

<1-65535>	Set a Pref-ID (1-65535)

Example

```
WS5100(config-wireless)#adoption-pref-id 500
```

20.1.4 ap

Wireless Configuration Commands

Defines the name and location of the access port

Syntax

```
ap [<AP index>|<MAC Address>][location|name]
```

Parameters

AP Index	Sets a single AP index. Use the `show wireless ap` command to view the AP's index value • location – Defines the location description of the AP • name – Sets the name for this AP
MAC Address	Lists an AP's MAC address. Use the `show wireless ap` command to view the AP's index

Example

```
WS5100(config-wireless)#ap 00-15-70-14-FE-C4 location 5th Floor
SalesUnit
WS5100(config-wireless)#

WS5100(config-wireless)#ap 1 location BLR  RMZ Ecospace
WS5100(config-wireless)#
```

20.1.5 ap-detection

Wireless Configuration Commands

Configures access port detection parameters

Syntax

```
ap-detection
[approved|enable|mu-assisted-scan|timeout (approved|unapproved)]

ap-detection approved add <1-200> (MAC Address)(SSID)
ap-detection mu-assisted-scan(enable|refresh<300-86400>)
```

Parameters

aap-version	AP detection configuration commands

approved	Sets the approved access port list
	• add <1-200> – Adds an entry to the approved access port list
	• MAC Address – Select either:
	  • MAC– Define a MAC address (in AA-BB-CC-DD-EE-FF format)
	  • any– Assigns any MAC address
	• SSID – Select either:
	  • LINE–Enter a string up to 32 characters
	  • any– Assigns any SSID

enable	Allows access ports to look for APs
mu-assisted-scan	Sets mobile unit assisted scanning configuration • enable – Enables mobile unit assisted scanning • refresh <30-86400> – Defines the period (in seconds) used by all scan-capable mobile units are polled to scan for neighboring access ports
timeout *<1-65535>*	The amount of time (in seconds) an AP remains in the list after it is no longer seen • approved • unapproved

Example

```
WS5100(config-wireless)#ap-detection enable
WS5100(config-wireless)#

WS5100(config-wireless)#ap-detection approved add 150 any any
WS5100(config-wireless)#

WS5100(config-wireless)#ap-detection mu-assisted-scan enable
WS5100(config-wireless)#

WS5100(config-wireless)#ap-detection mu-assisted-scan refresh 520
WS5100(config-wireless)#
```

20.1.6 ap-ip

- *Wireless Configuration Commands*

Modifies the static IP address for an access port

Syntax

```
ap-ip [<List of Indices/MAC address >|default-ap]

ap-ip <List of Indices> [static-ip|switch-ip]
ap-ip <List of Indices> (static-ip) <IP address/mask> <gateway IP>
ap-ip <List of Indices> (switch-ip)[add <IP address>|
              delete(<IP address Index>|<IP address>)|set-default]

ap-ip (default-ap) [add <IP address>|delete(<IP address Index>|<IP
address>)|set-default]
```

Parameters

<List of Indices> / MAC address	Use `show wireless ap` to view an AP's index or MAC address. Select the AP's index / MAC Address to modify its static IP address
	• static-ip – Sets the static IP address, netmask and gateway address of the AP
	  • A.B.C.D/M – Defines the static IP address and mask
	  • A.B.C.D – Sets the gateway IP address
	• switch-ip – Defines the static switch IP address
	  • add – Adds a static switch IP address
	  • delete – Deletes a static switch IP address
	  • set-default – Default switch IP address

default-ap	Sets the default static switch IP address
	• switch-ip – Static switch IP address
	  • add – Adds a static switch IP address
	  • delete – Deletes a static switch IP address
	  • set-default – Sets a default switch IP address

Example

```
WS5100(config-wireless)#ap-ip 1 static-ip 192.168.10.25/24
192.168.10.1
WS5100(config-wireless)#

WS5100(config-wireless)#ap-ip 1 switch-ip add 192.168.10.25
10.10.1.4
WS5100(config-wireless)#

WS5100(config-wireless)#ap-ip default-ap switch-ip set-default
WS5100(config-wireless)#
```

20.1.7 ap-timeout

Wireless Configuration Commands

Changes the default inactivity timeout for access ports

Syntax

```
ap-timeout <index> <40-180>
```

Parameters

<Index> <40-180>	Access-ports identified by a single MAC address or by a list of indices. Use `show wireless ap` to view the AP's index or MAC address • <40-180> – Sets the new inactivity timeout (in seconds)

Example

```
WS5100(config-wireless)#ap-timeout 1 40
WS5100(config-wireless)#
```

20.1.8 ap-udp-port

Wireless Configuration Commands

Configures the UDP port for layer 3 adoption of APs. You also need to configure the DHCP server serving the APs with the same parameter

Syntax

```
ap-udp-port <1-65535>
```

Parameters

<1-65535>	Sets the port number for layer 3 adoption of APs

Example

```
WS5100(config-wireless)#ap-udp-port 20
WS5100(config-wireless)#
```

20.1.9 broadcast-tx-speed

Wireless Configuration Commands

Configure the rate at which broadcast and multicast traffic is transmitted between the switch and mobile unit

Syntax

```
broadcast-tx-speed(range|throughput)
```

Parameters

range	Uses a lowest basic rate. Provides maximum range
throughput	Uses a highest basic rate. Provides maximum throughput (default)

Example

```
WS5100(config-wireless)#broadcast-tx-speed range
WS5100(config-wireless)#

WS5100(config-wireless)#broadcast-tx-speed throughput
WS5100(config-wireless)#
```

20.1.10 client

Wireless Configuration Commands

Use this command to configure a wireless client. This command creates an exclude-list or include list. Creating a list moves the user to a new mode ("`config-wireless-client-list`"). Refer to *config-wireless-client-list on page 20-12* for a `(config-wireless-client-list)` command summary

Syntax

```
client {exclude-list|include-list}(NAME)
```

Parameters

exclude-list	Sets the wireless client exclude list configuration. A MU NAC check is conducted, except for those in the exclude list. Devices in the exclude list will not have a NAC check performed

include-list	Defines the wireless client include list configuration. No MU NAC check is conducted, except for those in the include list. Devices in the include-list will have NAC checks

Usage Guidelines

Refer to the configurations below to:

- Create an exclude list:

```
WS5100(config-wireless)#client exclude-list protected-hosts
WS5100(config-wireless-client-list)#
```

- Add a host entry into the exclude list:

```
WS5100(config-wireless-client-list)# station printers
00:00:AA:DD:EE:11/00:00:FF:DD:EE:11
WS5100(config-wireless-client-list)# station testing-host1
00:11:AA:03:1B:FE
```

- Associate the exclude list to a WLAN:

```
WS5100(config-wireless-client-list)# wlan 1
```

- Configure RADIUS server parameters:

```
WS5100(config-wireless)# wlan 1 nac-server primary 192.168.0.1
WS5100(config-wireless)# wlan 1 nac-server primary secret 0
testing
WS5100(config-wireless)# wlan 1 nac-server secondary 192.168.1.1
WS5100(config-wireless)# wlan 1 nac-server secondary secret 0
testing123
```

- Enable NAC for a WLAN:

```
WS5100(config-wireless)# wlan 1 nac-mode do-nac-except-exclude-
list
```

- Undo a configuration:

```
WS5100(config-wireless)# client exclude-list protected-hosts
WS5100(config-wireless-client-client)# no station testing-host1
WS5100(config-wireless)# no client exclude-list protected-hosts
```

```
WS5100(config-wireless)# no wlan 1 nac-server primary
WS5100(config-wireless)# no wlan 1 nac-server primary secret
WS5100(config-wireless)# no wlan 1 nac-server secondary
WS5100(config-wireless)# no wlan 1 nac-server secondary radius-key
WS5100(config-wireless)# no wlan 1 nac exclude-list protected-
hosts
```

Example

```
WS5100(config-wireless)#client exclude-list JustMe
WS5100(config-wireless-client-list)#
```

20.1.10.1 config-wireless-client-list

Use `(config-wireless)# client` to enter the (`config-wireless-client-list`) instance. Use this instance to create an exclude list or include list.

Table 20.2 summarizes `config-wireless-client-list` commands:

Table 20.2 Exclude List Configuration Command

Command	***Description***
clrscr	Clears the display screen
end	Ends the current mode and moves to the EXEC mode
exit	Ends the current mode and moves to the previous mode
help	Displays the interactive help system
no	Negates a command or sets its defaults
service	Provides a means of troubleshooting and debugging
show	Displays running system information
station	Defines a MU's MAC configuration
wlan	Sets Wireless LAN related parameters

station

config-wireless-client-list

Adds a specified MAC entry into the client's exclude or include list

Syntax

```
(config-wireless-client-list) station (host-name)
[MU mac address|MU mac mask]
```

Parameters

host-name [MU mac address|MU mac mask]	Defines an index for this host entry in the client list. The host station name must be of size <1-21> • MU mac address –Sets the MU mac address in AA-BB-CC-DD-EE-FF or AA:BB:CC:DD:EE:FF or AABB.CCDD.EEFF format • MU mac mask – Sets the MU mac mask in AA-BB-CC-DD-EE-FF or AA:BB:CC:DD:EE:FF or AABB.CCDD.EEFF format

Example

```
WS5100(config-wireless-client-list)#station ExcludeList1
AA:BB:CC:DD:EE:FF
WS5100(config-wireless-client-list)#
```

wlan

config-wireless-client-list

Adds a client exclude list name into/from the WLAN

Syntax

```
wlan [<1-32>| WLAN-name]
```

Parameters

wlan [<1-32> | WLAN name]	• <1-32> – Sets a single WLAN index • WLAN name – A list (1,3,7) or range (3-7) of WLAN indices

Example

```
WS5100(config-wireless-client-list)#wlan 1
WS5100(config-wireless-client-list)#
```

20.1.11 clrscr

Wireless Configuration Commands

Clears the display screen

Syntax

```
clrscr
```

Parameters

None

Example

```
WS5100(config-wireless)#clrscr
WS5100(config-wireless)#
```

20.1.12 convert-ap

Wireless Configuration Commands

Changes the mode of operation of an AP to either sensor or standalone

Syntax

```
convert-ap <1-48>(default|sensor|standalone)
```

Parameters

<1-48>	Sets the indices of the APs to be converted (from the ['show wireless ap' command])
default	Does not force conversion. Lets the AP negotiate its normal mode of operation with the switch
sensor	Converts an AP300 to operate as an IDS sensor. **Note:** The switch will not be able to adopt this AP again until it is converted back to a AP300 using the [`sensor <1-256> revert-to-ap`] command

standalone	Converts a thin AP-4131 back to a stand-alone AP **Note:** The switch will not be able to adopt this AP again until the AP is converted back to a thin-AP using the AP's configuration interface

Example

```
WS5100(config-wireless)#convert-ap 1 default
WS5100(config-wireless)#
```

20.1.13 country-code

Wireless Configuration Commands

Sets the country of operation. All existing radio configuration will be erased

Syntax

```
country-code
```

Parameters

Abbreviation	Configures the switch to operate in a defined country

Usage Guidelines

Use the show wireless country code command to view the list of supported countries

Example

```
WS5100(config-wireless)#country-code ?
  ae  United Arab Emirates
  ar  Argentina
  at  Austria
  au  Australia
  ba  Bosnia Herzegovina
  be  Belgium
  bg  Bulgaria
  bh  Bahrain
  bm  Bermuda
  br  Brazil
  bs  Bahamas
  by  Belarus
  ca  Canada
  ch  Switzerland
  cl  Chile
  cn  China
```

```
co  Colombia
cr  Costa Rica
cy  Cyprus
cz  Czech Republic
de  Germany
dk  Denmark
do  Dominican Republic
ec  Ecuador
ee  Estonia
eg  Egypt
es  Spain
fi  Finland
fr  France
gb  United Kingdom
gr  Greece
gt  Guatemala
gu  Guam
hk  Hong Kong
hn  Honduras
hr  Croatia
ht  Haiti
hu  Hungary
id  Indonesia
ie  Ireland
il  Israel
in  India
is  Iceland
it  Italy
jo  Jordan
jp  Japan
kr  South Korea
kw  Kuwait
kz  Kazakhstan
li  Liechtenstein
lk  Sri Lanka
lt  Lithuania
lu  Luxembourg
lv  Latvia
ma  Morocco
mt  Malta
mx  Mexico
my  Malaysia
nl  Netherlands
no  Norway
nz  New Zealand
om  Oman
pe  Peru
ph  Philippines
pk  Pakistan
```

```
  pl  Poland
  pt  Portugal
  qa  Qatar
  ro  Romania
  ru  Russia
  sa  Saudi Arabia
  se  Sweden
  sg  Singapore
  si  Slovenia
  sk  Slovak Republic
  th  Thailand
  tr  Turkey
  tw  Taiwan
  ua  Ukraine
  us  United States
  uy  Uruguay
  ve  Venezuela
  vn  Vietnam
  za  South Africa

WS5100(config-wireless)#country-code
```

20.1.14 dhcp-sniff-state

Wireless Configuration Commands

Records mobile unit DHCP state information

Syntax

```
dhcp-sniff-state
```

Parameters

enable	Allows support for recording DHCP state information for mobile units

Example

```
WS5100(config-wireless)#dhcp-sniff-state enable
WS5100(config-wireless)#
```

20.1.15 dot11-shared-key-auth

Wireless Configuration Commands

Enables support for 802.11 shared key authentication

NOTE: Shared key authentication has known weaknesses that can compromise your WEP key. It should only be configured to accommodate wireless stations unable to carry out Open-System authentication

Syntax

```
dot11-shared-key-auth
```

Parameters

enable	Enables support for shared key authentication

Example

```
WS5100(config-wireless)#dot11-shared-key-auth enable
WS5100(config-wireless)#
```

20.1.16 end

Wireless Configuration Commands

Ends and exits the current mode and changes to the PRIV EXEC mode. The prompt changes to `WS5100#`

Syntax

```
end
```

Parameters

None

Example

```
WS5100(config-wireless)#end
WS5100#
```

20.1.17 exit

Wireless Configuration Commands

Ends the current mode and moves to the previous mode (GLOBAL-CONFIG). The prompt changes to `WS5100(config)#`

Syntax

```
exit
```

Parameters

None

Example

```
WS5100(config-wireless)#exit
WS5100(config)#
```

20.1.18 fix-broadcast-dhcp-rsp

Wireless Configuration Commands

Converts broadcast DHCP server responses to unicast

Syntax

```
fix-windows-dhcp
```

Parameters

enable	Enables support for converting broadcast DHCP server responses to unicast

Example

```
WS5100(config-wireless)#fix-broadcast-dhcp-rsp enable
WS5100(config-wireless)#
```

20.1.19 help

Wireless Configuration Commands

Displays the system's interactive help (in HTML format)

Syntax

```
help
```

Parameters

None

Example

```
WS5100(config-wireless)#help
CLI provides advanced help feature.  When you need help,
anytime at the command line please press '?'.

If nothing matches, the help list will be empty and you must backup
until entering a '?' shows the available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each possible
   argument.
2. Partial help is provided when an abbreviated argument is entered
   and you want to know what arguments match the input
   (e.g. 'show ve?'.)
WS5100(config-wireless)#
```

20.1.20 ids

Wireless Configuration Commands

Defines the *Wireless Intrusion Detection System* (WIPS) configuration

Syntax

```
ids(anomaly-detection|detect-window|ex-ops)

ids anomaly-detection(all|average-noise-level|bad-essid-frame|
beacon-broadcast-essid|invalid-8021x-frame|invalid-frame-length|
invalid-frame-type|multicast-source|non-changing-wep-iv|
null-destination|same-source-destination|tkip-countermeasures|
unencrypted-traffic|weak-wep-iv)(enable|filter-ageout)

ids detect-window<5-300>

ids ex-ops(80211-replay-fails|all|association-requests|
authentication-fails|crypto-replay-fails|decryption-fails|
disassociations|eap-naks|eap-starts|probe-requests|unassoc-frames)
(filter-ageout<0-86400>|threshold(mu|radio|switch)<0-9999>)
```

Parameters

anomaly-detection {options} (enable|filter-ageout)	Configures parameters related to the detection of anomalous frames on the RF network
	• all – Enables all types of anomalous frames
	• average-noise-level [enable|filter-ageout|threshold] – Enables and sets the filters and threshold levels for sudden changes in RSSI
	  • threshold – Sets the threshold for sudden changes in RSSI
	• bad-essid-frame – Enables an AP detector to find frames with bad ESSIDs
	• beacon-broadcast-essid – Enables an AP detector to find beacons with broadcast ESSIDs
	• invalid-8021x-frame – Detects invalid 802.1x frames
	• invalid-frame-length – Detects frames with an invalid length
	• invalid-frame-type – Detects frames with an invalid type
	• multicast-source – Broadcast or multicast source
	• non-changing-wep-iv – Detects frames wit h a non-changing WEP IV
	• null-destination – Sets all zeros for an address
	• same-source-destination – Identical source and destination addresses
	• tkip-countermeasures – Filters mobile units causing TKIIP countermeasures
	• unencrypted-traffic – Detects unencrypted-traffic
	• weak-wep-iv – Uses weak WEP sequence numbers
	  • enable – Enables monitoring and filtering
	  • filter-ageout – Sets the number of seconds mobile units are filtered out

detect-window<*5-300*>	Sets the number of seconds information is collected before analysis. All thresholds are a function of this window size

ex-ops {}	Sets values related to the detection of excessive operations on the RF network • 80211-replay-fails – 802.11 replay check failure • all – Changes for all types of excessive operations • association-requests – 802.11 authentication and association requests authentication-fails – Failure to authenticate with servers (RADIUS/Kerberos) • crypto-replay-fails – TKIP/CCMP IV replay check failure • decryption-fails – Decryption failures • disassociations – Disassociation and Deauthentication frames • eap-naks – Excessive EAP-NAKs. The threshold upper limit for this field is 65535 (the default limit is 0) • eap-starts – EAP (802.1x) Start frames • probe-requests – Probe Request frames • unassoc-frames – Frames from unassociated stations • filter-ageout<0-86400> – Sets the number of seconds mobile units will be filtered out • threshold (mu|radio|switch) <0-9999> – Sets the threshold allowed in the detection window mu–Uses the threshold for monitoring on a per mobile unit basis radio–Uses the threshold for monitoring on a per radio basis switch–Uses the threshold for monitoring at the switch level

Example

```
WS5100(config-wireless)*#ids anomaly-detection tkip-countermeasures
enable
WS5100(config-wireless)*#

WS5100(config-wireless)#ids detect-window 250
```

```
WS5100(config-wireless)#

WS5100(config-wireless)#ids ex-ops 80211-replay-fails filter-ageout
5200
WS5100(config-wireless)#
```

20.1.21 mac-auth-local

- *Wireless Configuration Commands*

Configures the local MAC authentication list

Syntax

```
mac-auth-local<1-1000> (allow|deny)(Starting MAC Address)(Ending
MAC Address)(range/list of WLAN indicies)WORD
```

Parameters

<1-1000>	Sets the mac-auth-local entry
allow	Allows mobile units that match this rule to associate
deny	Denies association to mobile units that match this rule
Starting MAC Address	Starting MAC address in AA-BB-CC-DD-EE-FF format
Ending MAC Address	Ending MAC address in AA-BB-CC-DD-EE-FF format
Range/List of WLAN Indices	Set the list (1,3,7) or range (3-7) of WLAN indices
WORD	Optional radio description substring

Example

```
WS5100(config-wireless)#mac-auth-local 452 allow 12.11.11.120
12.11.11.150 3-7 TestString
WS5100(config-wireless)#
```

20.1.22 manual-wlan-mapping

Wireless Configuration Commands

Manually maps WLANs configured on a radio

Syntax

```
manual-wlan-mapping
```

Parameters

enable	Enables support for manual WLAN mapping

Example

```
WS5100(config-wireless)#manual-wlan-mapping enable
WS5100(config-wireless)#
```

20.1.23 mobile-unit

Wireless Configuration Commands

Configures mobile unit related parameters

Syntax

```
mobile-unit [association-history(enable)|probe-history]
mobile-unit probe-history (add<1-200> <MAC Address>|enable)
```

Parameters

association-history	Enables a mobile unit's association history. • enable – Enables a mobile unit's association history
probe-history	Mobile unit probe logging configuration commands • add <1-200> – Adds a mobile unit to probe history logging. Select an index value between 1 and 200 to add probe logging MAC • MAC Address – Sets the MAC address of the mobile used for probe history logging

Example

```
WS5100(config-wireless)#mobile-unit probe-history enable
WS5100(config-wireless)#

WS5100(config-wireless)#mobile-unit association-history enable
WS5100(config-wireless)#

WS5100(config-wireless)#mobile-unit probe-history add 20 AA-BB-CC-
DD-EE-FF

WS5100(config-wireless)#
```

20.1.24 mobility

Wireless Configuration Commands

Sets mobility parameters

Syntax

```
mobility(enable|local-address|max-roam-period|peer)
mobility local-address (IP Address)
mobility max-roam-period<1-15>
mobililty peer (IP Address)
```

Parameters

enable	Enables mobility globally
local-address <IP address>	Sets the local address for mobility • A.B.C.D – IP address of A.B.C.D format
max-roam-period*<1-300>*	Sets the Max Roam Period for a mobile unit (in seconds)
peer <Peer IP Address>	Adds a peer to this mobility region • A.B.C.D – IP address of the Peer

Example

```
WS5100(config-wireless)#mobility enable
WS5100(config-wireless)#

WS5100(config-wireless)#mobility local-address 12.12.12.1
WS5100(config-wireless)#
```

```
WS5100(config-wireless)#mobility max-roam-period 10
WS5100(config-wireless)#

WS5100(config-wireless)#mobility peer 157.208.235.108
WS5100(config-wireless)#
```

20.1.25 multicast-packet-limit

Wireless Configuration Commands

Sets a multicast packet limit (per second) for a VLAN. This limits broadcast/multicast packets per VLAN. The default vlaue is 32 broadcast/multicast packets per second

Syntax

```
multicast-packet-limit <1-128> (<1-4094>|<vlan range>)
```

Parameters

<1-128>	Sets the multicast packet limit per second
<1-4094>	Defines the single VLAN ID (1-4094) the new limit applies to
<vlan range>	Defines the list (1,3,7) or range (3-7) of VLAN IDs

Example

```
WS5100(config-wireless)#multicast-packet-limit 120 50
WS5100(config-wireless)#

WS5100(config-wireless)#multicast-packet-limit 120 1,10,25
WS5100(config-wireless)#
```

20.1.26 multicast-throttle-watermark

Wireless Configuration Commands

Configures watermarks for supporting bursts of broadcast/multicast frames

Syntax

```
multicast-throttle-watermarks (low)<0-100> (high) <0-100>
```

Parameters

low <0-100>	Sets the low water-mark. If the percentage of free packets in the system is lower than this threshold, the incoming frame is dropped
high <0-100>	Sets the high water-mark. If the percentage of free packets in the system is between the low water-mark and this value, the packet is subjected to a random-early-drop. If free packets are greater than this value, the packet is processed

Example

```
WS5100(config-wireless)#multicast-throttle-watermarks low 10 high
20
WS5100(config-wireless)#
```

20.1.27 no

Wireless Configuration Commands

Negates a command or sets its defaults. All the parameters mentioned in the syntax can be negated using this command

Syntax

```
no(adopt-unconf-radio|adoption-pref-id|ap-detection|broadcast-tx-
speed|country-code|dhcp-sniff-state|dot11-shared-key-auth|fix-
windows-dhcp|ids|mac-auth-local|manual-wlan-mapping|mobile-
unit|mobility|oversized-frames|proxy-arp|qos-mapping|radio|self-
heal|sensor|service|smart-scan-channels|wlan)
```

Parameters

Refer to *Table 20.1 on page -1* for the parameters negated using the **no** command.

Example

```
WS5100(config-wireless)#no mobility enable
WS5100(config-wireless)#
```

20.1.28 proxy-arp

Wireless Configuration Commands

Responds to ARP requests from the RON to the WLAN on behalf of mobile units

Syntax

```
proxy-arp
```

Parameters

enable	Enables the support of proxy arp

Example

```
WS5100(config-wireless)#proxy-arp enable
WS5100(config-wireless)#
```

20.1.29 qos-mapping

Wireless Configuration Commands

Confiures QoS mappings between the wired and wireless domains

Syntax

```
qos-mapping(wired-to-wireless|wireless-to-wired)

qos-mapping wired-to-wireless(dot1p<0-7>|dscp<0-63>)
(background|best-effort|video|voice)

qos-mapping wireless-to-wired(background|best-effort|video|voice)
dot1p<0-7>
```

Parameters

wired-to-wireless	Mappings used while switching wired traffic over the air
dot1p<*0-7*>	Configures the mapping of 802.1p tags to access categories. You can specify more than one 802.1p tag (0-7)
dscp<*0-63*>	Configures the mapping of DSCP values to access categories. You can specify more than one DSCP value (0-63)
background	Prioritizes Background category traffic
best-effort	Prioritizes Best Effort category traffic

video	Prioritizes Video category traffic
voice	Prioritizes Voice category traffic
wireless-to-wired	Sets the mappings used while switching wireless traffic to the RON side
dot1p<*0-7*>	Configures the 802.1p tags that correspond to a selected access category

Example

```
WS5100(config-wireless)#qos-mapping wireless-to-wired background
dot1p 5
WS5100(config-wireless)#
```

20.1.30 radio

Wireless Configuration Commands

Sets radio related parameters

Syntax

```
radio (<1-1000>|RADIO|add|all-11a|all-11b|all-11bg|
configure-8021X|default-11a|default-11b|default-11bg|dns-name)

radio<1-1000>(adoption-pref-id|antenna-mode|base-bridge|
beacon-interval|bridge-fwd-delay <4-30>|bridge-hello <1-10>|
bridge-max-ageout <4-3600>|bridge-msg-age <6-40>|
bridge-priority <0-65535>|bss|channel-power|client-bridge|
coordinates|copy-config-from|description|detector|dtim-period|
enforce-spec-mgmt|enhanced-beacon-table|enhanced-probe-table|
location-led|location-message|mac|max-mobile-units|mu-power<0-20>|
neighbor-smart-scan|on-channel-scan|radio-number|reset|reset-ap|
rss|rts-threshold|run-acs|self-heal-offset|short-preamble|speed|
tag-type|timeout|wmm)

radio <1-1000> bss(<1-4>|add-wlans|auto>)WLAN

radio <1-1000> base-bridge [enable|max-clients <1-12>]

radio <1-1000> bridge-fwd-delay <4-30>

radio <1-1000> bridge-hello <1-10>

radio <1-1000> bridge-max-ageout <4-3600>
```

```
radio <1-1000> bridge-msg-age <6-40>

radio <1-1000> bridge-priority <0-65535>

radio <1-1000> channel-power(indoor|outdoor)(<1-200>|acs|random)
<4-20>

radio <1-1000> client-bridge [enable|mesh-timeout <2-200>|
ssid (SSID name)]

radio <1-1000> coordinates <-65535-65535> <-65535-65535>

radio 1 copy-config-from [<1-1000>|default-11a|default-11b|
default-11bg]

radio <1-1000> dtim-period<1-50> bss<1-4>

radio <1-1000> location-led {start-flashing|stop-flashing}

radio <1-1000> speed [1|11|12|18|2|24|36|48|54|5p5|6|9|basic1|
 basic11|basic12|basic18|basic2|basic24|basic36|basic48|basic54|
 basic5p5|basic6|basic9|default|range|throughput]

radio <1-1000> wmm(background|best-effort|video|voice)
aifsn<1-15>|burst<0-65535>|cw<0-15>)

radio <1-1000> wmm(video|voice)(acm [enable|max-mus <1-64>])

radio add <1-4096>(MAC Address)[11a[ap300|ap5131])|
11b[ap100|ap4131]|11bg [ap300|ap5131]]
```

Parameters

<1-1000>	Defines a single radio index
RADIO	Creates a list (1,3,7) or range (3-7) of radio indices
all-11a	All 11a radios currently in configuration
all-11b	Al 11b radios currently in configuration
all-11bg	All 11bg radios currently in configuration
configure-8021X	Configures the 802.1X username and password on adopted access ports
default-11a	Adopts the default 11a configuration template

default-11b	Adopts the default 11b configuration template
default-11bg	Adopts the default 11bg configuration template
adoption-pref-id <0-65535>	Employs a preference identifier for this radio port. The radio port is more likely to be adopted by a wireless switch that is a preferred switch
antenna-mode *<diversity|primary|secondary>*	Defines the antenna diversity mode. Select from the following options: • *diversity*–Full diversity (both antennas) • *primary*–Primary antenna only • *secondary*–Secondary antenna only **Note:** Before executing this command, ensure the radio is present and is a AP300
base-bridge (enable|max-clients <1-12>	Sets base bridge values • *enable* – Allows the given radio to act as a base bridge and accept connections from client bridges • *max-clients <1-12>* – Configures a base-bridge. Enter maximum client bridges allowed
beacon-interval*<50-200>*	Sets the beacon interval (in K-uSec)
bridge-fwd-delay <4-30>	Sets the STP bridge forward delay (in seconds) • <4-30> - Time in seconds
bridge-hello <1-10>	Sets the STP bridge hello (in seconds) • <1-10> - Time in seconds
bridge-max-ageout <4-3600>	Sets the STP bridge maximum ageout (in seconds) • <4-3600> - Time in seconds
bridge-msg-age <6-40>	Sets the STP bridge message age (in seconds) • <6-40> - Time in seconds
bridge-priority <0-65535>	Sets the STP bridge priority (in seconds) • <0-65535> - Priority value

bss (<*1-4*>|add-wlans|auto) WLAN	Maps WLANs to radio BSSIDs • <*1-4*>– Sets the BSS where WLANs are mapped • add-wlans – Adds new WLANs to existing radios. The other WLANs on the radios are left as is • auto–Sets the automatic assignment of a BSS. The user selects WLANs, and the system assigns them to a BSS automatically • WLAN–Defines a list (1,3,7) or range (3-7) of WLAN indices. When a BSS is also specified, the first WLAN is used as the primary WLAN. When the auto option is used, the system automatically assigns the first four WLANs as primaries on their respective BSSIDs
channel-power (indoor|outdoor) (<1-2000>|acs|random) <4-20>	Sets the location, channel and transmit power level • indoor – Defines an indoor location • outdoor – Defines an outdoor location • <1-2000> – Sets the channel number • acs – Enables ACS (*auto channel selection*). A radio will scan for the least congested channel at startup or switch reconfiguration • random – Random channel selection • <4-20> – Sets the power in dBm
client-bridge [enable| mesh-timeout <2-200>| ssid (SSID name)]	Defines client bridge settings • enable – Enables client-bridge functionality on radio • mesh-timeout [1|<2-200>] – Sets the client bridge link timeout • ssid (SSID name) – Defines the ESSID of the WLAN
coordinates <-65535-65535> <-65535-65535>	Configures the location of this radio in terms of x.y.z coordinates • <-65535-65535> – Sets the X coordinate • <-65535-65535> – Sets the Y coordinate • <-65535-65535> – Sets the Z coordinate

copy-config-from [<1-1000>|default-11a| default-11b| default-11bg]	Copies the configuration from a previously configured radio • <1-1000> – Defines a single radio index • default-11a – Uses the default 11a configuration template • default-11b – Uses the default 11b configuration template • default-11bg – Uses the default 11bg configuration template
description	Defines a description for this radio
detector	Dedicates this radio as a detector. No mobile units can associate to a detector
dtim-period*<1-50>* bss *<1-4>*	Set the DTIM period (number of beacons between successive DTIMs) radio **dtim-period***<1-50>* **bss***<1-4>* • <1-50> – Sets the DTIM period • bss <1-4>– *BSS* index
enforce-spec-mgmt (enable)	Enforces spectrum management checks on specified radios. Only mobile units that advertise spectrum management capabilities will be allowed to associate on this radio
enhanced-beacon-table	Enables the enhanced beacon table for AP locationing
enhanced-probe-table	Enables the enhanced probe table for MU locationing
location-led [start-flashing|stop-flashing]	Changes the mode of operation of the LEDs on an AP • start-flashing – Requests parent-ap of specified radio to begin flashing its LEDs to help locate it • stop-flashing – Requests parent-ap of specified radio to revert its LEDs to normal mode of operation
location-message	Specifies a message sent to all mobile units that associate with these radios. This message should not exceed 80 characters

mac <MAC address>	Changes the parent (access-port) MAC address of the radio
max-mobile-units *<1-256>*	Maximum number of mobile units allowed to associate
mu-power <0-20>	Power adjustment level for mobile units associated with this access-port. MUs that support this element will reduce their transmit power by the specified value • <0-20> – Power adjustment level in dBm
neighbor-smart-scan [<1-4096>|<radio range>]	Configures neighbor radios for smart scans • <1-4096> – Sets a single radio index • <radio range> – Set a list (1,3,7) or range (3-7) of radio indices
on-channel-scan	Enables rogue scanning on this radio
reset	Resets a radio (this will only reset the specified radio, not the complete access port)
reset-ap	Resets the parent AP (this will reset all radios on that access port)
rss (enable)	Enables *Remote Site Survivability* (RSS)
rts-threshold*<0-2347>*	Defines the RTS threshold in bytes
run-acs	Runs an auto-channel-selection on a radio. The radio should already have been configured for ACS support
self-heal-offset *<0-30>*	Configures the self-healing offset (measured in dBm), for regulatory **Note:** The offset is based off the regulatory maximum power for the specified channel ("show wireless regulatory" displays the max power allowed)

speed	Configures the basic and supported data rates/speed • 1 1-Mbps • 11 11-Mbps • 12 12-Mbps • 18 18-Mbps • 2 2-Mbps • 24 24-Mbps • 36 36-Mbps • 48 48-Mbps • 54 54-Mbps • 5p5 5.5-Mbps • 6 6-Mbps • 9 9-Mbps • basic1 basic 1-Mbps • basic11 basic 11-Mbps • basic12 basic 12-Mbps • basic18 basic 18-Mbps • basic2 basic 2-Mbps • basic24 basic 24-Mbps • basic36 basic 36-Mbps • basic48 basic 48-Mbps • basic54 basic 54-Mbps • basic5p5 basic 5.5-Mbps • basic6 basic 6-Mbps • basic9 basic 9-Mbps • default factory default rates based on radio-type • range all rates enabled, the lowest one set to basic • throughput all rates basic (only 802.11g clients are allowed on 802.11bg radios)

tag_type [aeroscout|cricket|newbury] (listen-addr) <MAC address>	Configures the WI-FI tag type.
	• *aeroscout* – Aeroscout active tag
	• *cricket* – Cricket (Motorola) Active tag
	• *newbury* – Newbury active tag
	  • listen-addr – Configures a multicast listening address for active tags
	  • AA-BB-CC-DD-EE-FF – Sets a multicast MAC address
	NOTE: For Aeroscout tags, the address is configurable. Unless the address is configured on the radio, the tag packet will not be forwarded to the switch from the AP

wmm(background|best-effort|video|voice) (aifsn<*1-15*>|burst<*0-65535*>| cw<*0-15*>) wmm(video|voice) (acm [enable|max-mus <1-64>]	Sets 802.11e/*Wireless Multi Media* (WMM) parameters (supported only on AP300) radio **wmm**(background|best-effort|video|voice)(aifsn<*1-15*>|burst<*0-65535*>|cw<*0-15*>) `(acm [enable|max-mus <1-64>]` • *background* – Prioritizes Background category traffic • *best-effort*– Prioritizes Best Effort category traffic • *video* – Prioritizes Video category traffic • *voice* – Prioritizes Voice category traffic • acm (enable|max-mus <1-64>)– Admission control parameters. Use `enable` to allow admission control.Enabling ACM on video enables ACM on the Voice access category Use `max-mus` to specify the number of mobile units that are allowed access on the specified categories • aifsn<*1-15*> – (*Arbitration Inter Frame Spacing Number*) Defines the wait time (in milliSeconds) between data frames. Derived using AIFSN and the slot-time

	• burst<*0-65535*> – (transmit-opportunity) Sets an interval when a particular WMM STA has the right to initiate transmissions onto the wireless medium • cw<*0-15*> – (Contention Window parameters) Wireless stations pick a number between 0 and the minimum contention window to wait before re-trying transmissions Stations then double their wait time on a collision, until it reaches the maximum contention window
add <1-1000> (MAC Address) [11a [ap300|ap5131]| 11b [ap100|ap4131] | 11bg [ap300|ap5131]]	Adds a new radio • <1-1000> – Defines the index where this radio is added • MAC – Sets a MAC address in AA-BB-CC-DD-EE-FF format • 11a – 802.11a type radio • 11b – 802.11b type radio • 11bg – 802.11bg type radio • ap300 – AP300 access port (default for 11a and 11bg). • ap5131 – AP-5131 type access port • ap4131 –AP-4131 type access port
dns-name WORD (MAC Address)	Configures the DNS name used in L3-Discovery on adopted access ports • AA-BB-CC-DD-EE-FF – Change the name only on the access port with a specified MAC address. If not specified, the DNS name update is sent to all adopted access ports

Example

```
WS5100(config-wireless)#radio 250 bss auto 3-5
WS5100(config-wireless)#
```

20.1.31 rate-limit

Wireless Configuration Commands

Sets the default rate limit per user

Syntax

```
rate-limit {down|up}<0-100000>
```

Parameters

down <0-100000>	Sets the up link direction - from the wireless client to the network Defines the rate in the range of <0-100000> kbps, 0=disable rate limit
up <0-100000>	Sets the down link direction - from network to wireless client Sets the rate in the range of <0-100000> kbps, 0=disable rate limit

Example

```
WS5100(config-wireless)#rate-limit down 1000
WS5100(config-wireless)#

WS5100(config-wireless)#rate-limit up 20000
WS5100(config-wireless)#
```

20.1.32 self-heal

Wireless Configuration Commands

Configures Self Healing values

Syntax

```
self-heal(interference-avoidance|neighbor-recovery)

self-heal interference-avoidance(enable|hold-time<0-65535>|
retries<0.0-15.0>)

self-heal neighbor-recovery(action|enable|neighbors|run-neighbor-
detect)
self-heal neighbor-recovery action(both|none|open-rates|raise-
power) radio(<1-1000>|RADIO)
self-heal neighbor-recovery neighbors<1-1000>(<1-1000>|RADIO)
```

Parameters

interference-avoidance	Interference avoidance configuration.
enable	Enables/disables interference avoidance
hold-time*<0-65535>*	The number of seconds to disable interference avoidance after a detection. This prevents a radio from changing channels continuously. Set the hold-time between 0-65535 seconds
retries*<0.0-15.0>*	Defines the average number retries to cause a radio to re-run auto channel selection. Set between 0-15
neighbor-recovery	Invokes neighbor recovery configuration commands
action (both|none|open-rates| raise-power) radio (*<1-1000>*|RADIO)	Defines the radio's self healing action when neighbors are detected as down • both – Raises the power to max and open all rates • none – No action taken • open-rates – Opens all rates • raise-power – Raises the power to maximum • **radio** – Modifies the action for specified radio(s) • *<1-1000>* – Sets a single radio index • RADIO – Defines a list (1,3,7) or range (3-7) of radio indices
enable	Monitors access ports and attempts to increase coverage on a detected failure
neighbors*<1-1000>* (<1-1000>|RADIO)	Adds a radio as a neighbor
run-neighbor-detect	Disassociates all mobile units, clears current neighbors and runs neighbor detection

Example

```
WS5100(config-wireless)#self-heal interference-avoidance enable
WS5100(config-wireless)#

WS5100(config-wireless)#self-heal interference-avoidance hold-time
600
WS5100(config-wireless)#

WS5100(config-wireless)#self-heal neighbor-recovery enable
Note: reducing the configured transmit power of radios will ensure
that there is room to increase power when a neighbor fails
WS5100(config-wireless)#

WS5100(config-wireless)#self-heal neighbor-recovery neighbors 1 1
WS5100(config-wireless)#
```

20.1.33 sensor

Wireless Configuration Commands

Configures *Wireless Intrusion Protection System* (WIPS) parameters

Syntax

```
sensor(<1-48>|default-config|ping-interval <2-60>|vlan)

sensor <1-48> [default-config|request-config|revert-to-ap]

sensor default-config(ip-mode|wips-server-ip)
sensor default-config ip-mode(dhcp|static(A.B.C.D/M)(A.B.C.D))
sensor default-config wips-server-ip(primary|secondary)(A.B.C.D)
```

Parameters

<1-48> [defaultconfig| requestconfig| revert-to-ap]	Select a sensor to reset/revert the AP to its original state. Use the `show wireless sensor` command to view the sensor index • default-config – Restores the internal configuration of the sensor to default values. This sends the configuration to the sensor • request-config – Polls the sensor for its latest configuration • revert-to-ap – Reverts an IDS sensor back to an access port that can service mobile-units

default-config (ip-mode|wips-server-ip)	Invokes the default configuration sent to sensors when configured
	• ip-mode – Configures the IP address of the sensors
	  • dhcp – Sensors use DHCP to obtain an IP address
	  • static (A.B.C.D/M)(A.B.C.D) – Sensors use the specific static IP address
	  A.B.C.D/M – Sets the sensor IP address and network mask
	  A.B.C.D – Specifies the gateway IP address for sensors
	• wips-server-ip – Specifies the IP addresses of the WIPS server
	  • primary (A.B.C.D) – Specifies the primary IP address of the WIPS server
	  • secondary (A.B.C.D) – Specifies the secondary IP address of the WIPS server

ping-interval <2-60>	Sets the ping interval (in seconds) between successive pings to sensors on the network
vlan<1-4094>	Configures VLANs where sensors are discovered

Example

```
WS5100(config-wireless)#sensor vlan 268 500
WS5100(config-wireless)#
```

20.1.34 service

Wireless Configuration Commands

Invokes service commands to troubleshoot or debug `(config-wireless)` instance configurations

Syntax

```
service(show|wireless)

service show(cli|wireless)
```

```
service show (wireless) [ap-history|ap-list|buffer-counters|
enhanced-beacon-table|enhanced-probe-table|legacy-load-balance|
mu-cache-buckets|mu-cache-entry|mvlan <1-32>|
radio(<1-1000>|description)|snmp-trap-throttle|vlan-cache-buckets|
vlan-cache-entry]

service wireless [ap-history|buffer-counters|clear-ap-log|
dump-core|enhanced-beacon-table|enhanced-probe-table|
idle-radio-send-multicast|legacy-load-balance|radio-misc-cfg|
rate-scale|request-ap-log|save-ap-log|snmp-trap-throttle|
vlan-cache]

service (wireless)ap-history [clear|enable]
service (wireless)buffer-counters (clear)
service (wireless)clear-ap-log <1-48>
service (wireless)idle-radio-send-multicast (enable)
service (wireless)request-ap-log <1-48>
```

Parameters

ap-history	Displays the access port history
ap-list	Listd AP configurations sorted by MAC address
buffer-counters	Allocation counts for various buffers
enhanced-beacon-table [config|report]	Displays details of the configuration and information gathered for AP locationing • *config* – Displays the configuration of AP locationing • *report* – Displays the information gathered for AP locationing
enhanced-probe-table [config|report]	Displays the configuration and information gathered for MU locationing. • *config* – Displays the configuration of MU locationing • *report* – Displays the information gathered for MU locationing
legacy-load-balance	Sets the legacy load balance algorithm compatibility mode
mu-cache-buckets	Displays wireless mobile units cache buckets
mu-cache-entry	Displays mobile unit cache information

mvlan <1-32>	Displays multi-Vlan Debug stats • <1-32> – Defines a single WLAN's index
radio [<1-1000>|description]	Sets a radio's serviceability parameters • <1-1000> – Defines a single radio's index • description – Displays the description and location coordinates of detected radios
snmp-trap-throttle	Displays stats related to SNMP trap throttling
vlan-cache-buckets	Displays VLAN cache buckets
vlan-cache-entry	Displays mobile unit VLAN information
service wireless	
ap-history [clear|enable]	AP history • *clear* – Deletes the history of all APs • *enable* – Enables the tracking of the AP history
buffer-counters (clear)	Allocation counts for various buffers • *clear* – Resets counters to zero
clear-ap-log <1-48>	Clears AP logs for the a selected index
dump-core	Creates a core file of the ccsrvr process

enhanced-beacon-table [channel-set (a|bg) <1-200> | enable | erase-report | max-ap <0-512> | scan-interval <10-60> | scan-time <100-1000>]	Configures an AP for detecting and locating other APs in the network
	• channel-set (a|bg) <1-200> – 802.11a / 802.11bg channel-set settings used for AP locationing
	  • (a|bg) – Adds channels to the Enhanced Beacon Table for 802.11a/bg. A seperate channel set can be configured for "a" and "bg" radios
	  • <1-200> – List of space separated channel number(s) between 1 and 200
	• enable – Enables or disables the gathering of information for AP locationing
	• erase-report – Erases AP beacon locationing reports captured by the switch
	• max-ap <0-512> – Sets the maximum number of APs allowed in the AP locationing table
	• scan-interval <10-60> – Defines the duration between two scans (in seconds)
	• scan-time <100-1000> – The time the radio dwells on each channel in the a/bg channel-set (in milli seconds)

enhanced-probe-table [enable | erase-report | max-mu <0-512> | preferred (add) <MAC Address> | window-time <10-60>]	Configures an AP for detecting and locating MUs. The switch maintains an enhanced-probe-table to track the probes received by an AP. • enable – Disables or enables the gathering of information for MU locationing • erase-report – Erases all MU Probe Table locationing reports collected by the switch • max-mu <0-512> – Configures the maximum number of MUs that can be scanned for Probe Table information • preferred <MAC Address> – Adds an entry to the preferred MU list. This will list MU MAC addresses • window-time <10-60> – Defines the time the probes are assimilated. The probe with the highest signal strength (dBm) is reported for a given AP MU pair
idle-radio-send-multicast (enable)	Enables the forwarding of multicast packets to radios without associated MUs
legacy-load-balance	Invokes a legacy load balance algorithm
radio-misc-cfg	Used for radio specific miscellaneous configurations
rate-scale	Enables wireless rate scaling (default).
request-ap-log <1-48>	Requests an AP log for a selected AP index
save-ap-log	Saves debug/error logs sent by the access-port
snmp-trap-throttle <1-20>	Limits the number of SNMP traps generated • <1-20> – Sets the maximum number of traps (per second) that can be generated
vlan-cache	Services a switch's VLAN cache

Usage Guidelines

To stop a service, use the `no` command. For instance, use `no service wireless idle-radio-send-multicast enable` to stop sending broadcast/multicast frames to idle radios

Example

```
WS5100(config-wireless)#service show wireless ap-history
AP MAC             Radio  Timestamp          Event       Reason
=================================================================
00-A0-F8-BF-8A-4B  N/A    20070926-20:23:10  Adoption    N/A
WS5100(config-wireless)#

WS5100(config-wireless)#service show wireless mvlan 20
Wlan 20: pool_size =1
-----------------------------------------------------
[ 0]: wlan=20, vlan_id=1, limit=0, users=0, log_sent=0
[ 1]: wlan=20, vlan_id=0, limit=0, users=0, log_sent=0
[ 2]: wlan=20, vlan_id=0, limit=0, users=0, log_sent=0
[ 3]: wlan=20, vlan_id=0, limit=0, users=0, log_sent=0
[ 4]: wlan=20, vlan_id=0, limit=0, users=0, log_sent=0
[ 5]: wlan=20, vlan_id=0, limit=0, users=0, log_sent=0
[ 6]: wlan=20, vlan_id=0, limit=0, users=0, log_sent=0
[ 7]: wlan=20, vlan_id=0, limit=0, users=0, log_sent=0
[ 8]: wlan=20, vlan_id=0, limit=0, users=0, log_sent=0
[ 9]: wlan=20, vlan_id=0, limit=0, users=0, log_sent=0
[10]: wlan=20, vlan_id=0, limit=0, users=0, log_sent=0
[11]: wlan=20, vlan_id=0, limit=0, users=0, log_sent=0
[12]: wlan=20, vlan_id=0, limit=0, users=0, log_sent=0
[13]: wlan=20, vlan_id=0, limit=0, users=0, log_sent=0
[14]: wlan=20, vlan_id=0, limit=0, users=0, log_sent=0
[15]: wlan=20, vlan_id=0, limit=0, users=0, log_sent=0
[16]: wlan=20, vlan_id=0, limit=0, users=0, log_sent=0
[17]: wlan=20, vlan_id=0, limit=0, users=0, log_sent=0
[18]: wlan=20, vlan_id=0, limit=0, users=0, log_sent=0
[19]: wlan=20, vlan_id=0, limit=0, users=0, log_sent=0
[20]: wlan=20, vlan_id=0, limit=0, users=0, log_sent=0
[21]: wlan=20, vlan_id=0, limit=0, users=0, log_sent=0
[22]: wlan=20, vlan_id=0, limit=0, users=0, log_sent=0
[23]: wlan=20, vlan_id=0, limit=0, users=0, log_sent=0
[24]: wlan=20, vlan_id=0, limit=0, users=0, log_sent=0
[25]: wlan=20, vlan_id=0, limit=0, users=0, log_sent=0
[26]: wlan=20, vlan_id=0, limit=0, users=0, log_sent=0
[27]: wlan=20, vlan_id=0, limit=0, users=0, log_sent=0
[28]: wlan=20, vlan_id=0, limit=0, users=0, log_sent=0
[29]: wlan=20, vlan_id=0, limit=0, users=0, log_sent=0
[30]: wlan=20, vlan_id=0, limit=0, users=0, log_sent=0
[31]: wlan=20, vlan_id=0, limit=0, users=0, log_sent=0
WS5100(config-wireless)#

WS5100(config-wireless)#service show wireless radio description
# access-port MAC      start BSS          radio  description
coordinates
1]  00-A0-F8-BF-8A-4B  00-A0-F8-BF-EF-B0  11bg   RADIO1
0 0 0
```

```
2]  00-A0-F8-BF-8A-4B  00-A0-F8-BF-ED-BC  11a    RADIO2
0 0 0
WS5100(config-wireless)#

WS5100(config-wireless)#service show wireless snmp-trap-throttle
throttle : 10 (default = 10)
traps allowed through throttle: 9
traps dropped through throttle: 0
WS5100(config-wireless)#
```

20.1.35 show

- *Wireless Configuration Commands*

Displays current system information running on the switch

Syntax

show<paramater>

Parameters

?	Displays all the parameters for which information can be viewed using the show command

Example

```
WS5100(config-wireless)#show ?
  access-list           Internet Protocol (IP)
  aclstats              Show ACL Statistics information
  alarm-log             Display all alarms currently in the system
  autoinstall           autoinstall configuration
  banner                Display Message of the Day Login banner
  boot                  Display boot configuration.
  clock                 Display system clock
  commands              Show command lists
  crypto                encryption module
  debugging             Debugging information outputs
  dhcp                  DHCP Server Configuration
  environment           show environmental information
  file                  Display filesystem information
  ftp                   Display FTP Server configuration
  history               Display the session command history
  interfaces            Interface status
  ip                    Internet Protocol (IP)
  ldap                  LDAP server
  licenses              Show any installed licenses
  logging               Show logging configuration and buffer
  mac                   Internet Protocol (IP)
```

```
  management              Display L3 Managment Interface name
  mobility                Display Mobility parameters
  ntp                     Network time protocol
  password-encryption     password encryption
  port-channel            Portchannel commands
  privilege               Show current privilege level
  radius                  RADIUS configuration commands
  redundancy-group        Display redundancy group parameters
  redundancy-history      Display state transition history of the
                          switch.
  redundancy-members      Display redundancy group members in detail
  running-config          Current Operating configuration
  securitymgr             Securitymgr parameters
  sessions                Display current active open connections
  snmp                    Display SNMP engine parameters
  snmp-server             Display SNMP engine parameters
  sole                    Smart Opportunistic Location Engine
                          Configuration
  spanning-tree           Display spanning tree information
  startup-config          Contents of startup configuration
  static-channel-group    static channel group membership
  terminal                Display terminal configuration parameters
  timezone                Display timezone
  upgrade-status          Display last image upgrade status
  users                   Display information about currently logged
                          in users
  version                 Display software & hardware version
  wireless                Wireless configuration commands
  wlan-acl                wlan based acl

WS5100(config-wireless)#show
```

20.1.36 wlan

▸ *Wireless Configuration Commands*

Configures Wireless LAN related commands

Syntax

```
wlan(<1-32>|WLAN)
(80211-extensions|aap-proxy-radius|accounting|add-vlan|
answer-bcast-ess|authentication-type| client-bridge-backhaul|
description|dot11i|enable|encryption-type|hold-time|hotspot|
inactivity-timeout|kdc|mobility|mu-mu-disallow|
nac-mode|nac-server|qos|radius|secure-beacon|
set-vlan-user-limit|ssid|syslog|vlan|wep128|wep64)

wlan<1-32> (80211-extensions)( move-command)(enable)
```

```
wlan<1-32> aap-proxy-radius (enable)(realm)<realm name> (strip)

wlan<1-32> (accounting)[none|radius|ssyslog]

wlan<1-32> (add-vlan)[<1-4094>|VLAN] (limit)<0-4096>

wlan<1-32> (authentication-type) [eap|hotspot|kerberos|mac-
auth|none]

wlan<1-32> (client-bridge-backhaul)(enable)

wlan<1-32> (dot11i)[handshake|key|key-rotation|key-rotation-
interval|opp-pmk-caching|phrase|pmk-caching|
preauthentication|second-key|tkip-cntrmeas-hold-time]

wlan<1-32> dot11i handshake timeout<100-5000> retransmit<1-10>
wlan<1-32> key[0|2|WORD]

wlan<1-32> encryption-type[ccmp|keyguard|none|tkip|tkip-ccmp|
wep128|wep128-keyguard|wep64]

wlan<1-32> hotspot[allow-list|webpage|webpage-location]
wlan<1-32> hotspot allow-list(Rule index)(IP address)
wlan<1-32> hotspot webpage [external|internal]
[failure|login|welcome]
wlan<1-32> hotspot webpage-location [advanced|external|internal]

wlan<1-32> inactivity-timeout <60-86400>

wlan<1-32> kdc
[password(0||LINE)|realm(LINE)|server(primary|secondary|timeout)]

wlan<1-32> kdc server [primary|secondary|timeout]auth-port<1-65535>
wlan<1-32> nac-mode [bypass-nac-except-include-list|do-nac-except-
exclude-list|none]

wlan<1-32> nac-server [primary|secondary|timeout]
wlan<1-32> nac-server [primary|secondary]
[A.B.C.D (auth-port)|radius-key (0|2|Shared Secret)]
wlan<1-32> nac-server [timeout] <1-300>

wlan<1-32> qos[classification| mcast-with-dot11i|mcast1|mcast2|
prioritize-voice|svp|weight <1-10>|wmm]
wlan<1-32> qos classification[background|best-effort|
video|voice|wmm]
wlan<1-32> qos wmm [8021p|background|best-effort|dscp|video|voice]
[aifsn|cw|txop-limit|acm]
```

```
wlan<1-32> radius[accounting|authentication-protocol|dscp|
dynamic-authorization|dynamic-vlan-assignment|
mobile-unit|reauth|server]

wlan<1-32> radius accounting[mode|timeout]
wlan<1-32> radius accounting mode[start-interim-stop(interval)
<60-3600>|start-stop|stop-only]
wlan<1-32> radius accounting timeout<1-60> retransmit<1-100>

wlan<1-32> radius authentication-protocol(chap|pap)


wlan<1-32> radius server[primary|secondary|timeout]
wlan<1-32> radius server[primary|secondary]
[ip-address(auth-port)<1024-65535>)(radius-key(0|2|LINE)]
wlan<1-32> radius server timeout<1-60> retransmit<1-10>

wlan<1-32> secure-beacon

wlan<1-32> (set-vlan-user-limit)[<1-4094>|VLAN][<0-4096>]

wlan<1-32> syslog (accounting) server<IP Address> port<Port Number>

wlan<1-32> tunnel<1-32> gateway<IP Address and mask>

wlan<1-32> VLAN [<1-4094>|VLAN]

wlan<1-32> wep128(key<1-4> (ascii|hex[0|2|WORD])|phrase(LINE)|
wep-default-key<1-4>)
```

Parameters

<1-32>	Defines a single WLAN index
WLAN	Set a list (1,3,7) or range (3-7) of WLAN indices
80211-extensions (move-command) (enable)	Enables support for 802.11 extensions • *move-command* – Enables support for the move-command (fast roaming). • enable – Enables this extension

aap-proxy-radius (enable) (realm) <name> (strip)	Enables configuring of proxying AAP radius requests • realm <name> – Provide proxy realm name • strip – Strip realm name while proxying requests
accounting (none|radius|syslog)	Defrines the accounting configuration on this WLAN • none – No accounting performed on this WLAN • radius – Uses RADIUS accounting on this WLAN • syslog – Uses Syslog accounting on this WLAN
add-vlan [<1-4094>|VLAN] (limit)	Instead of starting a new VLAN assignment for given WLAN, this command adds a VLAN assignment to an existing VLAN assignment. All prior VLAN settings are retained • [<1-4094>|VLAN] – Sets the VLAN range list. It can be either a single index or a list (1,3,7) or range (3-7) • limit – Sets user limits on VLANs for this WLAN **NOTE:** The `[no]` form of `add-vlan` command deletes the specified VLAN mapping over the specified WLAN range list If the specified mapping does not exist for a particular WLAN, a "specified vlan does not exists" message displays The delete action continues on remaining VLANs. If all the VLANs are deleted. A default VLAN assignment takes effect.
answer-bcast-ess	Allows this WLAN to respond to probes for broadcast ESS

authentication-type (eap|hotspot|kerberos| mac-auth|none)	Sets the authentication type for this WLAN • eap – EAP authentication (802.1X) • hotspot – Web based authentication • kerberos – Kerberos authentication (encryption will change to WEP128 if its not already wep128/keyguard) • mac-auth – MAC authentication (RADIUS lookup of MAC address) • none – None
client-bridge-backhaul (enable)	Enables the client bridge backhaul capability on this wlan.
description	Displays the description of this WLAN.
dot11i [handshake | key | key-rotation | key- rotationinterval| opp-pmk-caching | phrase|pmk-caching | preauthentication | secondkey| tkip-cntrmeas-hold-time]	Modifies tkip/ccmp (802.11i) related parameters • handshake (timeout <100-5000>) (retransmit<1-10>) – Sets a handshake for the timeout and retransmission intervals • timeout<100-5000> – Sets the timeout (in milliseconds) between retries • retransmit<1-10> – Sets the number of retransmission attempts

	• key(0|2|WORD) – Configure the key (PMK)
	  • 0 – Password is specified UNENCRYPTED
	  • 2 – Password is encrypted with password-encryption secret
	  • WORD – The 256bit (64 hex characters) long key
	• key-rotation (enable) – Controls the periodic update of the broadcast keys for associated mobile units
	• key-rotation-interval <1800-86400> – Configures the broadcast key rotation interval
	• opp-pmk-caching – Enables the opportunistic use of cached pairwise master keys (fast roaming with eap/802.1X)
	• phrase(0|2|LINE) – Configures the passphrase
	  • 0 – Password is specified UNENCRYPTED
	  • 2 – Password is encrypted with password-encryption secret
	  • LINE – Set passphrase between 8 and 63 characters
	• pmk-caching – Enables the use of cached pairwise master keys (fast roaming with eap/802.1X)
	• preauthentication – Enables support for 802.11i pre authentication
	• second-key(enable|key|phrase) (0|2|WORD) – Configures a secondary set of key/passphrase for this WLAN
	  • enable – Enables the use of a secondary key/passphrase
	  • key – Configures the key (PMK)
	  • phrase – Configures the passphrase
	  • 0 – Password is specified as UNENCRYPTED
	  • 2 – Password is encrypted with password-encryption secret

	• WORD – Sets the 256bit (64 hex characters) key • tkip-cntrmeas-hold-time <0-65535> – Configures the hold-time (in seconds) that clients are blocked whenTKIP countermeasures are invoked. Default is 60 seconds • wpa2-tkip (enable) – Enables support for WPA2-TKIP (in addition to WPA-TKIP) when TKIP is enabled on this WLAN
enable()	Enables specified WLAN(s)
encryption-type()	Sets the encryption type for this WLAN. Options include: • ccmp – AES Counter Mode CBC-MAC Protocol (AES-CCM CCMP) • keyguard – Keyguard-MCM (Mobile Computing Mode) • none – No encryption • tkip – Enables *Temporal Key Integrity Protocol* (TKIP) • tkip-ccmp – Enables both TKIP and CCMP on this WLAN • wep128 – Enables *Wired Equivalence Privacy* (WEP) with 128 bit keys • wep128-keyguard – Enables WEP128 as well as Keyguard-MCM on this WLAN • wep64 – Enables *Wired Equivalence Privacy* (WEP) with 64 bit keys **NOTE:** A WEP64 configuration is insecure when two WLANs are mapped to the same VLAN, and one uses no encryption and the other uses WEP.

hotspot()	Modifies hotspot related parameters • allow (rule index) (IP address) – Modifies hotspot allow-list parameters Users who have not yet authenticated must be allowed access to these IP addresses – Rule index – Allow-list Rule index (must be between (1-10) – IP address – Allow-list IP address • webpage (external|internal) (failure|login|welcome) – Modifies hotspot page parameters. – external – Modifies a hotspot's External Web page – internal – Modifies hotspot's Internal Web page
	– failure – Users are redirected to this Web page if they fail authentication – login – Users are prompted for their username and password within this Web page – welcome – Users are redirected to this Web page after they authenticate successfully • webpage-location (advanced|external|internal) – The location of the Web pages used for authentication. These pages can either be hosted on the switch or an external Web Server – advanced – Invokes login/welcome/failure Web pages created by the user on the switch – external – Invokes login/welcome/failure Web pages on an external server – internal – Invokes login/welcome/failure Web pages created automatically on the switch

inactivity-timeout *<60-86400>*	Sets an inactivity timeout in seconds. If a frame is not received from a mobile unit for this amount of time, the mobile unit is disassociated

kdc [password (0||LINE) | realm (LINE) | server (primary|secondary| timeout)] auth-port <1-65535>	Modifies KDC related parameters.
	• password(0|2|LINE) – Create a KDC server password (up to 127 characters)
	  • 0 – Password is specified UNENCRYPTED.
	  • 2 – Password is encrypted with a password-encryption secret.
	  • LINE – Defines a KDC server password (up to 127 characters)
	• realm(LINE) – Defines a KDC realm (up to 127 characters)
	  • LINE – Defines KDC realm (up to 127 characters)
	• server (primary|secondary) (IP address) auth-port <1-65535> – Modifies KDC server parameters
	  • primary – Defines the pPrimary KDC server
	  • secondary – Defines the secondary KDC server

	• IP address – Sets the KDC server IP address • auth-port<1-65535> – Sets the KDC server authentication port. Default is 88 • server(timeout)<1-60> – Modifies KDC server parameters • timeout – Defiens the time the switch waits for a response from the KDC Server before retrying
mobility (enable)	Enables L3 Mobility on WLAN(s)

mu-mu-disallow (switch-to-wired)	Disallows frames from one mobile unit to another mobile unit on this WLAN • switch-to-wired – Disallows by switching the frame out on the wired side (to allow an externalswitch to decide whether this frame is to be allowed or dropped)
nac-mode [bypass-nac-except-include-list|do-nac-except-exclude-list|none]	Sets the *Network Access Control (*NAC) mode configuration • bypass-nac-except-include-list – No MU NAC check is done except for those in include list. Devices in the include-list have NAC checks • do-nac-except-exclude-list – A MU NAC check is done except for those in the exclude list. Devices in the exclude list will not have any NAC checks • none – NAC disabled, no NAC is done. An MU can only get authenticated by a Radius server

nac-server () [primary|secondary|time out]	Configure a NAC server IP address and an optional authentication port number
	• [primary|secondary] [EAP Server IP Address|RADIUS Key] – Primary server or secondary server's IP address
	  • A.B.C.D (auth-port) – Set an EAP server IP address and EAP server authentication port (default: is 1812)
	  • RADIUS Key (0|2|Shared) – Create a Radius server shared secret, up to 127 characters
	  • 0 – Password is specified as UNENCRYPTED
	  • 2 – Password is encrypted with password-encryption secret
	  • Shared – Configures a NAC server shared secret
	• timeout <1-300> – Sets the time the switch waits for a response from the RADIUS server before retrying. This is a global setting for boththe primary and secondary servers
	NOTE: The `WS51000(config-wireless)# nac-server timeout<*> retransmit<*>` should be less than what is defined for an MU's timeout and retries. If the MU's time is less than the server's, a fallback to the secondary server will not work.

qos [classification | mcast-with-dot11i| mcast1 | mcast2 | prioritize-voice | svp | weight|wmm]	Quality of Service commands • classification [background|best-effort|video|voice|wmm] – Select how traffic on this WLAN is classified (relative prioritization on the access port) • *background* – Traffic on this WLAN is treated as background traffic • *best-effort* – Traffic on this WLAN is treated as best-effort • *video* – Traffic on this WLAN is treated as video • *voice* – Traffic on this WLAN is treated as voice • *wmm* – Use the WMM based classification (using DSCP or 802.1p tags) to classify traffic into different queues • *acm* – Admission Control Parameters

	• ip-address – Sets the RADIUS server's IP address • auth-port<1024-65535> – Establishes the RADIUS server's authentication port (default:1812) • radius-key – Sets the RADIUS server shared secret, up to 127 characters • 0 – Password is specified UNENCRYPTED • 2 – Password is encrypted with password-encryption secret • LINE – Defines RADIUS server shared secret, upto 127 characters • server timeout<1-300> retransmit<1-100> – Modify RADIUS/802.1X server parameters. • timeout<1-300> – Time (in seconds), the switch waits for a response from the RADIUS server before retrying • retransmit<1-100> – Number of retries before the switch gives up and disassociates the mobile unit **NOTE:** The `WS51000(config-wireless)# radius server timeout<*> retransmit<*>` should be less than what is defined for an MU's timeout and retries. If the MU's time is less than the server's, a fallback to the secondary server will not work
secure-beacon	Does not include the SSID of this WLAN in beacon frames
set-vlan-user-limit [<1-4094>|VLAN] [<0-4096>]	Sets user limits on VLANs for this WLAN • [<1-4094>|VLAN] – VLAN range list. It can be either a single index, a list (1,3,7) or a range (3-7) of indices • [<0-4096>] – Sets the VLAN index. The limit is <0-4096>

ssid	Enter the SSID of this WLAN
syslog (accounting) server <IP Address> port <Port number>	Syslog Accounting. • accounting – Modifies accounting parameters • server<IP Address> – Modifies the Syslog accounting server IP Address • port <Port Number> – Defines the Syslog server port The default port number is 514
vlan*<1-4094> [limit range]*	Sets the VLAN assignment of this WLAN. This command starts a new VLAN assignment for a WLAN index. All prior VLAN settings are erased • [<1-4094>|VLAN] –Establishesd the VLAN range list. It can be either a single index, a list (1,3,7) or a range (3-7) • limit – Sets user limits on VLANs for this WLAN
wep128 (key*<1-4>* (ascii|hex)<0|2|WORD> | phrase(LINE) | wep-default-key*<1-4>)*	Configures WEP128 parameters. • key*<1-4>* – Configures pre-shared hex keys • ascii – Sets keys as ascii characters (5 characters for wep64, 13 for wep128) • hex – Sets keys as hexadecimal characters (10 characters for wep64, 26 for wep128) • 0 – Password is specified UNENCRYPTED • 2 – Password is encrypted with password-encryption secret • WORD – Key (10 hex or 5 ascii characters for wep64, 26 hex or 13 ascii characters for wep128) • phrase – Specifies a passphrase from which keys are to be derived • LINE – Sets the passphrase (between 4 and 32 characters) • wep-defauly-key*<1-4>* – Defines the key index used for transmission from AP to MU

wep64	Configures WEP64 parameters

Example

```
WS5100(config-wireless)#wlan 25 accounting syslog
WS5100(config-wireless)#

WS5100(config-wireless)#wlan 25 answer-bcast-ess
WS5100(config-wireless)#

WS5100(config-wireless)#wlan 25 authentication-type kerberos
WS5100(config-wireless)#

WS5100(config-wireless)#wlan 25 description "TestWLAN"
WS5100(config-wireless)#

WS5100(config-wireless)#wlan 25 dot11i handshake timeout 2500
retransmit 5
WS5100(config-wireless)#

WS5100(config-wireless)#wlan 25 dot11i key-rotation enable
WS5100(config-wireless)#

WS5100(config-wireless)#wlan 25 dot11i key-rotation-interval 2000
WS5100(config-wireless)#

WS5100(config-wireless)#wlan 25 enable
WS5100(config-wireless)#

WS5100(config-wireless)#wlan 25 hotspot webpage external failure
"This feature is under development"
WS5100(config-wireless)#

WS5100(config-wireless)#wlan 25 kdc server primary 1.2.3.4 auth-
port 50000
WS5100(config-wireless)#

WS5100(config-wireless)#wlan 25 mobility enable

WS5100(config-wireless)#wlan 1 nac-mode bypass-nac-except-include-
list
WS5100(config-wireless)#

WS5100(config-wireless)#wlan 1 nac-server primary 11.22.33.22 auth-
port 1221
WS5100(config-wireless)#

WS5100(config-wireless)#
```

```
WS5100(config-wireless)#wlan 25 radius accounting timeout 30
retransmit 50
WS5100(config-wireless)#

WS5100(config-wireless)#wlan 25 radius mobile-unit timeout 30
retransmit 5
WS5100(config-wireless)#

WS5100(config-wireless)#wlan 25 ssid TestString
WS5100(config-wireless)#

WS5100(config-wireless)#wlan 25 symbol-extensions fast-roaming
enable
WS5100(config-wireless)#

WS5100(config-wireless)#wlan 25 syslog accounting server
12.13.14.125 port 5005
WS5100(config-wireless)#

WS5100(config-wireless)#wlan 24 qos mcast-with-dot11i enable
WS5100(config-wireless)#
```

20.1.37 wlan-bw-allocation

- *Wireless Configuration Commands*

Enables WLAN bandwidth allocation on all radios

Syntax

```
wlan-bw-allocation (enable)
```

Parameters

enable	Enables WLAN bandwidth allocation on all radios

Example

```
WS5100(config-wireless)#wlan-bw-allocation enable
WS5100(config-wireless)#
```

21

SOLE Instance

Use the `(config-sole)` instance to configure SOLE related configuration commands.

21.1 SOLE Config Commands

Table 21.1 summarizes `config-sole` commands:

Table 21.1 Location Engine Config Command Summary

Command	Description	Ref.
adapter	Configures the SOLE adapter	*page 21-2*
clrscr	Clears the display screen	*page 21-2*
end	Ends the current mode and moves to the EXEC mode	*page 21-3*
exit	Ends the current mode and moves to the previous mode	*page 21-3*
help	Displays the interactive help system in HTML format	*page 21-3*
no	Negated a command or sets defaults values	*page 21-4*
service	Invokes service commands to troubleshoot or debug `(config-if)` instance configurations	*page 21-5*
show	Displays running system information	*page 21-6*

21.1.1 adapter

SOLE Config Commands

Enables/disables a specified adapter, or all the adapters

Syntax

```
adapter (aeroscout) (enable)
```

Parameters

adapter (aeroscout) (enable)	SOLE adapter name. • aeroscout – Defines the name of the adapter • enable – Enables the SOLE adapter

Usage Guidelines

Use `[no] adapter [aeroscout(enable)|enable]` to disable aeroscout or all SOLE adapters. The SOLE adapter is `disabled` by default

Example

```
WS5100(config-sole)#adapter enable
WS5100(config-sole)#
```

21.1.2 clrscr

SOLE Config Commands

Clears the display screen

Syntax

```
clrscr
```

Parameters

None

Example

```
WS5100(config-sole)#clrscr
WS5100(config-sole)#
```

21.1.3 end

SOLE Config Commands

Ends and exits the current mode and moves to the PRIV EXEC mode. The prompt changes to `WS5100#`

Syntax

```
end
```

Parameters

None

Example

```
WS5100(config-sole)#end
WS5100#
```

21.1.4 exit

SOLE Config Commands

Ends the current mode and moves to the previous mode (GLOBAL-CONFIG). The prompt changes to `WS5100(config)#`

Syntax

```
exit
```

Parameters

None

Example

```
WS5100(config-sole)#exit
WS5100(config)#
```

21.1.5 help

SOLE Config Commands

Displays the system's interactive help system in HTML format

Syntax

```
help
```

Parameters

None.

Example

```
WS5100(config-sole)#help
CLI provides advanced help feature.  When you need help,
anytime at the command line please press '?'.

If nothing matches, the help list will be empty and you must backup
until entering a '?' shows the available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each possible
   argument.
2. Partial help is provided when an abbreviated argument is entered
   and you want to know what arguments match the input
   (e.g. 'show ve?'.)

WS5100(config-sole)#
```

21.1.6 no

SOLE Config Commands

Defines the name of the adapter or disables the adapter(s)

Syntax

```
no adapter (aeroscout) (enable)
```

Parameters

adapter (aeroscout) (enable)	SOLE adapter name • aeroscout – Defines the name of the adapter • enable – Use with `no` to disable all the SOLE adapters

Usage Guidelines

Use `[no] adapter [aeroscout(enable)|enable]` to disable specified or all SOLE adapters. The SOLE adapter is `disabled` by default

Example

```
WS5100(config-sole)#no adapter enable
WS5100(config-sole)#
```

21.1.7 service

SOLE Config Commands

Invokes service commands to troubleshoot or debug `(config-if)` instance configurations

Syntax

```
service (show) (cli)
```

Parameters

show (cli)	Displays the CLI tree of current mode

Example

```
WS5100(config-sole)#service show cli
Location Engine Config mode:
+-adapter
  +-ADAPTER
    +-enable [adapter (ADAPTER|) enable]
  +-enable [adapter (ADAPTER|) enable]
+-clrscr [clrscr]
+-end [end]
+-exit [exit]
+-help [help]
+-no
  +-adapter
    +-ADAPTER
      +-enable [no adapter (ADAPTER|) enable]
    +-enable [no adapter (ADAPTER|) enable]
+-quit [quit]
.....................................................................
.....................................................................
.....................................................................
.....................................................................
.....................................................................
.....................................................................
.....................................................................
WS5100(config-sole)#
```

21.1.8 show

SOLE Config Commands

Displays current system information

Syntax

```
show <parameters>
show sole [config(adapter)|stats (adapter)|status(adapter|engine)]
```

Parameters

?	Displays the parameters for which information can be viewed using the show command

Example

```
WS5100(config-sole)#show ?
  access-list           Internet Protocol (IP)
  aclstats              Show ACL Statistics information
  alarm-log             Display all alarms currently in the system
  autoinstall           autoinstall configuration
  banner                Display Message of the Day Login banner
  boot                  Display boot configuration.
  clock                 Display system clock
  commands              Show command lists
  crypto                encryption module
  debugging             Debugging information outputs
  dhcp                  DHCP Server Configuration
  environment           show environmental information
  file                  Display filesystem information
  ftp                   Display FTP Server configuration
  history               Display the session command history
  interfaces            Interface status
  ip                    Internet Protocol (IP)
  ldap                  LDAP server
  licenses              Show any installed licenses
  logging               Show logging configuration and buffer
  mac                   Internet Protocol (IP)
  management            Display L3 Managment Interface name
  mobility              Display Mobility parameters
  ntp                   Network time protocol
  password-encryption   password encryption
  port-channel          Portchannel commands
  privilege             Show current privilege level
  radius                RADIUS configuration commands
  redundancy-group      Display redundancy group parameters
```

```
  redundancy-history    Display state transition history of the
                        switch.
  redundancy-members    Display redundancy group members in detail
  running-config        Current Operating configuration
  securitymgr           Securitymgr parameters
  sessions              Display current active open connections
  snmp                  Display SNMP engine parameters
  snmp-server           Display SNMP engine parameters
  sole                  Smart Opportunistic Location Engine
                        Configuration
  spanning-tree         Display spanning tree information
  startup-config        Contents of startup configuration
  static-channel-group  static channel group membership
  terminal              Display terminal configuration parameters
  timezone              Display timezone
  upgrade-status        Display last image upgrade status
  users                 Display information about currently logged
                        in users
  version               Display software & hardware version
  wireless              Wireless configuration commands
  wlan-acl              wlan based acl

WS5100(config-sole)#show

WS5100(config-sole)#show sole config adapter

SOLE Adapter
 Adapter Type: AeroScout
 Adapter Version: 2.01
 Configured Status: disabled Operational Status: disabled
 Adapter Build Time: Thu Sep 13 21:44:45 2007
WS5100(config-sole)#

WS5100(config-sole)#show sole stats adapter
Adapter Type: AeroScout Adapter Status: disabled
Number of messages received from engine             : 0
Number of messages sent to engine                   : 0
Number of tag reports sent to engine                : 0
Time at which last message was received from engine : -
Time at which last message was sent to engine       : -
WS5100(config-sole)#
```

```
WS5100(config-sole)#show sole status adapter
#     Type     Status
-----------------------------
1  AeroScout  disabled
WS5100(config-sole)#


WS5100(config-sole)#show sole status engine
Type          Engine         State
-------------------------------------------
AeroScout   0.0.0.0          Offline
WS5100(config-sole)#
```

MOTOROLA INC.
1303 E. ALGONQUIN ROAD
SCHAUMBURG, IL 60196
http://www.motorola.com

72E-103896-01 Revision A
January 2008