About This Guide

Chapter 1. Introduction

CLI Overview ............................................................... 1-1
Getting Context Sensitive Help ....................................... 1-4
Using the no and default Forms of Commands ...................... 1-6
Using History Command ................................................. 1-7
  Setting the History Command Buffer Size ....................... 1-7
  Recalling Commands .................................................. 1-7
  Disabling the History Command Feature ......................... 1-8
  Basic Conventions .................................................... 1-8
Using CLI Editing Features and Shortcuts ......................... 1-9
  Moving the Cursor on the Command Line ....................... 1-9
  Completing a Partial Command Name ............................ 1-10
  Deleting Entries ...................................................... 1-11
  Re-displaying the Current Command Line ....................... 1-11
  Command Output pagination ....................................... 1-12
Chapter 2. Common Commands

Common Commands ........................................... 2-2
  clrsrr ....................................................... 2-3
  exit ......................................................... 2-4
  help ......................................................... 2-5
  no .......................................................... 2-7
  service ...................................................... 2-8
  terminal ..................................................... 2-19
  show ......................................................... 2-20
  autoinstall ............................................... 2-22
  banner ..................................................... 2-23
  commands .................................................. 2-24
  crypto ....................................................... 2-25
  environment ............................................... 2-28
  history ..................................................... 2-29
  interfaces ................................................. 2-30
  ip .......................................................... 2-32
  ldap ......................................................... 2-38
  licenses .................................................... 2-40
  logging ..................................................... 2-41
  mac ........................................................ 2-42
  management ............................................... 2-43
  mobility ..................................................... 2-44
  ntp ........................................................ 2-47
  privilege .................................................... 2-49
  radius ....................................................... 2-50
  redundancy-group ........................................ 2-51
  redundancy-history ..................................... 2-53
  redundancy-members .................................... 2-54
  snmp ......................................................... 2-55
  snmp-server ............................................... 2-56
  terminal ..................................................... 2-59
  timezone .................................................... 2-60
  users ......................................................... 2-61
Chapter 3. User Exec Commands

User Exec Commands ................................................................. 3-2
autoinstall ................................................................. 3-3
clear ................................................................. 3-4
cluster-cli ............................................................... 3-6
debug ................................................................. 3-7
disable ................................................................. 3-9
enable ................................................................. 3-10
logout ................................................................. 3-11
page ................................................................. 3-12
quit ................................................................. 3-13

Chapter 4. Privileged Exec Commands

Priv Exec Command ................................................................. 4-2
acknowledge ................................................................. 4-4
archive ................................................................. 4-5
autoinstall ............................................................... 4-7
cd ................................................................. 4-8
clear ................................................................. 4-9
clock ................................................................. 4-11
cluster-cli ............................................................... 4-12
Chapter 5. Global Configuration Commands

Global Configuration Commands ............................................ 5-2
  aaa ................................................................. 5-4
  access-list ......................................................... 5-5
  banner ............................................................ 5-6
  boot ............................................................... 5-7
  country-code ....................................................... 5-8
  crypto ............................................................ 5-11
  do ................................................................. 5-16
Chapter 6. crypto-isakmp

Crypto Isakmp Config commands

- authentication ........................................ 6-3
- clrscr. .................................................. 6-4
- encryption ............................................. 6-5
- end ......................................................... 6-6
- exit ......................................................... 6-7
- group ....................................................... 6-8
- hash ......................................................... 6-9
- help ......................................................... 6-10
- lifetime .................................................... 6-11
- no .......................................................... 6-12
- service ..................................................... 6-13
- show ......................................................... 6-14
Chapter 7. crypto-group
Crypto Client Config commands .................................................. 7-1
   clrscr ......................................................... 7-3
dns ................................................................. 7-4
dns ................................................................. 7-5
dns ................................................................. 7-6
dns ......................................................... 7-7
dns ......................................................... 7-8
dns ................................................................. 7-9
 wins ......................................................... 7-11

Chapter 8. crypto-peer
Crypto Peer Config commands .................................................. 8-1
   clrscr ......................................................... 8-3
dns ................................................................. 8-4
dns ......................................................... 8-5
dns ......................................................... 8-6
  dns ......................................................... 8-7
dns ......................................................... 8-8
dns ................................................................. 8-9
  dns ......................................................... 8-10

Chapter 9. crypto-ipsec
Crypto Ipsec Config commands .................................................. 9-1
   mode ......................................................... 9-3
show ................................................................. 9-4

Chapter 10. crypto-map
Trustpoint Config commands .................................................. 10-1
   clrscr ......................................................... 10-3
dns ................................................................. 10-4
dns ......................................................... 10-5
dns ......................................................... 10-6
  dns ......................................................... 10-7
  dns ......................................................... 10-9
  dns ......................................................... 10-10
Chapter 11. crypto-trustpoint Instance

Trustpoint Config commands ........................................ 11-1
  clrsr .............................................................. 11-3
  company-name .................................................... 11-4
  email ............................................................... 11-5
  end ................................................................. 11-6
  exit ................................................................. 11-7
  fqdn ............................................................... 11-8
  help ............................................................... 11-9
  ip-address ....................................................... 11-10
  no ................................................................. 11-11
  password ......................................................... 11-12
  rsakeypair ....................................................... 11-13
  service ......................................................... 11-14
  show .............................................................. 11-16
  subject-name .................................................... 11-18

Chapter 12. interface Instance

Interface Config commands ........................................... 12-1
  clrsr .............................................................. 12-3
  crypto ........................................................... 12-4
  description ...................................................... 12-5
  duplex ............................................................ 12-6
  end ............................................................... 12-7
  exit ............................................................... 12-8
  help .............................................................. 12-9
  ip ................................................................. 12-10
  management ....................................................... 12-11
  mtu ............................................................... 12-12
  no ................................................................. 12-13
  service ......................................................... 12-14
  show .............................................................. 12-17
  shutdown ......................................................... 12-20
  speed ............................................................ 12-21
Chapter 13. Extended ACL Instance

Extended ACL Config Commands ........................................ 13-1
  clrscr ................................................................. 13-3
  deny ................................................................. 13-4
  end ................................................................. 13-6
  exit ................................................................. 13-7
  help ................................................................. 13-8
  mark ................................................................. 13-9
  no ................................................................. 13-11
  permit ............................................................... 13-12
  service ............................................................. 13-14
  show ................................................................. 13-13
  terminal ............................................................ 13-18

Chapter 14. Standard ACL Instance

Standard ACL Config Commands ................................. 14-1
  clrscr ................................................................. 14-3
  deny ................................................................. 14-4
  end ................................................................. 14-5
  exit ................................................................. 14-6
  help ................................................................. 14-7
  mark ................................................................. 14-8
  no ................................................................. 14-9
  permit ............................................................... 14-10
  service ............................................................. 14-11
  show ................................................................. 14-13
  terminal ............................................................ 14-15

Chapter 15. Extended MAC ACL Instance

MAC Extended ACL Config Commands .......................... 15-1
  clrscr ................................................................. 15-3
  deny ................................................................. 15-4
  end ................................................................. 15-6
Chapter 16. Radius Server Instance

Radius Configuration Commands

authentication .......................... 16-3
cr . ...................................... 16-4
crl-check ................................ 16-6
d . .......................................... 16-7
de ........................................... 16-8
group .................................... 16-9
cr . .......................................... 16-10
d ........................................... 16-10
de ........................................... 16-11
group .................................... 16-11
guest-group ................................ 16-12
help ....................................... 16-12
no ......................................... 16-13
policy ................................... 16-14
rad-user ................................ 16-15
service .................................. 16-16
show ...................................... 16-16
terminal ................................ 16-18
Example—Creating a Group .......... 16-19
help ....................................... 16-21
ldap-server ............................... 16-22
nas ....................................... 16-23
no ......................................... 16-24
proxy ..................................... 16-25
rad-user .............................................................. 16-27
server ............................................................. 16-28
service ............................................................. 16-29
show ................................................................. 16-30
terminal ............................................................ 16-32

Chapter 17. Wireless Instance

Wireless Configuration Commands ................................ 17-1
adopt-unconf-radio ................................................. 17-4
adoption-pref-id ................................................... 17-5
ap-detection ......................................................... 17-6
broadcast-tx-speed .............................................. 17-8
c1rsc ................................................................. 17-9
convert-ap ........................................................... 17-10
country-code ......................................................... 17-11
dhcp-sniff-state ................................................... 17-14
dot11-shared-key-auth .......................................... 17-15
end ................................................................. 17-16
exit ................................................................. 17-17
fix-windows-dhcp .................................................. 17-18
help ................................................................. 17-19
ids ................................................................. 17-20
mac-auth-local ..................................................... 17-22
manual-wlan-mapping ............................................ 17-23
mobility ............................................................. 17-24
no ................................................................. 17-25
oversized-frames ............................................... 17-26
proxy-arp .......................................................... 17-27
qos-mapping ........................................................ 17-28
radio ............................................................... 17-29
self-heal ............................................................. 17-36
sensor ............................................................... 17-38
service ............................................................. 17-39
show ................................................................. 17-42
smart-scan-channels ............................................. 17-44
terminal ............................................................ 17-45
wlan ................................................................. 17-46
This preface introduces the 

WS5100 Series CLI Reference Guide

does contain the following sections:

- Who Should Use this Guide
- How to Use this Guide
- Conventions Used in this Guide
- Service Information

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 Series Switch within the wireless local area network. 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 Series Switch and associated network elements. This guide is organized into the following sections:

Table 1 Quick Reference on How This Guide Is Organized

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Jump to this section if you want to...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chapter 1, “Introduction”</td>
<td>Review the overall feature-set of the WS5100 Series Wireless Switch, as well as the many configuration options available.</td>
</tr>
<tr>
<td>Chapter 2, “Common Commands”</td>
<td>Summarizes the commands common amongst many contexts and instance contexts within the WS5100 Series Wireless Switch command line interface.</td>
</tr>
<tr>
<td>Chapter 3, “User Exec Commands”</td>
<td>Summarizes the User Exec commands within the WS5100 Series Wireless Switch command line interface.</td>
</tr>
<tr>
<td>Chapter 4, “Privileged Exec Commands”</td>
<td>Summarizes the Priv Exec commands within the WS5100 Series Wireless Switch command line interface.</td>
</tr>
<tr>
<td>Chapter 5, “Global Configuration Commands”</td>
<td>Summarizes the Global Config commands within the WS5100 Series Wireless Switch command line interface.</td>
</tr>
<tr>
<td>Chapter 6, “crypto-isakmp”</td>
<td>Summarizes the <code>crypto-isakmp</code> commands within the WS5100 Series Switch command line interface</td>
</tr>
<tr>
<td>Chapter 7, “crypto-group”</td>
<td>Summarizes the <code>crypto-group</code> commands within the WS5100 Series Switch command line interface</td>
</tr>
<tr>
<td>Chapter 8, “crypto-peer”</td>
<td>Summarizes the <code>crypto-peer</code> commands within the WS5100 Series Switch command line interface</td>
</tr>
<tr>
<td>Chapter 9, “crypto-ipsec”</td>
<td>Summarizes the <code>crypto-ipsec</code> commands within the WS5100 Series Switch command line interface</td>
</tr>
<tr>
<td>Chapter 10, “crypto-map”</td>
<td>Summarizes the <code>crypto-map</code> commands within the WS5100 Series Switch command line interface</td>
</tr>
<tr>
<td>Chapter 11, “crypto-trustpoint Instance”</td>
<td>Summarizes the <code>crypto trustpoint</code> commands within the WS5100 Series Wireless Switch command line interface</td>
</tr>
<tr>
<td>Chapter 12, “interface Instance”</td>
<td>Summarizes the <code>config-if</code> commands within the WS5100 Series Wireless Switch command line interface.</td>
</tr>
</tbody>
</table>
Table 1  Quick Reference on How This Guide Is Organized (Continued)

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Jump to this section if you want to...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chapter 13, “Extended ACL Instance”</td>
<td>Summarizes the <code>config-ext-nacl</code> commands within the WS5100 Series Switch command line</td>
</tr>
<tr>
<td>Chapter 14, “Standard ACL Instance”</td>
<td>Summarizes the <code>config-std-nacl</code> commands within the WS5100 Series Switch command line</td>
</tr>
<tr>
<td>Chapter 15, “Extended MAC ACL Instance”</td>
<td>Summarizes the <code>config-ext-macl</code> commands within the WS5100 Series Switch command line</td>
</tr>
<tr>
<td>Chapter 16, “Radius Server Instance”</td>
<td>Summarizes the <code>(config-radsrv)</code> instance commands within the WS5100 Series Wireless Switch command line interface</td>
</tr>
<tr>
<td>Chapter 17, “Wireless Instance”</td>
<td>Summarizes the <code>(config-wireless)</code> instance commands within the WS5100 Series Wireless Switch command line interface</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Table 1-1. Notational Convention used in the document</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Convention</strong></td>
</tr>
<tr>
<td>---</td>
</tr>
<tr>
<td><strong>bold</strong></td>
</tr>
<tr>
<td><strong>italics</strong></td>
</tr>
<tr>
<td>()</td>
</tr>
<tr>
<td>()</td>
</tr>
<tr>
<td>[ ]</td>
</tr>
<tr>
<td>_</td>
</tr>
<tr>
<td>?</td>
</tr>
</tbody>
</table>
Service Information

Symbol Technologies provides its customers with prompt and accurate customer support. Use the Symbol Support Center as the primary contact for any technical problem, question or support issue involving Symbol products.

If the Symbol Customer Support specialists cannot solve a problem, access to all technical disciplines within Symbol becomes available for further assistance and support. Symbol Customer Support responds to calls by email, telephone or fax within the time limits set forth in individual contractual agreements.

When contacting Symbol Customer Support, please provide the following information:

- serial number of unit
- model number or product name
- software type and version number

North American Contacts

Inside North America:

Symbol Technologies, Inc.
One Symbol Plaza Holtsville, New York 11742-1300
Telephone: 1-631-738-2400/1-800-SCAN 234
Fax: 1-631-738-5990

Symbol Support Center (for warranty and service information):

telephone: 1-800-653-5350
fax: (631) 738-5410
Email: support@symbol.com
International Contacts

Outside North America:
Symbol Technologies
Symbol Place
Winnersh Triangle, Berkshire, RG41 5TP
United Kingdom
0800-328-2424 (Inside UK)
+44 118 945 7529 (Outside UK)

Web Support Sites

MySymbolCare
http://www.symbol.com/services/msc/msc.html

Symbol Services Homepage
http://symbol.com/services

Symbol WS5100 Manuals
http://www.symbol.com/legacy_manuals/wire/ws5100.html

Symbol Developer Program
http://devzone.symbol.com

Additional Information

Obtain additional information by contacting Symbol at:
1-800-722-6234, inside North America
+1-516-738-5200, in/outside North America
http://symbol.com/
This chapter describes the commands that are defined by the WS5100 Series Command Line Interface (CLI). Access the CLI by running a terminal emulation program on a computer that is connected to the serial port at the front of the switch, or by using Telnet via secure shell (SSH) to access the switch over the network.

The default cli user is cli. The default username and password is admin and superuser, respectively.

1.1 CLI Overview

The Symbol command-line interface (CLI) is used for configuring, monitoring, and maintaining Symbol devices. This user interface allows you to execute commands, whether using a serial console or using remote access methods.

This chapter describes the basic features of the Symbol CLI’s and how to use them. Topics covered include an introduction to Symbol command modes, navigation and editing features, help features, and command history features.
To aid in the configuration of Symbol devices, the Symbol CLI is divided into different command modes. Each command mode has its own set of commands available for the configuration, maintenance, and monitoring. The commands available to you at any given time depend on the mode you are in. Enter a question mark (?) at the system prompt to view the list of commands available for each command mode/instance.

The use of specific commands allows you to navigate from one command mode to another. The standard order that a user would access the modes is as follows: USER EXEC mode; PRIV EXEC mode and GLOBAL CONFIG mode.

When you start a session on a switch, you generally begin in USER EXEC mode, which is one of two access levels of the EXEC mode. For security purposes, only a limited subset of EXEC commands are available in USER EXEC mode. This level of access is reserved for tasks that do not change the configuration of the switch, such as determining the current switch configuration.

In order to have access to all commands, you must enter PRIV EXEC mode, which is the second level of access for the EXEC mode. In PRIV EXEC mode, you can enter any EXEC command, as the PRIV EXEC mode is a superset of the USER EXEC mode commands.

Most EXEC mode commands are one-time commands, such as show commands, which show the current configuration status, and clear commands, which clear counters or interfaces. EXEC mode commands are not saved across reboots of the switch.

From PRIV EXEC mode, you can enter GLOBAL CONFIG mode. In this mode, you can enter commands that configure general system characteristics. You also can use global configuration mode to enter specific configuration modes. Configuration modes, including global configuration mode, allow you to make changes to the running configuration. If you later save the configuration, these commands are stored across switch reboots.

From global configuration mode you can enter a variety of protocol-specific or feature-specific configuration modes. The CLI hierarchy requires that you enter these specific configuration modes only through global configuration mode.

From global configuration modes, you can enter configuration submodes. Configuration submodes are used for the configuration of specific features within the scope of a given configuration mode.
The *Table 1.1* below summarizes all the commands available to configure and monitor WS5100 Series Switch.

**Table 1.1 CLI Context Hierarchy for WS5100 Series Switch**

<table>
<thead>
<tr>
<th>User Exec Mode</th>
<th>Priv Exec Mode</th>
<th>Global Configuration Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>autoinstall</td>
<td>acknowledge</td>
<td>aaa</td>
</tr>
<tr>
<td>clear</td>
<td>archive</td>
<td>access-list</td>
</tr>
<tr>
<td>clrscr</td>
<td>autoinstall</td>
<td>banner</td>
</tr>
<tr>
<td>cluster-cli</td>
<td>cd</td>
<td>boot</td>
</tr>
<tr>
<td>debug</td>
<td>clear</td>
<td>clrscr</td>
</tr>
<tr>
<td>disable</td>
<td>clock</td>
<td>country-code</td>
</tr>
<tr>
<td>enable</td>
<td>clrscr</td>
<td>crypto</td>
</tr>
<tr>
<td>exit</td>
<td>cluster-cli</td>
<td>do</td>
</tr>
<tr>
<td>help</td>
<td>configure</td>
<td>end</td>
</tr>
<tr>
<td>logout</td>
<td>copy</td>
<td>exit</td>
</tr>
<tr>
<td>no</td>
<td>debug</td>
<td>fallback</td>
</tr>
<tr>
<td>page</td>
<td>delete</td>
<td>ftp</td>
</tr>
<tr>
<td>quit</td>
<td>diff</td>
<td>help</td>
</tr>
<tr>
<td>service</td>
<td>dir</td>
<td>hostname</td>
</tr>
<tr>
<td>show</td>
<td>disable</td>
<td>interface</td>
</tr>
<tr>
<td>terminal</td>
<td>edit</td>
<td>ip</td>
</tr>
<tr>
<td></td>
<td>enable</td>
<td>license</td>
</tr>
<tr>
<td></td>
<td>erase</td>
<td>line</td>
</tr>
<tr>
<td></td>
<td>exit</td>
<td>local</td>
</tr>
<tr>
<td></td>
<td>halt</td>
<td>logging</td>
</tr>
<tr>
<td></td>
<td>help</td>
<td>mac</td>
</tr>
<tr>
<td></td>
<td>kill</td>
<td>no</td>
</tr>
<tr>
<td></td>
<td>logout</td>
<td>ntp</td>
</tr>
</tbody>
</table>
1.2 Getting Context Sensitive Help

Entering a question mark (?) at the system prompt displays a list of commands available for each command mode. You also can get a list of the arguments and keywords available for any command with the context-sensitive help feature.

<table>
<thead>
<tr>
<th>User Exec Mode</th>
<th>Priv Exec Mode</th>
<th>Global Configuration Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>mkdir</td>
<td>prompt</td>
<td></td>
</tr>
<tr>
<td>more</td>
<td>radius-server</td>
<td></td>
</tr>
<tr>
<td>no</td>
<td>redundancy</td>
<td></td>
</tr>
<tr>
<td>page</td>
<td>service</td>
<td></td>
</tr>
<tr>
<td>ping</td>
<td>show</td>
<td></td>
</tr>
<tr>
<td>pwd</td>
<td>snmp-server</td>
<td></td>
</tr>
<tr>
<td>quit</td>
<td>terminal</td>
<td></td>
</tr>
<tr>
<td>reload</td>
<td>timezone</td>
<td></td>
</tr>
<tr>
<td>rename</td>
<td>username</td>
<td></td>
</tr>
<tr>
<td>rmdir</td>
<td>wireless</td>
<td></td>
</tr>
<tr>
<td>service</td>
<td></td>
<td></td>
</tr>
<tr>
<td>show</td>
<td></td>
<td></td>
</tr>
<tr>
<td>telnet</td>
<td></td>
<td></td>
</tr>
<tr>
<td>terminal</td>
<td></td>
<td></td>
</tr>
<tr>
<td>traceroute</td>
<td></td>
<td></td>
</tr>
<tr>
<td>upgrade</td>
<td></td>
<td></td>
</tr>
<tr>
<td>upgrade-abort</td>
<td></td>
<td></td>
</tr>
<tr>
<td>write</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
To get help specific to a command mode, a command name, a keyword, or an argument, use any of the following commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>(prompt)# help</td>
<td>Displays a brief description of the help system.</td>
</tr>
<tr>
<td>(prompt)# abbreviated-command-entry?</td>
<td>Lists commands in the current mode that begin with a particular character string.</td>
</tr>
<tr>
<td>(prompt)# abbreviated-command-entry&lt;Tab&gt;</td>
<td>Completes a partial command name.</td>
</tr>
<tr>
<td>(prompt)#?</td>
<td>Lists all commands available in the command mode.</td>
</tr>
<tr>
<td>prompt)# command ?</td>
<td>Lists the available syntax options (arguments and keywords) for the command.</td>
</tr>
<tr>
<td>(prompt)# command keyword ?</td>
<td>Lists the next available syntax option for the command.</td>
</tr>
</tbody>
</table>

**NOTE** The system prompt will vary 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 character sequence, type in those characters followed immediately by the question mark (?). Do not include a space. This form of help is called **word help**, because it completes a word for you.

```
WS5100#service?
  service  Service Commands

WS5100#service
```

To list keywords or arguments, enter a question mark (?) in place of a keyword or argument. Include a space before the ?. This form of help is called **command syntax help**, because it shows you which keywords or arguments are available based on the command, keywords, and arguments you already have entered.

```
WS5100#service ?
  ap       access-port serviceability parameters
  clear    Reset functions
  copy     Copy from one file to another
  diag     Diagnostics
  diag-shell  Provide diag shell access
  radius   Enable radius server
```
save-cli     Save CLI tree for all modes in html format
show        Show running system information
start-shell Provide shell access
tethereal   Dump and analyze network traffic
wireless    Wireless parameters

WS5100#service
You can abbreviate commands and keywords to the number of characters that allow a unique abbreviation. For example, you can abbreviate the configure terminal command to config t. Because the abbreviated form of the command is unique, the switch will accept the abbreviated form and execute the command.

Entering the help command (available in any command mode) will provide the following description of the help system:

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 configuration command has a no form. In general, use the no form to disable a feature or function. Use the command without the no keyword to re enable a disabled feature or to enable a feature that is disabled by default.
1.4 Using History Command

The Symbol CCB CLI provides a history or record of commands that you have entered. This feature is particularly useful for recalling long or complex commands or entries. To use the command history feature, perform any of the tasks described in the following sections:

- Setting the History Command Buffer Size
- Recalling Commands
- Disabling the History Command Feature

1.4.1 Setting the History Command Buffer Size

By default, the system records 256 command lines in its history buffer. To set the number of command lines that the system will record during the current terminal session, use the following command in EXEC mode:

```
WS5100# history [size number-of-lines]
```

Sets the size of command history buffer.

```
WLAN Module# history
```

Enables command history feature.

Use `no history` command disables the command history feature.

1.4.2 Recalling Commands

To recall commands from the history buffer, use one of the following commands or key combinations:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ctrl-P or the Up Arrow key.</td>
<td>Recalls commands in the history buffer, beginning with the most recent command. Repeat the key sequence to recall successively older commands.</td>
</tr>
<tr>
<td>Ctrl-N or the Down Arrow key.</td>
<td>Returns to more recent commands in the history buffer after recalling commands with Ctrl-P or the Up Arrow key. Repeat the key sequence to recall successively more recent commands.</td>
</tr>
<tr>
<td>!!</td>
<td>Executes the last command from the command history buffer.</td>
</tr>
<tr>
<td>!&lt;n&gt;</td>
<td>Executes nth command from command history buffer.</td>
</tr>
</tbody>
</table>
### 1.4.3 Disabling the History Command Feature

The command history feature is automatically enabled. To disable it during the current terminal session, use the following command in EXEC mode:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>WLAN Module# no history</td>
<td>Disables command history for the current session.</td>
</tr>
</tbody>
</table>

### 1.4.4 Basic Conventions

Following are a few conventions to keep in mind while working within the command line interface:

- Always use `?` at the end of the command to view if there are any further sub modes that can be used. If yes, type the first few alphabets of the submode and press the tab key to add the submode. Continue using the `?` until you reach the final sub-submode that you would like to use for configuration of the WS5100 Series Switch.

- Pre-defined CLI commands and keywords are case-insensitive: `cfg = Cfg = CFG`. However, mostly for clarity, CLI commands and keywords are displayed in this guide using mixed case. For example, `apPolicy`, `trapHosts`, `channelInfo`.

- You can 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:

```
WS5000.(Cfg)> spol "Default Switch Policy"
WS5000.(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.
1.5 Using CLI Editing Features and Shortcuts

A variety of shortcuts and editing features are enabled for the Symbol CCB CLI. The following subsections 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

1.5.1 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 to make corrections or changes. Ctrl indicates the Control key, which must be pressed simultaneously with its associated letter key. Esc indicates the Escape key, which must be pressed first, followed by its associated letter key. Keys are not case sensitive. Many letters used for CLI navigation and editing 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 the letter used and the function.

<table>
<thead>
<tr>
<th>Keystrokes</th>
<th>Function Summary</th>
<th>Function Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Left Arrow or Ctrl-B</td>
<td>Back character</td>
<td>Moves the cursor one character to the left. When you enter a command that extends beyond a single line, you can press the Left Arrow or Ctrl-B keys repeatedly to scroll back toward the system prompt and verify the beginning of the command entry, or you can press the Ctrl-A key combination.</td>
</tr>
<tr>
<td>Right Arrow or Ctrl-F</td>
<td>Forward character</td>
<td>Moves the cursor one character to the right.</td>
</tr>
<tr>
<td>Esc, B</td>
<td>Back word</td>
<td>Moves the cursor back one word.</td>
</tr>
<tr>
<td>Esc, F</td>
<td>Forward word</td>
<td>Moves the cursor forward one word.</td>
</tr>
<tr>
<td>Ctrl-A</td>
<td>Beginning of line</td>
<td>Moves the cursor to the beginning of the line.</td>
</tr>
</tbody>
</table>
1.5.2 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 the command, then press the Tab key. The command line parser will complete the command if the string entered is unique to the command mode. If your keyboard does not have a Tab key, press Ctrl-I instead.

The CLI will recognize a command once you have entered enough characters to make the command unique. For example, if you enter conf in privileged EXEC mode, the CLI will be able to associate your entry with the configure command, because only the configure command begins with conf.

In the following example the CLI recognizes the unique string for privileged EXEC mode of conf 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 by the abbreviation. If you enter a set of
characters that could indicate 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 you enter and the question mark (?).

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

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

1.5.3 Deleting Entries

Use any of the following keys or key combinations to delete command entries if you make a mistake or change your mind:

<table>
<thead>
<tr>
<th>Keystrokes</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Backspace</td>
<td>Deletes the character to the left of the cursor.</td>
</tr>
<tr>
<td>Ctrl-D</td>
<td>Deletes the character at the cursor.</td>
</tr>
<tr>
<td>Ctrl-K</td>
<td>Deletes all characters from the cursor to the end of the command line.</td>
</tr>
<tr>
<td>Ctrl-W</td>
<td>Deletes the word up to the cursor.</td>
</tr>
<tr>
<td>Esc, D</td>
<td>Deletes from the cursor to the end of the word.</td>
</tr>
</tbody>
</table>

1.5.4 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 line entry. To redisplay the current command line (refresh the screen), use either of the following key combinations:

<table>
<thead>
<tr>
<th>Keystrokes</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ctrl-L</td>
<td>Redisplays the current command line.</td>
</tr>
</tbody>
</table>
1.5.5 Command Output pagination

When working with the Symbol CCB CLI, output often extends beyond the visible screen length. For cases where output continues beyond the bottom of the screen, such as with the output of many `?` or `show` commands, the output is paused and Press Any Key to Continue (Q to Quit) prompt is displayed at the bottom of the screen. To resume output, press the Return key to scroll down one line, or press the Spacebar to display the next full screen of output.

1.5.6 Transposing Mistyped Characters

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

<table>
<thead>
<tr>
<th>Keystrokes</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ctrl-T</td>
<td>Transposes the character to the left of the cursor with the character located at the cursor.</td>
</tr>
</tbody>
</table>

1.5.7 Controlling Capitalization

You can capitalize or lowercase words or capitalize a set of letters with simple key sequences. Note, however, that Symbol CCB commands are generally case-insensitive, and are typically all in lowercase. To change the capitalization of commands, use any of the following key sequences:

<table>
<thead>
<tr>
<th>Keystrokes</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Esc, C</td>
<td>Capitalizes the letters at the right of cursor.</td>
</tr>
<tr>
<td>Esc, L</td>
<td>Changes the letters at the right of cursor to lowercase.</td>
</tr>
</tbody>
</table>
This chapter explains the common CLI commands used amongst the USER EXEC and PRIV EXEC modes.

PRIV EXEC command set contains all of the commands available in USER EXEC mode, some commands can be entered in either mode. Commands that can be entered in either USER EXEC mode or PRIV EXEC mode are referred to as EXEC mode commands. If user or privileged is not specified in the documentation, assume that you can enter the referenced commands in either mode.
2.1 Common Commands

*Table 2.1* summarizes the commands common amongst many contexts and instance contexts within the WS5100 Series Switch command line interface.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Ref.</th>
</tr>
</thead>
<tbody>
<tr>
<td>clrscr</td>
<td>Clears the display screen.</td>
<td>page 2-3</td>
</tr>
<tr>
<td>exit</td>
<td>End current mode and down to previous mode.</td>
<td>page 2-4</td>
</tr>
<tr>
<td>help</td>
<td>Description of the interactive help system.</td>
<td>page 2-5</td>
</tr>
<tr>
<td>no</td>
<td>Negate a command or set its defaults.</td>
<td>page 2-7</td>
</tr>
<tr>
<td>service</td>
<td>Service Commands.</td>
<td>page 2-8</td>
</tr>
<tr>
<td>show</td>
<td>Shows running system information.</td>
<td>page 2-20</td>
</tr>
<tr>
<td>terminal</td>
<td>Set terminal line parameters.</td>
<td>page 2-19</td>
</tr>
</tbody>
</table>
2.1.1 clrscr

Use this command to clear the screen displaying the cli and start afresh at the prompt (#).

Syntax

```plaintext
clrscr
```

Parameters

None.

Usage Guidelines

Example

```plaintext
WS5100#clrscr
```
2.1.2 exit

Use this command to end current mode and move to the previous mode.

Syntax

```
exit
```

Parameters

None.

Usage Guidelines

Example

```
WS5100(config)#exit
```
2.1.3 help

Use this command to get access to the advanced help feature. You can also use "?" anytime at the command prompt to get access to the help topic.

When using this command, if nothing matches then 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?'.)

Syntax

help
or
?

Parameters

None.

Usage Guidelines

Example

WS5100>show ?
autoinstall autoinstall configuration
banner Display Message of the Day Login banner
commands Show command lists
crypto crypto
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 Media Access Control
management Display L3 Management 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

WS5100>show autoinstall ?
  | Output modifiers
> Output redirection
>> Output redirection appending
2.1.4 no

Use this command to either negate a command or set its defaults.

Syntax

no

Parameters

None.

Usage Guidelines

Example

WS5100>no ?
  autoinstall  autoinstall configuration command
  cluster-cli  Cluster context
  debug       Debugging functions
  page        Toggle paging
  service     Service Commands
2.1.5 service

Use this command to service/debug the WS5100 Series Switch.

Syntax

```
service (diag (enable | led ( 1 (amber ( flashing|off|on) | blue | red ) | 2 (amber ( flashing|off|on) | blue | red ) ) ) | limit (buffer|fan|filesys(etc2|flash|ram)|load(1|15|5)|maxFDs|pkbuffers|procRAM|ram|route|cache|tempreature) |period <100-30000>) | save-cli | show (cli|command-history|crash-info|diag|info|memory|natstats|process|reboot-history|rulestats|startup-log|upgrade-history))
```

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>diag</td>
<td>Diagnostics</td>
</tr>
<tr>
<td>save-cli</td>
<td>Save CLI tree for all modes in html format.</td>
</tr>
<tr>
<td>show</td>
<td>Show running system information</td>
</tr>
<tr>
<td>enable</td>
<td>Enables the service diagnostics mode</td>
</tr>
<tr>
<td>led</td>
<td>Use to configure LED display sequence</td>
</tr>
<tr>
<td>1</td>
<td>Use to configure upper LED. You can select from the following options:</td>
</tr>
<tr>
<td></td>
<td>• amber</td>
</tr>
<tr>
<td></td>
<td>• blue</td>
</tr>
<tr>
<td></td>
<td>• red</td>
</tr>
<tr>
<td>2</td>
<td>Use to configure lower LED. You can select from the following options</td>
</tr>
<tr>
<td></td>
<td>• amber</td>
</tr>
<tr>
<td></td>
<td>• blue</td>
</tr>
<tr>
<td></td>
<td>• red</td>
</tr>
<tr>
<td>limit</td>
<td>Use to set the diagnostic limit submodes/commands.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| buffer  | Use to configure the buffer usage warning limit. The warning limit can be set to one of the following buffer limit size:  
- 12 – 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 – 8 byte buffer limit |
| fan     | Use to set the fan speed limit. You can configure the fan speed limit for both, Fan 1 and Fan 2. |
| filesys | Use to set file system freespace limit. You can select the freespace limit for the following sub context:  
- etc2  
- flash  
- ram |
| load    | Use to configure aggregate processor load. You can select from the following submodes:  
- 1 – Aggregate processor load during the previous minute.  
- 15 – Aggregate processor load during the previous 15 minute.  
- 5 – Aggregate processor load during the previous 5 minute. |
| maxFDs  | Use to configure the maximum number of file descriptors. You can set anything between 0 to 32767 file descriptors. |
### CLI Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>pkbuffers</td>
<td>Use to configure and set the packet buffer head cache limit. You can set anything between 0 to 65535 as the buffer cache limit.</td>
</tr>
<tr>
<td>procRAM</td>
<td>Use to configure the RAM space used by a process. You can set the percentage of RAM space to be used by the processor from anything between 0.0 to 100.0 percent.</td>
</tr>
<tr>
<td>ram</td>
<td>Use to configure the free space for the RAM. You can configure the free space to anything between 0.0 to 100.0 percent.</td>
</tr>
<tr>
<td>routecache</td>
<td>Use to configure the IP route cache usage. Can be set with a value between 0 - 65553</td>
</tr>
<tr>
<td>temperature</td>
<td>Use to set the temperature sensor for the WS5100 Series Switch. You can set as many as 8 temperature sensors.</td>
</tr>
<tr>
<td>period</td>
<td>Use to set diagnostic period</td>
</tr>
<tr>
<td>&lt;100-30000&gt;</td>
<td>Use to configure Diagnostics period. You can set a value of anything between 100-30000 milli seconds. The default value is set to 1000 milliseconds.</td>
</tr>
<tr>
<td>save-cli</td>
<td>This command creates clitree.html which saves and displays the cli tree for all modes.</td>
</tr>
<tr>
<td>cli</td>
<td>Show CLI tree of current mode</td>
</tr>
<tr>
<td>command-history</td>
<td>Display command (except show commands) history</td>
</tr>
<tr>
<td>crash-info</td>
<td>Display information about core, panic and AP dump files</td>
</tr>
<tr>
<td>diag</td>
<td>Diagnostics</td>
</tr>
<tr>
<td>info</td>
<td>Show snapshot of available support information</td>
</tr>
<tr>
<td>memory</td>
<td>Show memory statistics</td>
</tr>
<tr>
<td>natstats</td>
<td>Show ACL rule stats</td>
</tr>
<tr>
<td>process</td>
<td>Show processes (sorted by memory usage)</td>
</tr>
<tr>
<td>reboot-history</td>
<td>Show reboot history</td>
</tr>
<tr>
<td>rulestats</td>
<td>Show ACL rule stats</td>
</tr>
<tr>
<td>startup-log</td>
<td>Show startup log</td>
</tr>
</tbody>
</table>
### Usage Guidelines

**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
  filesystem  file system freespace limit
  load    aggregate 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 diag limit buffer 32k ?
<0-65535>  buffer usage warning limit 0-65535

WS5100#service diag limit buffer 32k 4096

WS5100#service diag limit fan ?
<1-2>  Fan number

WS5100#service diag limit fan 1 ?
  low  Low speed limit

WS5100#service diag limit fan 1 low ?
<1000-15000>  Limit value from 1000 to 15,000

WS5100#service diag limit fan 1 low 1100
WS5100#service diag limit fan 2 low 10000
WS5100#Sep 01 15:51:54 2006: %DIAG-4-FANUNDERSPEED: Fan case under speed:
8881 RPM is under limit 10000 RPM

WS5100#service diag limit filesys ?
  etc2  /etc2 file system
  flash /flash file system
  ram    /ram file system

WS5100#service diag limit filesys flash ?
  WORD  limit from 0.0 to 100.0

WS5100#service diag limit filesys flash 20
WS5100#service diag limit filesys etc2 10
WS5100#service diag limit filesys ram 30

WS5100#service diag limit load ?
  1   during the previous minute
  15  during the previous 15 minutes
5 during the previous five minutes

WS5100#service diag limit load 5 ?
WORD percentage load from 0.0 to 100.0

WS5100#service diag limit load 5 50

WS5100#service diag limit maxFDs ?
<0-32767> 0-32767

WS5100#service diag limit maxFDs 30000

WS5100#service diag limit pkbuffers ?
<0-65535> limit from 0-65535

WS5100#service diag limit pkbuffers 4096
WS5100#service diag limit procRAM ?
WORD limit from 0.0-100.0

WS5100#service diag limit procRAM 10

WS5100#service diag limit ram ?
WORD limit from 0.0-100.0

WS5100#service diag limit ram 20

WS5100#service diag limit routecache ?
<0-65535> limit from 0-65535

WS5100#service diag limit routecache 10240

WS5100#service diag limit temperature ?
<1-8> temperature sensor number

WS5100#service diag period ?
<100-30000> Diagnostics period <100-30000> default 1000 milliseconds

WS5100#service diag period 20000

WS5100#service save-cli

/usr/scripts/genclitree.sh: /usr/scripts/genclitree.sh: 15: eth: not found
CLI command tree is saved as clitree.html.
This tree can be viewed via web at http://<ipaddr>/cli/clitree.html

WS5100#

WS5100>service show cli
User Exec mode:
+-autoinstall
  +-cluster-config
    +-enable [autoinstall (config|cluster-config|image) enable]
    +-url
      +-LINE [autoinstall (config|cluster-config|image) url LINE]
  +-enable [autoinstall (config|cluster-config|image) enable]
  +-url
    +-LINE [autoinstall (config|cluster-config|image) url LINE]
  +-image
    +-enable [autoinstall (config|cluster-config|image) enable]
    +-url
      +-LINE [autoinstall (config|cluster-config|image) url LINE]
    +-start [autoinstall start]
+-clear
+-crypto
  +-ike
    +-sa [clear crypto ike sa (A.B.C.D |)]
    +-A.B.C.D [clear crypto ike sa (A.B.C.D |)]
  +-ipsec
    +-sa [clear crypto ipsec sa (A.B.C.D |)]

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

<table>
<thead>
<tr>
<th>Date &amp; Time</th>
<th>User</th>
<th>Location</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aug 31 23:40:15</td>
<td>(null)</td>
<td>vty 131</td>
<td>wireless</td>
</tr>
<tr>
<td>Aug 31 23:40:15</td>
<td>(null)</td>
<td>vty 131</td>
<td>config t</td>
</tr>
<tr>
<td>Aug 31 23:40:15</td>
<td>(null)</td>
<td>vty 131</td>
<td>enable</td>
</tr>
<tr>
<td>Aug 31 23:40:14</td>
<td>(null)</td>
<td>vty 131</td>
<td>interface eth0</td>
</tr>
<tr>
<td>Aug 31 23:40:14</td>
<td>(null)</td>
<td>vty 131</td>
<td>config t</td>
</tr>
<tr>
<td>Aug 31 23:40:14</td>
<td>(null)</td>
<td>vty 131</td>
<td>enable</td>
</tr>
<tr>
<td>Aug 31 23:40:13</td>
<td>(null)</td>
<td>vty 131</td>
<td>line console 0</td>
</tr>
<tr>
<td>Aug 31 23:40:13</td>
<td>(null)</td>
<td>vty 131</td>
<td>config t</td>
</tr>
<tr>
<td>Aug 31 23:40:12</td>
<td>(null)</td>
<td>vty 131</td>
<td>enable</td>
</tr>
<tr>
<td>Aug 31 23:40:12</td>
<td>(null)</td>
<td>vty 131</td>
<td>enable</td>
</tr>
<tr>
<td>Aug 31 23:40:11</td>
<td>(null)</td>
<td>vty 131</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Aug 31 16:30:14</td>
<td>(null)</td>
<td>con 0</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Aug 31 16:30:04</td>
<td>(null)</td>
<td>con 0</td>
<td>en</td>
</tr>
<tr>
<td>Aug 31 16:29:21</td>
<td>(null)</td>
<td>con 0</td>
<td>exit</td>
</tr>
<tr>
<td>Aug 30 19:54:13</td>
<td>(null)</td>
<td>vty 130</td>
<td>enable</td>
</tr>
<tr>
<td>Aug 30 19:53:09</td>
<td>(null)</td>
<td>vty 130</td>
<td>disable</td>
</tr>
<tr>
<td>Aug 30 19:41:12</td>
<td>(null)</td>
<td>vty 130</td>
<td>clear mobility peer-</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>statistics 157.235.208.39</td>
</tr>
</tbody>
</table>

WS5100>service show crash-info
Coredump files:
Name                    Size    Date & Time
=============================================
imish_8990_200B.core.gz 299.5k   Aug 31 23:50

WS5100>

WS5100> service show info

4.0M out of 4.0M available for logs.
9.7M out of 11.4M available for history.
16.1M out of 18.6M available for crashinfo.

List of Files:
imish_8990_200B.core.gz         299.5k  Aug 31 23:50
messages.log                    200     Aug 30 15:32
snmpd.log                       316     Aug 30 15:33
startup.log                     16.5k   Aug 30 15:32
command.history                 9.6k    Aug 31 23:40
reboot.history                  2.3k    Aug 30 15:32
upgrade.history                 782     Aug 29 18:32

Please export these files or delete them for more space.

WS5100>

WS5100> service show memory

MemTotal:       256220 kB
MemFree:        155628 kB
Buffers:          1596 kB
Cached:          27912 kB
SwapCached:          0 kB
Active:          53832 kB
Inactive:        16272 kB
HighTotal:           0 kB
HighFree:          0 kB
LowTotal:       256220 kB
LowFree:        155628 kB
SwapTotal:           0 kB
SwapFree:           0 kB
Dirty:              0 kB
Writeback:          0 kB
Mapped:          50768 kB
Slab:             9984 kB
CommitLimit:    128108 kB
Committed_AS:    75368 kB
PageTables:        468 kB
WS5100 Series Switch CLI Reference Guide

VmallocTotal: 778200 kB
VmallocUsed: 19568 kB
VmallocChunk: 757824 kB

WS5100>

WS5100> service show process

<table>
<thead>
<tr>
<th>PID</th>
<th>STATUS</th>
<th>RSS</th>
<th>PPID</th>
<th>%CPU</th>
<th>%MEM</th>
<th>COMMAND</th>
</tr>
</thead>
<tbody>
<tr>
<td>320</td>
<td>S</td>
<td>10M</td>
<td>1</td>
<td>0.0</td>
<td>4.1</td>
<td>ccsrvr</td>
</tr>
<tr>
<td>345</td>
<td>S</td>
<td>8488</td>
<td>1</td>
<td>1.9</td>
<td>3.3</td>
<td>ccstatsd</td>
</tr>
<tr>
<td>387</td>
<td>S</td>
<td>5612</td>
<td>1</td>
<td>0.0</td>
<td>2.1</td>
<td>securitymgr</td>
</tr>
<tr>
<td>318</td>
<td>S</td>
<td>4480</td>
<td>1</td>
<td>0.0</td>
<td>1.7</td>
<td>snmpd</td>
</tr>
<tr>
<td>394</td>
<td>S</td>
<td>3932</td>
<td>1</td>
<td>0.0</td>
<td>1.5</td>
<td>imi</td>
</tr>
<tr>
<td>349</td>
<td>R</td>
<td>3424</td>
<td>1</td>
<td>0.0</td>
<td>1.3</td>
<td>isDiag</td>
</tr>
<tr>
<td>367</td>
<td>S</td>
<td>3264</td>
<td>279</td>
<td>0.0</td>
<td>1.2</td>
<td>radconfd</td>
</tr>
<tr>
<td>315</td>
<td>S</td>
<td>3208</td>
<td>279</td>
<td>0.0</td>
<td>1.2</td>
<td>CertMgr</td>
</tr>
<tr>
<td>391</td>
<td>S</td>
<td>3104</td>
<td>1</td>
<td>0.0</td>
<td>1.2</td>
<td>radiusd</td>
</tr>
<tr>
<td>373</td>
<td>S</td>
<td>2844</td>
<td>1</td>
<td>0.0</td>
<td>1.1</td>
<td>dhcpsvr</td>
</tr>
<tr>
<td>319</td>
<td>S</td>
<td>2744</td>
<td>1</td>
<td>0.0</td>
<td>1.0</td>
<td>licenseMgr</td>
</tr>
<tr>
<td>6823</td>
<td>S</td>
<td>2712</td>
<td>429</td>
<td>0.0</td>
<td>1.0</td>
<td>imish</td>
</tr>
<tr>
<td>6770</td>
<td>S</td>
<td>2668</td>
<td>1</td>
<td>0.0</td>
<td>1.0</td>
<td>imish</td>
</tr>
<tr>
<td>359</td>
<td>S</td>
<td>1824</td>
<td>1</td>
<td>0.0</td>
<td>0.7</td>
<td>nsm</td>
</tr>
<tr>
<td>339</td>
<td>S</td>
<td>1736</td>
<td>279</td>
<td>0.0</td>
<td>0.6</td>
<td>fileMgmt</td>
</tr>
<tr>
<td>291</td>
<td>S</td>
<td>1676</td>
<td>1</td>
<td>0.0</td>
<td>0.6</td>
<td>logd</td>
</tr>
<tr>
<td>375</td>
<td>S</td>
<td>1672</td>
<td>1</td>
<td>0.0</td>
<td>0.6</td>
<td>wccpd</td>
</tr>
<tr>
<td>279</td>
<td>S</td>
<td>1636</td>
<td>1</td>
<td>0.0</td>
<td>0.6</td>
<td>pmd</td>
</tr>
<tr>
<td>430</td>
<td>S</td>
<td>1636</td>
<td>1</td>
<td>0.0</td>
<td>0.6</td>
<td>stunnel</td>
</tr>
<tr>
<td>1370</td>
<td>S</td>
<td>1512</td>
<td>1</td>
<td>0.0</td>
<td>0.5</td>
<td>sshd</td>
</tr>
<tr>
<td>346</td>
<td>S</td>
<td>1448</td>
<td>1</td>
<td>0.0</td>
<td>0.5</td>
<td>mobd</td>
</tr>
<tr>
<td>340</td>
<td>S</td>
<td>1308</td>
<td>279</td>
<td>0.0</td>
<td>0.5</td>
<td>fileXferd</td>
</tr>
</tbody>
</table>

WS5100> service show reboot-history

Configured size of reboot history is 50

<table>
<thead>
<tr>
<th>Date &amp; Time</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aug 30 15:32:39 2006</td>
<td>startup</td>
</tr>
<tr>
<td>Aug 30 15:31:17 2006</td>
<td>shutdown (graceful:user)</td>
</tr>
<tr>
<td>Aug 30 13:31:13 2006</td>
<td>startup</td>
</tr>
<tr>
<td>Aug 29 18:40:38 2006</td>
<td>shutdown (ungraceful:unexpected cold restart)</td>
</tr>
<tr>
<td>Aug 29 18:39:15 2006</td>
<td>startup</td>
</tr>
<tr>
<td>Aug 28 12:38:09 2006</td>
<td>startup</td>
</tr>
<tr>
<td>Aug 23 13:33:02 2006</td>
<td>shutdown (ungraceful:unexpected cold restart)</td>
</tr>
<tr>
<td>Aug 21 13:10:09 2006</td>
<td>startup</td>
</tr>
<tr>
<td>Aug 17 15:10:21 2006</td>
<td>shutdown (graceful:user)</td>
</tr>
<tr>
<td>Aug 17 15:08:58 2006</td>
<td>startup</td>
</tr>
</tbody>
</table>
Aug 16 13:48:41 2006     startup
- - -                     shutdown (ungraceful:unexpected cold restart)
Aug 11 19:32:55 2006     startup

WS5100> service show startup-log
Aug 30 15:32:43 2006: %KERN-5-NOTICE: Linux version 2.6.13.4-ws-symbol
(wios-eng@wios-build) (gcc version 3.4.5) #1.
Aug 30 15:32:43 2006: %KERN-6-INFO: BIOS-provided physical RAM map:
Aug 30 15:32:43 2006: %KERN-6-INFO:  BIOS-e820: 0000000000000000 -
00000000009fc00 (usable).
Aug 30 15:32:43 2006: %KERN-6-INFO:  BIOS-e820: 000000000009fc00 -
00000000000a0000 (reserved).
Aug 30 15:32:43 2006: %KERN-6-INFO:  BIOS-e820: 00000000000a0000 -
00000000000a0000 (reserved).
Aug 30 15:32:43 2006: %KERN-6-INFO:  BIOS-e820: 00000000000e0000 -
00000000000f4000 (usable).
Aug 30 15:32:43 2006: %KERN-6-INFO:  BIOS-e820: 00000000000f4000 -
00000000000f5000 (ACPI data).
Aug 30 15:32:43 2006: %KERN-6-INFO:  BIOS-e820: 00000000000f5000 -
0000000001000000 (ACPI NVS).
Aug 30 15:32:43 2006: %KERN-6-INFO:  BIOS-e820: 0000000001000000 -
0000000001000000 (ACPI NVS).
Aug 30 15:32:43 2006: %KERN-6-INFO:  BIOS-e820: 0000000001000000 -
0000000001000000 (ACPI NVS).
Aug 30 15:32:43 2006: %KERN-6-INFO: DMI 2.3 present..
) @ 0x000f7720.
Aug 30 15:32:43 2006: KERN: ACPI: RSDT (v001 A M I OEMRSDT 0x09000512
MSFT 0x00000097) @ 0x0ff40000.
MSFT 0x00000097) @ 0x0ff40200.
Aug 30 15:32:43 2006: KERN: ACPI: MADT (v001 A M I OEMAPIC 0x09000512
MSFT 0x00000097) @ 0x0ff40300.
Aug 30 15:32:43 2006: KERN: ACPI: OEMB (v001 A M I OEMBIOS 0x09000512
MSFT 0x00000097) @ 0x0ff50040.
Aug 30 15:32:43 2006: KERN: ACPI: DSDT (v001 1ABVF 1ABVF007 0x00000007
INTL 0x02002026) @ 0x00000000.

WS5100> service show upgrade-history

Configured size of upgrade history is 50

<table>
<thead>
<tr>
<th>Date &amp; Time</th>
<th>Old Version</th>
<th>New Version</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aug 29 18:30:43 2006</td>
<td>3.0.0.0-180B</td>
<td>3.0.0.0-200B</td>
<td>Successful</td>
</tr>
<tr>
<td>Aug 17 15:07:03 2006</td>
<td>3.0.0.0-17872X</td>
<td>3.0.0.0-180B</td>
<td>Successful</td>
</tr>
<tr>
<td>Aug 11 19:29:41 2006</td>
<td>3.0.0.0-170B</td>
<td>3.0.0.0-17872X</td>
<td>Successful</td>
</tr>
<tr>
<td>Aug 11 19:28:52 2006</td>
<td>3.0.0.0-170B</td>
<td>3.0.0.0-170B</td>
<td>Unable to get update file. tftp: server says: File not found</td>
</tr>
<tr>
<td>Aug 09 17:30:25 2006</td>
<td>3.0.0.0-17174X</td>
<td>3.0.0.0-170B</td>
<td>Successful</td>
</tr>
<tr>
<td>Jul 26 15:17:14 2006</td>
<td>3.0.0.0-140D</td>
<td>3.0.0.0-17174X</td>
<td>Successful</td>
</tr>
<tr>
<td>Jul 26 15:16:40 2006</td>
<td>3.0.0.0-140D</td>
<td>3.0.0.0-140D</td>
<td>Unable to get update file. tftp: server says: File not found</td>
</tr>
<tr>
<td>Jul 26 15:16:08 2006</td>
<td>3.0.0.0-140D</td>
<td>3.0.0.0-140D</td>
<td>Unable to get update file. tftp: server says: File not found</td>
</tr>
<tr>
<td>Jul 19 19:52:38 2006</td>
<td>3.0.0.0-16786X</td>
<td>3.0.0.0-140D</td>
<td>Successful</td>
</tr>
<tr>
<td>Jul 19 19:52:07 2006</td>
<td>3.0.0.0-16786X</td>
<td>3.0.0.0-16786X</td>
<td>Unable to get update file. tftp: server says: File not found</td>
</tr>
</tbody>
</table>

WS5100>
2.1.6 terminal

Use this command to set the length/number of lines to be displayed on the terminal window.

Syntax

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

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>length</td>
<td>Set number of lines on a screen.</td>
</tr>
<tr>
<td>no</td>
<td>Negate a command or set its defaults.</td>
</tr>
<tr>
<td>width</td>
<td>Sets width/number of characters on a screen line.</td>
</tr>
</tbody>
</table>

Usage Guidelines

Example

```
WS5100>terminal length 100
WS5100>

WS5100>terminal width 200
WS5100>
```
2.2 show

Common Commands

This command is used to display the settings for the specified system component. There are a number of ways to invoke the show command:

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

Syntax

show [display_parameter]

Parameters

<table>
<thead>
<tr>
<th>Display Parameters</th>
<th>Description</th>
<th>Mode</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>autoinstall</td>
<td>Displays autoinstall configuration.</td>
<td>Common</td>
<td>page 2-22</td>
</tr>
<tr>
<td>banner</td>
<td>Displays message of the day login banner.</td>
<td>Common</td>
<td>page 2-23</td>
</tr>
<tr>
<td>commands</td>
<td>Displays command lists.</td>
<td>Common</td>
<td>page 2-24</td>
</tr>
<tr>
<td>crypto</td>
<td></td>
<td>Common</td>
<td>page 2-25</td>
</tr>
<tr>
<td>environment</td>
<td>Displays environmental information.</td>
<td>Common</td>
<td>page 2-29</td>
</tr>
<tr>
<td>history</td>
<td>Displays the session command history.</td>
<td>Common</td>
<td>page 2-29</td>
</tr>
<tr>
<td>interfaces</td>
<td>Displays interface status and configuration.</td>
<td>Common</td>
<td>page 2-30</td>
</tr>
<tr>
<td>ip</td>
<td>Displays internet protocol.</td>
<td>Common</td>
<td>page 2-32</td>
</tr>
<tr>
<td>ldap</td>
<td>Displays ldap server configuration parameters.</td>
<td>Common</td>
<td>page 2-38</td>
</tr>
<tr>
<td>licenses</td>
<td>Displays the installed licenses, if any.</td>
<td>Common</td>
<td>page 2-40</td>
</tr>
<tr>
<td>logging</td>
<td>Displays logging configuration and buffer.</td>
<td>Common</td>
<td>page 2-41</td>
</tr>
<tr>
<td>mac</td>
<td>Displays media access control IP configuration.</td>
<td>Common</td>
<td>page 2-42</td>
</tr>
<tr>
<td>management</td>
<td>Displays L3 management interface name.</td>
<td>Common</td>
<td>page 2-43</td>
</tr>
<tr>
<td>mobility</td>
<td>Displays mobility parameters.</td>
<td>Common</td>
<td>page 2-44</td>
</tr>
<tr>
<td>Display Parameters</td>
<td>Description</td>
<td>Mode</td>
<td>Example</td>
</tr>
<tr>
<td>--------------------</td>
<td>-------------</td>
<td>------</td>
<td>---------</td>
</tr>
<tr>
<td>ntp</td>
<td>Displays network time protocol.</td>
<td>Common</td>
<td>page 2-47</td>
</tr>
<tr>
<td>privilege</td>
<td>Displays current privilege level.</td>
<td>Common</td>
<td>page 2-49</td>
</tr>
<tr>
<td>radius</td>
<td>Displays radius configuration commands.</td>
<td>Common</td>
<td>page 2-50</td>
</tr>
<tr>
<td>redundancy-group</td>
<td>Displays redundancy group parameters.</td>
<td>Common</td>
<td>page 2-51</td>
</tr>
<tr>
<td>redundancy-history</td>
<td>Displays state transition history of the switch.</td>
<td>Common</td>
<td>page 2-53</td>
</tr>
<tr>
<td>redundancy-members</td>
<td>Displays redundancy group members in detail.</td>
<td>Common</td>
<td>page 2-54</td>
</tr>
<tr>
<td>snmp</td>
<td>Displays SNMP engine parameters.</td>
<td>Common</td>
<td>page 2-55</td>
</tr>
<tr>
<td>snmp-server</td>
<td>Displays SNMP engine parameters.</td>
<td>Common</td>
<td>page 2-56</td>
</tr>
<tr>
<td>terminal</td>
<td>Displays terminal configuration parameters.</td>
<td>Common</td>
<td>page 2-59</td>
</tr>
<tr>
<td>timezone</td>
<td>Displays timezone.</td>
<td>Common</td>
<td>page 2-60</td>
</tr>
<tr>
<td>users</td>
<td>Displays information about terminal lines.</td>
<td>Common</td>
<td>page 2-61</td>
</tr>
<tr>
<td>version</td>
<td>Displays software and hardware version.</td>
<td>Common</td>
<td>page 2-62</td>
</tr>
<tr>
<td>wireless</td>
<td>Displays wireless configuration commands.</td>
<td>Common</td>
<td>page 2-63</td>
</tr>
<tr>
<td>access-list</td>
<td>Displays access list Internet Protocol (IP) configuration.</td>
<td>Privilege/Global Config</td>
<td>page 2-70</td>
</tr>
<tr>
<td>alarm-log</td>
<td>Displays all alarms currently in the system.</td>
<td>Privilege/Global Config</td>
<td>page 2-71</td>
</tr>
<tr>
<td>boot</td>
<td>Displays boot configuration.</td>
<td>Privilege/Global Config</td>
<td>page 2-72</td>
</tr>
<tr>
<td>clock</td>
<td>Displays system clock.</td>
<td>Privilege/Global Config</td>
<td>page 2-73</td>
</tr>
<tr>
<td>debugging</td>
<td>Displays debugging setting.</td>
<td>Privilege/Global Config</td>
<td>page 2-74</td>
</tr>
<tr>
<td>file</td>
<td>Displays filesystem information.</td>
<td>Privilege/Global Config</td>
<td>page 2-75</td>
</tr>
</tbody>
</table>
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 | Use this to enter 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
autoinstall (config|cluster-config|image) enable
autoinstall (config|cluster-config|image) url LINE
autoinstall (config|cluster-config|image) enable
autoinstall (config|cluster-config|image) url LINE
autoinstall (config|cluster-config|image) enable
autoinstall (config|cluster-config|image) url LINE
autoinstall start
clear crypto ike sa ( A.B.C.D |)
clear crypto ike sa ( A.B.C.D |)
clear crypto ipsec sa (A.B.C.D |)
clear crypto ipsec sa (A.B.C.D |)
clear mobility mu (AA-BB-CC-DD-EE-FF|home-database|foreign-database|all)
clear mobility mu (AA-BB-CC-DD-EE-FF|home-database|foreign-database|all)
clear mobility mu (AA-BB-CC-DD-EE-FF|home-database|foreign-database|all)
clear mobility mu (AA-BB-CC-DD-EE-FF|home-database|foreign-database|all)
clear mobility mu-log
clear mobility peer-log
clear mobility peer-statistics (A.B.C.D|)
clear mobility peer-statistics (A.B.C.D|)
clear wireless-statistics
clrscr
cluster-cli enable
debug certmgr ( error|info|all )
debug certmgr ( error|info|all )
debug certmgr ( error|info|all )
debug ip ssh
debug mobility (cc|error|forwarding|mu|packet|peer|system)
debug mobility (cc|error|forwarding|mu|packet|peer|system)
debug mobility (cc|error|forwarding|mu|packet|peer|system)
debug mobility (cc|error|forwarding|mu|packet|peer|system)
debug mobility (cc|error|forwarding|mu|packet|peer|system)
debug mobility (cc|error|forwarding|mu|packet|peer|system)
debug mobility (cc|error|forwarding|mu|packet|peer|system)
-- MORE --, next page: Space, next line: Enter, quit: Control-C
.....................................................(contd)
### 2.2.4 crypto

*Common to all modes*

**Syntax**

```markdown
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**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipsec</td>
<td>ipsec</td>
</tr>
<tr>
<td>sa</td>
<td>security association</td>
</tr>
<tr>
<td>security-association</td>
<td>security association</td>
</tr>
<tr>
<td>lifetime</td>
<td>lifetime</td>
</tr>
<tr>
<td>transformset</td>
<td>transformset</td>
</tr>
<tr>
<td>isakmp</td>
<td>isakmp</td>
</tr>
<tr>
<td>policy</td>
<td>policy</td>
</tr>
<tr>
<td>sa</td>
<td>security association</td>
</tr>
<tr>
<td>key</td>
<td>Authentication key management</td>
</tr>
<tr>
<td>mypubkey</td>
<td>Public Key</td>
</tr>
<tr>
<td>map</td>
<td>map</td>
</tr>
<tr>
<td>interface</td>
<td>interface</td>
</tr>
<tr>
<td>tag</td>
<td>tag</td>
</tr>
<tr>
<td>pki</td>
<td>Public Key Infrastructure commands</td>
</tr>
<tr>
<td>request</td>
<td>Certificate Request</td>
</tr>
<tr>
<td>trustpoints</td>
<td>Show trustpoints</td>
</tr>
</tbody>
</table>
Usage Guidelines

Security engine periodically updates the IPSec and Isakamp statistics for every 60 seconds.

Example

```
WS5100(config)#show crypto pki request tptest
-----BEGIN CERTIFICATE REQUEST-----
MIIB2zCCAUQCAQAwaDELMAkGA1UEBhMCaW4xJjAQBgNVBAgTCWthcm5hdGFrYTESE
MBAGA1UEBXJYUMQxJGMRQDAgEBGCQDojBGA1UEBhMCaW4xJjAQBgNVBAcTCAo=
ZDAREMBAGA1UEAxMjZGVEQDQTEGA1UEBxMJYWYy7fX8c2MBAGA1UEBxMjZGVEQD
QTEGB2xJCYwMIGFMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgqQC3s8ZgAQCgYDK
-----END CERTIFICATE REQUEST-----

WS5100(config)#show crypto pki trustpoints

Trustpoint :default-trustpoint
-----------------------------------------------
Server certificate configured
Subject Name: Symbol Technologies
Issuer 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: monarch
Organizational Unit: wid
Location: bangalore
State: karnataka
Country: in
email: testuser@domain.com
Issuer Name: monarch
Organizational Unit: wid
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

```plaintext
show environment
```

Parameters

None.

Example

```plaintext
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|tunnel|vlan)
```

Parameters

<table>
<thead>
<tr>
<th>IFNAME</th>
<th>eth</th>
<th>switchport</th>
<th>tunnel</th>
<th>vlan</th>
</tr>
</thead>
</table>

Usage Guidelines

Example

```
WS5100(config)#show interfaces eth1
Interface eth1
   Hardware Type Ethernet, Interface Mode Layer 2, address is 00-a0-f8-65-b0-4e
      index 2 metric 1 mtu 1500 <UP,BROADCAST,RUNNING,MULTICAST>
      Speed: Admin Auto, Operational 100M
      Duplex: Admin Auto, Operational Full
      Switchport Settings: Mode: Access, Access Vlan: 2100
      input packets 38766, bytes 9483540, dropped 0, multicast packets 13377
      input errors 0, length 0, overrun 0, CRC 0, frame 0, fifo 0, missed 0
      output packets 4, bytes 336, dropped 0
      output errors 0, aborted 0, carrier 0, fifo 0, heartbeat 0, window 0
      collisions 0

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
```
WS5100(config)#interface tunnel 1
Sep 14 18:38:17 2006: %DAEMON-5-NOTICE: WIOS_SECURITYMGR[414]: DNSALG: Application gateway started

WS5100(config-if)#show interfaces tunnel 1
Interface tunnel1
   Hardware Type Tunnel, Interface Mode Layer 3
   index 9 metric 1 mtu 1476  <UP,RUNNING,NOARP>
   Tunnel source UNKNOWN, destination UNKNOWN
   Tunnel protocol/transport GRE/IP, Tunnel TTL 255
   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
   collisions 0
2.2.8 ip

Common to all modes

Syntax

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

Parameters

<table>
<thead>
<tr>
<th>access-group</th>
<th>Display ACLs attached to an interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>IFNAME</td>
<td>The name of the interface to which the ACL is associated. It lists the details of ACLs configured on the particular Layer 3 or Layer 2 interface.</td>
</tr>
<tr>
<td>eth</td>
<td>The name of the ethernet interface to which the ACL is associated.</td>
</tr>
<tr>
<td>vlan</td>
<td>The name of the VLAN interface to which the ACL is associated.</td>
</tr>
<tr>
<td>arp</td>
<td>Display Address Resolution Protocol</td>
</tr>
<tr>
<td>ddns</td>
<td>Displays DDNS configuration</td>
</tr>
<tr>
<td>binding</td>
<td>DNS Address bindings</td>
</tr>
<tr>
<td>dhcp</td>
<td>Displays DHCP Server Configuration</td>
</tr>
<tr>
<td>bind</td>
<td>DNS Address bindings</td>
</tr>
<tr>
<td>pool</td>
<td>DHCP Pools</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------</td>
<td>-------------------------------------------------------</td>
</tr>
<tr>
<td>dhcp-vendor-options</td>
<td>DHCP Option 43 parameters received from DHCP server</td>
</tr>
<tr>
<td>domain-name</td>
<td>Default domain for DNS</td>
</tr>
<tr>
<td>http</td>
<td>Hyper Text Transfer Protocol</td>
</tr>
<tr>
<td>secure-server</td>
<td>Secure HTTP server</td>
</tr>
<tr>
<td>server</td>
<td>HTTP server</td>
</tr>
<tr>
<td>interface</td>
<td>IP interface status and configuration</td>
</tr>
<tr>
<td>IFNAME</td>
<td>Interface name</td>
</tr>
<tr>
<td>brief</td>
<td>Brief summary of IP status and configuration</td>
</tr>
<tr>
<td>tunnel</td>
<td>Tunnel Interface</td>
</tr>
<tr>
<td>vlan</td>
<td>Vlan Interface</td>
</tr>
<tr>
<td>name-server</td>
<td>DNS nameservers</td>
</tr>
<tr>
<td>route</td>
<td>IP routing table</td>
</tr>
<tr>
<td>A.B.C.D</td>
<td>Network in the IP routing table to display</td>
</tr>
<tr>
<td>A.B.C.D/M</td>
<td>IP prefix <code>&lt;network&gt;/&lt;length&gt;</code>, e.g., 35.0.0.0/8</td>
</tr>
<tr>
<td>detail</td>
<td>IP routing table in detail</td>
</tr>
<tr>
<td>routing</td>
<td>IP routing status</td>
</tr>
<tr>
<td>ssh</td>
<td>Secured Shell (SSH) server</td>
</tr>
<tr>
<td>telnet</td>
<td>Telnet server</td>
</tr>
</tbody>
</table>
Usage Guidelines

1. It has been noted that the interface status and vlan status is displayed as UP inspite of a disconnection. In such a case you need to shutdown the vlan. Follow the steps given below:

   a. Check the status of 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 status of the VLAN is UP even if eth1 / eth2 is disconnected then 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. Now check the status and you will note that VLAN has now been disassociated and the status is now 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 instance may also happen when a DHCP interface is disconnected. The DHCP is not effected though because it runs on a virtual interface and not on the physical interface. In this case it is the physical interface that is disconnected not the virtual interface. In WS5100, when the ethernet interface comes back up, it will restart the dhcp client on any virtual interfaces (SVIs) of which the physical interface is a member port. This ensures that if the interface was disconnected and reconnected to a different interface it will get a new ip address, route, name server, domain name etc. corresponding to the new dhcp server/scope.
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#show ip dhcp pool

ip dhcp pool pooll
  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 pool10
  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`

<table>
<thead>
<tr>
<th>Interface</th>
<th>IP-Address</th>
<th>Status</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan1</td>
<td>157.235.208.233(DHCP)</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>tunnel1</td>
<td>unassigned</td>
<td>up</td>
<td>up</td>
</tr>
</tbody>
</table>

WS5100# `show ip interface tunnel 1 brief`

<table>
<thead>
<tr>
<th>Interface</th>
<th>IP-Address</th>
<th>Status</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>tunnel1</td>
<td>unassigned</td>
<td>up</td>
<td>up</td>
</tr>
</tbody>
</table>

WS5100# `show ip interface vlan 1 brief`

<table>
<thead>
<tr>
<th>Interface</th>
<th>IP-Address</th>
<th>Status</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan1</td>
<td>157.235.208.233(DHCP)</td>
<td>up</td>
<td>up</td>
</tr>
</tbody>
</table>

WS5100# `show ip name-server`
157.235.3.195 dynamic
157.235.3.196 dynamic

WS5100# `show ip nat translations inside source`

<table>
<thead>
<tr>
<th>S/D Dir</th>
<th>Actual Address</th>
<th>NATed Address</th>
<th>ACL</th>
<th>Overload-If</th>
</tr>
</thead>
</table>

WS5100# `show ip nat translations outside destination`

<table>
<thead>
<tr>
<th>S/D Dir</th>
<th>Actual Address</th>
<th>NATed Address</th>
<th>ACL</th>
<th>Overload-If</th>
</tr>
</thead>
</table>

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**

<table>
<thead>
<tr>
<th>ldap</th>
<th>LDAP Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>configuration</td>
<td>ldap server configuration parameters</td>
</tr>
<tr>
<td>primary</td>
<td>primary ldap server</td>
</tr>
<tr>
<td>secondary</td>
<td>secondary ldap server</td>
</tr>
</tbody>
</table>

**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: 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 19:11:58 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

2.2.12 mac

- Common to all modes

Syntax

```
show mac (access-list)
```

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>access-list</td>
<td>List MAC access lists</td>
</tr>
</tbody>
</table>

Example
2.2.13 management

Syntax

   show management

Parameters

None.

Example

   WS5100>show management
   Mgmt Interface: vlan1
   WS5100>
2.2.14 mobility

Common to all modes

Syntax

show mobility (forwarding | global | mu (AA-BB-CC-DD-EE-FF | detail))
mu-log | mu-statistics (AA-BB-CC-DD-EE-FF) | peer (A.B.C.D | detail) | peer-log)

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mobility</td>
<td>Display Mobility Parameters</td>
</tr>
<tr>
<td>forwarding</td>
<td>Display MU Info in the forwarding plane</td>
</tr>
<tr>
<td>global</td>
<td>Global Mobility parameters</td>
</tr>
<tr>
<td>mu</td>
<td>Mobility MUs</td>
</tr>
<tr>
<td>AA-BB-CC-DD-EE-FF</td>
<td>MAC address of the MU</td>
</tr>
<tr>
<td>detail</td>
<td>Detailed information display</td>
</tr>
<tr>
<td>mu-log</td>
<td>Display Mobility MU Event Log</td>
</tr>
<tr>
<td>mu-statistics</td>
<td>Display Mobility MU Stats</td>
</tr>
<tr>
<td>AA-BB-CC-DD-EE-FF</td>
<td>MAC address of the MU</td>
</tr>
<tr>
<td>peer</td>
<td>Display Mobility peers</td>
</tr>
<tr>
<td>A.B.C.D</td>
<td>IP address of Peer</td>
</tr>
<tr>
<td>detail</td>
<td>Detailed information display</td>
</tr>
<tr>
<td>peer-log</td>
<td>Display Mobility Peer Event Log</td>
</tr>
</tbody>
</table>
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
Mac-Address        IP-Address       State       Tunnel         HS-Vlan
WS5100>

WS5100> show mobility global
  Mobility Global Parameters
  Admin-Status                      : DISABLED
  Operational-Status                : DISABLED (Admin-status is DISABLED)
  Local-Address                     : 0.0.0.0
  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-face           |Rx                                         |Tx
   wlan_port          |unicast    MC         BC         Error     |unicast    MC
   BC          Error
   0          0         0         0         0         0         0         0
2.2.15 ntp

Common to all modes

Syntax

show ntp (association (detail)|status)

Parameters

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ntp</td>
<td>Network time protocol</td>
</tr>
<tr>
<td>association</td>
<td>NTP associations</td>
</tr>
<tr>
<td>detail</td>
<td>Displays NTP association details.</td>
</tr>
<tr>
<td>status</td>
<td>Displays NTP status.</td>
</tr>
</tbody>
</table>

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
filtoffset = 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00
filterror = 16000.00 16000.00 16000.00 16000.00 16000.00 16000.00 16000.00 16000.00 16000.00
WS5100(config)#show ntp status
Clock is unsynchronized, stratum 16, reference is INIT
actual frequency is 0.0000 Hz, precision is 2**-20
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 1395.000 msec,
2.2.16 privilege

Common to all modes

Syntax

show privilege

Parameters

None.

Example

WS5100>show privilege
Current user privilege: superuser

WS5100>
2.2.17 radius

Common to all modes

Syntax

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

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>radius</td>
<td>Radius configuration commands</td>
</tr>
<tr>
<td>configuration</td>
<td>radius server configuration parameters</td>
</tr>
<tr>
<td>eap</td>
<td>Eap parameters</td>
</tr>
<tr>
<td>configuration</td>
<td>Eap configuration</td>
</tr>
<tr>
<td>group</td>
<td>Radius group configuration</td>
</tr>
<tr>
<td>nas</td>
<td>client information</td>
</tr>
<tr>
<td>A.B.C.D/M</td>
<td>client ip address / mask</td>
</tr>
<tr>
<td>proxy</td>
<td>proxy information</td>
</tr>
<tr>
<td>rad-user</td>
<td>Radius user information</td>
</tr>
<tr>
<td>trust-point</td>
<td>Radius trust-point configuration</td>
</tr>
</tbody>
</table>

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
2.2.18 redundancy-group

Common to all modes

Syntax

    show redundancy-group (config | runtime)

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>config</td>
<td>Display configured redundancy group information.</td>
</tr>
<tr>
<td>runtime</td>
<td>Display runtime redundancy group information</td>
</tr>
</tbody>
</table>

Example

WS5100> 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 : 0
Switch running image version : 3.0.0.0-200B

WS5100>

WS5100> 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
Radios in selfhealing mode : 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

WS5100>

WS5100(config)#show redundancy-group

Redundancy Group Configuration Detail
Redundancy Feature : Enabled
Redundancy group ID : 1
Redundancy Mode : Primary
Redundancy Interface IP : 10.10.10.10
Number of configured peer(s) : 1
Heartbeat-period : 5 Seconds
Hold-period : 15 Seconds
Discovery-period : 30 Seconds
Handle STP : Disabled
Switch Installed License : 48
Switch running image version : 3.0.0.0-19635X

Redundancy Group Runtime Information
Redundancy Protocol Version : 2.0
Redundancy Group License : 48
Cluster AP Adoption Count : 1
Switch AP Adoption Count : 1
Redundancy State : Discovery
Radio Portals adopted by Group : 2
Radio Portals adopted by this Switch : 2
Rogue APs detected in this Group : 0
Rogue APs detected by this Switch : 0
MUs associated in this Group : 1
MUs associated in this Switch : 1
Selfhealing APs in this Group : 0
Selfhealing APs in this Switch : 0
Group maximum AP adoption capacity : 48
Switch Adoption capacity : 48
Established Peer(s) Count : 0
Redundancy Group Connectivity status : Not all members connected
2.2.19 redundancy-history

Common to all modes

Syntax

show redundancy-history

Parameters

None.

Example

WS5100>show redundancy-history
State Transition History

<table>
<thead>
<tr>
<th>Time</th>
<th>Event Triggered</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sep 06 18:20:56 2006</td>
<td>Redundancy Disabled</td>
<td>Disabled</td>
</tr>
</tbody>
</table>

WS5100>
2.2.20  redundancy-members

- Common to all modes

Syntax

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

Parameters

<table>
<thead>
<tr>
<th>A.B.C.D</th>
<th>IP address of member switch</th>
</tr>
</thead>
</table>

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
### 2.2.21 snmp

- **Common to all modes**

**Syntax**

```
show snmp (user(manager | operator))
```

**Parameters**

<table>
<thead>
<tr>
<th>User</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>user</td>
<td>Displays the SNMP user.</td>
</tr>
<tr>
<td>manager</td>
<td>show manager information.</td>
</tr>
<tr>
<td>operator</td>
<td>show operator information.</td>
</tr>
</tbody>
</table>

**Example**

```
WS5100>show snmp user manager
userName    access  engineId                Authentication  Encryption
snmpmanager  ro      80000184017f000001      MD5                 DES
snmpoperator ro      80000184017f000001      MD5                 DES
WS5100>
```

```
WS5100>show snmp user operator
userName    access  engineId                Authentication
snmpmanager  ro      80000184017f000001      MD5                 DES
snmpoperator ro      80000184017f000001      MD5                 DES
WS5100>
```
### 2.2.22 snmp-server

- **Common to all modes**

**Syntax**

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

**Parameters**

<table>
<thead>
<tr>
<th>Module Type</th>
<th>Trap Type</th>
<th>Enabled? [Y/N]</th>
</tr>
</thead>
<tbody>
<tr>
<td>snmp</td>
<td>coldstart</td>
<td>N</td>
</tr>
<tr>
<td>snmp</td>
<td>linkdown</td>
<td>N</td>
</tr>
<tr>
<td>snmp</td>
<td>linkup</td>
<td>N</td>
</tr>
<tr>
<td>snmp</td>
<td>authenticationFail</td>
<td>N</td>
</tr>
<tr>
<td>nsm</td>
<td>dhcpIPChanged</td>
<td>N</td>
</tr>
<tr>
<td>redundancy</td>
<td>memberUp</td>
<td>N</td>
</tr>
<tr>
<td>redundancy</td>
<td>memberDown</td>
<td>N</td>
</tr>
<tr>
<td>redundancy</td>
<td>memberMisConfigured</td>
<td>N</td>
</tr>
<tr>
<td>redundancy</td>
<td>adoptionExceeded</td>
<td>N</td>
</tr>
<tr>
<td>redundancy</td>
<td>grpAuthLevelChanged</td>
<td>N</td>
</tr>
<tr>
<td>misc</td>
<td>lowFsSpace</td>
<td>N</td>
</tr>
<tr>
<td>misc</td>
<td>processMaxRestartsReached</td>
<td>N</td>
</tr>
<tr>
<td>wireless station</td>
<td>associated</td>
<td>N</td>
</tr>
<tr>
<td>wireless station</td>
<td>disassociated</td>
<td>N</td>
</tr>
<tr>
<td>wireless station</td>
<td>deniedAssociationOnCapability</td>
<td>N</td>
</tr>
<tr>
<td>wireless station</td>
<td>deniedAssociationOnShortPream</td>
<td>N</td>
</tr>
</tbody>
</table>

**Example**

WS5100>show snmp-server traps

Global enable flag for Traps

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  |
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  |
<table>
<thead>
<tr>
<th>wireless station</th>
<th>deniedAssociationOnSpectrum</th>
<th>N</th>
</tr>
</thead>
<tbody>
<tr>
<td>wireless station</td>
<td>deniedAssociationOnErr</td>
<td>N</td>
</tr>
<tr>
<td>wireless station</td>
<td>deniedAssociationOnSSID</td>
<td>N</td>
</tr>
<tr>
<td>wireless station</td>
<td>deniedAssociationOnRates</td>
<td>N</td>
</tr>
<tr>
<td>wireless station</td>
<td>deniedAssociationOnInvalidWPAWPA2IE</td>
<td>N</td>
</tr>
<tr>
<td>wireless station</td>
<td>deniedAssociationAsPortCapacityReached</td>
<td>N</td>
</tr>
<tr>
<td>wireless station</td>
<td>tkipCounterMeasures</td>
<td>N</td>
</tr>
<tr>
<td>wireless station</td>
<td>deniedAuthentication</td>
<td>N</td>
</tr>
<tr>
<td>wireless station</td>
<td>radiusAuthFailed</td>
<td>N</td>
</tr>
<tr>
<td>wireless radio</td>
<td>adopted</td>
<td>N</td>
</tr>
<tr>
<td>wireless radio</td>
<td>unadopted</td>
<td>N</td>
</tr>
<tr>
<td>wireless radio</td>
<td>detectedRadar</td>
<td>N</td>
</tr>
<tr>
<td>wireless ap-detection</td>
<td>externalAPDetected</td>
<td>N</td>
</tr>
<tr>
<td>wireless self-healing</td>
<td>activated</td>
<td>N</td>
</tr>
<tr>
<td>wireless ids</td>
<td>excessiveAuthAssociation</td>
<td>N</td>
</tr>
<tr>
<td>wireless ids</td>
<td>excessiveProbes</td>
<td>N</td>
</tr>
<tr>
<td>misc</td>
<td>savedConfigModified</td>
<td>N</td>
</tr>
</tbody>
</table>

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> 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> 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>
2.2.23 terminal

Common to all modes

Syntax

show terminal

Parameters

None.

Example

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

- Common to all modes

**Syntax**

```
show timezone
```

**Parameters**

None.

**Example**

```
WS5100>show timezone
Timezone is Etc/UTC
WS5100>
```
### 2.2.25 users

- **Common to all modes**

**Syntax**

```plaintext
show users
```

**Parameters**

None.

**Example**

```
WS5100> show users
Line       PID   User        Uptime      Location
0 con 0  306               6d07h11m     ttyS0
130 vty 0  1961               02:51:45     0
WS5100>
```
2.2.26 version

- Common to all modes

Syntax

show version (verbose)

Parameters

<table>
<thead>
<tr>
<th>verbose</th>
<th>Display software &amp; hardware details</th>
</tr>
</thead>
</table>

Example

WS5100>show version
WS5100 version 3.0.0.0-200B
Copyright (c) 2006 Symbol Technologies, Inc.
Booted from primary.
Switch uptime is 6 days, 7 hours 23 minutes
CPU is Intel(R) Pentium(R) 4 CPU 2.00GHz
256220 kB of on-board RAM
ide device hda disk model Kouwell DOM capacity 501760 blocks, cache 0
WS5100>

WS5100>show version verbose
WS5100 version 3.0.0.0-200B
Copyright (c) 2006 Symbol Technologies, Inc.
Booted from primary.
Switch uptime is 6 days, 7 hours 22 minutes
CPU is Intel(R) Pentium(R) 4 CPU 2.00GHz
256220 kB of on-board RAM
ide device hda disk model Kouwell DOM capacity 501760 blocks, cache 0
Failed to open /proc/pci for input
WS5100>
2.2.27 wireless

Common to all modes

Syntax


show wireless ap (<1-48>|AA-BB-CC-DD-EE-FF)
show wireless ap-detection-config
Show wireless ap-images
show wireless ap-unadopted
show wireless approved-aps
show wireless channel-power (11a (indoor | outdoor) | 11b (indoor | outdoor) | 11bg indoor | outdoor))
show wireless config
show wireless hotspot-config <1-32>
show wireless ids (filter-list)
show wireless mac-auth-local<1-1000>
show wireless mobile-unit (<1-4096> | AA-BB-CC-DD-EE-FF | statistics)
show wireless phrase-to-key (wep128 | wep64)
show wireless qos-mapping (wire-to-wireless | wireless-to-wired)
show wireless radio ( <1-1000> | beacon-table | config ( <1-1000> | default-11a | default-11b | default-11bg) | monitor-table | statistics)
show wireless regulatory (country codes)
show wireless self-heal-config <1-1000>
show wireless sensor (default-config | discovered-sensors)
show wireless unapproved-aps
show wireless wireless-switch-statistics (detail)
show wireless wlan (config( <1-32> | all | enabled) | statistics <1-32>)}
### Parameters

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ap</strong></td>
<td>Status of adopted access-port</td>
</tr>
<tr>
<td>&lt;1-48&gt;</td>
<td>The index of the access-port for detailed information</td>
</tr>
<tr>
<td>AA-BB-CC-DD-EE-FF</td>
<td>The MAC address of a access-port for detailed information</td>
</tr>
<tr>
<td><strong>ap-detection-config</strong></td>
<td>Detected-AP Configuration Parameters</td>
</tr>
<tr>
<td><strong>ap-images</strong></td>
<td>List of access-port images on the wireless switch</td>
</tr>
<tr>
<td><strong>ap-unadopted</strong></td>
<td>List of unadopted access-port</td>
</tr>
<tr>
<td><strong>approved-aps</strong></td>
<td>Approved APs seen by access-port scans</td>
</tr>
<tr>
<td><strong>channel-power</strong></td>
<td>List of available channel and power levels for a radio</td>
</tr>
<tr>
<td>11a</td>
<td>radio is of type 802.11a</td>
</tr>
<tr>
<td>11b</td>
<td>radio is of type 802.11b</td>
</tr>
<tr>
<td>11bg</td>
<td>radio is of type 802.11bg</td>
</tr>
<tr>
<td>indoor</td>
<td>radio is placed indoor</td>
</tr>
<tr>
<td>outdoor</td>
<td>radio is placed outdoor</td>
</tr>
<tr>
<td><strong>config</strong></td>
<td>Wireless Configuration Parameters</td>
</tr>
<tr>
<td><strong>hotspot-config</strong></td>
<td>Wlan hotspot configuration</td>
</tr>
<tr>
<td>&lt;1-32&gt;</td>
<td>A wlan index &lt;1-32&gt;</td>
</tr>
<tr>
<td><strong>ids</strong></td>
<td>Intrusion detection parameters</td>
</tr>
<tr>
<td><strong>filter-list</strong></td>
<td>Display the list of currently filtered mobile-units</td>
</tr>
<tr>
<td><strong>mac-auth-local</strong></td>
<td>list out the mac-auth-local entries</td>
</tr>
<tr>
<td>&lt;1-1000&gt;</td>
<td>mac-auth-local entry to display</td>
</tr>
<tr>
<td><strong>mobile-unit</strong></td>
<td>Details of associated mobile-units</td>
</tr>
<tr>
<td>&lt;1-4096&gt;</td>
<td>Index of mobile-unit</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>AA-BB-CC-DD-EE-FF</td>
<td>MAC address of mobile-unit</td>
</tr>
<tr>
<td>statistics</td>
<td>mobile-unit rf statistics</td>
</tr>
<tr>
<td><strong>phrase-to-key</strong></td>
<td>display the WEP keys generated by a passphrase</td>
</tr>
<tr>
<td>wep128</td>
<td>display WEP128 keys</td>
</tr>
<tr>
<td>wep64</td>
<td>display WEP64 keys</td>
</tr>
<tr>
<td><strong>qos-mapping</strong></td>
<td>Quality of Service mappings used for mapping WMM access categories and 802.1p / DSCP tags.</td>
</tr>
<tr>
<td>wired-to-wireless</td>
<td>Mappings used when traffic is switched from wired to the wireless side.</td>
</tr>
<tr>
<td>wireless-to-wired</td>
<td>Mappings used when traffic is switched from wireless to the wired side.</td>
</tr>
<tr>
<td><strong>radio</strong></td>
<td>Radio related commands</td>
</tr>
<tr>
<td>&lt;1-1000&gt;</td>
<td>A single radio index</td>
</tr>
<tr>
<td>beacon-table</td>
<td>The Radio-to-Radio beacon table</td>
</tr>
<tr>
<td>config</td>
<td>Radio configuration</td>
</tr>
<tr>
<td>&lt;1-1000&gt;</td>
<td>A single radio index</td>
</tr>
<tr>
<td>default-11a</td>
<td>default 11a configuration template</td>
</tr>
<tr>
<td>default-11b</td>
<td>default 11b configuration template</td>
</tr>
<tr>
<td>default-11bg</td>
<td>default 11bg configuration template</td>
</tr>
<tr>
<td>monitor-table</td>
<td>The Radio-to-Radio monitoring table</td>
</tr>
<tr>
<td>statistics</td>
<td>Radio statistics</td>
</tr>
<tr>
<td><strong>regulatory</strong></td>
<td>Regulatory (allowed channel/power) information for a particular country.</td>
</tr>
<tr>
<td><strong>self-heal-config</strong></td>
<td>Self-Healing Configuration Parameters</td>
</tr>
<tr>
<td>&lt;1-1000&gt;</td>
<td>A single radio index</td>
</tr>
<tr>
<td>all</td>
<td>All Configured radios</td>
</tr>
<tr>
<td><strong>sensor</strong></td>
<td>Wireless Intrusion Protection System parameters</td>
</tr>
</tbody>
</table>
Example

```plaintext
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
max-detected-aps         : 100
mu-assisted scan         : disabled
mu-assisted scan refresh : 1800 seconds
configured approved-aps  :
Index | Bss Mac           | Ssid
-------------------------------------------------------
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
```
Common Commands

<p>| | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>ap300</td>
<td>AP300-IDS-Sensor</td>
<td>295064</td>
<td>00.00-04</td>
</tr>
<tr>
<td>4</td>
<td>ap100</td>
<td>AP100</td>
<td>31034</td>
<td>02.05-00</td>
</tr>
<tr>
<td>5</td>
<td>ap4131</td>
<td>AP4131</td>
<td>191440</td>
<td>07.00-01</td>
</tr>
<tr>
<td>6</td>
<td>ap4131</td>
<td>Revert-AP4131</td>
<td>665704</td>
<td>00.00-00</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Excessive Operations</th>
<th>Threshold(mu radio switch)</th>
<th>Filter-Ageout</th>
</tr>
</thead>
<tbody>
<tr>
<td>probe-requests</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>association-requests</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>disassociations</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>authentication-fails</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>crypto-replay-fails</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>80211-replay-fails</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>decryption-fails</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>unassoc-frames</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>eap-starts</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
### Anomaly Detection

<table>
<thead>
<tr>
<th>Anomaly Lookup</th>
<th>Status</th>
<th>Filter-Ageout</th>
</tr>
</thead>
<tbody>
<tr>
<td>probe-requests</td>
<td>disabled</td>
<td>60 Sec</td>
</tr>
<tr>
<td>association-requests</td>
<td>disabled</td>
<td>60 Sec</td>
</tr>
<tr>
<td>disassociations</td>
<td>disabled</td>
<td>60 Sec</td>
</tr>
<tr>
<td>authentication-fails</td>
<td>disabled</td>
<td>60 Sec</td>
</tr>
<tr>
<td>crypto-replay-fails</td>
<td>disabled</td>
<td>60 Sec</td>
</tr>
<tr>
<td>80211-replay-fails</td>
<td>disabled</td>
<td>60 Sec</td>
</tr>
<tr>
<td>decryption-fails</td>
<td>disabled</td>
<td>60 Sec</td>
</tr>
<tr>
<td>unassoc-frames</td>
<td>disabled</td>
<td>60 Sec</td>
</tr>
<tr>
<td>eap-starts</td>
<td>disabled</td>
<td>60 Sec</td>
</tr>
<tr>
<td>null-destination</td>
<td>disabled</td>
<td>60 Sec</td>
</tr>
<tr>
<td>same-source-destination</td>
<td>disabled</td>
<td>60 Sec</td>
</tr>
<tr>
<td>multicast-source</td>
<td>disabled</td>
<td>60 Sec</td>
</tr>
<tr>
<td>weak-wep-iv</td>
<td>disabled</td>
<td>60 Sec</td>
</tr>
<tr>
<td>tkip-countermeasures</td>
<td>disabled</td>
<td>60 Sec</td>
</tr>
<tr>
<td>invalid-frame-length</td>
<td>disabled</td>
<td>60 Sec</td>
</tr>
</tbody>
</table>

WS5100>

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

WS5100>

WS5100> `show wireless mobile-unit statistics`

% Error: None of the mobile-units are associated!!
2.2.28 access-list

This CLI command lists all the access lists (numbered and named) configured on the switch. The numbered access list displays all numbered ACLs configured and the named access-list displays the details of the name ACL configured.

Syntax

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

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;1-99&gt;</td>
<td>IP standard access list</td>
</tr>
<tr>
<td>&lt;100-199&gt;</td>
<td>IP extended access list</td>
</tr>
<tr>
<td>&lt;1300-1999&gt;</td>
<td>IP standard access list (expanded range)</td>
</tr>
<tr>
<td>&lt;2000-2699&gt;</td>
<td>IP extended access list (expanded range)</td>
</tr>
<tr>
<td>WORD</td>
<td>Name of ACL</td>
</tr>
</tbody>
</table>

Example
### 2.2.29 alarm-log

- **Privilege / Global Config**

#### Syntax

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

#### Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;1-65535&gt;</code></td>
<td>Display details for specific alarm id</td>
</tr>
<tr>
<td>acknowledged</td>
<td>Display acknowledged alarms currently in the system</td>
</tr>
<tr>
<td>all</td>
<td>Display all alarms currently in the system</td>
</tr>
<tr>
<td>count</td>
<td>Display count of alarms currently in the system</td>
</tr>
<tr>
<td>new</td>
<td>Display new alarms currently in the system</td>
</tr>
<tr>
<td>severity-to-limit</td>
<td>Display all alarms having specified or higher severity</td>
</tr>
<tr>
<td>critical</td>
<td>Display all critical alarms</td>
</tr>
<tr>
<td>informational</td>
<td>Display all informational or higher severity alarms</td>
</tr>
<tr>
<td>major</td>
<td>Display all major or higher severity alarms</td>
</tr>
<tr>
<td>normal</td>
<td>Display all normal or higher severity alarms</td>
</tr>
<tr>
<td>warning</td>
<td>Display all warning or higher severity alarms</td>
</tr>
</tbody>
</table>

#### Example
2.2.30 boot

Privileged / Global Config

Syntax

show boot

Parameters

None.

Example

WS5100#show boot

<table>
<thead>
<tr>
<th>Image</th>
<th>Build Date</th>
<th>Install Date</th>
<th>Version</th>
</tr>
</thead>
</table>

Current Boot : Primary
Next Boot : Primary
Software Fallback : Enabled
WS5100#
2.2.31 clock

Privilege / Global Config

Syntax

show clock

Parameters

None.

Example

WS5100#show clock
Sep 13 16:46:27 UTC 2006
WS5100#
2.2.32 debugging

Privileged / Global Config

Syntax

    show debugging

Parameters

None.

Example
2.2.33 file

Syntax

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

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>information</td>
<td>Display file information</td>
</tr>
<tr>
<td>FILE</td>
<td>Display information on FILE</td>
</tr>
<tr>
<td>systems</td>
<td>List filesystems</td>
</tr>
</tbody>
</table>

Example

```
WS5100#show file systems
File Systems:

<table>
<thead>
<tr>
<th>Size(b)</th>
<th>Free(b)</th>
<th>Type</th>
<th>Prefix</th>
</tr>
</thead>
<tbody>
<tr>
<td>13704192</td>
<td>11904000</td>
<td>flash</td>
<td>nvram:</td>
</tr>
<tr>
<td>19524608</td>
<td>16866304</td>
<td>flash</td>
<td>flash:</td>
</tr>
</tbody>
</table>

WS5100#
```
2.2.34 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#
```
2.2.35 password-encryption

Privileged / Global Config

Syntax

show password-encryption (status)

Parameters

<table>
<thead>
<tr>
<th>status</th>
<th>Display password-encryption status</th>
</tr>
</thead>
</table>

Example

WS5100#show password-encryption status
Password encryption is disabled
WS5100#
2.2.36 running-config

Privilege / Global Config

Displays the contents of the configuration file for the switch including all configured MAC and IP access lists and which access groups are applied to an interface.

Syntax

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

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>full</td>
<td>full configuration</td>
</tr>
<tr>
<td>include-factory</td>
<td>Include Factory Defaults</td>
</tr>
</tbody>
</table>

Example

```
WS5100#show running-config full
!
! 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
!
```
wireless
!
crypto pki trustpoint local
  subject-name 11 11 11 11 11 11
crypto pki trustpoint default-trustpoint
  subject-name Symbol Technologies
crypto pki trustpoint slocal
!
radius-server local
!
interface eth1

WS5100#show running-config include-factory

! configuration of WS5100 version 3.0.0.0-200B!
version 1.0
!
no service password-encryption
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 snmp ssh telnet
username admin privilege superuser
username operator password 1 fe96dd39756ac41b74283a9292652d366d73931f
username operator access console snmp ssh telnet
username operator privilege monitor
username manager password 1 45b27d6483fc630981ad5096ff26a7956ce0c038
username manager access console snmp ssh telnet
username manager privilege superuser
!
!
ip domain-lookup
service pm max-sys-restarts 2
no service pm sys-restart
service diag period 1000
service diag enable
no country-code
redundancy group-id 1
redundancy interface-ip 0.0.0.0
redundancy mode primary
redundancy heartbeat-period 5
redundancy hold-period 15
redundancy discovery-period 30
no redundancy handle-stp enable
no redundancy enable
-- MORE --, next page: Space, next line: Enter, quit: Control-C

.............................................
### 2.2.37 securitymgr

- **Privilege / Global Config**

**Syntax**

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

**Parameters**

<table>
<thead>
<tr>
<th>debug-logs</th>
<th>Debug information</th>
</tr>
</thead>
</table>

**Example**
2.2.38 sessions

Privilege / Global Config

Syntax
show sessions

Parameters
None.

Example

```
WS5100#show sessions
SESSION USER LOCATION IDLE START TIME
  1 cli Console 006days Jan 1 00:00:00 1970
** 2 cli 157.235.206.39 00:00m Jan 1 00:00:00 1970
WS5100#`
```
2.2.39 startup-config

Privilege / Global Config

Syntax

show startup-config

Parameters

None.

Example

WS5100#show startup-config
!
! configuration of WS5100 version 3.0.0.0-16786X!
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
snmp-server user manager v3 encrypted auth md5
0xfdc2a886f072f0d6094bd7
snmp-server user operator v3 encrypted auth md5
0xfb2392a14cf80787b878006ab968a29b
crypto ipsec security-association lifetime kilobytes 4608000
!
wireless
!
crypto pki trustpoint slocal.................................
2.2.40 upgrade-status

Privilege / Global Config

Syntax

show upgrade-status detail

Parameters

<table>
<thead>
<tr>
<th>detail</th>
<th>Last image upgrade log</th>
</tr>
</thead>
</table>

Example

WS5100#show upgrade-status detail
Last Image Upgrade Status : Successful
Last Image Upgrade Time : Tue Aug 29 18:32:17 2006
--------------------------------------------------------
var2 is 10 percent full
/tmp is 5 percent full
Free Memory 151944 kB
FWU invoked via Linux shell
Running from partition /dev/hda6, partition to update is /dev/hda5
Reading image file header
Removing other partition
Added 3.0.0.0-180B *
Making file system
Extracting files (this can take some time).
Version of firmware update file is 3.0.0.0-200B
Creating LILO files
Running LILO
Added 3.0.0.0-180B *
Added 3.0.0.0-200B
Successful
WS5100#
Logging in to the switch places you in USER EXEC command mode. Typically, log-in will require a user name and a password. You may try three times to enter a password before the connection attempt is refused. The USER EXEC commands available at the user level are a subset of those available at the privileged level. In general, the user EXEC commands allow you to connect to remote devices, perform basic tests, and list system information.

To list the available USER EXEC commands, use the `?` at the command prompt. The USER EXEC mode prompt consists of the host name of the device followed by an angle bracket (`>`). The default host name is generally WLAN Module. You can change the host name using the `hostname GLOBAL CONFIG` command.
3.1 User Exec Commands

Table 3.1 summarizes the User Exec commands within the WS5100 Series Switch command line interface.

Table 3.1 User Exec commands Summary

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Ref.</th>
</tr>
</thead>
<tbody>
<tr>
<td>autoinstall</td>
<td>autoinstall configuration command.</td>
<td>page 3-3</td>
</tr>
<tr>
<td>clear</td>
<td>autoinstall configuration command.</td>
<td>page 3-4</td>
</tr>
<tr>
<td>clrscr</td>
<td>the display screen.</td>
<td>page 2-3</td>
</tr>
<tr>
<td>cluster-cli</td>
<td>Cluster context.</td>
<td>page 3-6</td>
</tr>
<tr>
<td>debug</td>
<td>Debugging functions.</td>
<td>page 3-7</td>
</tr>
<tr>
<td>disable</td>
<td>Turn off privileged mode command.</td>
<td>page 3-9</td>
</tr>
<tr>
<td>enable</td>
<td>Turn on privileged mode command.</td>
<td>page 3-10</td>
</tr>
<tr>
<td>exit</td>
<td>End current mode and down to previous mode.</td>
<td>page 2-4</td>
</tr>
<tr>
<td>help</td>
<td>Description of the interactive help system.</td>
<td>page 2-5</td>
</tr>
<tr>
<td>logout</td>
<td>Exit from the EXEC.</td>
<td>page 3-11</td>
</tr>
<tr>
<td>no</td>
<td>Negate a command or set its defaults.</td>
<td>page 2-7</td>
</tr>
<tr>
<td>page</td>
<td>Toggle paging.</td>
<td>page 3-12</td>
</tr>
<tr>
<td>quit</td>
<td>Exit current mode and down to previous mode.</td>
<td>page 3-13</td>
</tr>
<tr>
<td>service</td>
<td>Service Commands.</td>
<td>page 2-8</td>
</tr>
<tr>
<td>terminal</td>
<td>Show running system information.</td>
<td>page 2-19</td>
</tr>
</tbody>
</table>
3.1.1 autoinstall

Use this command to configure the auto-install feature of the WS5100 Series Switch.

Syntax

autoinstall start
autoinstall (config|cluster-config|image) url LINE

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Enables all the autoinstall features.</td>
</tr>
</tbody>
</table>

Usage Guidelines

Example

WS5100>autoinstall enable
WS5100>
### 3.1.2 clear

*User Exec Commands*

Use this command to reset the previous command implemented by you.

**Syntax**
```
clear (crypto (ike sa ( A.B.C.D| )|ipsec sa(A.B.C.D | ) )| mobility(mu|mu-log|peer-log|peer-statistics)| wireless-statistics )
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>crypto</td>
<td>crypto</td>
</tr>
<tr>
<td>mobility</td>
<td>Clear Mobility Attributes</td>
</tr>
<tr>
<td>wireless-statistics</td>
<td>Clear all wireless statistics</td>
</tr>
<tr>
<td>ike</td>
<td></td>
</tr>
<tr>
<td>ipsec</td>
<td>Security association</td>
</tr>
<tr>
<td>sa</td>
<td></td>
</tr>
<tr>
<td>remote peer IP address</td>
<td>IP address of the remote peer</td>
</tr>
<tr>
<td>peer IP address</td>
<td>IP address of the peer</td>
</tr>
<tr>
<td>mu</td>
<td>Clear Mobile-unit</td>
</tr>
<tr>
<td>AA-BB-CC-DD-EE-FF</td>
<td>MAC address of the MU</td>
</tr>
<tr>
<td>all</td>
<td>All MUs (Home and Foreign)</td>
</tr>
<tr>
<td>foreign-database</td>
<td>MUs present in the Foreign MU Database</td>
</tr>
<tr>
<td>home-database</td>
<td>MUs present in the Home MU Database</td>
</tr>
<tr>
<td>mu-log</td>
<td>Clear Mobility MU-Event Log</td>
</tr>
<tr>
<td>peer-log</td>
<td>Clear Mobility PEER-Event Log</td>
</tr>
<tr>
<td>peer-statistics</td>
<td>Clear Mobility Peer Statistics</td>
</tr>
<tr>
<td>A.B.C.D</td>
<td>IP address of the peer</td>
</tr>
</tbody>
</table>
Usage Guidelines

Example

WS5100> clear crypto ike sa 111.222.333.01
WS5100>

WS5100> clear crypto ipsec sa
WS5100>
3.1.3 cluster-cli

User Exec Commands

Use this command to cluster all the CLI pertaining to the context it appears in.

Syntax

```
cluster-cli enable
```

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Enables cluster context</td>
</tr>
</tbody>
</table>

Usage Guidelines

Example

```
WS5100> cluster-cli enable
WS5100>
```
3.1.4 debug

User Exec Commands

Use this command to debug the WS5100 Series Switch.

Syntax

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

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>certmgr</td>
<td>Certificate Manager Debugging Messages</td>
</tr>
<tr>
<td>ip</td>
<td>Internet Protocol (IP)</td>
</tr>
<tr>
<td>mobility</td>
<td>L3 Mobility</td>
</tr>
<tr>
<td>all</td>
<td>Trace error and informational messages from Certificate Manager</td>
</tr>
<tr>
<td>error</td>
<td>Trace error messages from Certificate Manager</td>
</tr>
<tr>
<td>info</td>
<td>Trace informational messages from Certificate Manager</td>
</tr>
<tr>
<td>ssh</td>
<td>Secured Shell (SSH) server</td>
</tr>
<tr>
<td>cc</td>
<td>ccserver events</td>
</tr>
<tr>
<td>error</td>
<td>Error</td>
</tr>
<tr>
<td>forwarding</td>
<td>Dataplane forwarding</td>
</tr>
<tr>
<td>mu</td>
<td>MU events and state changes</td>
</tr>
<tr>
<td>packet</td>
<td>Control Packets</td>
</tr>
<tr>
<td>peer</td>
<td>Peer establishment</td>
</tr>
<tr>
<td>system</td>
<td>System events</td>
</tr>
</tbody>
</table>

Usage Guidelines
Example

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>
3.1.5 disable

To use this command you first have to enable the PRIV mode. Use this command to turn off and move out of the PRIV mode.

Syntax

disable

Parameters

None.

Usage Guidelines

Example

WS5100>disable
WS5100>
### 3.1.6 enable

#### User Exec Commands

Use this command to enter into the PRIV mode.

**Syntax**

```
enable
```

**Parameters**

None.

**Usage Guidelines**

**Example**

```
WS5100>enable
```
3.1.7 logout

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

**Syntax**
```
logout
```

**Parameters**
None.

**Usage Guidelines**

**Example**
The WS5100 Series Switch logs off on execution of this command.
3.1.8 page

User Exec Commands

Use this command to toggle paging.

Syntax

page

Parameters

None.

Usage Guidelines

Example
3.1.9 **quit**

*User Exec Commands*

Use this command to exit from the current mode and go down to previous mode.

**Syntax**

```
quit
```

**Parameters**

None.

**Usage Guidelines**

**Example**

The WS5100 Series Switch logs off on execution of this command.
Most of the PRIV EXEC mode commands set operating parameters, privileged-level access should be password protected to prevent unauthorized use. The PRIV EXEC command set includes those commands contained in USER EXEC mode. PRIV EXEC mode also provides access to configuration modes through the configure command, 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 PRIV EXEC mode enter the following CLI command at the prompt:

```
WS5100#enable
```

PRIV EXEC mode is sometimes referred to as enable mode, because the enable command is used to enter the mode.

If a password has been configured on the system, you will be prompted to enter it before being allowed access to privileged EXEC mode. The password is not displayed on the screen and is case sensitive. If an enable password has not been set, PRIV EXEC mode can be accessed only from the router console (terminal connected to the console port). The system administrator uses the enable secret or enable password.
4.1 Priv Exec Command

*Table 4.1* summarizes the Priv Exec commands within the WS5100 Series Switch command line interface.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Ref.</th>
</tr>
</thead>
<tbody>
<tr>
<td>acknowledge</td>
<td>Acknowledge alarms.</td>
<td>page 4-4</td>
</tr>
<tr>
<td>archive</td>
<td>Manage archive files.</td>
<td>page 4-5</td>
</tr>
<tr>
<td>autoinstall</td>
<td>autoinstall configuration command.</td>
<td>page 4-7</td>
</tr>
<tr>
<td>cd</td>
<td>Change current directory.</td>
<td>page 4-8</td>
</tr>
<tr>
<td>clear</td>
<td>Reset functions.</td>
<td>page 4-9</td>
</tr>
<tr>
<td>clock</td>
<td>Configure software system clock.</td>
<td>page 4-11</td>
</tr>
<tr>
<td>clrscr</td>
<td>the display screen.</td>
<td>page 2-3</td>
</tr>
<tr>
<td>cluster-cli</td>
<td>Cluster context.</td>
<td>page 4-12</td>
</tr>
<tr>
<td>configure</td>
<td>Enter configuration mode.</td>
<td>page 4-13</td>
</tr>
<tr>
<td>copy</td>
<td>Copy from one file to another.</td>
<td>page 4-14</td>
</tr>
<tr>
<td>debug</td>
<td>Debugging functions.</td>
<td>page 4-15</td>
</tr>
<tr>
<td>delete</td>
<td>Deletes specified file from the system.</td>
<td>page 4-16</td>
</tr>
<tr>
<td>diff</td>
<td>Display differences between two files.</td>
<td>page 4-17</td>
</tr>
<tr>
<td>dir</td>
<td>List files on a filesystem.</td>
<td>page 4-18</td>
</tr>
<tr>
<td>disable</td>
<td>Turn off privileged mode command.</td>
<td>page 4-19</td>
</tr>
<tr>
<td>edit</td>
<td>Edit a text file.</td>
<td>page 4-20</td>
</tr>
<tr>
<td>enable</td>
<td>Turn on privileged mode command.</td>
<td>page 4-22</td>
</tr>
<tr>
<td>erase</td>
<td>Erase a filesystem.</td>
<td>page 4-23</td>
</tr>
<tr>
<td>exit</td>
<td>End current mode and down to previous mode.</td>
<td>page 2-4</td>
</tr>
<tr>
<td>halt</td>
<td>Halt wireless switch.</td>
<td>page 4-24</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
<td>Ref.</td>
</tr>
<tr>
<td>----------</td>
<td>-------------------------------------------------------</td>
<td>-------</td>
</tr>
<tr>
<td>help</td>
<td>Description of the interactive help system.</td>
<td>page 2-5</td>
</tr>
<tr>
<td>kill</td>
<td>Kill specified session.</td>
<td>page 4-25</td>
</tr>
<tr>
<td>logout</td>
<td>Exit from the EXEC.</td>
<td>page 4-26</td>
</tr>
<tr>
<td>mkdir</td>
<td>Create a directory.</td>
<td>page 4-27</td>
</tr>
<tr>
<td>more</td>
<td>Display the contents of a file.</td>
<td>page 4-28</td>
</tr>
<tr>
<td>no</td>
<td>Negate a command or set its defaults.</td>
<td>page 2-7</td>
</tr>
<tr>
<td>page</td>
<td>Toggle paging.</td>
<td>page 4-30</td>
</tr>
<tr>
<td>ping</td>
<td>Send ICMP echo messages.</td>
<td>page 4-31</td>
</tr>
<tr>
<td>pwd</td>
<td>Display current directory.</td>
<td>page 4-32</td>
</tr>
<tr>
<td>quit</td>
<td>Exit current mode and down to previous mode.</td>
<td>page 4-33</td>
</tr>
<tr>
<td>reload</td>
<td>Halt and perform a warm reboot.</td>
<td>page 4-34</td>
</tr>
<tr>
<td>rename</td>
<td>Rename a file.</td>
<td>page 4-35</td>
</tr>
<tr>
<td>rmdir</td>
<td>Delete a directory.</td>
<td>page 4-36</td>
</tr>
<tr>
<td>service</td>
<td>Service Commands.</td>
<td>page 2-8</td>
</tr>
<tr>
<td>terminal</td>
<td>Show running system information.</td>
<td>page 2-19</td>
</tr>
<tr>
<td>telnet</td>
<td>Open a telnet connection.</td>
<td>page 4-37</td>
</tr>
<tr>
<td>traceroute</td>
<td>Trace route to destination.</td>
<td>page 4-38</td>
</tr>
<tr>
<td>upgrade</td>
<td>Upgrade software image.</td>
<td>page 4-39</td>
</tr>
<tr>
<td>upgrade-abort</td>
<td>Abort an ongoing upgrade.</td>
<td>page 4-41</td>
</tr>
<tr>
<td>write</td>
<td>Write running configuration to memory or terminal.</td>
<td>page 4-42</td>
</tr>
</tbody>
</table>
4.1.1 acknowledge

Priv Exec Command

Use this command to acknowledge alarms generated by the WS5100 Series Switch.

Syntax

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

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>alarm-log</td>
<td>Acknowledge alarms</td>
</tr>
<tr>
<td>&lt;1-65535&gt;</td>
<td>Acknowledge specific alarm id</td>
</tr>
<tr>
<td>all</td>
<td>Acknowledge all alarms</td>
</tr>
</tbody>
</table>

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

Use this command to manage archive files.

Syntax

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

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>tar</td>
<td>Use to manipulate (create, list or extract) a tar file</td>
</tr>
<tr>
<td>/table</td>
<td>List files in a tar file</td>
</tr>
<tr>
<td>/create</td>
<td>Create a tar file</td>
</tr>
<tr>
<td>/xtract</td>
<td>Extract files from a tar file</td>
</tr>
<tr>
<td>FILE</td>
<td>Tar filename</td>
</tr>
<tr>
<td>URL</td>
<td>Tar file URL</td>
</tr>
</tbody>
</table>

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 Aug 17 08:25:50 2006 hotspot
  drwx  120  Fri Sep  8 12:27:20 2006 log
  drwx  1024 Thu Sep  7 16:23:34 2006 crashinfo
  drwx  1024 Wed Aug 23 15:30:19 2006 backup
  -rw- 173056 Fri Sep  8 14:39:48 2006 out.tar
```
Which files are tared?

```
WS5100# archive tar /table flash:/out.tar
  drwxrwxrwt 0/600 0 2006-09-08 12:27:20 flash/log
  -rw-r--r-- 0/0 381 2006-09-08 12:27:28 flash/log/snmpd.log
  -rw-r--r-- 0/0 151327 2006-09-08 14:37:26 flash/log/messages.log
  -rw-r--r-- 0/0 17318 2006-09-08 12:27:29 flash/log/startup.log
  drwxrwxrwt 0/600 0 2006-09-08 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 autoinstall

*Priv Exec Command*

Use this CLI to configure auto-installation feature of the WS5100 Series Switch.

**Syntax**

```
autoinstall start
autoinstall [config|cluster-config|image] url LINE
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>start</td>
<td>start the autoinstall sequence</td>
</tr>
<tr>
<td>cluster-config</td>
<td>enable autoinstall of cluster-config</td>
</tr>
<tr>
<td>config</td>
<td>enable autoinstall of config</td>
</tr>
<tr>
<td>image</td>
<td>enable autoinstall of image</td>
</tr>
</tbody>
</table>

**Example**
4.1.4 cd

Priv Exec Command

Use this CLI to change the current directory.

Syntax

```
cd [DIR]
```

Parameters

<table>
<thead>
<tr>
<th>DIR</th>
<th>Change current directory to DIR.</th>
</tr>
</thead>
</table>

Usage Guidelines

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#
```
4.1.5 clear

*Priv Exec Command*

Use this CLI to reset the current context.

**Syntax**

```
clear [alarm-log|arp-cache|crypto|ip|logging|mobility|wireless-statistics]
clear alarm-log (<1-65535>|acknowledge|all|new)
clear crypto (ike|ipsec) sa (remote peer)
clear ip (dhcp(binding) [*|A.B.C.D]|nat(translation) *)
clear mobility (mu|mu-log|peer-log|peer-statistics)
clear mobility mu (<MAC Address> | all | foreign-database | home-database)
```

**Parameters**

- **alarm-log**
  - Clear alarm-log
  - `<1-65535>` – Clear specific alarm id
  - `acknowledge` – Clear acknowledged alarms
  - `all` – Clear all alarms
  - `new` – Clear new alarms

- **arp-cache**
  - Clear Arp Cache

- **crypto**
  - `crypto`
    - `ike` – clear ike
    - `ipsec` – clear ipsec
    - `sa` – Security Association
    - `remote-peer` – Remote Peer IP address

- **ip**
  - Clears Internet Protocol (IP) DHCP/NAT.
    - `dhcp` – DHCP Server Configuration
    - `binding` – DHCP Address bindings
    - `*` – Clear all bindings
    - `A.B.C.D` – Clear a specific binding
    - `nat` – Network Address Translation (NAT)
    - `translation` – Clears specified Translation.

- **logging**
  - Modify message logging facilities
Example

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>mobility</strong></td>
<td>Clear Mobility Attributes</td>
</tr>
<tr>
<td></td>
<td>• <strong>mu</strong> – Clear Mobile-unit</td>
</tr>
<tr>
<td></td>
<td>• <strong>MAC Address</strong> – MAC address of the MU</td>
</tr>
<tr>
<td></td>
<td>• <strong>all</strong> – All MUs (Home and Foreign)</td>
</tr>
<tr>
<td></td>
<td>• <strong>foreign-database</strong> – MUs present in the Foreign MU Database</td>
</tr>
<tr>
<td></td>
<td>• <strong>home-database</strong> – MUs present in the Home MU Database</td>
</tr>
<tr>
<td></td>
<td>• <strong>mu-log</strong> – Clear Mobility MU-Event Log</td>
</tr>
<tr>
<td></td>
<td>• <strong>peer-log</strong> – Clear Mobility PEER-Event Log</td>
</tr>
<tr>
<td></td>
<td>• <strong>peer-statistics</strong> – Clear Mobility Peer Statistics</td>
</tr>
<tr>
<td><strong>wireless-statistics</strong></td>
<td>Clear all wireless statistics</td>
</tr>
</tbody>
</table>
4.1.6 clock

Use this command to configure the software system clock.

Syntax

```
```

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>set</td>
<td>Set system date &amp; time</td>
</tr>
</tbody>
</table>

Usage Guidelines

Example

```
WS5100#clock set 15:10:30 08 Sep 2006
WS5100#show clock
Sep 08 15:10:31 UTC 2006
```
4.1.7 cluster-cli

Priv Exec Command

Use this CLI command to enable the cluster context.

Syntax

cluster-cli enable

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Enables cluster context</td>
</tr>
</tbody>
</table>

Example
4.1.8 configure

Priv Exec Command

Use this CLI to enter into configuration mode.

Syntax

configure terminal

Parameters

<table>
<thead>
<tr>
<th>terminal</th>
<th>Configure from the terminal</th>
</tr>
</thead>
</table>

Usage Guidelines

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 from one file to another file.

Syntax

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

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FILE</td>
<td>File from which to copy</td>
</tr>
<tr>
<td>URL</td>
<td>URL from which to copy</td>
</tr>
</tbody>
</table>

Usage Guidelines

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 switch running-config?

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

Priv Exec Command

Use this CLI for debugging purpose. Apart from all this CLI is also used to debug various features of the WS5100 Series Switch.

Syntax

ddebug all
ddebug [other features]

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Enable all debugging</td>
</tr>
</tbody>
</table>

Usage Guidelines

Example

WS5100#debug ?
  all          Enable all debugging
  cc           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
  nsm          Network Service Module (NSM)
  pktdrvr      Pktdrvr (kernel wireless) debugging messages
  pm           Process Monitor
  radius       Radius server debugging messages
  redundancy   Redundancy Protocol debugging messages
  securitymgr  Security Manager Debugging Messages
  wireless-statistics  wireless statistics
4.1.11 delete

Priv Exec Command

Use this command to delete the specified file from the system.

Syntax

    delete ([/force|/recursive]) .FILE

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>/force</td>
<td>Force deletion without prompt</td>
</tr>
<tr>
<td>/recursive</td>
<td>Recursive delete</td>
</tr>
<tr>
<td>FILE</td>
<td>Filename(s) to be deleted</td>
</tr>
</tbody>
</table>

Usage Guidelines

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

Use this CLI to view the difference between 2 files.

Syntax

diff (FILE|URL) (FILE|URL)

Parameters

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>FILE</td>
<td>Display the differences between FILE</td>
</tr>
<tr>
<td>URL</td>
<td>Display the differences between URL</td>
</tr>
</tbody>
</table>

Usage Guidelines

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 eve password 0 mypassword123
 rad-user vasavi password 0 mypassword123
 group kumar2
 rad-user sumi
- policy wlan 2
+ policy vlan 44
+ policy wlan 10
!
 rad-user sumi
 group kumar3
!
4.1.13 **dir**

*Priv Exec Command*

Use this CLI to view the list of files on a filesystem.

**Syntax**

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

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>/all</td>
<td>List all files</td>
</tr>
<tr>
<td>/recursive</td>
<td>List files recursively</td>
</tr>
<tr>
<td>DIR</td>
<td>List files in named file path</td>
</tr>
<tr>
<td>all-filesystems</td>
<td>List files on all filesystems</td>
</tr>
<tr>
<td></td>
<td>Output modifiers</td>
</tr>
<tr>
<td>&gt;</td>
<td>Output redirection</td>
</tr>
<tr>
<td>&gt;&gt;</td>
<td>Output redirection appending</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

**Example**

WS5100#dir

Directory of flash:

<table>
<thead>
<tr>
<th>Mode</th>
<th>Permissions</th>
<th>Size</th>
<th>Date</th>
<th>Time</th>
<th>File</th>
</tr>
</thead>
<tbody>
<tr>
<td>drwx</td>
<td>1024</td>
<td>Wed Jul 19 19:14:05 2006</td>
<td>hotspot</td>
<td></td>
<td></td>
</tr>
<tr>
<td>drwx</td>
<td>120</td>
<td>Wed Aug 30 15:32:44 2006</td>
<td>log</td>
<td></td>
<td></td>
</tr>
<tr>
<td>drwx</td>
<td>1024</td>
<td>Thu Aug 31 23:50:09 2006</td>
<td>crashinfo</td>
<td></td>
<td></td>
</tr>
<tr>
<td>-rw-</td>
<td>14271</td>
<td>Tue Jul 25 15:16:41 2006</td>
<td>Radius-config</td>
<td></td>
<td></td>
</tr>
<tr>
<td>-rw-</td>
<td>14271</td>
<td>Wed Jul 26 15:42:08 2006</td>
<td>flash:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>drwx</td>
<td>1024</td>
<td>Wed Aug 9 17:35:08 2006</td>
<td>radius</td>
<td></td>
<td></td>
</tr>
<tr>
<td>-rw-</td>
<td>3426</td>
<td>Wed Jul 26 16:08:02 2006</td>
<td>running-config-new</td>
<td></td>
<td></td>
</tr>
<tr>
<td>-rw-</td>
<td>13163</td>
<td>Wed Jul 26 16:08:42 2006</td>
<td>radius-config</td>
<td></td>
<td></td>
</tr>
<tr>
<td>-rw-</td>
<td>80898</td>
<td>Thu Aug 17 14:59:39 2006</td>
<td>cli_commands.txt</td>
<td></td>
<td></td>
</tr>
<tr>
<td>-rw-</td>
<td>65015</td>
<td>Fri Aug 11 19:57:37 2006</td>
<td>cli_commands_180B.txt</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

WS5100#
4.1.14 disable

Use this command to turn off privileged mode command.

Syntax

disable

Parameters

None.

Usage Guidelines

Example

WS5100#disable
WS5100>
4.1.15 edit

Priv Exec Command

Use this CLI command to edit a text file.

Syntax

edit FILE

Parameters

| FILE | Name of the file to be edited. |

Usage Guidelines

Example

S5100# edit startup-config
GNU nano 1.2.4                      File: startup-config
!
! configuration of WS5100 version 3.0.0.0-19193X!
version 1.0
!
! service prompt crash-info
!
username ksd
username jskdf
username admin privilege superuser
username admin password 1
8e67bb26b358e2ed20fe552ed6fb832f397a507d
username admin privilege superuser
username operator password 1
fe96dd39756ac41b74283a9292652d366d73931f
username manager privilege superuser
username manager password 1
8e67bb26b358e2ed20fe552ed6fb832f397a507d
username manager privilege superuser
username test password 1
d1168bcad36bbdec594be55f5020cf0e086859
username test access ssh
username test privilege superuser
!
!
ip access-list extended remote
[ Read 423 lines ]
^G Get Help ^O WriteOut ^R Read File ^Y Prev
Page ^K Cut Text ^C Cur Pos
^X Exit ^J Justify ^W Where Is ^V Next
Page ^U UnCut Txt ^T To Spell
< this command will open the startup-config file for editing >
< edit & save the config file & exit>
WS5100#
4.1.16 enable

Priv Exec Command

Use this CLI command to Turn on privileged mode command.

Syntax

   enable

Parameters

None.

Usage Guidelines

Example

  WS5100#enable
  WS5100#
**4.1.17 erase**

*Priv Exec Command*

Use this CLI command to erase a filesystem.

**Syntax**

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

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>nvram:</td>
<td>Erase everything in nvram:</td>
</tr>
<tr>
<td>flash:</td>
<td>Erase everything in flash:</td>
</tr>
<tr>
<td>startup-config</td>
<td>Reset configuration to factory default</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

**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

Use this CLI command to stop the WS5100 Series Switch.

Syntax

halt

Parameters

None.

Usage Guidelines

Example

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

Priv Exec Command

Use this CLI command to kill a specified session.

Syntax

    kill session <1-16>

Parameters

| session | Active session. There are 16 active sessions which can be killed |

Usage Guidelines

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
** 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

Use this CLI command to exit from the EXEC mode.

Syntax

   logout

Parameters

None.

Usage Guidelines

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

Use this CLI command to create a new directory in the filesystem.

Syntax

```
mkdir DIR
```

**Parameters**

<table>
<thead>
<tr>
<th>DIR</th>
<th>Directory name</th>
</tr>
</thead>
</table>

**Usage Guidelines**

**Example**

```
WS5100#mkdir TestDIR
WS5100#
```
4.1.22 more

Priv Exec Command

Use this CLI command to view the contents of a file.

Syntax

more FILE

Parameters

| FILE | Displays the content of the file |

Usage Guidelines

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 12:27:35 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-DHCPPIP: 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

Use this CLI command to toggle between the page.

Syntax

page

Parameters

None.

Usage Guidelines

Example

WS5100#page
WS5100#
4.1.24 ping

Priv Exec Command

Use this CLI command to send ICMP echo messages.

Syntax

ping WORD

Parameters

| WORD | Ping destination address or hostname. |

Usage Guidelines

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

Use this CLI command to view the contents of the current directory.

Syntax

pwd

Parameters

None.

Usage Guidelines

Example

WS5100#pwd
flash:/
WS5100#
4.1.26 quit

Priv Exec Command

Use this CLI command to exit from the current mode and move down to previous mode.

Syntax

\[ quit \]

Parameters

None.

Usage Guidelines

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

Use this CLI to halt the WS5100 Series Switch and perform a warm reboot.

Syntax
reload

Parameters
None.

Usage Guidelines

Example
WS5100#reload
Privileged Exec Commands

4.1.28 rename

Priv Exec Command

Use this CLI command to rename a file in the existing filesystem.

Syntax

rename FILE FILE

Parameters

| FILE  | File to be rename. |

Usage Guidelines

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_180B.txt
cli_commands.txt cli_commands.save
-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

Use this CLI command to delete an existing file from the file system.

Syntax

rmdir DIR

Parameters

<table>
<thead>
<tr>
<th>DIR</th>
<th>Name of the Directory to be deleted.</th>
</tr>
</thead>
</table>

Usage Guidelines

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
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

Use this command to open a telnet session.

Syntax

telnet WORD (PORT|)

Parameters

| WORD | IP address or hostname of a remote system |

Usage Guidelines

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 traceroute

Priv Exec Command

Use this CLI command to trace the route to destination.

Syntax

traceroute (WORD | ip WORD)

Parameters

<table>
<thead>
<tr>
<th>WORD</th>
<th>Trace route to destination address or hostname</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip</td>
<td>IP Trace</td>
</tr>
</tbody>
</table>

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#
### 4.1.32 upgrade

**Priv Exec Command**

Use this CLI command to upgrade the software image on the Ws5100 Series Switch.

**Syntax**

```
upgrade URL (background)
```

**Parameters**

<table>
<thead>
<tr>
<th>URL</th>
<th>Location of firmware image</th>
</tr>
</thead>
</table>

**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

hdal, 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 hd1, 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#
4.1.33 upgrade-abort

Priv Exec Command

Use this CLI command to abort the process of an ongoing upgrade.

**Syntax**

upgrade-abort

**Parameters**

None.

**Usage Guidelines**

**Example**

WS5100#upgrade-abort
% Error: No upgrade in progress

WS5100#upgrade tftp://157.235.208.105:/img

background
WS5100#Sep 08 16:01:38 2006: %KERN-4-WARNING:
EXT3-fs warning: maximal mount count reached, running e2fsck is recommended.
Sep 08 16:01:38 2006: %KERN-6-INFO: EXT3 FS on hda1, internal journal.
%KERN-6-INFO: kjournald starting. Commit interval 5 seconds.
Sep 08 16:01:43 2006: %KERN-6-INFO: EXT3 FS on hda6, internal journal.
Sep 08 16:01:43 2006: %KERN-6-INFO: EXT3-fs:

mounted filesystem with ordered data mode..
WS5100#upgrade-abort
WS5100#
WS5100#show upgrade-status
Last Image Upgrade Status : Extracting files

(this can take some time). Aborted
Last Image Upgrade Time : Fri Sep  8 16:01:54 2006
4.1.34 write

Priv Exec Command

Use this command to write running configuration to memory or terminal

Syntax

write [memory | terminal]

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>memory</td>
<td>Write to NV memory</td>
</tr>
<tr>
<td>terminal</td>
<td>Write to terminal</td>
</tr>
</tbody>
</table>

Usage Guidelines

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
!............................
Global Configuration Commands

The term *global* is used to indicate characteristics or features that affect the system as a whole. Global configuration mode is used to configure the system globally, or to enter specific configuration modes to configure specific elements such as interfaces or protocols. Use the `configure terminal` command, under PRIV EXEC, to enter 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 that you are now in global configuration mode. The prompt for global configuration mode consists of the host-name of the device followed by (config) and the pound sign (#).
Commands entered in global configuration mode update the running configuration file as soon as they are entered. However, these changes are not saved into the startup configuration file until you issue the `copy running-config startup-config` EXEC mode command.

### 5.1 Global Configuration Commands

*Table 5.1* summarizes the Global Config commands within the WS5100 Series Switch command line interface.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Ref.</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>aaa</code></td>
<td>Authentication, Authorization and Accounting.</td>
<td>5-4</td>
</tr>
<tr>
<td><code>access-list</code></td>
<td>Add an access list entry.</td>
<td>5-5</td>
</tr>
<tr>
<td><code>banner</code></td>
<td>Define a login banner.</td>
<td>5-6</td>
</tr>
<tr>
<td><code>boot</code></td>
<td>Reboots the wireless switch.</td>
<td>5-7</td>
</tr>
<tr>
<td><code>clrscr</code></td>
<td>Clear the display screen.</td>
<td>2-3</td>
</tr>
<tr>
<td><code>country-code</code></td>
<td>Configure the country of operation. All existing radio configuration will be erased.</td>
<td>5-8</td>
</tr>
<tr>
<td><code>crypto</code></td>
<td>Encryption related commands.</td>
<td>5-11</td>
</tr>
<tr>
<td><code>do</code></td>
<td>Run commands from Exec mode.</td>
<td>5-16</td>
</tr>
<tr>
<td><code>end</code></td>
<td>End current mode and change to EXEC mode.</td>
<td>5-17</td>
</tr>
<tr>
<td><code>exit</code></td>
<td>End current mode and down to previous mode.</td>
<td>2-4</td>
</tr>
<tr>
<td><code>fallback</code></td>
<td>Configures software fallback feature.</td>
<td>5-18</td>
</tr>
<tr>
<td><code>ftp</code></td>
<td>Configure FTP Server.</td>
<td>5-19</td>
</tr>
<tr>
<td><code>help</code></td>
<td>Description of the interactive help system.</td>
<td>2-5</td>
</tr>
<tr>
<td><code>hostname</code></td>
<td>Set system’s network name.</td>
<td>5-20</td>
</tr>
<tr>
<td><code>interface</code></td>
<td>Select an interface to configure.</td>
<td>5-21</td>
</tr>
<tr>
<td><code>ip</code></td>
<td>Internet Protocol (IP).</td>
<td>5-22</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
<td>Ref.</td>
</tr>
<tr>
<td>-------------</td>
<td>--------------------------------------------------</td>
<td>---------</td>
</tr>
<tr>
<td>license</td>
<td>license management command.</td>
<td>page 5-26</td>
</tr>
<tr>
<td>line</td>
<td>Configure a terminal line.</td>
<td>page 5-27</td>
</tr>
<tr>
<td>local</td>
<td>Local user authentication.</td>
<td>page 5-28</td>
</tr>
<tr>
<td>logging</td>
<td>Modify message logging facilities.</td>
<td>page 5-29</td>
</tr>
<tr>
<td>mac</td>
<td>Configure MAC access-lists.</td>
<td>page 5-31</td>
</tr>
<tr>
<td>no</td>
<td>Negate a command or set its defaults .</td>
<td>page 2-7</td>
</tr>
<tr>
<td>ntp</td>
<td>Configure NTP.</td>
<td>page 5-32</td>
</tr>
<tr>
<td>prompt</td>
<td>Set system’s prompt.</td>
<td>page 5-36</td>
</tr>
<tr>
<td>radius-server</td>
<td>Enter radius-server mode.</td>
<td>page 5-37</td>
</tr>
<tr>
<td>redundancy</td>
<td>Configure redundancy group parameters.</td>
<td>page 5-39</td>
</tr>
<tr>
<td>service</td>
<td>Service Commands.</td>
<td>page 5-41</td>
</tr>
<tr>
<td>terminal</td>
<td>Show running system information.</td>
<td>page 2-19</td>
</tr>
<tr>
<td>snmp-server</td>
<td>Modify SNMP engine parameters.</td>
<td>page 5-43</td>
</tr>
<tr>
<td>terminal</td>
<td>Set terminal line parameters.</td>
<td>page 5-50</td>
</tr>
<tr>
<td>timezone</td>
<td>Configure the timezone.</td>
<td>page 5-51</td>
</tr>
<tr>
<td>username</td>
<td>Establish User Name Authentication.</td>
<td>page 5-52</td>
</tr>
<tr>
<td>vpn</td>
<td>vpn</td>
<td>page 5-53</td>
</tr>
<tr>
<td>wireless</td>
<td>Configure Wireless Parameters.</td>
<td>page 5-54</td>
</tr>
</tbody>
</table>
5.1.1 aaa

Global Configuration Commands

Displays the current aaa (Authentication, Authorization and Accounting) settings managed by WS5100 Series Wireless Switch.

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>authentication</td>
<td>Authentication configuration parameters</td>
</tr>
<tr>
<td>login</td>
<td>Set authentication lists for logins</td>
</tr>
<tr>
<td>default</td>
<td>The default authentication list</td>
</tr>
<tr>
<td>local</td>
<td>Use local user database</td>
</tr>
<tr>
<td>none</td>
<td>No authentication</td>
</tr>
<tr>
<td>radius</td>
<td>Use external radius server</td>
</tr>
<tr>
<td>nas</td>
<td>nas identifier. This parameter accepts a string of 64 characters.</td>
</tr>
<tr>
<td>vpn-authentication</td>
<td>vpn authentication using radius</td>
</tr>
<tr>
<td>primary</td>
<td>primary address</td>
</tr>
<tr>
<td>secondary</td>
<td>secondary address</td>
</tr>
<tr>
<td>A.B.C.D</td>
<td>address</td>
</tr>
</tbody>
</table>

Usage Guidelines

Example
5.1.2 access-list

Global Configuration Commands

Use this CLI command to add an access list entry.

Syntax

access-list

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) (wlan <1-32>|) (log) (rule-precedence <1-500>|)

access-list (<100-199>|<2000-2699>) (deny|permit|mark (8021p <0-7> | tos <0-255>)) (icmp) (A.B.C.D/M | host A.B.C.D | any) (A.B.C.D/M | host A.B.C.D | any) (wlan <1-32>|) (log) (rule-precedence <1-500>|)

access-list (<100-199>|<2000-2699>) (deny|permit|mark (8021p <0-7> | tos <0-255>)) (ip) (A.B.C.D/M | host A.B.C.D | any) (A.B.C.D/M | host A.B.C.D | any) (wlan <1-32>|) (log) (rule-precedence <1-500>|)

access-list (<100-199>|<2000-2699>) (deny|permit|mark (8021p <0-7> | tos <0-255>)) (tcp|udp) (A.B.C.D/M | host A.B.C.D | any) (eq <1-65535> | range <1-65535> <1-65535> |) (A.B.C.D/M | host A.B.C.D | any) (eq <1-65535> | range <1-65535> <1-65535> |) (wlan <1-32>|) (log) (rule-precedence <1-500>|)

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Enter a brief description</th>
</tr>
</thead>
</table>

Usage Guidelines

Example

EXAMPLE OUTPUT HERE
5.1.3 banner

Use this CLI command to define a login banner for the WS5100 Series Wireless Switch.

**Syntax**

banner(motd(LINE|default))

**Parameters**

<table>
<thead>
<tr>
<th>motd</th>
<th>Set Message of the Day banner</th>
</tr>
</thead>
<tbody>
<tr>
<td>LINE</td>
<td>Custom MOTD string</td>
</tr>
<tr>
<td>default</td>
<td>Default MOTD string</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

**Example**

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

WS5100 release 3.0.0.0-200B
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 3.0.0.0-200B
Login as 'cli' to access CLI.
WS5100 login: cli
Welcome to CLI
Welcome to CLI
WS5100>
5.1.4 boot

This CLI command is used to reboot the WS5100 Series Wireless Switch.

Syntax

boot(system [primary|secondary])

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>system</td>
<td>Specify boot image to use after reboot</td>
</tr>
<tr>
<td>primary</td>
<td>Primary image</td>
</tr>
<tr>
<td>secondary</td>
<td>Secondary image</td>
</tr>
</tbody>
</table>

Usage Guidelines

Example

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

The system is going down NOW !!

% Connection is closed by administrator!
Please stand by while rebooting the system.
5.1.5 country-code

*Global Configuration Commands*

Use this CLI command to configure the country of operation.

**Syntax**

country-code

**Parameters**

None.

**Usage Guidelines**

All existing radio configuration will be erased when this command is used.

**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
da Canada
dc Switzerland
dl Chile
dn China
dc Colombia
cr Costa Rica
cy Cyprus
cz Czech Republic
de Germany
dk Denmark
do Dominican Republic
dc Ecuador
dn Estonia
dg Egypt
dn Spain
fi Finland
fr France
gb United Kingdom
```
<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Country</th>
</tr>
</thead>
<tbody>
<tr>
<td>gr</td>
<td>Greece</td>
</tr>
<tr>
<td>gt</td>
<td>Guatemala</td>
</tr>
<tr>
<td>gu</td>
<td>Guam</td>
</tr>
<tr>
<td>hk</td>
<td>Hong Kong</td>
</tr>
<tr>
<td>hn</td>
<td>Honduras</td>
</tr>
<tr>
<td>hr</td>
<td>Croatia</td>
</tr>
<tr>
<td>ht</td>
<td>Haiti</td>
</tr>
<tr>
<td>hu</td>
<td>Hungary</td>
</tr>
<tr>
<td>id</td>
<td>Indonesia</td>
</tr>
<tr>
<td>ie</td>
<td>Ireland</td>
</tr>
<tr>
<td>il</td>
<td>Israel</td>
</tr>
<tr>
<td>in</td>
<td>India</td>
</tr>
<tr>
<td>is</td>
<td>Iceland</td>
</tr>
<tr>
<td>it</td>
<td>Italy</td>
</tr>
<tr>
<td>jo</td>
<td>Jordan</td>
</tr>
<tr>
<td>jp</td>
<td>Japan</td>
</tr>
<tr>
<td>kr</td>
<td>South Korea</td>
</tr>
<tr>
<td>kw</td>
<td>Kuwait</td>
</tr>
<tr>
<td>kz</td>
<td>Kazakhstan</td>
</tr>
<tr>
<td>li</td>
<td>Liechtenstein</td>
</tr>
<tr>
<td>lk</td>
<td>Sri Lanka</td>
</tr>
<tr>
<td>lt</td>
<td>Lithuania</td>
</tr>
<tr>
<td>lu</td>
<td>Luxembourg</td>
</tr>
<tr>
<td>lv</td>
<td>Latvia</td>
</tr>
<tr>
<td>ma</td>
<td>Morocco</td>
</tr>
<tr>
<td>mt</td>
<td>Malta</td>
</tr>
<tr>
<td>mx</td>
<td>Mexico</td>
</tr>
<tr>
<td>my</td>
<td>Malaysia</td>
</tr>
<tr>
<td>nl</td>
<td>Netherlands</td>
</tr>
<tr>
<td>no</td>
<td>Norway</td>
</tr>
<tr>
<td>nz</td>
<td>New Zealand</td>
</tr>
<tr>
<td>om</td>
<td>Oman</td>
</tr>
<tr>
<td>pe</td>
<td>Peru</td>
</tr>
<tr>
<td>ph</td>
<td>Philippines</td>
</tr>
<tr>
<td>pk</td>
<td>Pakistan</td>
</tr>
<tr>
<td>pl</td>
<td>Poland</td>
</tr>
<tr>
<td>pt</td>
<td>Portugal</td>
</tr>
<tr>
<td>qa</td>
<td>Qatar</td>
</tr>
<tr>
<td>ro</td>
<td>Romania</td>
</tr>
<tr>
<td>ru</td>
<td>Russia</td>
</tr>
<tr>
<td>sa</td>
<td>Saudi Arabia</td>
</tr>
<tr>
<td>se</td>
<td>Sweden</td>
</tr>
<tr>
<td>sg</td>
<td>Singapore</td>
</tr>
<tr>
<td>si</td>
<td>Slovenia</td>
</tr>
<tr>
<td>sk</td>
<td>Slovak Republic</td>
</tr>
<tr>
<td>th</td>
<td>Thailand</td>
</tr>
<tr>
<td>tr</td>
<td>Turkey</td>
</tr>
<tr>
<td>tw</td>
<td>Taiwan</td>
</tr>
<tr>
<td>ua</td>
<td>Ukraine</td>
</tr>
</tbody>
</table>
us  United States
uy  Uruguay
ve  Venezuela
vn  Vietnam
za  South Africa
WS5100(config)#country-code
5.1.6 crypto

Use this CLI commands to configure the encryption related commands.

**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 <identifier> (tftp | ftp)
crypto key generate (rsa <identifier>) <key pair> <key pair>
crypto zeroize (rsa <identifier>)
```
**crypto**

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

`crypto pki (authenticate|enroll|export|import|trustpoint)`

`crypto pki authenticate <name> (terminal|tftp|ftp)`

`crypto pki enroll <name> (request|self-signed)`

`crypto pki export <name> (request|trustpoint) (tftp|ftp)`

**Parameters**

<table>
<thead>
<tr>
<th>Table</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ipsec</strong></td>
<td>ipsec configuration</td>
</tr>
<tr>
<td><strong>security association</strong></td>
<td>security association</td>
</tr>
<tr>
<td>**lifetime(kilobytes</td>
<td>seconds) &lt;value&gt;**</td>
</tr>
<tr>
<td></td>
<td>- kilobytes – lifetime in kilobytes</td>
</tr>
<tr>
<td></td>
<td>- seconds – lifetime in seconds</td>
</tr>
<tr>
<td><strong>transform-set &lt;setname1&gt;....&lt;setname 9&gt;</strong></td>
<td>Use the crypto ipsec transform-set command to define the transform configuration for securing data.</td>
</tr>
<tr>
<td></td>
<td>- ah-md5-hmac</td>
</tr>
<tr>
<td></td>
<td>- ah-sha-hmac</td>
</tr>
<tr>
<td></td>
<td>- esp-3des</td>
</tr>
<tr>
<td></td>
<td>- esp-aes</td>
</tr>
<tr>
<td></td>
<td>- esp-aes-192</td>
</tr>
<tr>
<td></td>
<td>- esp-aes-256</td>
</tr>
<tr>
<td></td>
<td>- esp-des</td>
</tr>
<tr>
<td></td>
<td>- esp-md5-hmac</td>
</tr>
<tr>
<td></td>
<td>- esp-sha-hmac</td>
</tr>
</tbody>
</table>

The transform-set is then assigned to a crypto map using the map’s set transform-set command. See *crypto-ipsec on page 9-1*.  

**isakmp**

Internet Security Association and Key Management Protocol.

**client**

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

**identity**

Global Identity type

**keepalive**

Number of seconds between DPD messages
key | peer key
---|---
peer | remote peer
policy | Isakmp Policy

**key** | Authentication key management
---|---
export | import

rsa<identifier> | Rsa Keypair identifier Associated with Keypair
(tftp|ftp) | URL to send the key to.
generate

=key pair> | Size of Keypair. Should be between 1024-2048
zeroize

map<name> | crypto map entry name of 32 character length
---|---
isakmp | Ipsec-isakmp
manual | Ipsec-manual
dynamic | dynamic map entry (remote VPN configuration)

**pki** | Configure certificate parameters. Public Key Infrastructure is a protocol that creates encrypted public keys using digital certificates from Certificate Authorities. PKI ensures that each online party is who they claim to be.
---|---
authenticate | Authenticate and import CA Certificate
enroll | Enroll
export | Export
import | Import
trustpoint | Define a CA trustpoint
request | Certificate Request mode of enrollment
self-signed | Selfsigned Mode of enrollment
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. This feature will be corrected in the next release.

```
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 ?
```
Global Configuration Commands

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
domain End current mode and change to EXEC mode
definition 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)#
5.1.7 do

Global Configuration Commands

Use this CLI command to run commands from the other exec mode — User Exec and Priv Exec modes.

Syntax

do (command of other mode)

Parameters

None.

Usage Guidelines

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.
5.1.8 end

Use this CLI command to end the current mode and change to Exec mode.

Syntax
end

Parameters
None.

Usage Guidelines

Example

WS5100(config)#end

WS5100#?
Priv Exec commands:
  acknowledge  Acknowledge alarms
  archive      Manage archive files
  autoinstall  autoinstall configuration command
  cd           Change current directory

............................................
............................................
5.1.9 fallback

- Global Configuration Commands

Use this CLI command to enable and configures software fallback feature. Failure to boot with configured "use on boot" image allows booting with other image.

Syntax

```
fallback(enable)
```

Parameters

| enable | Enable software fallback feature. |

Usage Guidelines

Example

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

Use this CLI command to configure the FTP server.

Syntax

- `ftpenable`
- `ftp password(0|1|LINE)`
- `ftp rootdir(DIR)`

Parameters

<table>
<thead>
<tr>
<th>enable</th>
<th>Enable FTP Server.</th>
</tr>
</thead>
</table>
| password | Configure FTP password. You can set the password using one of the following options:
|          | • 0 — Password is specified UNENCRYPTED. |
|          | • 1 — Password is encrypted with SHA1 algorithm. |
|          | • LINE — Password. |
| rootdir  | Configure FTP root dir. Set the ROOT directory location of the FTP server using:
|          | • DIR — Used to set root dir of the ftp server. |

Usage Guidelines

Example

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

Use this CLI command to change the name of the systems network.

**Syntax**

```
hostname (WORD)
```

**Parameters**

| WORD       | Used to provide the name for the systems network. |

**Usage Guidelines**

**Example**

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

Use this CLI command to select and interface to configure.

**Syntax**

```
interface (IFNAME|eth|tunnel|vlan)
```

**Parameters**

<table>
<thead>
<tr>
<th>IFNAME</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IFNAME</td>
<td>Interface name</td>
</tr>
<tr>
<td>eth</td>
<td>Ethernet interface</td>
</tr>
<tr>
<td>tunnel</td>
<td>Tunnel interface</td>
</tr>
<tr>
<td>vlan</td>
<td>Vlan interface</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

**Example**

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

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

#### Global Configuration Commands

<table>
<thead>
<tr>
<th>Syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip (access-list</td>
</tr>
<tr>
<td>ip (access-list (extended(&lt;100-199</td>
</tr>
<tr>
<td>ip default-gateway(A.B.C.D)</td>
</tr>
<tr>
<td>ip dhcp (bootp</td>
</tr>
<tr>
<td>ip dhcp bootp (ignore)</td>
</tr>
<tr>
<td>ip dhcp excluded-address(A.B.C.D)</td>
</tr>
<tr>
<td>ip dhcp option (option name)</td>
</tr>
<tr>
<td>ip dhcp ping (timeout(&lt;1-10))</td>
</tr>
<tr>
<td>ip dhcp pool (pool name)</td>
</tr>
<tr>
<td>ip dhcp restart</td>
</tr>
<tr>
<td>ip domain-lookup</td>
</tr>
<tr>
<td>ip domain-name (WORD)</td>
</tr>
<tr>
<td>ip http (secure-server</td>
</tr>
<tr>
<td>ip local (pool (default (low-ip-address (A.B.C.D))) )</td>
</tr>
<tr>
<td># ip name-server (A.B.C.D)</td>
</tr>
<tr>
<td>ip nat (inside</td>
</tr>
<tr>
<td>ip nat (inside (destination</td>
</tr>
<tr>
<td>ip nat (inside (destination (static (A.B.C.D))</td>
</tr>
<tr>
<td>ip nat (inside (destination</td>
</tr>
<tr>
<td>ip nat (outside (destination</td>
</tr>
</tbody>
</table>

**NOTE** Using `access-list extended` command leads you to (config-ext-nacl) instance. For more details see Extended ACL Instance on page 13-1

Using `access-list extended` command leads you to (config-std-nacl) instance. For more details see Standard ACL Instance on page 14-1
ip nat (outside (destination (static (A.B.C.D)) | source))
ip nat (outside (destination | source (list (WORD)) | static (A.B.C.D))
ip route (A.B.C.D | A.B.C.D/M)
ip routing
ip ssh (port | rsa)
ip ssh (port (<0-65536>))
ip ssh (rsa (keypair-name (WORD)))
ip telnet (port (<0-65535>))

Parameters

<table>
<thead>
<tr>
<th>feature</th>
<th>description</th>
</tr>
</thead>
<tbody>
<tr>
<td>access-list</td>
<td>ACL Config. Using the access list parameter options you enter the ext-nacl context and std-nacl context. The prompt now changes to the context you have entered. For more details, see Extended ACL Instance on page 13-1 for extended ACL and Standard ACL Instance on page 14-1 for standard ACL.</td>
</tr>
<tr>
<td>default-gateway</td>
<td>Configure default gateway</td>
</tr>
<tr>
<td>A.B.C.D</td>
<td>IP gateway address</td>
</tr>
<tr>
<td>dhcp</td>
<td>DHCP Server configuration</td>
</tr>
<tr>
<td>bootp</td>
<td>BOOTP specific configuration</td>
</tr>
<tr>
<td>ignore</td>
<td>Configure DHCP Server to ignore BOOTP requests</td>
</tr>
<tr>
<td>excluded-address</td>
<td>Prevent DHCP Server from assigning certain addresses</td>
</tr>
<tr>
<td>A.B.C.D</td>
<td>Low IP Address</td>
</tr>
<tr>
<td>option</td>
<td>Define DHCP server option name.</td>
</tr>
<tr>
<td>ping</td>
<td>Specify ping parameters used by DHCP Server</td>
</tr>
<tr>
<td>timeout</td>
<td>Specify ping timeout between 1-10 seconds.</td>
</tr>
<tr>
<td>pool</td>
<td>Configure DHCP server address pool</td>
</tr>
<tr>
<td>restart</td>
<td>Restart DHCP Server to get the DHCP config changes into effect</td>
</tr>
<tr>
<td>domain-lookup</td>
<td>Enable Domain Name Service (DNS)</td>
</tr>
<tr>
<td><strong>domain-name</strong></td>
<td>Set default domain for DNS</td>
</tr>
<tr>
<td>----------------</td>
<td>---------------------------</td>
</tr>
<tr>
<td><strong>http</strong></td>
<td>Hyper Text Transfer Protocol (HTTP)</td>
</tr>
<tr>
<td><strong>secure-server</strong></td>
<td>Secure HTTP server (HTTPS)</td>
</tr>
<tr>
<td><strong>secure-trustpoint</strong></td>
<td>Enter the name of the trustpoint to be used for secure connection</td>
</tr>
<tr>
<td><strong>server</strong></td>
<td>HTTP server</td>
</tr>
<tr>
<td><strong>localhost</strong></td>
<td>Used only to serve requests from localhost</td>
</tr>
<tr>
<td><strong>local</strong></td>
<td>vpn local ip pool configuration</td>
</tr>
<tr>
<td><strong>pool</strong></td>
<td>Address pool</td>
</tr>
<tr>
<td><strong>default</strong></td>
<td></td>
</tr>
<tr>
<td><strong>low-ip-address</strong></td>
<td></td>
</tr>
<tr>
<td><strong>A.B.C.D</strong></td>
<td>Internet Protocol</td>
</tr>
<tr>
<td><strong>name-server</strong></td>
<td>Add a Nameserver to the DNS</td>
</tr>
<tr>
<td><strong>A.B.C.D</strong></td>
<td>IP address of Nameserver to add</td>
</tr>
<tr>
<td><strong>nat</strong></td>
<td>Network Address Translation (NAT)</td>
</tr>
<tr>
<td>(inside</td>
<td>outside)</td>
</tr>
<tr>
<td><strong>destination</strong></td>
<td>Destination address</td>
</tr>
<tr>
<td><strong>static</strong></td>
<td>Static</td>
</tr>
<tr>
<td><strong>A.B.C.D</strong></td>
<td>Inside local IP address (A.B.C.D)</td>
</tr>
<tr>
<td><strong>source</strong></td>
<td>Source address</td>
</tr>
<tr>
<td><strong>list</strong></td>
<td>Access list</td>
</tr>
<tr>
<td><strong>WORD</strong></td>
<td>Access list name</td>
</tr>
<tr>
<td><strong>static</strong></td>
<td></td>
</tr>
<tr>
<td><strong>A.B.C.D</strong></td>
<td>Inside local IP address (A.B.C.D)</td>
</tr>
<tr>
<td><strong>route</strong></td>
<td>Establish static routes</td>
</tr>
</tbody>
</table>
Global Configuration Commands

Usage Guidelines

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

- `ext-nacl` — extended ACL. For more details see Extended ACL Instance on page 13-1.
- `std-nacl` — Standard ACL. For more details see Standard ACL Instance on page 14-1.
- You can clear the ip dhcp binding using the `clear` command.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>A.B.C.D</td>
<td>IP destination prefix</td>
</tr>
<tr>
<td>A.B.C.D/M</td>
<td>IP destination prefix</td>
</tr>
<tr>
<td><code>routing</code></td>
<td>Turn on IP routing</td>
</tr>
<tr>
<td><code>ssh</code></td>
<td>Secured SHell (SSH) server</td>
</tr>
<tr>
<td><code>port</code></td>
<td>Listening port. Value can be anything between 0-65536.</td>
</tr>
<tr>
<td><code>rsa</code></td>
<td>RSA encryption key</td>
</tr>
<tr>
<td><code>keypair-name</code></td>
<td>Configure RSA keypair to be used for encryption</td>
</tr>
<tr>
<td><code>WORD</code></td>
<td>RSA keypair name</td>
</tr>
<tr>
<td><code>telnet</code></td>
<td>Telnet server</td>
</tr>
<tr>
<td><code>port</code></td>
<td>Value of the listening port. The value can be anything between 0-65535</td>
</tr>
</tbody>
</table>

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

Example

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

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

- Global Configuration Commands

Syntax

license

Parameters

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

Usage Guidelines

Example
5.1.15 line

Use this CLI command to configure the terminal line.

Syntax

```
line(console|vty)
```

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>console</td>
<td>Primary terminal line. You can configure a value between 0-0.</td>
</tr>
<tr>
<td>vty</td>
<td>Virtual terminal. You can configure a value between 0-871.</td>
</tr>
</tbody>
</table>

Usage Guidelines

Example
5.1.16 local

Global Configuration Commands

Use this CLI command to set the username and password for local user authentication.

Syntax

```
local(username,password)
```

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>username</td>
<td>Enter local user name. The username can be a string of upto 64 characters.</td>
</tr>
<tr>
<td>password</td>
<td>Enter local user password. The password can be a string of upto 21 characters.</td>
</tr>
</tbody>
</table>

Usage Guidelines

Example

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

Use this CLI command to modify message logging facilities of the WS5100 Series Wireless Switch.

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| aggregation-time | Set number of seconds for aggregating repeated messages. The value can be  
configured between 1-60 seconds.                                      |
| buffered     | Set buffered logging level.                                                 |
| console      | Set console logging level.                                                  |
| monitor      | Set terminal lines logging level.                                           |
| syslog       | Set 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                                                      |
Usage Guidelines

Example

WS5100(config)#logging aggregation-time 20
WS5100(config)#
5.1.18 mac

Use this CLI command to configure MAC access-lists.

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

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>access-list</td>
<td>ACL config for the MAC address.</td>
</tr>
<tr>
<td>extended</td>
<td>MAC Extended ACL</td>
</tr>
<tr>
<td>WORD</td>
<td>Enter the name of the ACL.</td>
</tr>
</tbody>
</table>

**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 you enter the following contexts:

- `.ext-macl` — extended MAC ACL. For more details see [Extended MAC ACL Instance on page 15-1](#)
5.1.19 ntp

Global Configuration Commands

Use this CLI command to configure NTP over the WS5100 Series Wireless Switch.

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>
### Global Configuration Commands

#### Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>access-group</code></td>
<td>Control NTP access</td>
</tr>
<tr>
<td><code>peer</code></td>
<td>Provide full access</td>
</tr>
<tr>
<td><code>query-only</code></td>
<td>Allow only control queries</td>
</tr>
<tr>
<td><code>serve</code></td>
<td>Provide server and query access</td>
</tr>
<tr>
<td><code>serve-only</code></td>
<td>Provide only server access</td>
</tr>
<tr>
<td><code>&lt;1-99&gt;</code></td>
<td>Standard IP access list</td>
</tr>
<tr>
<td><code>&lt;1300-1999&gt;</code></td>
<td>Standard IP access list (expanded range)</td>
</tr>
<tr>
<td><code>authenticate</code></td>
<td>Authenticate time sources</td>
</tr>
<tr>
<td><code>authentication-key</code></td>
<td>Authentication key for trusted time sources</td>
</tr>
<tr>
<td><code>md5</code></td>
<td>MD5 authentication</td>
</tr>
<tr>
<td><code>WORD</code></td>
<td>Authentication key</td>
</tr>
<tr>
<td><code>autokey</code></td>
<td>Enable NTP autokey authentication scheme</td>
</tr>
<tr>
<td><code>client-only</code></td>
<td>Switch will be a client to other trusted-hosts in the autokey group</td>
</tr>
<tr>
<td><code>host</code></td>
<td>Configure the switch as a trusted host</td>
</tr>
<tr>
<td><code>broadcast</code></td>
<td>Configure NTP broadcast service</td>
</tr>
<tr>
<td><code>client</code></td>
<td>Listen to NTP broadcasts</td>
</tr>
<tr>
<td><code>destination</code></td>
<td>Configure broadcast destination address</td>
</tr>
<tr>
<td><code>WORD</code></td>
<td>Destination broadcast IP address</td>
</tr>
<tr>
<td><code>key</code></td>
<td>Broadcast key</td>
</tr>
<tr>
<td><code>&lt;1-65534&gt;</code></td>
<td>Key ID</td>
</tr>
<tr>
<td><code>version</code></td>
<td>NTP version</td>
</tr>
<tr>
<td><code>&lt;1-4&gt;</code></td>
<td>NTP Version number</td>
</tr>
<tr>
<td><code>broadcastdelay</code></td>
<td>Estimated round-trip delay</td>
</tr>
<tr>
<td><code>&lt;1-999999&gt;</code></td>
<td>Round-trip delay in microseconds</td>
</tr>
</tbody>
</table>
### Usage Guidelines

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>master</strong></td>
<td>Act as a NTP master clock</td>
</tr>
<tr>
<td><code>&lt;1-15&gt;</code></td>
<td>Stratum number for the NTP master clock</td>
</tr>
<tr>
<td><strong>peer</strong></td>
<td>Configure NTP peer</td>
</tr>
<tr>
<td><strong>server</strong></td>
<td>Configure NTP server</td>
</tr>
<tr>
<td><strong>WORD</strong></td>
<td></td>
</tr>
<tr>
<td>autokey</td>
<td>Configure autokey peer authentication scheme</td>
</tr>
<tr>
<td>key</td>
<td>Configure peer authentication key</td>
</tr>
<tr>
<td><code>&lt;1-65534&gt;</code></td>
<td>Peer key number</td>
</tr>
<tr>
<td>prefer</td>
<td>Prefer this peer when possible</td>
</tr>
<tr>
<td>version</td>
<td>Configure NTP version</td>
</tr>
<tr>
<td><code>&lt;1-4&gt;</code></td>
<td>NTP version number</td>
</tr>
<tr>
<td><strong>trusted-key</strong></td>
<td>Key numbers for trusted time sources</td>
</tr>
<tr>
<td><code>&lt;1-65534&gt;</code></td>
<td>Key number</td>
</tr>
</tbody>
</table>
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)#
5.1.20 prompt

Global Configuration Commands

Use this CLI command to configure and set the systems prompt.

Syntax

    prompt (LINE)

Parameters

| LIMNE | Enter the new prompt that will be displayed by the system/WS5100 Series Wireless Switch. |

Usage Guidelines

Example

    WS5100(config)#prompt NobleMan
    NobleMan
5.1.21 radius-server

Use this CLI command to enter the RADIUS Server mode. The WS5100 system prompt will change from the default config mode to Radius server mode.

**NOTE**

radius-server local mode leads you to the radius-server context. For more details see Radius Server Instance on page 16-1

**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**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>host</td>
<td>Specify a RADIUS server A.B.C.D IP address of RADIUS server</td>
</tr>
<tr>
<td>key</td>
<td>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, up to 127 characters</td>
</tr>
<tr>
<td>local</td>
<td>Configure local radius server parameters. This takes you to a new config-radius-server context. Refer Radius Server Instance for more details.</td>
</tr>
<tr>
<td>retransmit</td>
<td>Specify the number of retries to active server &lt;0-100&gt; Number of retries for a transaction (default is 3)</td>
</tr>
<tr>
<td>timeout</td>
<td>Time to wait for a RADIUS server to reply &lt;1-1000&gt; Wait time (default 5 seconds)</td>
</tr>
</tbody>
</table>
Usage Guidelines

Example

WS5100(config)#radius-server local
WS5100(config-radsrv)#
5.1.22 redundancy

Use this CLI command to configure redundancy group parameters.

Syntax

redundancy(discovery-period|enable|group-id|handle-stp|heartbeat-period|hold-period|interface-ip|member-ip|mode)

redundancy discovery-period <10-60>
redundancy enable
redundancy group-id <1-65535>
redundancy handle-stp(enable)
redundancy heartbeat-period
redundancy hold-period <10-255>
redundancy interface-ip(A.B.C.D)
redundancy member-ip (A.B.C.D)
redundancy mode(primary|standby)

Parameters

<table>
<thead>
<tr>
<th>discovery-period</th>
<th>Set the redundancy discovery interval.</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;10-60&gt;</td>
<td>discovery time in secs (default is 30)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>enable</th>
<th>Enable redundancy protocol.</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>group-id</th>
<th>Set the redundancy group id</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;1-65535&gt;</td>
<td>Redundancy group Id</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>handle-stp</th>
<th>Delay the redundancy protocol state machine exec, considering STP.</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Set handle-stp to true</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>heartbeat-period</th>
<th>Set the redundancy heartbeat interval. The heartbeat-period must always be less than the hold-period.</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;1-255&gt;</td>
<td>heartbeat interval in secs (default is 5)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>hold-period</th>
<th>Set the redundancy hold interval.</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;10-255&gt;</td>
<td>hold interval in secs (default is 15)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>interface-ip</th>
<th>Set redundancy interface IP address.</th>
</tr>
</thead>
<tbody>
<tr>
<td>A.B.C.D</td>
<td>IP address of the switch</td>
</tr>
</tbody>
</table>
member-ip

<table>
<thead>
<tr>
<th>member-ip</th>
<th>Add member to this redundancy group.</th>
</tr>
</thead>
<tbody>
<tr>
<td>A.B.C.D</td>
<td>IP address of the member</td>
</tr>
</tbody>
</table>

mode

<table>
<thead>
<tr>
<th>mode</th>
<th>set the redundancy mode.</th>
</tr>
</thead>
<tbody>
<tr>
<td>primary</td>
<td>mode can be primary</td>
</tr>
<tr>
<td>standby</td>
<td>mode can be standby</td>
</tr>
</tbody>
</table>

Usage Guidelines

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)#
5.1.23 service

Use this CLI commands to retrieve system data that includes tables, log files, configuration, status and operation, for use in debugging and problem resolution while troubleshooting the WS5100 Series Wireless Switch configuration.

Syntax

service(advanced-vty|ap|clear|dhcp|diag-shell|password-encryption|pm|max-sys-restarts|sys-restart|prompt|radius|save-cli|set|show|start-shell|terminal-length|tether|wireless)

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>advanced-vty</td>
<td>Enable advanced mode vty interface</td>
</tr>
<tr>
<td>ap</td>
<td>access-port serviceability parameters</td>
</tr>
<tr>
<td>clear</td>
<td>Remove specified support information</td>
</tr>
<tr>
<td>dhcp</td>
<td>Enable the DHCP Server service</td>
</tr>
<tr>
<td>diag-shell</td>
<td>Provide diag shell access</td>
</tr>
<tr>
<td>password-encryption</td>
<td>Encrypt passwords in configuration</td>
</tr>
<tr>
<td>pm(max-sys-restarts</td>
<td>sys-restart)</td>
</tr>
<tr>
<td>prompt</td>
<td>Enable crash-info prompt</td>
</tr>
<tr>
<td>radius</td>
<td>Enable radius server</td>
</tr>
<tr>
<td>save-cli</td>
<td>Save CLI tree for all modes in html format</td>
</tr>
<tr>
<td>set</td>
<td>Set service parameters</td>
</tr>
<tr>
<td>show</td>
<td>Show running system information</td>
</tr>
</tbody>
</table>

process restart is one count lesser than what is configured.
## Usage Guidelines

### Example

EXAMPLE OUTPUT HERE

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>start-shell</td>
<td>Provide shell access</td>
</tr>
<tr>
<td>terminal-length</td>
<td>System wide terminal length configuration</td>
</tr>
<tr>
<td>tethereal</td>
<td>Dump and analyze network traffic</td>
</tr>
<tr>
<td>wireless</td>
<td>Wireless parameters</td>
</tr>
</tbody>
</table>
5.1.24 snmp-server

Use this CLI command to modify 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|miscellaneous|nsm|redundancy|snmp|wireless|wireless-statistics)

snmp-server enable traps all
snmp-server enable traps miscellaneous
  (lowFsSpace|processMaxRestartsReached|savedConfigModified)

snmp-server enable traps nsm dhcpIPChanged

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

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

snmp-server enable traps wireless
  (ap-detection|ids|radio|
   self-healing|station)
snmp-server enable traps wireless  ap-detection externalAPDetected
snmp-server enable traps wireless  ids
  (excessiveAuthAssociation|excessiveProbes)

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|
   deniedAssociationOnInvalidWPAPAE2|deniedAssociationOnRates|
   deniedAssociationOnSSID|deniedAssociationOnShortPream|
   deniedAssociationOnSpectrum|deniedAuthentication|disassociated|
   radiusAuthFailed|tkipCounterMeasures)

snmp-server enable traps wireless-statistics
  (min-packets|mobile-unit|radio|wireless-switch|wlan)

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-signal-less-than|
gave-up-percent-greater-than|nu-percent-greater-than|
um-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|
um-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

Parameters

<table>
<thead>
<tr>
<th>(community)</th>
<th>Set community string and access privileges</th>
</tr>
</thead>
<tbody>
<tr>
<td>ro</td>
<td>Read-only access with this community string</td>
</tr>
<tr>
<td>rw</td>
<td>Read-write access with this community string</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>(contact)</th>
<th>Text for mib object sysContact</th>
</tr>
</thead>
<tbody>
<tr>
<td>LINE</td>
<td>Identification of the contact person for this managed node</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>(enable) traps ()</th>
<th>Enable SNMP traps</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>enable all traps</td>
</tr>
<tr>
<td>miscellaneous ()</td>
<td>Enable miscellaneous traps</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>lowFsSpace</th>
<th>Available file system space is lower than the limit</th>
</tr>
</thead>
<tbody>
<tr>
<td>processMaxRestartsReached</td>
<td>Process has reached max restart</td>
</tr>
<tr>
<td>savedConfigModified</td>
<td>Saved configuration has been modified</td>
</tr>
<tr>
<td>nsm</td>
<td>Enable nsm traps</td>
</tr>
<tr>
<td>dhcpIPChanged</td>
<td>DHCP IP changed</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>--------------------------------------------</td>
</tr>
<tr>
<td>redundancy ()</td>
<td>Enable redundancy traps</td>
</tr>
<tr>
<td>adoptionExceeded</td>
<td>Redundancy port adoption exceeded</td>
</tr>
<tr>
<td>grpAuthLevelChanged</td>
<td>Redundancy group Authorization Level changed</td>
</tr>
<tr>
<td>memberDown</td>
<td>Redundancy member down</td>
</tr>
<tr>
<td>memberMisConfigured</td>
<td>Redundancy member mis-configuration</td>
</tr>
<tr>
<td>memberUp</td>
<td>Redundancy member up</td>
</tr>
<tr>
<td>snmp ()</td>
<td>Enable SNMP traps</td>
</tr>
<tr>
<td>authenticationFail</td>
<td>Enable authentication failure trap</td>
</tr>
<tr>
<td>coldstart</td>
<td>Enable coldStart trap</td>
</tr>
<tr>
<td>linkdown</td>
<td>Enable linkDown trap</td>
</tr>
<tr>
<td>linkup</td>
<td>Enable linkUp trap</td>
</tr>
<tr>
<td>wireless ()</td>
<td>Enable wireless traps</td>
</tr>
<tr>
<td>ap-detection ()</td>
<td>Enable wireless AP detection traps</td>
</tr>
<tr>
<td>externalAPDetected</td>
<td>External AP detected</td>
</tr>
<tr>
<td>ids ()</td>
<td>Enable wireless IDS traps</td>
</tr>
<tr>
<td>excessiveAuthAssociation</td>
<td>Excessive association authentication</td>
</tr>
<tr>
<td>excessiveProbes</td>
<td>Excessive probes</td>
</tr>
<tr>
<td>radio ()</td>
<td>Enable wireless radio traps</td>
</tr>
<tr>
<td>adopted</td>
<td>Radio adopted</td>
</tr>
<tr>
<td>detectedRadar</td>
<td>Radio detected radar</td>
</tr>
<tr>
<td>unadopted</td>
<td>Radio unadopted</td>
</tr>
<tr>
<td>self-healing ()</td>
<td>Enable self healing traps</td>
</tr>
<tr>
<td>activated</td>
<td>Self healing activated</td>
</tr>
<tr>
<td>station ()</td>
<td>Enable wireless station traps</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>associated</td>
<td>Wireless station associated</td>
</tr>
<tr>
<td>deniedAssociationAsPortCapacityReached</td>
<td>Wireless station denied association due to port capacity reached</td>
</tr>
<tr>
<td>deniedAssociationOnCapability</td>
<td>Wireless station denied association due to unsupported capability</td>
</tr>
<tr>
<td>deniedAssociationOnErr</td>
<td>Wireless station denied association due to internal error</td>
</tr>
<tr>
<td>deniedAssociationOnInvalidWPAWPA2IE</td>
<td>Wireless station denied association due to invalid/absent WPA/WPA2 IE</td>
</tr>
<tr>
<td>deniedAssociationOnRates</td>
<td>Wireless station denied association due to incompatible Transmission rates</td>
</tr>
<tr>
<td>deniedAssociationOnSSID</td>
<td>Wireless station denied association due to invalid SSID</td>
</tr>
<tr>
<td>deniedAssociationOnShortPream</td>
<td>Wireless station denied association due to lack of short preamble support</td>
</tr>
<tr>
<td>deniedAssociationOnSpectrum</td>
<td>Wireless station denied association due to lack of spectrum management capability</td>
</tr>
<tr>
<td>deniedAuthentication</td>
<td>Wireless station denied 802.11 authentication</td>
</tr>
<tr>
<td>disassociated</td>
<td>Wireless station disassociated</td>
</tr>
<tr>
<td>radiusAuthFailed</td>
<td>Wireless station failed radius authentication</td>
</tr>
<tr>
<td>tkipCounterMeasures</td>
<td>TKIP counter measures invoked</td>
</tr>
<tr>
<td>wireless-statistics ( )</td>
<td>Modify wireless-stats rate traps</td>
</tr>
<tr>
<td>min-packets</td>
<td>Minimum packets for sending the trap. This can be set with a decimal number in the range of &lt;1-65535&gt;</td>
</tr>
<tr>
<td>mobile-unit ( )</td>
<td>Modify mobile-unit rate traps</td>
</tr>
<tr>
<td>radio ( )</td>
<td>Modify radio rate traps</td>
</tr>
<tr>
<td>wireless-switch ( )</td>
<td>Modify wireless-switch rate traps</td>
</tr>
<tr>
<td>wlan ( )</td>
<td>Modify wlan rate traps</td>
</tr>
<tr>
<td><strong>avg-bit-speed-less-than &lt; &gt;</strong></td>
<td>Average bit speed in Mbps is less than — &lt; A decimal number greater than 0.00 and less than or equal to 54.00&gt;</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>avg-retry-greater-than &lt; &gt;</strong></td>
<td>Average retry is greater than — &lt; A decimal number greater than 0.00 and less than or equal to 16.00&gt;</td>
</tr>
<tr>
<td><strong>avg-signal-less-than &lt; &gt;</strong></td>
<td>Average signal in dBm is less than — &lt; A decimal number less than -0.00 and greater than or equal to -120.00&gt;</td>
</tr>
<tr>
<td><strong>gave-up-percent-greater-than &lt; &gt;</strong></td>
<td>Percentage of pkts dropped is greater than — &lt; A decimal number greater than 0.00 and less than or equal to 100.00&gt;</td>
</tr>
<tr>
<td><strong>nu-percent-greater-than &lt; &gt;</strong></td>
<td>Percentage of non-unicast pkts is greater than — &lt; A decimal number greater than 0.00 and less than or equal to 100.00&gt;</td>
</tr>
<tr>
<td><strong>pktsp-s-greater-than &lt; &gt;</strong></td>
<td>Packets per sec is greater than — &lt; A decimal number greater than 0.00 and less than or equal to 100000.00&gt;</td>
</tr>
<tr>
<td><strong>tput-greater-than &lt; &gt;</strong></td>
<td>Throughput in Mbps is greater than — &lt; A decimal number greater than 0.00 and less than or equal to 1000000.00&gt;</td>
</tr>
<tr>
<td><strong>undecrypt-percent-greater-than &lt; &gt;</strong></td>
<td>Percentage of undecryptable pkts is greater than — &lt; A decimal number greater than 0.00 and less than or equal to 100.00&gt;</td>
</tr>
<tr>
<td><strong>num-mobile-units-greater-than &lt; &gt;</strong></td>
<td>Number of associated mobile-unit is greater than a decimal number in the range of &lt;1-4096&gt;</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>host</strong></th>
<th>snmp server host</th>
</tr>
</thead>
<tbody>
<tr>
<td>A.B.C.D</td>
<td>snmp server host IP-address</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>location</strong></th>
<th>Text for mib object sysLocation</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th><strong>manager</strong></th>
<th>Enable SNMP manager</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Enable SNMP version v2 and v3</td>
</tr>
<tr>
<td>v2</td>
<td>Enable SNMP version v2</td>
</tr>
<tr>
<td>v3</td>
<td>Enable SNMP version v3</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>sysname</strong></th>
<th>snmp system name</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th><strong>user</strong></th>
<th>Define a user who can access SNMP engine</th>
</tr>
</thead>
<tbody>
<tr>
<td>manager</td>
<td>Manager user</td>
</tr>
<tr>
<td>operator</td>
<td>Operator user</td>
</tr>
<tr>
<td>------------------</td>
<td>----------------------------</td>
</tr>
<tr>
<td>v3()</td>
<td>User using v3 security model</td>
</tr>
<tr>
<td>auth()</td>
<td>Authentication parameters for the user</td>
</tr>
<tr>
<td>encrypted()</td>
<td>Specifying password as md5 digests</td>
</tr>
<tr>
<td>md5</td>
<td>Use HMAC MD5 algorithm for authentication</td>
</tr>
<tr>
<td>PASSWD</td>
<td>Authentication password for user</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

**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)#
5.1.25 terminal

Global Configuration Commands

Use this CLI command to set the length /number of lines to be displayed on the terminal window.

Syntax

terminal (monitor | no)

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>monitor</td>
<td>Copy debug output to the current terminal line</td>
</tr>
<tr>
<td>no</td>
<td>Negate a command or set its defaults</td>
</tr>
</tbody>
</table>

Usage Guidelines

Example

WS5100(config)#terminal monitor
WS5100(config)#
5.1.26 timezone

Use this CLI command to configure the timezone settings of the WS5100 Series Wireless Switch.

Syntax

timezone

Parameters

<table>
<thead>
<tr>
<th>TIMEZONE</th>
<th>Press &lt;tab&gt; to traverse list of files. This displays list of files containing timezone information.</th>
</tr>
</thead>
<tbody>
<tr>
<td>America/</td>
<td></td>
</tr>
<tr>
<td>Asia/</td>
<td></td>
</tr>
<tr>
<td>Atlantic/</td>
<td></td>
</tr>
<tr>
<td>Australia/</td>
<td></td>
</tr>
<tr>
<td>Etc/</td>
<td></td>
</tr>
<tr>
<td>Europe/</td>
<td></td>
</tr>
<tr>
<td>Pacific/</td>
<td></td>
</tr>
<tr>
<td>Africa/</td>
<td></td>
</tr>
</tbody>
</table>

Usage Guidelines

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)#

5.1.27 username

Global Configuration Commands

Use this CLI command to establish the user name authentication for the WS5100 Series Wireless Switch.

Syntax

username

Parameters

| WORD | Enter a name to authenticate the WS5100 switch. The username should be between 1 and 28 characters. |

Usage Guidelines

Example

WS5100(config)#username GoldenSwitch
WS5100(config)#
5.1.28 vpn

Use this CLI command to configure VPN

Syntax

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>authentication-method</td>
<td>Use this to select the authentication method</td>
</tr>
<tr>
<td>local</td>
<td>Used for user based authentication</td>
</tr>
<tr>
<td>radius</td>
<td>Used to radius server authentication</td>
</tr>
</tbody>
</table>

Usage Guidelines

Virtual Private Network. 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
5.1.29 wireless

Global Configuration Commands

Use this CLI command to configure the wireless parameters of the WS5100 Series Wireless Switch. This command will lead you to config-wireless instance. For more details see Wireless Instance on page 17-1.

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 entered the wireless instance as the prompt changes from the regular WS5100(config)# to WS5100(config-wireless)#.

Example

WS5100(config)#wireless
WS5100(config-wireless)#
Use `crypto isakmp policy(priority)` to instantiate `config-crypto-isakmp instance`.

### 6.1 Crypto Isakmp Config commands

*Table 6.1* summarizes the `crypto-isakmp` commands within the WS5100 Series Switch command line interface.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Ref.</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>authentication</code></td>
<td>Set authentication method for protection suite</td>
<td>page 6-3</td>
</tr>
<tr>
<td><code>clrscr</code></td>
<td>Clears the display screen</td>
<td>page 6-4</td>
</tr>
<tr>
<td><code>encryption</code></td>
<td>Set encryption algorithm for protection suite</td>
<td>page 6-5</td>
</tr>
<tr>
<td><code>end</code></td>
<td>End current mode and change to EXEC mode</td>
<td>page 6-6</td>
</tr>
<tr>
<td><code>exit</code></td>
<td>End current mode and down to previous mode</td>
<td>page 6-7</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
<td>Ref.</td>
</tr>
<tr>
<td>---------</td>
<td>--------------------------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>group</td>
<td>Set the Diffie-Hellman group</td>
<td>page 6-8</td>
</tr>
<tr>
<td>hash</td>
<td>Set hash algorithm for protection suite</td>
<td>page 6-9</td>
</tr>
<tr>
<td>help</td>
<td>Description of the interactive help system</td>
<td>page 6-10</td>
</tr>
<tr>
<td>lifetime</td>
<td>Set lifetime for ISAKMP security association</td>
<td>page 6-11</td>
</tr>
<tr>
<td>no</td>
<td>Negate a command or set its defaults</td>
<td>page 6-12</td>
</tr>
<tr>
<td>service</td>
<td>Service Commands</td>
<td>page 6-13</td>
</tr>
<tr>
<td>show</td>
<td>Show running system information</td>
<td>page 6-14</td>
</tr>
</tbody>
</table>
6.1.1 authentication

Use this CLI command to authenticate rsa-sig and pre-share keys.

Syntax
   authentication(pre-share|rsa-sig)

Parameters

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>pre-share</td>
<td>pre shared key</td>
</tr>
<tr>
<td>rsa-sig</td>
<td>rsa signature</td>
</tr>
</tbody>
</table>

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

Use this CLI command to clear the display screen.

Syntax

```
clrscr
```

Parameters

None.

Usage Guidelines

Example

```
WS5100(config-crypto-isakmp)#clr
WS5100(config-crypto-isakmp)#
```
6.1.3 encryption

Use this CLI command to configure the encryption level of the data transmitted using the WS5100 Wireless Switch using crypto-isakmp command.

Syntax

```
encryption(3des|aes|aes-192|aes-256|des)
```

Parameters

<table>
<thead>
<tr>
<th>3des</th>
<th>3des - Triple data encryption standard</th>
</tr>
</thead>
<tbody>
<tr>
<td>aes</td>
<td>aes - advanced data encryption standard</td>
</tr>
<tr>
<td>aes-192</td>
<td>aes-192 - advanced data encryption standard</td>
</tr>
<tr>
<td>aes-256</td>
<td>aes-256 - advanced data encryption standard</td>
</tr>
<tr>
<td>des</td>
<td>des - data encryption standard</td>
</tr>
</tbody>
</table>

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

Use this CLI command to end and exit from the current mode and change to PRIV EXEC mode. The prompt now changes to `WS5100#`.

**Syntax**
```
end
```

**Parameters**
None.

**Usage Guidelines**

**Example**
```
WS5100(config-crypto-isakmp)#end
WS5100#
```
6.1.5 exit

Use this CLI command to end current mode and down to previous mode (GLOBAL-CONFIG). The prompt now changes to `WS5100(config)#`.

**Syntax**

`exit`

**Parameters**

None.

**Usage Guidelines**

**Example**

`WS5100(config-crypto-isakmp)#exit`
`WS5100(config)#`
6.1.6 group

Use this CLI command to specify the Diffie-Hellman group (1 or 2) to be used by this IKE policy to generate the keys (which are then used to create the IPSec SA).

Syntax

```
group(1|2|5)
```

Parameters

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>768-bit mod P</td>
</tr>
<tr>
<td>2</td>
<td>1024-bit mod P</td>
</tr>
<tr>
<td>5</td>
<td></td>
</tr>
</tbody>
</table>

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

Use this CLI command to specify the hash algorithm to be used to authenticate the data transmitted over the IKE SA.

Syntax

```
hash (md5 | sha)
```

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>md5</td>
<td>Choose the md5 hash algorithm.</td>
</tr>
<tr>
<td>sha</td>
<td>Choose the sha hash algorithm.</td>
</tr>
</tbody>
</table>

Example

```
WS5100(config-crypto-isakmp)#hash sha
WS5100(config-crypto-isakmp)#
```
6.1.8 help

Use this CLI command to access the systems 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

Use this CLI command to specify how long an IKE SA is valid before expiring.

Syntax

    lifetime <seconds>

Parameters

| <seconds> | Specify how many seconds an IKE SA will last before expiring. 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**

Use this CLI command to negate a command or set its defaults.

**Syntax**

```
no <previous command used>
```

**Parameters**

Use the commands that you have configured under this instance.

**Example**

```
WS5100(config-crypto-isakmp)#no lifetime
WS5100(config-crypto-isakmp)#
```
6.1.11 service

Use this CLI command to invoke the service commands to troubleshoot or debug the instance configurations.

Syntax

```
service(clear|diag-shell|save-cli|show|start-shell|tethereal)
```

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear</td>
<td>Remove specified support information</td>
</tr>
<tr>
<td>diag-shell</td>
<td>Provide diag shell access</td>
</tr>
<tr>
<td>save-cli</td>
<td>Save CLI tree for all modes in html format</td>
</tr>
<tr>
<td>show</td>
<td>Show running system information</td>
</tr>
<tr>
<td>start-shell</td>
<td>Provide shell access</td>
</tr>
<tr>
<td>tethereal</td>
<td>Dump and analyze network traffic</td>
</tr>
</tbody>
</table>

Example

```
WS5100(config-crypto-isakmp)#service show ?
clear Remove specified support information
diag-shell Provide diag shell access
show  Show running system information
start-shell Provide shell access
tethereal Dump and analyze network traffic
```

```
WS5100(config-crypto-isakmp)#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 7.6k Oct 9 18:19
- 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-isakmp)#
```
### 6.1.12 show

Use this CLI command to view the current system information that is running on the WS5100 Series Wireless Switch.

**Syntax**

```
show <parameter>
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>?</td>
<td>Displays all the parameters for which the information can be viewed using the show command.</td>
</tr>
</tbody>
</table>

**Example**

```bash
WS5100(config-crypto-isakmp)#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 Management 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
```
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>snmp-server</td>
<td>Display SNMP engine parameters</td>
</tr>
<tr>
<td>startup-config</td>
<td>Contents of startup configuration</td>
</tr>
<tr>
<td>terminal</td>
<td>Display terminal configuration parameters</td>
</tr>
<tr>
<td>timezone</td>
<td>Display timezone</td>
</tr>
<tr>
<td>upgrade-status</td>
<td>Display last image upgrade status</td>
</tr>
<tr>
<td>users</td>
<td>Display information about terminal lines</td>
</tr>
<tr>
<td>version</td>
<td>Display software &amp; hardware version</td>
</tr>
<tr>
<td>wireless</td>
<td>Wireless configuration commands</td>
</tr>
</tbody>
</table>

WS5100(config-crypto-isakmp)#show
Use `crypto isakmp(client) configuration group default` to initiate `config-crypto-group` instance.

### 7.1 Crypto Client Config commands

Table 7.1 summarizes the `config-crypto-group` commands within the WS5100 Series Switch command line interface.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Ref.</th>
</tr>
</thead>
<tbody>
<tr>
<td>clrscr</td>
<td>Clears the display screen</td>
<td>page 7-3</td>
</tr>
<tr>
<td>dns</td>
<td>Domain Name Server</td>
<td>page 7-4</td>
</tr>
<tr>
<td>end</td>
<td>End current mode and change to EXEC mode</td>
<td>page 7-5</td>
</tr>
<tr>
<td>exit</td>
<td>End current mode and down to previous mode</td>
<td>page 7-6</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
<td>Ref.</td>
</tr>
<tr>
<td>---------</td>
<td>--------------------------------------</td>
<td>---------</td>
</tr>
<tr>
<td>help</td>
<td>Description of the interactive help system</td>
<td>page 7-7</td>
</tr>
<tr>
<td>service</td>
<td>Service Commands</td>
<td>page 7-8</td>
</tr>
<tr>
<td>show</td>
<td>Show running system information</td>
<td>page 7-9</td>
</tr>
<tr>
<td>wins</td>
<td>Windows name server</td>
<td>page 7-11</td>
</tr>
</tbody>
</table>
7.1.1 clrscr

Use this CLI command to clear the display screen.

Syntax

   clrscr

Parameters

None.

Example

   WS5100(config-crypto-group)#clr
   WS5100(config-crypto-group)#
7.1.2 dns

Use this CLI command to specify the DNS server address(es) to assign to a client.

Syntax

dns <IP Address>

Parameters

<table>
<thead>
<tr>
<th>&lt;IP Address&gt;</th>
<th>The first DNS server address to assign.</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;IP Address&gt; optional</td>
<td>The second DNS server address to assign.</td>
</tr>
</tbody>
</table>

Example

WS5100(config-crypto-group)#dns-server 172.1.17.1 172.1.17.3
WS5100(config-crypto-group)#
7.1.3 end
Use this CLI command to end and exit from the current mode and change to PRIV EXEC mode. The prompt now changes to WS5100#.

Syntax
   end

Parameters
   None.

Usage Guidelines

Example
   WS5100 (config-crypto-group)#end
   WS5100#
7.1.4 exit

Use this CLI command to end current mode and down to previous mode (GLOBAL-CONFIG). The prompt now changes to WS5100(config)#.

Syntax

exit

Parameters

None.

Example

WS5100(config-crypto-group)#exit
WS5100(config)#
7.1.5 help

Use this CLI command to access 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 back up 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

Use this CLI command to invoke the service commands to troubleshoot or debug the (config-crypto-isakmp) instance configurations.

Syntax

service(clear|diag-shell|save-cli|show|start-shell|tethereal)

Parameters

<table>
<thead>
<tr>
<th>clear</th>
<th>Remove specified support information</th>
</tr>
</thead>
<tbody>
<tr>
<td>diag-shell</td>
<td>Provide diag shell access</td>
</tr>
<tr>
<td>save-cli</td>
<td>Save CLI tree for all modes in html format</td>
</tr>
<tr>
<td>show</td>
<td>Show running system information</td>
</tr>
<tr>
<td>start-shell</td>
<td>Provide shell access</td>
</tr>
<tr>
<td>tethereal</td>
<td>Dump and analyze network traffic</td>
</tr>
</tbody>
</table>

Example

WS5100(config-crypto-group)#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-group)#service show

WS5100(config-crypto-group)#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    7.8k   Oct 9 18:46
  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-group)#
7.1.7 show

Use this CLI command to view the current system information that is running on the WS5100 Series Wireless Switch.

Syntax

    show <parameter>

Parameters

| ? | Displays all the parameters for which the information can be viewed using the show command. |

Example

    WS5100(config-crypto-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 Management 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
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>snmp-server</td>
<td>Display SNMP engine parameters</td>
</tr>
<tr>
<td>startup-config</td>
<td>Contents of startup configuration</td>
</tr>
<tr>
<td>terminal</td>
<td>Display terminal configuration parameters</td>
</tr>
<tr>
<td>timezone</td>
<td>Display timezone</td>
</tr>
<tr>
<td>upgrade-status</td>
<td>Display last image upgrade status</td>
</tr>
<tr>
<td>users</td>
<td>Display information about terminal lines</td>
</tr>
<tr>
<td>version</td>
<td>Display software &amp; hardware version</td>
</tr>
<tr>
<td>wireless</td>
<td>Wireless configuration commands</td>
</tr>
</tbody>
</table>

WS5100(config-crypto-group)#show
7.1.8 **wins**

Use this CLIL command to specify the Windows Internet Naming Service (WINS) name servers to assign to a client.

**Syntax**

```
wins <IP Address> <IP Address>
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;IP Address&gt;</td>
<td>The first WINS server address to assign.</td>
</tr>
<tr>
<td>&lt;IP Address&gt; optional</td>
<td>The second WINS server address to assign.</td>
</tr>
</tbody>
</table>

**Example**

```
WS5100(config-crypto-group)#wins 128.2.11.1 128.2.19.23
WS5100(config-crypto-group)#
```
Use `crypto isakmp(peer) [IP Address|dns|hostname]` to initiate a config-crypto-peer instance.

### 8.1 Crypto Peer Config commands

Table 8.1 summarizes the `config-crypto-peer` commands within the WS5100 Series Switch command line interface.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Ref.</th>
</tr>
</thead>
<tbody>
<tr>
<td>clrscr</td>
<td>Clears the display screen</td>
<td>page 8-3</td>
</tr>
<tr>
<td>end</td>
<td>End current mode and change to EXEC mode</td>
<td>page 8-4</td>
</tr>
<tr>
<td>exit</td>
<td>End current mode and down to previous mode</td>
<td>page 8-5</td>
</tr>
<tr>
<td>help</td>
<td>Description of the interactive help system</td>
<td>page 8-6</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
<td>Ref.</td>
</tr>
<tr>
<td>---------</td>
<td>------------------------------</td>
<td>-------</td>
</tr>
<tr>
<td>no</td>
<td>Negate a command or set its defaults</td>
<td>page 8-7</td>
</tr>
<tr>
<td>service</td>
<td>Service Commands</td>
<td>page 8-8</td>
</tr>
<tr>
<td>set</td>
<td>set</td>
<td>page 8-9</td>
</tr>
<tr>
<td>show</td>
<td>Show running system information</td>
<td>page 8-10</td>
</tr>
</tbody>
</table>
8.1.1 clrscr

Use this CLI command to clear the display screen.

Syntax

clrscr

Parameters

None.

Example

WS5100(config-crypto-peer)#clr
WS5100(config-crypto-peer)
8.1.2 end

Use this CLI command to end and exit from the current mode and change to PRIV EXEC mode. The prompt now changes to WS5100#.

Syntax

   end

Parameters

None.

Usage Guidelines

Example

   WS5100(config-crypto-peer)#end
   WS5100#
8.1.3 exit

Use this CLI command to end current mode and down to previous mode (GLOBAL-CONFIG). The
prompt now changes to WS5100(config)#.

Syntax

exit

Parameters
None.

Example

WS5100(config-crypto-peer)#exit
WS5100(config)#
8.1.4 help

Use this CLI command to access the systems 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**

Use this CLI command to negate a command or set its defaults.

**Syntax**

```
no <previous command used>
```

**Parameters**

Use the commands that you have configured under this instance.

**Example**

```
WS5100(config-crypto-peer)#no aggressive-mode
WS5100(config-crypto-peer)#
```
8.1.6 service

Use this CLI command to invoke the service commands to troubleshoot or debug the (config-crypto-isakmp) instance configurations.

**Syntax**

```
service(clear|diag-shell|save-cli|show|start-shell|tethereal)
```

**Parameters**

<table>
<thead>
<tr>
<th>clear</th>
<th>Remove specified support information</th>
</tr>
</thead>
<tbody>
<tr>
<td>diag-shell</td>
<td>Provide diag shell access</td>
</tr>
<tr>
<td>save-cli</td>
<td>Save CLI tree for all modes in html format</td>
</tr>
<tr>
<td>show</td>
<td>Show running system information</td>
</tr>
<tr>
<td>start-shell</td>
<td>Provide shell access</td>
</tr>
<tr>
<td>tethereal</td>
<td>Dump and analyze network traffic</td>
</tr>
</tbody>
</table>

**Example**

WS5100(config-crypto-peer)#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-peer)#service show

WS5100(config-crypto-peer)#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       8.0k  Oct 9  19:26
  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-peer)#
8.1.7 set

Use this CLI command to configure the aggressive-mode of crypto-peer.

Syntax

    set aggressive-mode (password)

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>aggressive-mode</td>
<td>aggressive mode</td>
</tr>
<tr>
<td>password</td>
<td>password</td>
</tr>
</tbody>
</table>

Example

WS5100(config-crypto-peer)#set aggressive-mode password CheckMeIn
WS5100(config-crypto-peer)#
8.1.8 show

Use this CLI command to view the current system information that is running on the WS5100 Series Wireless Switch.

Syntax

```
show <parameter>
```

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>?</td>
<td>Displays all the parameters for which the information can be viewed using the show command.</td>
</tr>
</tbody>
</table>

Example

```
WS5100(config-crypto-peer)# 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
evironment        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-peer)#show
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 then assigned to a crypto map using the map’s set transform-set command. For more details see crypto-map transform-set page 10-11.

9.1 Crypto Ipsec Config commands

Table 9.1 summarizes the config-crypto-ipsec commands within the WS5100 Series Switch command line interface

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Ref.</th>
</tr>
</thead>
<tbody>
<tr>
<td>clrscr</td>
<td>Clears the display screen</td>
<td>page 6-4</td>
</tr>
<tr>
<td>end</td>
<td>End current mode and change to EXEC mode</td>
<td>page 6-6</td>
</tr>
<tr>
<td>exit</td>
<td>End current mode and down to previous mode</td>
<td>page 6-7</td>
</tr>
<tr>
<td>help</td>
<td>Description of the interactive help system</td>
<td>page 6-10</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
<td>Ref.</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
<td>------</td>
</tr>
<tr>
<td>mode</td>
<td>IPSec Transporation Mode</td>
<td>page 9-3</td>
</tr>
<tr>
<td>no</td>
<td>Negate a command or set its defaults</td>
<td>page 6-12</td>
</tr>
<tr>
<td>service</td>
<td>Service Commands</td>
<td>page 6-13</td>
</tr>
<tr>
<td>show</td>
<td>Show running system information</td>
<td>page 9-4</td>
</tr>
</tbody>
</table>
9.1.1 mode

Use this CLI command to configure the IP Sec transportation mode.

Syntax

mode (transport | tunnel)

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>transport</td>
<td>Transport Mode</td>
</tr>
<tr>
<td>tunnel</td>
<td>Tunnel Mode</td>
</tr>
</tbody>
</table>

Example

WS5100 (config-crypto-ipsec)# mode transport
WS5100 (config-crypto-ipsec)#
9.1.2 show

Syntax
clrscr

Parameters

| ? | Displays all the parameters for which the 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 Management 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
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>timezone</td>
<td>Display timezone</td>
</tr>
<tr>
<td>upgrade-status</td>
<td>Display last image upgrade status</td>
</tr>
<tr>
<td>users</td>
<td>Display information about terminal lines</td>
</tr>
<tr>
<td>version</td>
<td>Display software &amp; hardware version</td>
</tr>
<tr>
<td>wireless</td>
<td>Wireless configuration commands</td>
</tr>
</tbody>
</table>

WS5100(config-crypto-ipsec)#show
config-crypto-map CLI commands are used to define a Certificate Authority (CA) trustpoint. This is a separate instance by itself but belongs to the crypto pki trustpoint mode under config instance.

### 10.1 Trustpoint Config commands

*Table 10.1* summarizes the config-crypto-map commands within the WS5100 Series Switch command line interface.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Ref.</th>
</tr>
</thead>
<tbody>
<tr>
<td>clrscr</td>
<td>Clears the display screen</td>
<td></td>
</tr>
<tr>
<td>end</td>
<td>End current mode and change to EXEC mode</td>
<td></td>
</tr>
<tr>
<td>exit</td>
<td>End current mode and down to previous mode</td>
<td></td>
</tr>
<tr>
<td>help</td>
<td>Description of the interactive help system</td>
<td></td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
<td>Ref.</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
<td>------</td>
</tr>
<tr>
<td>match</td>
<td>Match values</td>
<td></td>
</tr>
<tr>
<td>no</td>
<td>Negate a command or set its defaults</td>
<td></td>
</tr>
<tr>
<td>service</td>
<td>Service Commands</td>
<td></td>
</tr>
<tr>
<td>set</td>
<td>Set values for encryption/decryption</td>
<td></td>
</tr>
<tr>
<td>show</td>
<td>Show running system information</td>
<td></td>
</tr>
</tbody>
</table>
10.1.1 **clrscr**

Use this CLI command to clear the display screen.

**Syntax**

    clrscr

**Parameters**

None.

**Example**

    WS5100(config-crypto-map)#clr
    WS5100(config-crypto-map)
10.1.2 end

Use this CLI command to end and exit from the current mode and change to PRIV EXEC mode. The prompt now changes to WS5100#.

Syntax

```plaintext
end
```

Parameters

None.

Usage Guidelines

Example

```plaintext
WS5100(config-crypto-map)#end
WS5100#
```
10.1.3 exit

Use this CLI command to end current mode and down to previous mode (GLOBAL-CONFIG). The prompt now changes to WS5100(config)#.

Syntax
   exit

Parameters
None.

Example
   WS5100(config-crypto-map)#exit
   WS5100(config)#
10.1.4 help

Use the CLI 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

Use this CLI 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 to be secured. There are two types of crypto map entries: ipsec-manual and ipsec-ike. Each entry is given an index, which is 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 to be transmitted on an interface, the crypto map set associated with that interface is processed in order. The first crypto map entry that matches the packet will be used to secure the packet. If a suitable SA exists, that 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 an SA. If an SA does not exist, or if the packet fails any of the security checks (bad authentication, traffic does not match SA selectors, etc.), 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 you wish 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 (see crypto map on page 151). If no ACL is configured for a crypto map, then 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 product. The source information must be the local OS product and the destination must be the peer. Only extended access-lists can be used in crypto maps.
Example

The following example shows setting up an ACL (called TestList) and then 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

Use this CLI command to negate a command or set its defaults.

Syntax

no <previous command used>

Parameters

Use the commands that you have configured under this instance.

Example

WS5100(config-crypto-map)#no aggressive-mode
WS5100(config-crypto-map)#
10.1.7 service

Use this CLI command to invoke the service commands to troubleshoot or debug the (config-crypto-isakmp) instance configurations.

Syntax

```
service(clear|diag-shell|save-cli|show|start-shell|tethereal)
```

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear</td>
<td>Remove specified support information</td>
</tr>
<tr>
<td>diag-shell</td>
<td>Provide diag shell access</td>
</tr>
<tr>
<td>save-cli</td>
<td>Save CLI tree for all modes in html format</td>
</tr>
<tr>
<td>show</td>
<td>Show running system information</td>
</tr>
<tr>
<td>start-shell</td>
<td>Provide shell access</td>
</tr>
<tr>
<td>tethereal</td>
<td>Dump and analyze network traffic</td>
</tr>
</tbody>
</table>

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**

Use this CLI command to set the various set parameters of the peer device.

**Syntax**

- `set localid mode|peer|pfs|security-association|session-key|transformset`
- `set localid (IP Address|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**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>localid</strong></td>
<td></td>
</tr>
<tr>
<td>address</td>
<td></td>
</tr>
<tr>
<td>dn</td>
<td></td>
</tr>
<tr>
<td>hostname</td>
<td></td>
</tr>
<tr>
<td><strong>mode</strong></td>
<td></td>
</tr>
<tr>
<td>aggressive</td>
<td>aggressive mode</td>
</tr>
<tr>
<td>main</td>
<td>main mode</td>
</tr>
</tbody>
</table>
| **peer** | Use the set peer command to set the IP address of the peer device. This can be set for multiple remote peers. Remote peer can be either in IP Address or hostname.  

**NOTE** For manual mode, only one remote peer can be added for crypto map. |
| IP address | Enter the IP address of the peer device. If this is 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) that will be required during IPSec negotiation of security associations for this crypto map. Use the no form of this command to require no PFS. |
### group 1
IPSec is required to use Diffie-Hellman Group 1 (768-bit modulus) exchange during IPSec SA key generation.

### group 2
IPSec is required to use Diffie-Hellman Group 2 (1024-bit modulus) exchange during IPSec SA key generation.

### group 5
IPSec is required to use Diffie-Hellman Group 5

#### security-association
Use the set security-association lifetime command to define the lifetime (in kilobytes and/or seconds) of the IPSec SAs created by this crypto map.

<table>
<thead>
<tr>
<th>level(perhost)</th>
<th>ipsec sa level</th>
</tr>
</thead>
<tbody>
<tr>
<td>lifetime(kilobyte</td>
<td>seconds)</td>
</tr>
<tr>
<td></td>
<td>• kilobytes – SA lifetime limit in kilobytes.</td>
</tr>
<tr>
<td></td>
<td>• seconds – SA lifetime limit in seconds</td>
</tr>
</tbody>
</table>

#### session-key
Use the set session-key command to define the encryption and authentication keys for this crypto map.

| inbound | Use this keyword to define encryption keys for inbound traffic. |
| outbound | Use this keyword to define encryption keys for outbound traffic. |
| ah | Authentication header protocol |
| esp | Encapsulating security payload protocol. |
| SPI | Security Parameter Index |
| cipher <hex key data> | Specify encryption/decryption key. |
| authenticator <hex key data> | Specify authentication key. |

#### transformset <name>
Use the set transform-set command to assign a transform-set to a crypto map.
Usage Guidelines

```plaintext
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.

```plaintext
WS5100(config-crypto-map)#set pfs
``` If left at the default setting, no perfect forward secrecy (PFS) will be used during IPSec SA key generation. If PFS is specified, then the specified Diffie-Hellman Group exchange will be used for the initial and all subsequent key generation, thus providing no data linkage between prior keys and future keys.

```plaintext
WS5100(config-crypto-map)#set security-association lifetime (kilobytes|seconds)
``` Values can be entered for this command in both kilobytes and seconds. Whichever limit is reached first will end the security association.

```plaintext
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".

```plaintext
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 (see crypto ipsec transform-set <setname> <parameters> on page 150).

If no transform-set is configured for a crypto map, then the entry is incomplete and will have no effect on the system. For manual key crypto maps, only one transform set can be specified.

Example

```plaintext
WS5100(config-crypto-map)#set localid hostname TestMapHost
WS5100(config-crypto-map)#
```
10.1.9 show

Use this CLI command to view the current system information that is running on the WS5100 Series Wireless Switch.

Syntax

```
show <parameter>
```

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>?</td>
<td>Displays all the parameters for which the information can be viewed using the show command.</td>
</tr>
</tbody>
</table>

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
```
crypto-map

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
config-crypto-trustpoint CLI commands are used to define a Certificate Authority (CA) trustpoint. This is a separate instance by itself but belongs to the `crypto pki trustpoint` mode under `config` instance.

### 11.1 Trustpoint Config commands

Table 11.1 summarizes the `config-crypto-trustpoint` commands within the WS5100 Series Switch command line interface.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Ref.</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>clrscr</code></td>
<td>Clears the display screen</td>
<td>page 11-3</td>
</tr>
<tr>
<td><code>company-name</code></td>
<td>Company Name(Applicable only for request)</td>
<td>page 11-4</td>
</tr>
<tr>
<td><code>email</code></td>
<td>email</td>
<td>page 11-5</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
<td>Ref.</td>
</tr>
<tr>
<td>------------</td>
<td>-------------------------------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>end</td>
<td>End current mode and change to EXEC mode</td>
<td>page 11-6</td>
</tr>
<tr>
<td>exit</td>
<td>End current mode and down to previous mode</td>
<td>page 11-7</td>
</tr>
<tr>
<td>fqdn</td>
<td>Domain Name Configuration</td>
<td>page 11-8</td>
</tr>
<tr>
<td>help</td>
<td>Description of the interactive help system</td>
<td>page 11-9</td>
</tr>
<tr>
<td>ip-address</td>
<td>Internet Protocol (IP)</td>
<td>page 11-10</td>
</tr>
<tr>
<td>no</td>
<td>Negate a command or set its defaults</td>
<td>page 11-11</td>
</tr>
<tr>
<td>password</td>
<td>Challenge Password(Applicable only for request)</td>
<td>page 11-12</td>
</tr>
<tr>
<td>rsakeypair</td>
<td>Rsa Keypair to associate with the trustpoint</td>
<td>page 11-13</td>
</tr>
<tr>
<td>service</td>
<td>Service Commands</td>
<td>page 11-14</td>
</tr>
<tr>
<td>show</td>
<td>Show running system information</td>
<td>page 11-16</td>
</tr>
<tr>
<td>subject-name</td>
<td>Subject Name is a collection of required parameters to</td>
<td>page 11-18</td>
</tr>
</tbody>
</table>
11.1.1 clrscr

Use this CLI command to clear the display screen.

**Syntax**

```
clrscr
```

**Parameters**

None.

**Usage Guidelines**

**Example**

```
WS5100 (config-trustpoint) # clrscr
WS5100 (config-trustpoint) #
```
11.1.2 company-name

Trustpoint Config commands

Company Name(Applicable only for request)

Syntax

calendar

Parameters

<table>
<thead>
<tr>
<th>WORD</th>
<th>Company Name(2 to 64 characters)</th>
</tr>
</thead>
</table>

Usage Guidelines

Example

WS5100 (config-trustpoint)#company-name RetailKing
WS5100 (config-trustpoint)#
11.1.3 email

Trustpoint Config commands

Use this CLI command to configure your email ID for the trustpoint.

Syntax

```plaintext
email
```

Parameters

<table>
<thead>
<tr>
<th>WORD</th>
<th>email address(2 to 64 characters)</th>
</tr>
</thead>
</table>

Usage Guidelines

Example

```plaintext
WS5100(config-trustpoint)#email abcTestemailID@symbol.com
WS5100(config-trustpoint)#
```
11.1.4 end

Use this CLI command to end and exit from the current mode and change to PRIV EXEC mode. The prompt now changes to WS5100#.

Syntax

    end

Parameters

None.

Usage Guidelines

Example

    WS5100(config-trustpoint)#end
    WS5100#
11.1.5 exit

- Trustpoint Config commands

Use this CLI command to end current mode and down to previous mode (GLOBAL-CONFIG). The prompt now changes to WS5100(config)#

Syntax

```plaintext
exit
```

Parameters

None.

Usage Guidelines

Example

```plaintext
WS5100(config-trustpoint)#exit
WS5100(config)#
```
11.1.6 fqdn

Trustpoint Config commands

Use this CLI command to configure the domain name of the trustpoint.

Syntax
fqdn

Parameters
None

Usage Guidelines

Example
WS5100(config-trustpoint)#fqdn RetailKing.com
WS5100(config-trustpoint)#
11.1.7 help

Trustpoint Config commands

Use this CLI command to access the system's interactive help system.

Syntax

help

Parameters

None.

Usage Guidelines

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 Config commands

Use this CLI command to configure a IP adress for the trustpoint.

Syntax

ip-address

Parameters

| A.B.C.D | Enter the IP address to be configured for the trustpoint. |

Usage Guidelines

Example

WS5100(config-trustpoint)#ip-address 157.200.200.02
WS5100(config-trustpoint)#
11.1.9 no

- Trustpoint Config commands

Use this CLI command to negate a command or set its defaults.

Syntax

no <previous command used>

Parameters

None.

Usage Guidelines

Example

WS5100(config-trustpoint)#no ip-address
WS5100(config-trustpoint)#
11.1.10 password

Trustpoint Config commands

Use this CLI command to set the challenge password, applicable only for requests, to access trustpoint.

Syntax

password(0|2|WORD)

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Password is specified UNENCRYPTED. The password should be between 4 to 20 characters.</td>
</tr>
<tr>
<td>2</td>
<td>Password is encrypted with password-encryption secret. The string length of encrypted password should be of 44 to 64 characters.</td>
</tr>
<tr>
<td>WORD</td>
<td>Password(4 to 20 characters)</td>
</tr>
</tbody>
</table>

Usage Guidelines

Example

WS5100(config-trustpoint)#password 0 TestPassword
WS5100(config-trustpoint)#
11.1.11 rsakeypair

Trustpoint Config commands

Use this CLI command to configure a RSA Keypair to associate with the trustpoint.

Syntax

rsakeypair

Parameters

- **WORD**: Rsa Keypair Identifier

Usage Guidelines

RSA Key Pair Support feature allows you to configure WS5100 Series Wireless Switch to have Rivest, Shamir, and Adelman (RSA) key pairs. Thus, the WS5100 Series Wireless Switch software can maintain a different key pair for each identity certificate.

Example
### 11.1.12 service

**Trustpoint Config commands**

Use this CLI command to invoke the service commands to troubleshoot or debug the crypto pki trustpoint instance configurations.

**Syntax**

```
service(clear|diag-shell|save-cli|show|start-shell|tethereal)
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear</td>
<td>Remove specified support information.</td>
</tr>
<tr>
<td>diag-shell</td>
<td>Provide diagnostic shell access to debug and test the WS5100 Series Wireless Switch.</td>
</tr>
<tr>
<td>save-cli</td>
<td>Saves the CLI tree for all modes in html format.</td>
</tr>
<tr>
<td>show</td>
<td>Show running system information.</td>
</tr>
<tr>
<td>start-shell</td>
<td>Provide shell access.</td>
</tr>
<tr>
<td>tethereal</td>
<td>Dump and analyze network traffic.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

**Example**

```
WS5100(config-trustpoint)#service diag-shell
Diagnostic shell started for testing
diag >
```

Reboots the switch
Delete specified file from the system.
Exit from the CLI
Configures firmware fallback feature
Description of the interactive help system
Exit from the CLI
Negate a command or set its defaults
Halt and perform a warm reboot
Service Commands
Show running system information
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 Config commands**

Use this CLI command to view the current system information that is running on the WS5100 Series Wireless Switch.

**Syntax**

`show <parameter>`

**Parameters**

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>?</td>
<td>Displays all the parameters for which the information can be viewed using the show command.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

**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 Management 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     Display current active open connections
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      Display 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             Display wireless configuration commands

WS5100(config-trustpoint)#show access-list
Standard IP access list 1
   deny any rule-precedence 1
WS5100(config-trustpoint)#

WS5100(config-trustpoint)#show sessions
SESSION   USER       LOCATION        IDLE         START TIME
1       cli    Console           06:12m      Jan 1 00:00:00 1970
** 2       cli    157.235.206.39    00:00m      Jan 1 00:00:00 1970
WS5100(config-trustpoint)#

WS5100(config-trustpoint)#show users
Line       PID   User        Uptime      Location
  0 con 0  306               06:14:07     ttyS0
 130 vty 0  2744               00:25:49     0
WS5100(config-trustpoint)#

WS5100(config-trustpoint)#show upgrade-status
Last Image Upgrade Status : Successful
Last Image Upgrade Time   : Tue Aug 29 18:32:17 2006
WS5100(config-trustpoint)#
11.1.14 subject-name

Trustpoint Config commands

Use this CLI to create a subject name to configure a trustpoint. Subject name is a collection of required parameters to configure a trustpoint.

Syntax

subject-name

Parameters

<table>
<thead>
<tr>
<th>WORD</th>
<th>Enter a brief description as prompted by the parameter.</th>
</tr>
</thead>
</table>

Usage Guidelines

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)#
Use \texttt{(config-if)} instance to configure the interfaces — ethernet, vlan and tunnel associated with the WS5100 Series Wireless Switch.

### 12.1 Interface Config commands

Table 12.1 summarizes the \texttt{config-if} commands within the WS5100 Series Switch command line.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Ref.</th>
</tr>
</thead>
<tbody>
<tr>
<td>\texttt{clrscr}</td>
<td>Clears the display screen</td>
<td>page 12-3</td>
</tr>
<tr>
<td>\texttt{crypto}</td>
<td>crypto</td>
<td>page 12-4</td>
</tr>
<tr>
<td>\texttt{description}</td>
<td>Interface specific description</td>
<td>page 12-5</td>
</tr>
<tr>
<td>\texttt{duplex}</td>
<td>Set duplex to interface</td>
<td>page 12-6</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
<td>Ref.</td>
</tr>
<tr>
<td>-------------</td>
<td>---------------------------------------------------------------</td>
<td>--------</td>
</tr>
<tr>
<td>end</td>
<td>End current mode and change to EXEC mode</td>
<td>page 12-7</td>
</tr>
<tr>
<td>exit</td>
<td>End current mode and down to previous mode</td>
<td>page 12-8</td>
</tr>
<tr>
<td>help</td>
<td>Description of the interactive help system</td>
<td>page 12-9</td>
</tr>
<tr>
<td>ip</td>
<td>Internet Protocol (IP)</td>
<td>page 12-10</td>
</tr>
<tr>
<td>management</td>
<td>Sets the selected interface as management interface</td>
<td>page 12-11</td>
</tr>
<tr>
<td>mtu</td>
<td>Set mtu value for vlan interface</td>
<td>page 12-12</td>
</tr>
<tr>
<td>no</td>
<td>Negate a command or set its defaults</td>
<td>page 12-13</td>
</tr>
<tr>
<td>service</td>
<td>Service Commands</td>
<td>page 12-14</td>
</tr>
<tr>
<td>show</td>
<td>Show running system information</td>
<td>page 12-17</td>
</tr>
<tr>
<td>shutdown</td>
<td>Shutdown the selected interface</td>
<td>page 12-20</td>
</tr>
<tr>
<td>speed</td>
<td>Configure speed</td>
<td>page 12-21</td>
</tr>
<tr>
<td>switchport</td>
<td>Set switching mode characteristics</td>
<td>page 12-22</td>
</tr>
<tr>
<td>terminal</td>
<td>Set terminal line parameters</td>
<td>page 12-24</td>
</tr>
<tr>
<td>tunnel</td>
<td>protocol-over-protocol tunneling</td>
<td>page 12-25</td>
</tr>
</tbody>
</table>
12.1.1 clrscr

Use this CLI command to clear the display screen.

Syntax

```
clrscr
```

Parameters

None.

Usage Guidelines

Example

```
WS5100(config-if)#clrscr
WS5100(config-if)#
```
12.1.2 crypto

▶ Interface Config commands

Syntax

```plaintext
crypto map (WORD)
```

Parameters

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>map</td>
<td></td>
</tr>
<tr>
<td>WORD</td>
<td></td>
</tr>
</tbody>
</table>

Usage Guidelines

At any given instance you can add only one crypto mapset to one interface. WS5100 wireless switch does not support the same cryptomap set to be attached to multiple interfaces.

Example

EXAMPLE OUTPUT HERE
12.1.3 **description**

*Interface Config commands*

Use this CLI command to create an interface specific description.

**Syntax**

```plaintext
description
```

**Parameters**

<table>
<thead>
<tr>
<th>LINE</th>
<th>Characters describing this interface</th>
</tr>
</thead>
</table>

**Usage Guidelines**

**Example**

```
WS5100(config-if)#description "interface for RetailKing"
WS5100(config-if)#
```
12.1.4 duplex

Interface Config commands

Use this CLI command to configure a duplex type to the interface.

**NOTE**

- Duplexity can only be set for Ethernet type Interface. You need to enter the (config-if) instance using eth parameter of interface mode.
- Duplex can not be set until speed is set to non-auto value

**Syntax**

duplex(auto|full|half)

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>auto</td>
<td>set auto-negotiate</td>
</tr>
<tr>
<td>full</td>
<td>set full-duplex</td>
</tr>
<tr>
<td>half</td>
<td>set half-duplex</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

**Example**
12.1.5 end

Use this CLI command to end and exit from the current mode and change to PRIV EXEC mode. The prompt now changes to WS5100#.

Syntax
end

Parameters
None.

Usage Guidelines

Example
WS5100(config-if)# end
WS5100#
12.1.6 exit

Use this CLI command to end current mode and down to previous mode (GLOBAL-CONFIG). The prompt now changes to WS5100(config) #.

Syntax
exit

Parameters
None.

Usage Guidelines

Example

WS5100(config-if)#exit
WS5100(config) #
12.1.7 help

Use this CLI command to access the system's interactive help system.

**Syntax**
```
help
```

**Parameters**
None.

**Usage Guidelines**

**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

Use this CLI command to configure the IP address for the assigned ethernet, VLAN or tunnel.

Syntax

```plaintext
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)
ip helper-address A.B.C.D
ip nat (inside|outside)
```

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>access-group</td>
<td>Access group</td>
</tr>
<tr>
<td>(&lt;1-99&gt;</td>
<td>&lt;100-199&gt;)</td>
</tr>
<tr>
<td>(&lt;1300-1999&gt;</td>
<td>&lt;2000-2699&gt;)</td>
</tr>
<tr>
<td>WORD</td>
<td>Access List Name</td>
</tr>
<tr>
<td>in</td>
<td>Incoming packets</td>
</tr>
<tr>
<td>address</td>
<td>Set the IP address of an interface</td>
</tr>
<tr>
<td>A.B.C.D/M</td>
<td>IP address (e.g. 10.0.0.1/8)</td>
</tr>
<tr>
<td>dhcp</td>
<td>Use DHCP Client to obtain IP address for this interface</td>
</tr>
<tr>
<td>helper-address</td>
<td>Forward DHCP and BOOTP packets</td>
</tr>
<tr>
<td>A.B.C.D</td>
<td>IP to which DHCP and BOOTP packets are forwarded</td>
</tr>
<tr>
<td>nat</td>
<td>Network Address Translation (NAT)</td>
</tr>
<tr>
<td>inside</td>
<td>Inside interface</td>
</tr>
<tr>
<td>outside</td>
<td>Outside interface</td>
</tr>
</tbody>
</table>

Usage Guidelines

Example
12.1.9 management

Use this CLI command to configure the selected interface as management interface.

Syntax

```
management
```

Parameters

None.

Usage Guidelines

Example
12.1.10 mtu

Interface Config commands

Use this CLI command to set the mtu value for an VLAN interface.

NOTE This command is valid only with an VLAN interface.

Syntax

mtu <512-1500>

Parameters

| <512-1500> | Value of MTU in bytes. |

Usage Guidelines

Example

WS5100(config)#interface vlan 20
WS5100(config-if)#mtu 520
WS5100(config-if)#
12.1.11 no

Use this CLI command to negate a command or set its defaults.

**Syntax**

```
no <previous command used>
```

**Parameters**

None.

**Usage Guidelines**

**Example**

```
WS5100(config-if)# no mtu
WS5100(config-if)#
```
12.1.12 service

Use this CLI command to invoke the service commands to troubleshoot or debug the (config-if) instance configurations.

Syntax

    service (ap|clear|diag-shell|save-cli|show|start-shell|tethereal|wireless)
    service ap force-dump

Parameters

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ap</td>
<td>access-port serviceability parameters</td>
</tr>
<tr>
<td>force-dump</td>
<td>trigger the access-port to send a crash-dump to the wireless-switch.</td>
</tr>
<tr>
<td>clear</td>
<td>Remove specified support information.</td>
</tr>
<tr>
<td>diag-shell</td>
<td>Provide diagnostic shell access to debug and test the WS5100 Series Wireless Switch.</td>
</tr>
<tr>
<td>save-cli</td>
<td>Saves the CLI tree for all modes in html format.</td>
</tr>
<tr>
<td>show</td>
<td>Show running system information.</td>
</tr>
<tr>
<td>start-shell</td>
<td>Provide shell access.</td>
</tr>
<tr>
<td>tethereal</td>
<td>Dump and analyze network traffic.</td>
</tr>
<tr>
<td>wireless</td>
<td>Wireless parameters</td>
</tr>
</tbody>
</table>

Usage Guidelines

Example

    WS5100(config-if)#service ap force-dump
    WS5100(config-if)#
WS5100(config-if)#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-if)#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-if)#

WS5100(config-if)#service show

ap               access-port serviceability parameters
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
wireless        Wireless parameters

WS5100(config-if)#service show

WS5100(config-if)#service start-shell

Last password used: password with MAC 00:a0:f8:65:ea:8e
Password:

WS5100(config-if)#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-if)#service tethereal

WS5100(config-if)#service wireless ?
dump-core Create a core file of the ccsrvr process
dump-state Create a ccsrdr.dump file in nvram with internal state information
mu-history Enable mu association history
mu-history-clear Delete all mu association history files
rate-scale Enable wireless rate scaling (default)
request-ap-log Request ap Log

WS5100(config-if)#service wireless request-ap-log 1 ?
file output to file
log output to syslog

WS5100(config-if)#
12.1.13 show

Use this CLI command to view the current system information that is running on the WS5100 Series Wireless Switch.

Syntax
show <parameter>

Parameters

| ? | Displays all the parameters for which the information can be viewed using the show command. |

Usage Guidelines

Example

```
WS5100(config-if)#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 Management 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-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

<table>
<thead>
<tr>
<th>Image</th>
<th>Build Date</th>
<th>Install Date</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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
    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
regulatory
information
for a particular country
self-heal-config            Self-Healing Configuration Parameters
sensor
parameters
unapproved-aps              Unapproved APs seen by access-port or
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)#
12.1.14 shutdown

Interface Config commands

Use this CLI command to shutdown the selected interface.

**Syntax**

```
shutdown
```

**Parameters**

None.

**Usage Guidelines**

**Example**

```
WS5100(config-if)#shutdown
WS5100(config-if)#
```
12.1.15 speed

Use this CLI command to configure the speed of the selected interface in Mbps.

Syntax

```
speed(10|100|1000|auto)
```

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>Force 10 Mbps operation</td>
</tr>
<tr>
<td>100</td>
<td>Force 100 Mbps operation</td>
</tr>
<tr>
<td>1000</td>
<td>Force 1000 Mbps operation</td>
</tr>
<tr>
<td>auto</td>
<td>Enable AUTO speed configuration</td>
</tr>
</tbody>
</table>

Usage Guidelines

Example

```
WS5100(config-if)#speed auto
WS5100(config-if)#
```
### 12.1.16 switchport

**Interface Config commands**

Use this CLI command to set switching mode characteristics of the selected interface.

**Syntax**

```plaintext
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**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>access</strong></td>
<td>Set access mode characteristics</td>
</tr>
<tr>
<td><strong>vlan</strong></td>
<td>Set VLAN when interface is in access mode</td>
</tr>
<tr>
<td><strong>&lt;1-4094&gt;</strong></td>
<td>Access VLAN ID</td>
</tr>
<tr>
<td><strong>mode</strong></td>
<td>Set the mode of the Layer2 interface</td>
</tr>
<tr>
<td><strong>access</strong></td>
<td>Set the Layer2 interface as access</td>
</tr>
<tr>
<td><strong>trunk</strong></td>
<td>Set the Layer2 interface as trunk</td>
</tr>
<tr>
<td><strong>trunk</strong></td>
<td>Set trunking mode characteristics</td>
</tr>
<tr>
<td><strong>(allowed)</strong></td>
<td>Set trunking mode allowed vlan characteristics</td>
</tr>
<tr>
<td><strong>vlan</strong></td>
<td>Set the allowed VLANs</td>
</tr>
<tr>
<td><strong>add</strong></td>
<td>Add VLANs to the current list</td>
</tr>
<tr>
<td><strong>none</strong></td>
<td>Allow no VLANs to Xmit/Rx through the Layer2 interface</td>
</tr>
<tr>
<td><strong>remove</strong></td>
<td>Remove VLANs from the current list</td>
</tr>
<tr>
<td><strong>VLAN_ID</strong></td>
<td>The List of the VLAN IDs that will be added/removed. e.g. 10-20,25,30-35</td>
</tr>
<tr>
<td><strong>(native)</strong></td>
<td>Set native trunking characteristics</td>
</tr>
<tr>
<td><strong>tagged</strong></td>
<td>Tag the native vlan</td>
</tr>
<tr>
<td><strong>vlan</strong></td>
<td>Set the native VLAN for classifying untagged traffic</td>
</tr>
<tr>
<td><strong>&lt;1-4094&gt;</strong></td>
<td>The native VLAN id when interface is in trunking mode</td>
</tr>
</tbody>
</table>
Usage Guidelines

Example

WS5100(config-if)#switchport mode access
WS5100(config-if)#
12.1.17 terminal

Use this command to set the length/number of lines to be displayed on the terminal window.

Syntax

```
terminal (monitor | no)
terminal no (monitor)
```

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>monitor</code></td>
<td>Copy debug output to the current terminal line</td>
</tr>
<tr>
<td><code>no</code></td>
<td>Negate a command or set its defaults</td>
</tr>
<tr>
<td><code>monitor</code></td>
<td>Copy debug output to the current terminal line</td>
</tr>
</tbody>
</table>

Usage Guidelines

Example

```
WS5100 (config-if)# terminal no monitor
WS5100 (config-if)#

WS5100 (config-if)# terminal monitor
WS5100 (config-if)#
```
12.1.18 tunnel

Use this CLI command to configure protocol-over-protocol tunneling.

Syntax

- `tunnel(destination|source|ttl)`
- `tunnel destination A.B.C.D`
- `tunnel source A.B.C.D`
- `tunnel ttl <1-255>`

Parameters

<table>
<thead>
<tr>
<th>destination</th>
<th>source</th>
<th>A.B.C.D</th>
<th>ttl</th>
<th>&lt;1-255&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>destination of tunnel packets</td>
<td>source of tunnel packets</td>
<td>Internet Protocol (IP)</td>
<td>set time to live</td>
<td>ttl in seconds.</td>
</tr>
</tbody>
</table>

Usage Guidelines

Example

EXAMPLE OUTPUT HERE
Use (config-ext-nacl) instance to configure the ip access-list extended ACLs associated with the WS5100 Series Wireless Switch.

### 13.1 Extended ACL Config Commands

*Table 13.1* summarizes the `config-ext-nacl` commands within the WS5100 Series Switch command line.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Ref.</th>
</tr>
</thead>
<tbody>
<tr>
<td>clrscr</td>
<td>Clears the display screen</td>
<td>page 13-3</td>
</tr>
<tr>
<td>deny</td>
<td>Specify packets to reject</td>
<td>page 13-4</td>
</tr>
<tr>
<td>end</td>
<td>End current mode and change to EXEC mode</td>
<td>page 13-6</td>
</tr>
<tr>
<td>exit</td>
<td>End current mode and down to previous mode</td>
<td>page 13-7</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
<td>Ref.</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
<td>-----</td>
</tr>
<tr>
<td>help</td>
<td>Description of the interactive help system</td>
<td>page 13-8</td>
</tr>
<tr>
<td>mark</td>
<td>Specify packets to mark</td>
<td>page 13-9</td>
</tr>
<tr>
<td>no</td>
<td>Negate a command or set its defaults</td>
<td>page 13-11</td>
</tr>
<tr>
<td>permit</td>
<td>Specify packets to forward</td>
<td>page 13-12</td>
</tr>
<tr>
<td>service</td>
<td>Service Commands</td>
<td>page 13-14</td>
</tr>
<tr>
<td>show</td>
<td>Show running system information</td>
<td>page 13-16</td>
</tr>
<tr>
<td>terminal</td>
<td>Set terminal line parameters</td>
<td>page 13-18</td>
</tr>
</tbody>
</table>
13.1.1 clrscr

Use this CLI command to clear the display screen.

Syntax

clrscr

Parameters

None.

Usage Guidelines

Example

WS5100(config-ext-nacl)#clrscr
WS5100(config-ext-nacl)#
13.1.2 deny

Extended ACL Config Commands

Use this CLI command to specify packets that you want to reject.

Syntax

deny (icmp|ip|tcp|udp)

deny icmp (Source IP Address) (Destination Address)
(log|rule-precedence<1-5000>|wlan<1-32>)

deny icmp (Source IP Address) (Destination Address)
rule-precedence<1-5000>

deny icmp (Source IP Address) (Destination Address)
wlan<1-32> log rule-precedence<1-5000>

Syntax

deny ip (Source IP Address) (Destination IP Address)
(log|rule-precedence<1-500>|wlan<1-32>)

deny ip (Source IP Address) (Destination IP Address)
rule-precedence<1-500>

deny ip (Source IP Address) (Destination IP Address)
rul-rule-precedence<1-500>

deny ip (Source IP Address) (Destination IP Address)
wlan<1-32> log rule-precedence<1-500>

Syntax

deny (tcp|udp) (Source IP Address) (Destination IP Address)
(log|rule-precedence<1-5000>)

deny (tcp|udp) (Source IP Address) (Destination IP Address) log wlan <1-32>

deny (tcp|udp) (Source IP Address) (Destination IP Address) log rule-precedence <1-5000>

deny (tcp|udp) (Source IP Address) (Destination IP Address) log
(eq <1-65535>|range <1-65535> <1-65535>)

Syntax

deny (tcp|udp) (Source IP Address) (Destination IP Address) log
(eq <1-65535> |range <1-65535> <1-65535>)
deny (tcp|udp) (Source IP Address) (eq <1-65535>|range <1-65535> <1-65535>) (Destination IP Address) (eq <1-65535>|range <1-65535> <1-65535>)
log wlan <1-32>

deny (tcp|udp) (Source IP Address) (eq <1-65535>|range <1-65535> <1-65535>) (Destination IP Address) (eq <1-65535>|range <1-65535> <1-65535>)
log rule-precedence <1-5000>

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>icmp</td>
<td>ICMP Protocol</td>
</tr>
<tr>
<td>ip</td>
<td>Any Internet Protocol</td>
</tr>
<tr>
<td>Source IP</td>
<td>Source IP address can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>- A.B.C.D/M – Source IP address range to match</td>
</tr>
<tr>
<td></td>
<td>- any – Any source IP address</td>
</tr>
<tr>
<td></td>
<td>- host – Single host address</td>
</tr>
<tr>
<td>Destination IP</td>
<td>Destination IP address can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>- A.B.C.D/M – Destination IP address range to match</td>
</tr>
<tr>
<td></td>
<td>- any – Any destination IP address</td>
</tr>
<tr>
<td></td>
<td>- host – Single host address</td>
</tr>
<tr>
<td>&lt;0-255&gt;</td>
<td>ICMP Type</td>
</tr>
<tr>
<td>log</td>
<td>Log matches against this entry</td>
</tr>
<tr>
<td>rule-precedence&lt;1-5000&gt;</td>
<td>Access-list entry precedence</td>
</tr>
<tr>
<td>wlan&lt;1-32&gt;</td>
<td>Filter packets based on WLAN</td>
</tr>
<tr>
<td>eq&lt;1-65535&gt;</td>
<td>Match a specific destination port</td>
</tr>
<tr>
<td>range&lt;1-65535&gt; &lt;1-65535&gt;</td>
<td>Match a range of destination ports. You can select between Starting destination port and Ending destination port.</td>
</tr>
</tbody>
</table>

Usage Guidelines

Example

EXAMPLE OUTPUT HERE
13.1.3 end

Extended ACL Config Commands

Use this CLI command to end and exit from the current mode and change to PRIV EXEC mode. The prompt now changes to WS5100#.

Syntax

end

Parameters

None.

Usage Guidelines

Example

WS5100(config-ext-nacl)#end
WS5100#
13.1.4 exit

Extended ACL Config Commands

Use this CLI command to end current mode and down to previous mode (GLOBAL-CONFIG). The prompt now changes to \texttt{WS5100(config)#}.

**Syntax**

\texttt{exit}

**Parameters**

None.

**Usage Guidelines**

**Example**

\texttt{WS5100(config-ext-nacl)#exit}
\texttt{WS5100(config)#}
**13.1.5 help**

- **Extended ACL Config Commands**

Use this CLI command to access the system's interactive help system.

**Syntax**

`help`

**Parameters**

None.

**Usage Guidelines**

**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)#
```
13.1.6 mark

Extended ACL Config Commands

Use this CLI command to specify packet that you want to mark.

Syntax

mark(8021p|tos) (<0-7>|<0-255>) {icmp|ip|tcp|udp} (Source IP Address) (Destination IP Address)

mark(8021p|tos) (<0-7>|<0-255>) icmp (Source IP Address) (Destination IP Address) (<0-255>|log|wlan<1-32> rule-precedence<1-5000>

Syntax

mark(8021p|tos) (<0-7>|<0-255>) ip (Source IP Address) (Destination IP Address) (log|rule-precedence|wlan) log

mark(8021p|tos) (<0-7>|<0-255>) ip (Source IP Address) (Destination IP Address) (log|rule-precedence|wlan) rule-precedence<1-500

mark(8021p|tos) (<0-7>|<0-255>) ip (Source IP Address) (Destination IP Address) (log|wlan) rule-precedence<1-500

mark(8021p|tos) (<0-7>|<0-255>) ip (Source IP Address) (Destination IP Address) (log|rule-precedence|wlan|A.B.C.D) wlan<1-32> log rule-precedence<1-500

Syntax

mark(8021p|tos) (<0-7>|<0-255>) {tcp|udp} (Source IP Address) (Destination IP Address) (eq<1-65535>|log|range<1-65535> <1-65535>| rule-precedence<1-5000>|wlan<1-32>)

mark(8021p|tos) (<0-7>|<0-255>) {tcp|udp} (Source IP Address) (Destination IP Address) (eq<1-65535>|log|range<1-65535> <1-65535>| rule-precedence<1-5000>|wlan<1-32>) log

mark(8021p|tos) (<0-7>|<0-255>) {tcp|udp} (Source IP Address) (Destination IP Address) (eq<1-65535>|log|range<1-65535> <1-65535>| rule-precedence<1-5000>|wlan<1-32>) log wlan<1-32>

mark(8021p|tos) (<0-7>|<0-255>) {tcp|udp} (Source IP Address) (Destination IP Address) (eq<1-65535>|log|range<1-65535> <1-65535>| rule-precedence<1-5000>|wlan<1-32>) log rule-precedence<1-5000>
### Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8021p &lt;0-7&gt;</td>
<td>Modify 802.1p VLAN user priority</td>
</tr>
<tr>
<td>tos &lt;0-255&gt;</td>
<td>Modify TOS bits in IP header</td>
</tr>
<tr>
<td>icmp</td>
<td>ICMP Protocol</td>
</tr>
<tr>
<td>ip</td>
<td>Any Internet Protocol</td>
</tr>
<tr>
<td>tcp</td>
<td>TCP Protocol</td>
</tr>
<tr>
<td>udp</td>
<td>UDP Protocol</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Source IP Address</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>A.B.C.D/M</td>
<td>Source IP address range to match</td>
</tr>
<tr>
<td>any</td>
<td>Any source IP address</td>
</tr>
<tr>
<td>host</td>
<td>Single host address</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Destination IP Address</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>A.B.C.D/M</td>
<td>Destination IP address range to match</td>
</tr>
<tr>
<td>any</td>
<td>Any Destination IP address</td>
</tr>
<tr>
<td>host</td>
<td>Single host address</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>&lt;0-255&gt;</th>
<th>ICMP Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>log</td>
<td>Log matches against this entry</td>
</tr>
<tr>
<td>rule-precedence(1-5000)</td>
<td>Access-list entry precedence</td>
</tr>
<tr>
<td>wlan(1-32)</td>
<td>Filter packets based on WLAN</td>
</tr>
<tr>
<td>eq &lt;1-65535&gt;</td>
<td>Match a specific source port</td>
</tr>
<tr>
<td>range&lt;1-65535&gt; &lt;1-65535&gt;</td>
<td>Match a range of source ports</td>
</tr>
</tbody>
</table>

### Usage Guidelines

### Example

EXAMPLE OUTPUT HERE
13.1.7 no

- Extended ACL Config Commands

Use this CLI command to negate a command or set its defaults.

**Syntax**

```
no(deny|mark|permit)
```

This command negates all the syntax combinatins that you have used in `deny`, `mark` and `permit` to configure the Extended ACL.

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>deny</td>
<td>Specify packets to reject</td>
</tr>
<tr>
<td>mark</td>
<td>Specify packets to mark</td>
</tr>
<tr>
<td>permit</td>
<td>Specify packets to forward</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

**Example**
13.1.8 permit

Extended ACL Config Commands

Syntax

permit (icmp|ip|tcp|udp)

permit icmp (Source IP Address) (Destination Address) (log|rule-precedence <1-5000>|wlan <1-32>)

permit icmp (Source IP Address) (Destination Address) log rule-precedence <1-5000>

permit icmp (Source IP Address) (Destination Address) wlan <1-32> log rule-precedence <1-5000>

Syntax

permit ip (Source IP Address) (Destination IP Address) (log|rule-precedence <1-500>|wlan <1-32>)

permit ip (Source IP Address) (Destination IP Address) log rule-precedence <1-500>

permit ip (Source IP Address) (Destination IP Address) rule-precedence <1-500>

permit ip (Source IP Address) (Destination IP Address) wlan <1-32> log rule-precedence <1-500>

Syntax

permit (tcp|udp) (Source IP Address) (Destination IP Address)

permit (tcp|udp) (Source IP Address) (Destination IP Address) log

permit (tcp|udp) (Source IP Address) (Destination IP Address) log wlan <1-32>

permit (tcp|udp) (Source IP Address) (Destination IP Address) log rule-precedence <1-5000>

permit (tcp|udp) (Source IP Address) (eq <1-65535> | range <1-65535> <1-65535>) (Destination IP Address) (eq <1-65535> | range <1-65535> <1-65535>)

permit (tcp|udp) (Source IP Address) (eq <1-65535> | range <1-65535> <1-65535>) (Destination IP Address) (eq <1-65535> | range <1-65535> <1-65535>) log
Extended ACL Instance

`permit (tcp|udp) (Source IP Address) (eq <1-65535>|range <1-65535> <1-65535>) (Destination IP Address) (eq <1-65535>|range <1-65535> <1-65535>) log wlan <1-32>`

`permit (tcp|udp) (Source IP Address) (eq <1-65535>|range <1-65535> <1-65535>) (Destination IP Address) (eq <1-65535>|range <1-65535> <1-65535>) log rule-precedence <1-5000>`

### Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>icmp</code></td>
<td>ICMP Protocol</td>
</tr>
<tr>
<td><code>ip</code></td>
<td>Any Internet Protocol</td>
</tr>
<tr>
<td><code>Source IP</code></td>
<td>Source IP address can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• A.B.C.D/M – Source IP address range to match</td>
</tr>
<tr>
<td></td>
<td>• any – Any source IP address</td>
</tr>
<tr>
<td></td>
<td>• host – Single host address</td>
</tr>
<tr>
<td><code>Destination IP</code></td>
<td>Destination IP address can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• A.B.C.D/M – Destination IP address range to match</td>
</tr>
<tr>
<td></td>
<td>• any – Any destination IP address</td>
</tr>
<tr>
<td></td>
<td>• host – Single host address</td>
</tr>
<tr>
<td><code>&lt;0-255&gt;</code></td>
<td>ICMP Type</td>
</tr>
<tr>
<td><code>log</code></td>
<td>Log matches against this entry</td>
</tr>
<tr>
<td><code>rule-precedence &lt;1-5000&gt;</code></td>
<td>Access-list entry precedence</td>
</tr>
<tr>
<td><code>wlan &lt;1-32&gt;</code></td>
<td>Filter packets based on WLAN</td>
</tr>
<tr>
<td><code>eq &lt;1-65535&gt;</code></td>
<td>Match a specific destination port</td>
</tr>
<tr>
<td><code>range &lt;1-65535&gt; &lt;1-65535&gt;</code></td>
<td>Match a range of destination ports. You can select between Starting destination port and Ending destination port.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

### Example
13.1.9 **service**

*Extended ACL Config Commands*

Use this CLI command to invoke the service commands to troubleshoot or debug the \(\text{(config-if)}\) instance configurations.

**Syntax**

```
service(clear|diag-shell|save-cli|show|start-shell|tethereal)
```

**Parameters**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear</td>
<td>Remove specified support information.</td>
</tr>
<tr>
<td>diag-shell</td>
<td>Provide diagnostic shell access to debug and test the WS5100 Series Wireless Switch.</td>
</tr>
<tr>
<td>save-cli</td>
<td>Saves the CLI tree for all modes in html format.</td>
</tr>
<tr>
<td>show</td>
<td>Show running system information.</td>
</tr>
<tr>
<td>start-shell</td>
<td>Provide shell access.</td>
</tr>
<tr>
<td>tethereal</td>
<td>Dump and analyze network traffic.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

**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 start-shell
Last password used: password with MAC 00:a0:f8:65:ea:8e
Password:

WS5100(config-ext-nacl)#service tethereal ?
LINE tetheral 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
13.1.10 show

Extended ACL Config Commands

Use this CLI command to view the current system information that is running on the WS5100 Series Wireless Switch.

Syntax

show<parameter>

Parameters

<table>
<thead>
<tr>
<th>?</th>
<th>Displays all the parameters for which the information can be viewed using the show command.</th>
</tr>
</thead>
</table>

Usage Guidelines

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)
idap idap server
licenses Show any installed licenses
logging Show logging configuration and buffer
mac Media Access Control
management Display L3 Management 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.
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>redundancy-members</td>
<td>Display redundancy group members in detail</td>
</tr>
<tr>
<td>running-config</td>
<td>Current Operating configuration</td>
</tr>
<tr>
<td>securitymgr</td>
<td>Display debug info for ACL, VPN and NAT</td>
</tr>
<tr>
<td>sessions</td>
<td>Display current active open connections</td>
</tr>
<tr>
<td>snmp</td>
<td>Display SNMP engine parameters</td>
</tr>
<tr>
<td>snmp-server</td>
<td>Display SNMP engine parameters</td>
</tr>
<tr>
<td>startup-config</td>
<td>Contents of startup configuration</td>
</tr>
<tr>
<td>terminal</td>
<td>Display terminal configuration parameters</td>
</tr>
<tr>
<td>timezone</td>
<td>Display timezone</td>
</tr>
<tr>
<td>upgrade-status</td>
<td>Display last image upgrade status</td>
</tr>
<tr>
<td>users</td>
<td>Display information about terminal lines</td>
</tr>
<tr>
<td>version</td>
<td>Display software &amp; hardware version</td>
</tr>
<tr>
<td>wireless</td>
<td>Wireless configuration commands</td>
</tr>
</tbody>
</table>

WS5100(config-ext-nacl)#show
13.1.11 terminal

Extended ACL Config Commands

Use this command to set the length /number of lines to be displayed on the terminal window.

Syntax

```
terminal (monitor|no)
terminal no (monitor)
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>monitor</td>
<td>Copy debug output to the current terminal line</td>
</tr>
<tr>
<td>no</td>
<td>Negate a command or set its defaults</td>
</tr>
<tr>
<td>monitor</td>
<td>Copy debug output to the current terminal line</td>
</tr>
</tbody>
</table>

Usage Guidelines

Example

```
WS5100 (config-ext-nacl) # terminal monitor
WS5100 (config-ext-nacl) #

WS5100 (config-ext-nacl) # terminal no monitor
WS5100 (config-ext-nacl) #
```
Standard ACL Instance

Use `(config-std-nacl)` instance to configure the `ip access-list standard` ACLs associated with the WS5100 Series Wireless Switch.

### 14.1 Standard ACL Config Commands

*Table 14.1* summarizes the `config-std-nacl` commands within the WS5100 Series Switch command line.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Ref.</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>clrscr</code></td>
<td>Clears the display screen</td>
<td>page 14-3</td>
</tr>
<tr>
<td><code>deny</code></td>
<td>Specify packets to reject</td>
<td>page 14-4</td>
</tr>
<tr>
<td><code>end</code></td>
<td>End current mode and change to EXEC mode</td>
<td>page 14-5</td>
</tr>
<tr>
<td><code>exit</code></td>
<td>End current mode and down to previous mode</td>
<td>page 14-6</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
<td>Ref.</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
<td>------</td>
</tr>
<tr>
<td>help</td>
<td>Description of the interactive help system</td>
<td>page 14-7</td>
</tr>
<tr>
<td>mark</td>
<td>Specify packets to mark</td>
<td>page 14-8</td>
</tr>
<tr>
<td>no</td>
<td>Negate a command or set its defaults</td>
<td>page 14-9</td>
</tr>
<tr>
<td>permit</td>
<td>Specify packets to forward</td>
<td>page 14-10</td>
</tr>
<tr>
<td>service</td>
<td>Service Commands</td>
<td>page 14-11</td>
</tr>
<tr>
<td>show</td>
<td>Show running system information</td>
<td>page 14-13</td>
</tr>
<tr>
<td>terminal</td>
<td>Set terminal line parameters</td>
<td>page 14-15</td>
</tr>
</tbody>
</table>
14.1.1 clrscr

Use this CLI command to clear the display screen.

**Syntax**

```
clrscr
```

**Parameters**

None.

**Usage Guidelines**

**Example**

```
WS5100(config-std-nacl)#clrscr
WS5100(config-std-nacl)#
```
**14.1.2 deny**

*Standard ACL Config Commands*

Use this CLI command to specify packets that you want to reject.

**Syntax**

```plaintext
deny (A.B.C.D/M | any | host)
deny any (log | rule-precedence <1-500>)
deny any rule-precedence <1-500>
deny any wlan <1-32> (log | rule-precedence) (rule-precedence) <1-500>
deny host A.B.C.D
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>A.B.C.D/M</td>
<td>Source IP address range to match</td>
</tr>
<tr>
<td>any</td>
<td>Any source IP address</td>
</tr>
<tr>
<td>log</td>
<td>Log matches against this entry</td>
</tr>
<tr>
<td>rule-precedence &lt;1-500&gt;</td>
<td>Access-list entry precedence</td>
</tr>
<tr>
<td>&lt;1-500&gt;</td>
<td>Precedence Value</td>
</tr>
<tr>
<td>wlan &lt;1-32&gt;</td>
<td>Filter packets based on WLAN</td>
</tr>
<tr>
<td>&lt;1-32&gt;</td>
<td>WLAN index</td>
</tr>
<tr>
<td>host</td>
<td>Single host address</td>
</tr>
<tr>
<td>A.B.C.D</td>
<td>Exact source IP address to match</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

**Example**

```plaintext
WS5100(config-std-nacl)#deny any log rule-precedence 50
WS5100(config-std-nacl)#

WS5100(config-std-nacl)#deny any rule-precedence 60
WS5100(config-std-nacl)#

WS5100(config-std-nacl)#deny any wlan 30 log rule-precedence 250
WS5100(config-std-nacl)#
```
14.1.3 end

- **Standard ACL Config Commands**

Use this CLI command to end and exit from the current mode and change to PRIV EXEC mode. The prompt now changes to WS5100#.

**Syntax**

```plaintext
end
```

**Parameters**

None.

**Usage Guidelines**

**Example**

```plaintext
WS5100(config-std-nacl)#end
WS5100#
```
14.1.4 exit

Standard ACL Config Commands

Use this CLI command to end current mode and down to previous mode (GLOBAL-CONFIG). The prompt now changes to WS5100(config)#.

Syntax

exit

Parameters

None.

Usage Guidelines

Example

WS5100(config-std-nacl)#exit
WS5100(config)#
14.1.5 help

Use the CLI command to access the system's interactive help system.

**Syntax**
```
help
```

**Parameters**
None.

**Usage Guidelines**

**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)#
```
14.1.6 mark

**Standard ACL Config Commands**

Use this CLI command to specify packet that you want to mark.

**Syntax**

```plaintext
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>|wlan<1-32>|A.B>C.D)
mark(8021.1p<0-7>|tos<0-255>) any wlan<1-32>(log|rule-precedence<1-5000>)
```

**Parameters**

- 8021.1p: 802.1p priority
- tos: IP tos
- A.B.C.D/M: IP address/Mask
- any: Any
- host: Host
- log: Log
- rule-precedence: Rule precedence
- wlan: WLAN

**Usage Guidelines**

**Example**

EXAMPLE OUTPUT HERE
14.1.7 no

Use this CLI command to negate a command or set its defaults.

**Syntax**

```
no(deny|mark|permit)
```

This command negates all the syntax combinations that you have used in `deny`, `mark` and `permit` to configure the Extended ACL.

**Parameters**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>deny</td>
<td>Specify packets to reject</td>
</tr>
<tr>
<td>mark</td>
<td>Specify packets to mark</td>
</tr>
<tr>
<td>permit</td>
<td>Specify packets to forward</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

**Example**
14.1.8 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**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>A.B.C.D/M</td>
<td>Source IP address range to match</td>
</tr>
<tr>
<td>any</td>
<td>Any source IP address</td>
</tr>
<tr>
<td>log</td>
<td>Log matches against this entry</td>
</tr>
<tr>
<td>rule-precedence&lt;1-500&gt;</td>
<td>Access-list entry precedence</td>
</tr>
<tr>
<td>&lt;1-500&gt;</td>
<td>Precedence Value</td>
</tr>
<tr>
<td>wlan&lt;1-32&gt;</td>
<td>Filter packets based on WLAN</td>
</tr>
<tr>
<td>&lt;1-32&gt;</td>
<td>WLAN index</td>
</tr>
<tr>
<td>host</td>
<td>Single host address</td>
</tr>
<tr>
<td>A.B.C.D</td>
<td>Exact source IP address to match</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

**Example**

```
WS5100(config-std-nacl)#permit any log rule-precedence 50
WS5100(config-std-nacl)#

WS5100(config-std-nacl)#permit any rule-precedence 60
WS5100(config-std-nacl)#

WS5100(config-std-nacl)#permit any wlan 30 log rule-precedence 250
WS5100(config-std-nacl)#
```
14.1.9 service

Standard ACL Config Commands

Use this CLI command to invoke the service commands to troubleshoot or debug the (config-if) instance configurations.

Syntax

```
service(clear|diag-shell|save-cli|show|start-shell|tethereal)
```

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear</td>
<td>Remove specified support information.</td>
</tr>
<tr>
<td>diag-shell</td>
<td>Provide diagnostic shell access to debug and test the WS5100 Series Wireless Switch.</td>
</tr>
<tr>
<td>save-cli</td>
<td>Saves the CLI tree for all modes in html format.</td>
</tr>
<tr>
<td>show</td>
<td>Show running system information.</td>
</tr>
<tr>
<td>start-shell</td>
<td>Provide shell access.</td>
</tr>
<tr>
<td>tethereal</td>
<td>Dump and analyze network traffic.</td>
</tr>
</tbody>
</table>

Usage Guidelines

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 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)#
### 14.1.10 show

**Standard ACL Config Commands**

Use this CLI command to view the current system information that is running on the WS5100 Series Wireless Switch.

**Syntax**

```plaintext
show <parameter>
```

**Parameters**

| ? | Displays all the parameters for which the information can be viewed using the show command. |

**Usage Guidelines**

**Example**

```plaintext
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 Management 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.
```
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>redundancy-members</td>
<td>Display redundancy group members in detail</td>
</tr>
<tr>
<td>running-config</td>
<td>Current Operating configuration</td>
</tr>
<tr>
<td>securitymgr</td>
<td>Display debug info for ACL, VPN and NAT</td>
</tr>
<tr>
<td>sessions</td>
<td>Display current active open connections</td>
</tr>
<tr>
<td>snmp</td>
<td>Display SNMP engine parameters</td>
</tr>
<tr>
<td>snmp-server</td>
<td>Display SNMP engine parameters</td>
</tr>
<tr>
<td>startup-config</td>
<td>Contents of startup configuration</td>
</tr>
<tr>
<td>terminal</td>
<td>Display terminal configuration parameters</td>
</tr>
<tr>
<td>timezone</td>
<td>Display timezone</td>
</tr>
<tr>
<td>upgrade-status</td>
<td>Display last image upgrade status</td>
</tr>
<tr>
<td>users</td>
<td>Display information about terminal lines</td>
</tr>
<tr>
<td>version</td>
<td>Display software &amp; hardware version</td>
</tr>
<tr>
<td>wireless</td>
<td>Wireless configuration commands</td>
</tr>
</tbody>
</table>

WS5100(config-std-nacl)#show
14.1.11 terminal

Standard ACL Config Commands

Use this command to set the length /number of lines to be displayed on the terminal window.

Syntax

terminal (monitor|no)
terminal no (monitor)

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>monitor</td>
<td>Copy debug output to the current terminal line</td>
</tr>
<tr>
<td>no</td>
<td>Negate a command or set its defaults</td>
</tr>
<tr>
<td>monitor</td>
<td>Copy debug output to the current terminal line</td>
</tr>
</tbody>
</table>

Usage Guidelines

Example

WS5100(config-std-nacl)# terminal monitor
WS5100(config-std-nacl)#

WS5100(config-std-nacl)# terminal no monitor
WS5100(config-std-nacl)#
Use (config-ext-macl) instance to configure the \texttt{mac access-list extended} ACLs associated with the WS5100 Series Wireless Switch.

### 15.1 MAC Extended ACL Config Commands

\textit{Table 15.1} summarizes the \texttt{config-ext-macl} commands within the WS5100 Series Switch command line.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Ref.</th>
</tr>
</thead>
<tbody>
<tr>
<td>clrscr</td>
<td>Clears the display screen</td>
<td>page 15-3</td>
</tr>
<tr>
<td>deny</td>
<td>Specify packets to reject</td>
<td>page 15-4</td>
</tr>
<tr>
<td>end</td>
<td>End current mode and change to EXEC mode</td>
<td>page 15-6</td>
</tr>
<tr>
<td>exit</td>
<td>End current mode and down to previous mode</td>
<td>page 15-7</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
<td>Ref.</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
<td>-----</td>
</tr>
<tr>
<td>help</td>
<td>Description of the interactive help system</td>
<td>page 15-8</td>
</tr>
<tr>
<td>mark</td>
<td>Specify packets to mark</td>
<td>page 15-9</td>
</tr>
<tr>
<td>no</td>
<td>Negate a command or set its defaults</td>
<td>page 15-11</td>
</tr>
<tr>
<td>permit</td>
<td>Specify packets to forward</td>
<td>page 15-12</td>
</tr>
<tr>
<td>service</td>
<td>Service Commands</td>
<td>page 15-13</td>
</tr>
<tr>
<td>show</td>
<td>Show running system information</td>
<td>page 15-15</td>
</tr>
<tr>
<td>terminal</td>
<td>Set terminal line parameters</td>
<td>page 15-17</td>
</tr>
</tbody>
</table>
15.1.1 clrscr

MAC Extended ACL Config Commands

Use this CLI command to clear the display screen.

Syntax

    clrscr

Parameters

None.

Usage Guidelines

Example

    WS5100(config-ext-macl)#clrscr
    WS5100(config-ext-macl)#
### 15.1.2 deny

**MAC Extended ACL Config Commands**

Use this CLI command to specify packets that you want to reject.

**Syntax**

```cli
deny (Source MAC Address) (Destination MAC Address)
  (dot1p<0-7>|type|vlan<1-4095>|wlan<1-32>) rule-precedence<1-5000>

deny (Source MAC Address) (Destination MAC Address) dot1p<0-7>
  rule-precedence<1-5000>

deny (Source MAC Address) (Destination MAC Address) type
  (<1-65535>|arp|ip|ipv6|vlan|wisp>) rule-precedence<1-5000>

deny (Source MAC Address) (Destination MAC Address) wlan<1-32>
  (dot1p<0-7>|type|vlan<1-4095>) rule-precedence<1-5000>
```

**Parameters**

<table>
<thead>
<tr>
<th>Source Mask</th>
<th>Destination Mask</th>
<th>Source MAC Address can be one of the following:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>• any — Any source host</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• host — Exact source MAC address to match</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Source Mask</th>
<th>Destination Mask</th>
<th>Destination MAC Address can be one of the following</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>• any — Any destination host</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• host — Exact destination MAC address to match</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dot1p&lt;0-7&gt;</td>
<td>802.1p priority</td>
</tr>
<tr>
<td>rule-precedence&lt;1-5000&gt;</td>
<td>Access-list entry precedence</td>
</tr>
<tr>
<td>type(&lt;1-65535&gt;</td>
<td>arp</td>
</tr>
<tr>
<td>vlan&lt;1-4095&gt;</td>
<td>VLAN ID</td>
</tr>
<tr>
<td>wlan&lt;1-32&gt;</td>
<td>Filter packets based on WLAN</td>
</tr>
</tbody>
</table>
Usage Guidelines

Example

EXAMPLE OUTPUT HERE
15.1.3 end

MAC Extended ACL Config Commands

Use this CLI command to end and exit from the current mode and change to PRIV EXEC mode. The prompt now changes to WS5100#.

Syntax

end

Parameters

None.

Usage Guidelines

Example

WS5100(config-ext-macl)#end
WS5100#

WS5100#
15.1.4 exit

MAC Extended ACL Config Commands

Use this CLI command to end current mode and down to previous mode (GLOBAL-CONFIG). The
prompt now changes to WS5100(config)#.

Syntax
exit

Parameters
None.

Usage Guidelines

Example
WS5100(config-ext-macl)#exit
WS5100(config)#
15.1.5 help

MAC Extended ACL Config Commands

Use this CLI command to access the system's interactive help system.

Syntax

```plaintext
help
```

Parameters

None.

Usage Guidelines

Example

```plaintext
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)#
```
### 15.1.6 mark

**MAC Extended ACL Config Commands**

Use this CLI command to specify packet that you want to mark.

**Syntax**

```plaintext
mark(802.1p<0-7>|tos<0-255>)(Source MAC Address)(Destination MAC Address)
dot1p<0-7>rule-precedence<1-5000>
mark(802.1p<0-7>|tos<0-255>)(Source MAC Address)(Destination MAC Address)
type(1-65535)|arp|ip|ipv6|vlan|wisp)rule-precedence<1-5000>
mark(802.1p<0-7>|tos<0-255>)(Source MAC Address)(Destination MAC Address)
vlan<1-4095>rule-precedence<1-5000>
mark(802.1p<0-7>|tos<0-255>)(Source MAC Address)(Destination MAC Address)
vlan<1-32}(dot1p<0-7>|type|vlan<1-4095>)rule-precedence<1-5000>
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8021p&lt;0-7&gt;</td>
<td>Modify 802.1p VLAN user priority</td>
</tr>
<tr>
<td>tos&lt;0-255&gt;</td>
<td>Modify TOS bits in IP header</td>
</tr>
<tr>
<td><strong>Source MAC Address</strong></td>
<td>Source MAC Address can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• <code>any</code> – Any source host</td>
</tr>
<tr>
<td></td>
<td>• <code>host</code> – Exact source MAC address to match</td>
</tr>
<tr>
<td><strong>Destination MAC Address</strong></td>
<td>Destination MAC Address can be one of the following</td>
</tr>
<tr>
<td></td>
<td>• <code>any</code> – Any destination host</td>
</tr>
<tr>
<td></td>
<td>• <code>host</code> – Exact destination MAC address to match</td>
</tr>
<tr>
<td>dot1p&lt;0-7&gt;</td>
<td>802.1p priority</td>
</tr>
<tr>
<td>rule-precedence&lt;1-5000&gt;</td>
<td>Access-list entry precedence</td>
</tr>
</tbody>
</table>
Usage Guidelines

| type{<1-65535>|arp|ip|ipv6|vlan|wisp} | EtherType  |
|---------------------------------------|------------|
| vlan{<1-4095>}                        | VLAN ID    |
| wlan{<1-32>}                          | Filter packets based on WLAN |

Example

EXAMPLE OUTPUT HERE
15.1.7 no

MAC Extended ACL Config Commands

Use this CLI command to negate a command or set its defaults.

Syntax

no(deny|mark|permit)

This command negates all the syntax combinatins that you have used in deny, mark and permit to configure the Extended ACL.

Parameters

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>deny</td>
<td>Specify packets to reject</td>
</tr>
<tr>
<td>mark</td>
<td>Specify packets to mark</td>
</tr>
<tr>
<td>permit</td>
<td>Specify packets to forward</td>
</tr>
</tbody>
</table>

Usage Guidelines

Example

EXAMPLE OUTPUT HERE
15.1.8 permit

MAC Extended ACL Config Commands

Use this CLI command to specify packets that you want to forward.

Syntax

```
permit(Source MAC Address) (Destination MAC Address)
(dot1p<0-7> | type| vlan<1-4095> | wlan<1-32>) rule-precedence<1-5000>
```

```
permit(Source MAC Address) (Destination MAC Address) dot1p<0-7>
rule-precedence<1-5000>
```

```
permit(Source MAC Address) (Destination MAC Address) type
(<1-65535> | arp| ip| ipv6| vlan| wisp>) rule-precedence<1-5000>
```

```
permit(Source MAC Address) (Destination MAC Address) wlan<1-32>
(dot1p<0-7> | type| vlan<1-4095>) rule-precedence<1-5000>
```

Parameters

<table>
<thead>
<tr>
<th>Source MAC Address</th>
<th>Source MAC Address can be one of the following:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Source MAC address and mask</td>
</tr>
<tr>
<td></td>
<td>any</td>
</tr>
<tr>
<td></td>
<td>Any source host</td>
</tr>
<tr>
<td></td>
<td>host</td>
</tr>
<tr>
<td></td>
<td>Exact source MAC address to match</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Destination MAC Address</th>
<th>Destination MAC Address can be one of the following</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Destination MAC address and mask</td>
</tr>
<tr>
<td></td>
<td>any</td>
</tr>
<tr>
<td></td>
<td>Any destination host</td>
</tr>
<tr>
<td></td>
<td>host</td>
</tr>
<tr>
<td></td>
<td>Exact destination MAC address to match</td>
</tr>
</tbody>
</table>

| dot1p<0-7> | 802.1p priority |
| rule-precedence<1-5000> | Access-list entry precedence |
| type(<1-65535>|arp|ip|ipv6|vlan|wisp) | EtherType |
| vlan<1-4095> | VLAN ID |
| wlan<1-32> | Filter packets based on WLAN |
15.1.9 service

MAC Extended ACL Config Commands

Syntax

Use this CLI command to invoke the service commands to troubleshoot or debug the (config-if) instance configurations.

Syntax

```
service(clear|diag-shell|save-cli|show|start-shell|tethereal)
```

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear</td>
<td>Remove specified support information.</td>
</tr>
<tr>
<td>diag-shell</td>
<td>Provide diagnostic shell access to debug and test the WS5100 Series Wireless Switch.</td>
</tr>
<tr>
<td>save-cli</td>
<td>Saves the CLI tree for all modes in html format.</td>
</tr>
<tr>
<td>show</td>
<td>Show running system information.</td>
</tr>
<tr>
<td>start-shell</td>
<td>Provide shell access.</td>
</tr>
<tr>
<td>tethereal</td>
<td>Dump and analyze network traffic.</td>
</tr>
</tbody>
</table>

Usage Guidelines

Example

```
WS5100(config-ext-macl)#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-macl)#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-macl)#

WS5100(config-ext-macl)#service show ?
cli Show CLI tree of current mode
crash-info Display command (except show commands) history.
info Display information about core, panic and AP dump files
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-macl)#service show

WS5100(config-ext-macl)#service start-shell
Last password used: password with MAC 00:a0:f8:65:ea:8e
WS5100(config-ext-macl)#

WS5100(config-ext-macl)#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-macl)#service tethereal
15.1.10 show

MAC Extended ACL Config Commands

Use this CLI command to view the current system information that is running on the WS5100 Series Wireless Switch.

Syntax

```plaintext
show<parameter>
```

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>?</td>
<td>Displays all the parameters for which the information can be viewed using the show command.</td>
</tr>
</tbody>
</table>

Usage Guidelines

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 state transition history of the switch.
```
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>redundancy-members</td>
<td>Display redundancy group members in detail</td>
</tr>
<tr>
<td>running-config</td>
<td>Current Operating configuration</td>
</tr>
<tr>
<td>securitymgr</td>
<td>Display debug info for ACL, VPN and NAT</td>
</tr>
<tr>
<td>sessions</td>
<td>Display current active open connections</td>
</tr>
<tr>
<td>snmp</td>
<td>Display SNMP engine parameters</td>
</tr>
<tr>
<td>snmp-server</td>
<td>Display SNMP engine parameters</td>
</tr>
<tr>
<td>startup-config</td>
<td>Contents of startup configuration</td>
</tr>
<tr>
<td>terminal</td>
<td>Display terminal configuration parameters</td>
</tr>
<tr>
<td>timezone</td>
<td>Display timezone</td>
</tr>
<tr>
<td>upgrade-status</td>
<td>Display last image upgrade status</td>
</tr>
<tr>
<td>users</td>
<td>Display information about terminal lines</td>
</tr>
<tr>
<td>version</td>
<td>Display software &amp; hardware version</td>
</tr>
<tr>
<td>wireless</td>
<td>Wireless configuration commands</td>
</tr>
</tbody>
</table>

WS5100(config-ext-macl)#show
15.11 **terminal**

> **MAC Extended ACL Config Commands**

Use this command to set the length /number of lines to be displayed on the terminal window.

**Syntax**

```command
terminal (monitor|no)
terminal no (monitor)
```

**Parameters**

<table>
<thead>
<tr>
<th></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>monitor</td>
<td>Copy debug output to the current terminal line</td>
</tr>
<tr>
<td>no</td>
<td>Negate a command or set its defaults</td>
</tr>
<tr>
<td>monitor</td>
<td>Copy debug output to the current terminal line</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

**Example**

```command
WS5100 (config-ext-macl)# terminal monitor
WS5100 (config-ext-macl)#

WS5100 (config-ext-macl)# terminal no monitor
WS5100 (config-ext-macl)#
```
The `radius-server local` cli command takes you to radius server mode. The local (Onboard) radius server configuration commands are listed under this mode. Use `(config-radsrv)` instance to configure local radius server parameters associated with the WS5100 Series Wireless Switch.

### 16.1 Radius Configuration Commands

*Table 16.1* summarizes the Global Config commands within the WS5100 Series Switch command line.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Ref.</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>authentication</code></td>
<td>Radius authentication</td>
<td>page 16-3</td>
</tr>
<tr>
<td><code>ca</code></td>
<td>Configure ca certificate parameters</td>
<td>page 16-4</td>
</tr>
<tr>
<td><code>clrscr</code></td>
<td>Clears the display screen</td>
<td>page 16-5</td>
</tr>
<tr>
<td><code>crl-check</code></td>
<td>Certificate Revocation List (CRL) check</td>
<td>page 16-6</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
<td>Ref.</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
<td>-----</td>
</tr>
<tr>
<td>end</td>
<td>End current mode and change to EXEC mode</td>
<td>page 16-7</td>
</tr>
<tr>
<td>exit</td>
<td>End current mode and down to previous mode</td>
<td>page 16-8</td>
</tr>
<tr>
<td>group</td>
<td>Configure radius user group parameters.</td>
<td>page 16-9</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE</strong> This command create another sub-instance called config-radsrv-group with its own set of command summary.</td>
<td></td>
</tr>
<tr>
<td>help</td>
<td>Description of the interactive help system</td>
<td>page 16-21</td>
</tr>
<tr>
<td>ldap-server</td>
<td>ldap server parameters</td>
<td>page 16-22</td>
</tr>
<tr>
<td>nas</td>
<td>Radius client</td>
<td>page 16-23</td>
</tr>
<tr>
<td>no</td>
<td>Negate a command or set its defaults</td>
<td>page 16-24</td>
</tr>
<tr>
<td>proxy</td>
<td>Radius proxy server</td>
<td>page 16-25</td>
</tr>
<tr>
<td>rad-user</td>
<td>Radius user configuration</td>
<td>page 16-27</td>
</tr>
<tr>
<td>server</td>
<td>Configure server certificate parameters</td>
<td>page 16-28</td>
</tr>
<tr>
<td>service</td>
<td>Service Commands</td>
<td>page 16-29</td>
</tr>
<tr>
<td>show</td>
<td>Show running system information</td>
<td>page 16-30</td>
</tr>
<tr>
<td>terminal</td>
<td>Set terminal line parameters</td>
<td>page 16-32</td>
</tr>
</tbody>
</table>
16.1.1 authentication

Radius Configuration Commands

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

<table>
<thead>
<tr>
<th>data-source</th>
<th>Radius Datasource for user authentication</th>
</tr>
</thead>
<tbody>
<tr>
<td>eap-auth-type</td>
<td>Radius Eap and Default authentication type configuration</td>
</tr>
<tr>
<td>all</td>
<td>Enable both ttls and peap</td>
</tr>
<tr>
<td>peap-gtc</td>
<td>Eap type peap with Default auth type gtc</td>
</tr>
<tr>
<td>peap-mschapv2</td>
<td>Eap type peap with Default auth type mschapv2</td>
</tr>
<tr>
<td>tls</td>
<td>Eap type tls</td>
</tr>
<tr>
<td>ttls-md5</td>
<td>EAP type ttls with Default auth type md5</td>
</tr>
<tr>
<td>ttls-mschapv2</td>
<td>EAP type ttls with Default auth type mschapv2</td>
</tr>
<tr>
<td>ttls-pap</td>
<td>EAP type ttls with Default auth type pap</td>
</tr>
</tbody>
</table>

Usage Guidelines

Example
### 16.1.2 ca

> Radius Configuration Commands

Use this CLI command to configure CA (Certificate Authority) parameters.

**Syntax**

```
ca trust-point(WORD)
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>trust-point</td>
<td>Trust point configuration</td>
</tr>
<tr>
<td>WORD</td>
<td>Existing trust point name</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Configure the trustpoint that is used by the local radius server. Ensure you create the `trustpoint` before it is used by the `crypto pki trustpoint` command.

**Example**
**16.1.3 clrscr**

*Radius Configuration Commands*

Use this CLI command to clear the display screen.

**Syntax**

```plaintext
clrscr
```

**Parameters**

None.

**Usage Guidelines**

**Example**

```
WS5100(config-radsrv)#clrscr
WS5100(config-radsrv)#
```
16.1.4 crl-check

Radius Configuration Commands

Use this CLI command to enable Certificate Revocation List (CRL) check. To enable the certificate revocation list ensure the crl list is loaded using `crypto pki import <trustpoint-name> crl` command.

Syntax

`crl-check`

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>enable CRL check</td>
</tr>
</tbody>
</table>

Usage Guidelines

Example

```
WS5100(config-radsrv)#crl-check enable
WS5100(config-radsrv)#
```
### 16.1.5 end

*Radius Configuration Commands*

Use this CLI command to end and exit from the current mode and change to PRIV EXEC mode. The prompt now changes to `WS5100#`.

**Syntax**

```
end
```

**Parameters**

None.

**Usage Guidelines**

**Example**

```
WS5100(config-radsrv)#end
WS5100#
```
16.1.6 exit

Radius Configuration Commands

Use this CLI command to end current mode and down to previous mode (GLOBAL-CONFIG). The prompt now changes to WS5100(config)#.

Syntax

exit

Parameters

None.

Usage Guidelines

Example

WS5100(config-radsrv)#exit
WS5100(config)#
### 16.1.7 group

Use this CLI command to configure radius user group parameters. The system moves to a sub-instance mode when you create a new group and the prompt changes from **WS5100 (config-radsrv)#** to **WS5100 (config-radsrv-group)#**.

*Table 16.2* summarizes the Radius User Group commands within the (config-radsrv-group) sub-instance.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Ref.</th>
</tr>
</thead>
<tbody>
<tr>
<td>clrscr</td>
<td>Clears the display screen</td>
<td></td>
</tr>
<tr>
<td>end</td>
<td>End current mode and change to EXEC mode</td>
<td></td>
</tr>
<tr>
<td>exit</td>
<td>End current mode and down to previous mode</td>
<td></td>
</tr>
<tr>
<td>group</td>
<td>Configure radius user group parameters</td>
<td></td>
</tr>
<tr>
<td>guest-group</td>
<td>Guest group configuration</td>
<td></td>
</tr>
<tr>
<td>help</td>
<td>Description of the interactive help system</td>
<td></td>
</tr>
<tr>
<td>no</td>
<td>Negate a command or set its defaults</td>
<td></td>
</tr>
<tr>
<td>policy</td>
<td>Radius group access policy configuration</td>
<td></td>
</tr>
<tr>
<td>rad-user</td>
<td>Add Radius user to this group</td>
<td></td>
</tr>
<tr>
<td>service</td>
<td>Service Commands</td>
<td></td>
</tr>
<tr>
<td>show</td>
<td>Show running system information</td>
<td></td>
</tr>
<tr>
<td>terminal</td>
<td>Set terminal line parameters</td>
<td></td>
</tr>
</tbody>
</table>
16.1.7.1 clrscr

Radius Configuration Commands

Use this CLI command to clear the display screen.

Syntax

    clrscr

Parameters

None.

Example

    WS5100(config-radsrv-group)#clrscr
    WS5100(config-radsrv-group)#

16.1.7.2 end

Radius Configuration Commands

Use this CLI command to end and exit from the current mode and change to PRIV EXEC mode. The prompt now changes to WS5100#.

Syntax

    end

Parameters

None.

Example

    WS5100(config-radsrv-group)#end
    WS5100#
16.1.7.3 exit

Radius Configuration Commands

Use this CLI command to end current mode and down to previous mode (config-radsrv). The prompt now changes to WS5100(config) #.

Syntax
exit

Parameters
None.

Example
WS5100(config-radsrv-group)#exit
WS5100(config-radsrv)#group

16.1.7.4 group

Radius Configuration Commands

Use this CLI command to configure radius user group parameters.

Syntax
 group

Parameters

<table>
<thead>
<tr>
<th>WORD</th>
<th>Radius group name</th>
</tr>
</thead>
</table>

Example
WS5100(config-radsrv-group)#group TestGroup
WS5100(config-radsrv-group)#
16.1.7.5 guest-group

Use this CLI command to configure a guest group.

Syntax

    guest-group

Parameters

| enable       | Enable this group as guest group |

Example

    WS5100(config-radsrv-group)#guest-group enable
    WS5100(config-radsrv-group)#

16.1.7.6 help

Use this CLI command to access the system's interactive help system.

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)#
16.1.7.7 no

*Radius Configuration Commands*

Use this CLI 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**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>policy</strong></td>
<td>Radius group access policy configuration</td>
</tr>
<tr>
<td><strong>day</strong></td>
<td>Reset day of access policy for this group</td>
</tr>
<tr>
<td><strong>time</strong></td>
<td>Configure time of access policy for this group</td>
</tr>
<tr>
<td><strong>vlan</strong></td>
<td>VLAN id for this group</td>
</tr>
<tr>
<td><strong>wlan</strong></td>
<td>Configure wlan access policy for this group</td>
</tr>
<tr>
<td>&lt;1-32&gt;</td>
<td>Wlan Range</td>
</tr>
<tr>
<td>all</td>
<td>Remove all the wlan’s allowed</td>
</tr>
<tr>
<td><strong>rad-user</strong></td>
<td>Remove user from this group</td>
</tr>
<tr>
<td>WORD</td>
<td>Existing user name in this group</td>
</tr>
<tr>
<td>all</td>
<td>Remove all users from this group</td>
</tr>
<tr>
<td><strong>service</strong></td>
<td>Service Commands</td>
</tr>
<tr>
<td>radius</td>
<td>Disable radius server</td>
</tr>
</tbody>
</table>

**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 wlan
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)#

16.1.7.8 policy

Radius Configuration Commands

Use this CLI command to configure Radius group access policy.

Syntax

policy {day|time|vlan|wlan}
policy day {all|fr|mo|sa|su|th|tu|we|weekdays}
policy 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 Allow access only in week days (Mo-Fr)

time Configure time of access policy for this group

start Start time

end End Time must be greater than the start time
Example

```bash
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)#
```

16.1.7.9 **rad-user**

*Radius Configuration Commands*

Use the CLI command to add Radius user to this group.

**Syntax**

```
rad-user
```

**Parameters**

| WORD | Existing radius user name |

**Example**
### 16.1.7.10 service

**Radius Configuration Commands**

Use this CLI command to invoke the service commands to troubleshoot or debug the (config-radsrv-group) instance configurations. This command is also used to enable RADIUS server.

**Syntax**

```
service (clear|diag-shell|radius|save-cli|show|start-shell|tethereal)
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear</td>
<td>Remove specified support information</td>
</tr>
<tr>
<td>diag-shell</td>
<td>Provide diag shell access</td>
</tr>
<tr>
<td>radius</td>
<td>Enable radius server restart</td>
</tr>
<tr>
<td>save-cli</td>
<td>Save CLI tree for all modes in html format</td>
</tr>
<tr>
<td>show</td>
<td>Show running system information</td>
</tr>
<tr>
<td>start-shell</td>
<td>Provide shell access</td>
</tr>
<tr>
<td>tethereal</td>
<td>Dump and analyze network traffic</td>
</tr>
</tbody>
</table>

**Example**

```
WS5100(config-radsrv-group)#service radius restart
WS5100(config-radsrv-group)#
```

### 16.1.7.11 show

**Radius Configuration Commands**

Use this CLI command to view the current system information that is running on the WS5100 Series Wireless Switch.

**Syntax**

```
show <parameter>
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>?</td>
<td>Displays all the parameters for which the information can be viewed using the show command.</td>
</tr>
</tbody>
</table>
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 Management 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)#
16.1.7.12 terminal

Radius Configuration Commands

Use this command to set the length/number of lines to be displayed on the terminal window.

Syntax

```
terminal (monitor|no)
terminal no (monitor)
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>monitor</td>
<td>Copy debug output to the current terminal line</td>
</tr>
<tr>
<td>no</td>
<td>Negate a command or set its defaults</td>
</tr>
<tr>
<td>monitor</td>
<td>Copy debug output to the current terminal line</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

**Example**

```
WS5100(config-radsrv-group)#terminal monitor
WS5100(config-radsrv-group)#

WS5100(config-radsrv-group)#terminal no monitor
WS5100(config-radsrv-group)#
```
16.1.7.13 Example—Creating a Group

The usage of (config-radsrv-group) sub-instance is explained through an example illustrated below:

1. Create a group called **Sales** in the local radius server database.
   
   ```
   WS5100(config-radsrv)#group sales
   ```

2. Check the Radius user group configuration commands.
   
   ```
   WS5100(config-radsrv-group)#?
   ```
   Radius user group configuration commands:
   ```
   clrscr       Clears the display screen
   end          End current mode and change to EXEC mode
   exit         End current mode and down to previous mode
   group        Configure radius user group paramaters
   guest-group  Guest group configuration
   help         Description of the interactive help system
   no           Negate a command or set its defaults
   policy       Radius group access policy configuration
   rad-user     Add Radius user to this group
   service      Service Commands
   show         Show running system information
   ```

3. Use **policy** command to configure the group policies for the group created in Step 1.
   
   ```
   WS5100(config-radsrv-group)#policy ?
   ```
   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 **policy vlan** command to assign an vlan id of 10 to group Sales
   
   ```
   WS5100(config-radsrv-group)#policy vlan 10
   ```

5. Use **policy wlan** command to allow only authorised users to access this groups 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 group Sales
   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 service.
   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.
### 16.1.8 help

**Radius Configuration Commands**

Use this CLI command to access the system’s interactive help system.

#### Syntax

```
help
```

#### Parameters

None.

#### Usage Guidelines

**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)#
```
16.1.9 ldap-server

Radius Configuration Commands

Use this CLI command to configure LDAP server parameters.

Syntax

ldap-server (primary|secondary) host (A.B.C.D)

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>primary</td>
<td>primary LDAP server configuration</td>
</tr>
<tr>
<td>secondary</td>
<td>secondary LDAP server configuration</td>
</tr>
<tr>
<td>host</td>
<td>LDAP server IP configuration</td>
</tr>
<tr>
<td>A.B.C.D</td>
<td>LDAP server IP address</td>
</tr>
</tbody>
</table>

Usage Guidelines

Example
16.1.10 nas

Radius Configuration Commands

Use this CLI to configure the RADIUS client.

Syntax

nas {A.B.C.D/M} key {0|2|LINE}

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>A.B.C.D/M</td>
<td>Radius Client IP address</td>
</tr>
<tr>
<td>key</td>
<td>Radius Client shared key</td>
</tr>
<tr>
<td>0</td>
<td>Password is specified UNENCRYPTED</td>
</tr>
<tr>
<td>2</td>
<td>Password is encrypted with password-encryption secret</td>
</tr>
<tr>
<td>LINE</td>
<td>The secret (client shared secret), upto 32 characters.</td>
</tr>
</tbody>
</table>

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!!
16.1.11 no

Radius Configuration Commands

Use this CLI command to negate a command or set its defaults.

Syntax

no{authentication|ca|crl-check|group|ldap-server|nas|proxy|rad-user|server|service}

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>authentication</td>
<td>Radius authentication</td>
</tr>
<tr>
<td>ca</td>
<td>Configure ca certificate parameters</td>
</tr>
<tr>
<td>crl-check</td>
<td>Certificate Revocation List (CRL) check</td>
</tr>
<tr>
<td>group</td>
<td>Local radius server group configuration</td>
</tr>
<tr>
<td>ldap-server</td>
<td>Ldap server parameters</td>
</tr>
<tr>
<td>nas</td>
<td>Radius client</td>
</tr>
<tr>
<td>proxy</td>
<td>Radius proxy server</td>
</tr>
<tr>
<td>rad-user</td>
<td>Radius user configuration</td>
</tr>
<tr>
<td>server</td>
<td>Configure server certificate parameters</td>
</tr>
<tr>
<td>service</td>
<td>Service Commands</td>
</tr>
</tbody>
</table>

Usage Guidelines

Example

WS5100(config-radsrv)#no authentication data-source
WS5100(config-radsrv)#

WS5100(config-radsrv)#no ca trust-point
WS5100(config-radsrv)#
### 16.1.12 proxy

*Radius Configuration Commands*

Use this CLI command to configure RADIUS proxy server.

**Syntax**

```
proxy(realm|retry-count|retry-delay)
proxy realm(WORD) server(A.B.C.D) port(<1024-65535>) secret (0|2|WORD)
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>realm</strong> WORD</td>
<td>Realm name</td>
</tr>
<tr>
<td><strong>server</strong> A.B.C.D</td>
<td>proxy server ip address</td>
</tr>
<tr>
<td><strong>port</strong> &lt;1024-65535&gt;</td>
<td>proxy server port</td>
</tr>
<tr>
<td><strong>secret</strong> 0/2/WORD</td>
<td>proxy server secret string</td>
</tr>
<tr>
<td><strong>retry-count</strong> &lt;3-6&gt;</td>
<td>Proxy server retry count value</td>
</tr>
<tr>
<td><strong>retry-delay</strong> &lt;5-10&gt;</td>
<td>Proxy server retry delay time</td>
</tr>
<tr>
<td>0</td>
<td>Password is specified UNENCRYPTED</td>
</tr>
<tr>
<td>2</td>
<td>Password is encrypted with password-encryption</td>
</tr>
<tr>
<td><strong>WORD</strong></td>
<td>the proxy server shared secret upto 32 characters</td>
</tr>
<tr>
<td><strong>WORD</strong></td>
<td>the proxy server shared secret upto 32 characters</td>
</tr>
<tr>
<td><strong>&lt;3-6&gt;</strong></td>
<td>Retry count (in numbers)</td>
</tr>
<tr>
<td><strong>&lt;5-10&gt;</strong></td>
<td>retry delay time (in seconds)</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
**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)#
16.1.13 rad-user

Radius Configuration Commands

Use this CLI to configure RADIUS user parameters.

Syntax

```
rad-user (WORD) password (0|2) WORD
```

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>WORD</td>
<td>Enter user name upto 64 characters length</td>
</tr>
<tr>
<td>password(0</td>
<td>2)WORD</td>
</tr>
<tr>
<td>0</td>
<td>Password is specified UNENCRYPTED</td>
</tr>
<tr>
<td>2</td>
<td>Password is encrypted with password-encryption secret</td>
</tr>
<tr>
<td>WORD</td>
<td>Enter password upto 21 characters length</td>
</tr>
</tbody>
</table>

Usage Guidelines

Example

```
WS5100(config-radsrv)# rad-user TestRadUser password "I SPY U"
WS5100(config-radsrv)#
```
16.1.14 server

Radius Configuration Commands

Use this CLI command to configure server certificate parameters. You must create a trustpoint using `crypto-pki-trustpoint` or have an existing trustpoint to configure `server`.

**Syntax**

```
server trust-point
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>trust-point</td>
<td>Trust point configuration</td>
</tr>
<tr>
<td>WORD</td>
<td>Existing trust point name</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

**Example**

```
WS5100(config-radsrv)#server trust-point TestTP
%%Error: Specified Trust-point does not exists
WS5100(config-radsrv)#
```
16.1.15 service

Radius Configuration Commands

Use this CLI command to invoke the service commands to troubleshoot or debug the
(instance) instance configurations. This command is also used to enable RADIUS server.

Syntax

```
service(clear|diag-shell|radius|save-cli|show|start-shell|tethereal)
```

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear</td>
<td>Remove specified support information</td>
</tr>
<tr>
<td>diag-shell</td>
<td>Provide diag shell access</td>
</tr>
<tr>
<td>radius</td>
<td>Enable radius server restart</td>
</tr>
<tr>
<td>save-cli</td>
<td>Save CLI tree for all modes in html format</td>
</tr>
<tr>
<td>show</td>
<td>Show running system information</td>
</tr>
<tr>
<td>start-shell</td>
<td>Provide shell access</td>
</tr>
<tr>
<td>tethereal</td>
<td>Dump and analyze network traffic</td>
</tr>
</tbody>
</table>

Example

```
WS5100(config-radsrv-group)#service radius restart
WS5100(config-radsrv-group)#
```
16.1.16 show

Radius Configuration Commands

Use this CLI command to view the current system information that is running on the WS5100 Series Wireless Switch.

Syntax

show<parameter>

Parameters

? Displays all the parameters for which the 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 Display 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 Management 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
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sessions</td>
<td>Display current active open connections</td>
</tr>
<tr>
<td>snmp</td>
<td>Display SNMP engine parameters</td>
</tr>
<tr>
<td>snmp-server</td>
<td>Display SNMP engine parameters</td>
</tr>
<tr>
<td>startup-config</td>
<td>Contents of startup configuration</td>
</tr>
<tr>
<td>terminal</td>
<td>Display terminal configuration parameters</td>
</tr>
<tr>
<td>timezone</td>
<td>Display timezone</td>
</tr>
<tr>
<td>upgrade-status</td>
<td>Display last image upgrade status</td>
</tr>
<tr>
<td>users</td>
<td>Display information about terminal lines</td>
</tr>
<tr>
<td>version</td>
<td>Display software &amp; hardware version</td>
</tr>
<tr>
<td>wireless</td>
<td>Wireless configuration commands</td>
</tr>
</tbody>
</table>

WS5100(config-radsrv)#show
16.1.17 terminal

**Radius Configuration Commands**

Use this command to set the length/number of lines to be displayed on the terminal window.

**Syntax**

```
terminal (monitor|no)
terminal no (monitor)
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>monitor</td>
<td>Copy debug output to the current terminal line</td>
</tr>
<tr>
<td>no</td>
<td>Negate a command or set its defaults</td>
</tr>
<tr>
<td>monitor</td>
<td>Copy debug output to the current terminal line</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

**Example**

```
WS5100(config-radsrv)#terminal monitor
WS5100(config-radsrv)#

WS5100(config-radsrv)#terminal no monitor
WS5100(config-radsrv)#
```
Use (`config-wireless`) instance to configure local radius server parameters associated with the WS5100 Series Wireless Switch.

### 17.1 Wireless Configuration Commands

*Table 17.1* summarizes the Global Config commands within the WS5100 Series Switch command line.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Ref.</th>
</tr>
</thead>
<tbody>
<tr>
<td>adopt-unconf-radio</td>
<td>Adopt a radio even if its not yet configured. The default templates will be used for configuration.</td>
<td>page 17-4</td>
</tr>
<tr>
<td>adoption-pref-id</td>
<td>A preference identifier for this wireless switch. All radios configured with this preference identifier are more likely to be adopted by this wireless-switch</td>
<td>page 17-5</td>
</tr>
<tr>
<td>ap-detection</td>
<td>AP detection configuration commands</td>
<td>page 17-6</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
<td>Ref.</td>
</tr>
<tr>
<td>--------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------</td>
</tr>
<tr>
<td>broadcast-tx-speed</td>
<td>Set the rate at which broadcast and multicast traffic should be transmitted</td>
<td>page 17-8</td>
</tr>
<tr>
<td>clrscr</td>
<td>Clears the display screen</td>
<td>page 17-9</td>
</tr>
<tr>
<td>convert-ap</td>
<td>Change the mode of operation of an AP</td>
<td>page 17-10</td>
</tr>
<tr>
<td>country-code</td>
<td>Configure the country of operation. All existing radio configuration will be erased</td>
<td>page 17-11</td>
</tr>
<tr>
<td>dhcp-sniff-state</td>
<td>Record mobile-unit DHCP state information</td>
<td>page 17-14</td>
</tr>
<tr>
<td>dot11-shared-key-auth</td>
<td>Enable support for 802.11 shared key authentication.</td>
<td>page 17-15</td>
</tr>
<tr>
<td>end</td>
<td>End current mode and change to EXEC mode</td>
<td>page 17-16</td>
</tr>
<tr>
<td>exit</td>
<td>End current mode and down to previous mode</td>
<td>page 17-17</td>
</tr>
<tr>
<td>fix-windows-dhcp</td>
<td>Convert Windows DHCP server responses to be Unicast instead of Broadcast</td>
<td>page 17-18</td>
</tr>
<tr>
<td>help</td>
<td>Description of the interactive help system</td>
<td>page 17-19</td>
</tr>
<tr>
<td>ids</td>
<td>Intrusion Detection configuration commands</td>
<td>page 17-20</td>
</tr>
<tr>
<td>mac-auth-local</td>
<td>local mac authentication list</td>
<td>page 17-22</td>
</tr>
<tr>
<td>manual-wlan-mapping</td>
<td>Allow manual mapping/un-mapping of wlans to configured radios</td>
<td>page 17-23</td>
</tr>
<tr>
<td>mobility</td>
<td>Configure Mobility parameters</td>
<td>page 17-24</td>
</tr>
<tr>
<td>no</td>
<td>Negate a command or set its defaults</td>
<td>page 17-25</td>
</tr>
<tr>
<td>oversized-frames</td>
<td>Attempt to use oversized frames for data traffic</td>
<td>page 17-26</td>
</tr>
<tr>
<td>proxy-arp</td>
<td>Respond to ARP requests from the RON to WLAN on behalf of mobile-units</td>
<td>page 17-27</td>
</tr>
<tr>
<td>qos-mapping</td>
<td>QoS mappings between the wired and wireless domains</td>
<td>page 17-28</td>
</tr>
<tr>
<td>radio</td>
<td>Radio related commands</td>
<td>page 17-29</td>
</tr>
<tr>
<td>self-heal</td>
<td>Self Healing configuration commands</td>
<td>page 17-36</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
<td>Ref.</td>
</tr>
<tr>
<td>-----------------</td>
<td>-------------------------------------------------------</td>
<td>------------</td>
</tr>
<tr>
<td>sensor</td>
<td>Wireless Intrusion Protection System parameters</td>
<td>page 17-38</td>
</tr>
<tr>
<td>service</td>
<td>Service Commands</td>
<td>page 17-39</td>
</tr>
<tr>
<td>show</td>
<td>Show running system information</td>
<td>page 17-42</td>
</tr>
<tr>
<td>smart-scan-channels</td>
<td>Specify a list of channels that are used on the network. This list will be provided to mobile-units that can support partial scanning</td>
<td>page 17-44</td>
</tr>
<tr>
<td>terminal</td>
<td>Set terminal line parameters</td>
<td>page 17-45</td>
</tr>
<tr>
<td>wlan</td>
<td>Wireless LAN related commands</td>
<td>page 17-46</td>
</tr>
</tbody>
</table>
17.1.1 adopt-unconf-radio

Wireless Configuration Commands

Use this CLI command to adopt a radio even if its not yet configured. The default templates will be used for configuration.

Syntax

```
adopt-unconf-radio
```

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Enable the adoption of unconfigured radios</td>
</tr>
</tbody>
</table>

Usage Guidelines

Example

```
WS5100(config-wireless)#adopt-unconf-radio enable
WS5100(config-wireless)#
```
17.1.2 adoption-pref-id

Wireless Configuration Commands

Use this CLI command as a preference identifier for the WS5100 wireless switch. All radios configured with this preference identifier are more likely to be adopted by this wireless-switch.

**Syntax**

```
adoption-pref-id
```

**Parameters**

<table>
<thead>
<tr>
<th>&lt;1-65535&gt;</th>
<th>Select a Pref-ID within 1-65535.</th>
</tr>
</thead>
</table>

**Usage Guidelines**

**Example**

```
WS5100(config-wireless)#adoption-pref-id 500
WS5100(config-wireless)#
```
17.1.3 ap-detection

Wireless Configuration Commands

Use this CLI command to configure AP detection.

Syntax

```
ap-detection (approved|enable|max-aps|mu-assisted-scan|timeout)
ap-detection approved add <1-200> (MAC Address)(SSID)
ap-detection mu-assisted-scan (enable|refresh<10-86400>)
```

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>approved</td>
<td>The approved AP list</td>
</tr>
<tr>
<td>add</td>
<td>Add an entry to the approved AP list.</td>
</tr>
<tr>
<td>&lt;1-200&gt;</td>
<td>Index where this approved entry will be added: &lt;1-200&gt;</td>
</tr>
<tr>
<td>MAC Address</td>
<td>You can select either:</td>
</tr>
<tr>
<td></td>
<td>• MAC–Mac address in AA-BB-CC-DD-EE-FF format</td>
</tr>
<tr>
<td></td>
<td>• any–any Mac address</td>
</tr>
<tr>
<td>SSID</td>
<td>You can select either:</td>
</tr>
<tr>
<td></td>
<td>• LINE–A string of up to 32 characters</td>
</tr>
<tr>
<td></td>
<td>• any–any ssid</td>
</tr>
<tr>
<td>enable</td>
<td>Allow access-ports to look for APs</td>
</tr>
<tr>
<td>max-aps&lt;1-1000&gt;</td>
<td>Select the maximum amount of entries for unapproved-seen and approved-</td>
</tr>
<tr>
<td></td>
<td>seen that can showed.</td>
</tr>
<tr>
<td>mu-assisted-scan</td>
<td>mobile-unit assisted scanning</td>
</tr>
<tr>
<td>enable</td>
<td>enable mobile-unit assisted scanning</td>
</tr>
<tr>
<td>refresh&lt;10-86400&gt;</td>
<td>The period in seconds with which all scan-capable mobile-units are</td>
</tr>
<tr>
<td></td>
<td>requested to scan for neighboring APs.</td>
</tr>
<tr>
<td>timeout &lt;1-65535&gt;</td>
<td>The amount of seconds a AP will remain in the list after it is no longer seen</td>
</tr>
</tbody>
</table>

Usage Guidelines
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 max-aps 250
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)#

WS5100(config-wireless)#ap-detection timeout 500
WS5100(config-wireless)#
17.1.4 broadcast-tx-speed

Wireless Configuration Commands

Use this CLI command to configure the rate at which broadcast and multicast traffic should be transmitted between the WS5100 wireless switch and MU's.

Syntax

broadcast-tx-speed(range|throughput)

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>range</td>
<td>use lowest basic rate. Provides maximum range</td>
</tr>
<tr>
<td>throughput</td>
<td>use highest basic rate. Provides maximum throughput (default)</td>
</tr>
</tbody>
</table>

Usage Guidelines

Example

WS5100(config-wireless)#broadcast-tx-speed range
WS5100(config-wireless)#

WS5100(config-wireless)#broadcast-tx-speed throughput
WS5100(config-wireless)#
17.1.5 clrscr

Wireless Configuration Commands

Use this CLI command to clear the display screen.

Syntax

    clrscr

Parameters

None.

Usage Guidelines

Example

    WS5100(config-wireless)#clrscr
    WS5100(config-wireless)#
17.1.6 convert-ap

Wireless Configuration Commands

Use this CLI command to change the mode of operation of an AP to either sensor or standalone.

Syntax

```
convert-ap <1-48>(default|sensor|standalone)
```

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;1-48&gt;</td>
<td>Indices of the APs to be converted, from the ['show wireless ap' command]</td>
</tr>
<tr>
<td>default</td>
<td>do not force any conversion. Let the AP negotiate its normal mode of operation with the switch.</td>
</tr>
<tr>
<td>sensor</td>
<td>Convert an AP300 to operate as an IDS sensor. <strong>NOTE</strong> The switch will not be able to adopt this AP again until it is converted back to a regular AP300 using the [sensor MAC revert-to-ap] command</td>
</tr>
<tr>
<td>standalone</td>
<td>Convert a thin AP4131 back to a stand-alone AP. <strong>NOTE</strong> The switch will not be able to adopt this AP again until the AP is converted back to a thin-AP using the APs configuration interface</td>
</tr>
</tbody>
</table>

Usage Guidelines

Example
17.1.7 country-code

Wireless Configuration Commands

Use this CLI command to configure the country of operation. All existing radio configuration will be erased when you use this command.

Syntax

```
country-code
```

Parameters

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ae</td>
<td>United Arab Emirates</td>
</tr>
<tr>
<td>ar</td>
<td>Argentina</td>
</tr>
<tr>
<td>at</td>
<td>Austria</td>
</tr>
<tr>
<td>au</td>
<td>Australia</td>
</tr>
<tr>
<td>ba</td>
<td>Bosnia Herzegovina</td>
</tr>
<tr>
<td>be</td>
<td>Belgium</td>
</tr>
<tr>
<td>bg</td>
<td>Bulgaria</td>
</tr>
<tr>
<td>bm</td>
<td>Bahrain</td>
</tr>
<tr>
<td>br</td>
<td>Brazil</td>
</tr>
<tr>
<td>bs</td>
<td>Bahamas</td>
</tr>
<tr>
<td>by</td>
<td>Belarus</td>
</tr>
<tr>
<td>ca</td>
<td>Canada</td>
</tr>
<tr>
<td>ch</td>
<td>Switzerland</td>
</tr>
<tr>
<td>cl</td>
<td>Chile</td>
</tr>
<tr>
<td>cn</td>
<td>China</td>
</tr>
<tr>
<td>co</td>
<td>Colombia</td>
</tr>
<tr>
<td>cr</td>
<td>Costa Rica</td>
</tr>
<tr>
<td>cy</td>
<td>Cyprus</td>
</tr>
<tr>
<td>cz</td>
<td>Czech Republic</td>
</tr>
<tr>
<td>de</td>
<td>Germany</td>
</tr>
<tr>
<td>dk</td>
<td>Denmark</td>
</tr>
<tr>
<td>do</td>
<td>Dominican Republic</td>
</tr>
<tr>
<td>ec</td>
<td>Ecuador</td>
</tr>
<tr>
<td>ee</td>
<td>Estonia</td>
</tr>
<tr>
<td>eg</td>
<td>Egypt</td>
</tr>
<tr>
<td>es</td>
<td>Spain</td>
</tr>
</tbody>
</table>

Abbreviation Use the country abbreviation to configure the WS5100 switch to operate in a particular country.
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
17.1.8 dhcp-sniff-state

Wireless Configuration Commands

Use this CLI command to record mobile-unit DHCP state information.

Syntax

dhcp-sniff-state

Parameters

| enable | Enable support for recording DHCP state information for mobile-units. |

Usage Guidelines

Example

WS5100(config-wireless)#dhcp-sniff-state enable
WS5100(config-wireless)#
17.1.9 dot11-shared-key-auth

Wireless Configuration Commands

Use this CLI command to Enable support for 802.11 shared key authentication.

Syntax

```
dot11-shared-key-auth
```

Parameters

| enable | Enable support for shared key authentication. |

Usage Guidelines

**NOTE** Shared key authentication has known weaknesses that can compromise your WEP key. It should only be configured to accommodate wireless stations that are unable to carry out Open-System authentication.

Example

```
WS5100(config-wireless)#dot11-shared-key-auth enable
WS5100(config-wireless)#
```
17.1.10 end

Wireless Configuration Commands

Use this CLI command to end and exit from the current mode and change to PRIV EXEC mode. The prompt now changes to WS5100#.

Syntax

end

Parameters

None.

Usage Guidelines

Example

WS5100(config-wireless)#end
WS5100#
17.1.11 **exit**

Wireless Configuration Commands

Use this CLI command to exit current mode and down to previous mode (GLOBAL-CONFIG). The prompt now changes to `WS5100(config)#`.

**Syntax**
```
exit
```

**Parameters**
None.

**Usage Guidelines**

**Example**
```
WS5100(config-wireless)#exit
WS5100(config)#
```
17.1.12 fix-windows-dhcp

Wireless Configuration Commands

Use this CLI command to convert Windows DHCP server responses to be Unicast instead of Broadcast

Syntax

fix-windows-dhcp

Parameters

<table>
<thead>
<tr>
<th>enable</th>
<th>Enable support for converting Windows DHCP server responses</th>
</tr>
</thead>
</table>

Usage Guidelines

Example

```
WS5100(config-wireless)#fix-windows-dhcp enable
WS5100(config-wireless)#
```
17.1.13 **help**

Wireless Configuration Commands

Use the CLI command to access the system's interactive help system.

**Syntax**

```plaintext
help
```

**Parameters**

None.

**Usage Guidelines**

**Example**

```plaintext
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)#
```
17.1.14 ids

Wireless Configuration Commands

Use this CLI command to configure Intrusion Detection System.

Syntax

```
ids (anomaly-detection|detect-window|ex-ops)
```

```
ids anomaly-detection (all|invalid-frame-length|multicast-source|null-destination|same-source-destination|tkip-countermeasures|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-starts|probe-requests|unassoc-frames) (filter-ageout <0-86400> | threshold (mu|radio|switch) <0-9999>)
```

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>anomaly-detection</td>
<td>Configure parameters related to the detection of anomalous frames on the RF network.</td>
</tr>
<tr>
<td>all</td>
<td>Enable for all types of anomalous frames</td>
</tr>
<tr>
<td>invalid-frame-length</td>
<td>invalid frame lengths</td>
</tr>
<tr>
<td>multicast-source</td>
<td>broadcast or multicast source</td>
</tr>
<tr>
<td>null-destination</td>
<td>all zero's address</td>
</tr>
<tr>
<td>same-source-destination</td>
<td>identical source and destination addresses</td>
</tr>
<tr>
<td>tkip-countermeasures</td>
<td>filter mobile units that cause tkip countermeasures</td>
</tr>
<tr>
<td>weak-wep-iv</td>
<td>use of weak wep sequence numbers</td>
</tr>
<tr>
<td>enable</td>
<td>Enable monitoring and filtering</td>
</tr>
<tr>
<td>filter-ageout</td>
<td>Set the number of seconds for which mobile units will be filtered out.</td>
</tr>
<tr>
<td>detect-window &lt;5-300&gt;</td>
<td>Set the number of seconds for which information will be collected before analysis. All the thresholds are a function of this window size.</td>
</tr>
<tr>
<td>ex-ops</td>
<td>Configure parameters related to the detection of excessive operations on the RF network.</td>
</tr>
</tbody>
</table>
### Usage Guidelines

<table>
<thead>
<tr>
<th>Event Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>80211-replay-fails</td>
<td>802.11 replay check failure</td>
</tr>
<tr>
<td>all</td>
<td>Change for all types of excessive operations</td>
</tr>
<tr>
<td>association-requests</td>
<td>802.11 Authentication and Association Requests</td>
</tr>
<tr>
<td>authentication-fails</td>
<td>Failure to Authenticate with servers (Radius/Kerberos)</td>
</tr>
<tr>
<td>crypto-replay-fails</td>
<td>TKIP/CCMP IV replay check failure</td>
</tr>
<tr>
<td>decryption-fails</td>
<td>decryption failures</td>
</tr>
<tr>
<td>disassociations</td>
<td>Disassociation and Deauthentication frames</td>
</tr>
<tr>
<td>eap-starts</td>
<td>EAP (802.1x) Start frames</td>
</tr>
<tr>
<td>probe-requests</td>
<td>Probe Request frames</td>
</tr>
<tr>
<td>unassoc-frames</td>
<td>frames from unassociated stations</td>
</tr>
<tr>
<td>filter-ageout&lt;0-86400&gt;</td>
<td>Configure the number of seconds for which mobile units will be filtered out</td>
</tr>
<tr>
<td>threshold (mu/radio/switch)</td>
<td>Configure the threshold of events allowed in the detection window.</td>
</tr>
<tr>
<td></td>
<td>• mu–Use the threshold for monitoring on a per-mobile-unit basis.</td>
</tr>
<tr>
<td></td>
<td>• radio–Use the threshold for monitoring on a per-radio basis.</td>
</tr>
<tr>
<td></td>
<td>• switch–Use the threshold for monitoring at the switch level.</td>
</tr>
<tr>
<td>&lt;0-9999&gt;</td>
<td>The threshold of events allowed in the detection window</td>
</tr>
</tbody>
</table>

### Example

```bash
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)#
```
17.1.15 mac-auth-local

Wireless Configuration Commands

Use this CLI command to configure local MAC authentication list.

Syntax

mac-auth-local <1-1000> (allow|deny) (Starting MAC Address) (Ending MAC Address) (range/list of WLAN indices) WORD

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;1-1000&gt;</td>
<td>mac-auth-local entry</td>
</tr>
<tr>
<td>allow</td>
<td>allow mobile-units that match this rule to associate</td>
</tr>
<tr>
<td>deny</td>
<td>deny association to mobile-units that match this rule</td>
</tr>
<tr>
<td>Starting MAC Address</td>
<td>Starting mac address in AA-BB-CC-DD-EE-FF format</td>
</tr>
<tr>
<td>Ending MAC Address</td>
<td>Ending mac address in AA-BB-CC-DD-EE-FF format</td>
</tr>
<tr>
<td>Range/List of WLAN Indices</td>
<td>A list (eg: 1,3,7) or range (eg: 3-7) of wlan indices</td>
</tr>
<tr>
<td>WORD</td>
<td>Optional radio description substring</td>
</tr>
</tbody>
</table>

Usage Guidelines

Example

WS5100(config-wireless)# mac-auth-local 452 allow 12.11.11.120 12.11.11.150 3-7 TestString
WS5100(config-wireless)#
17.1.16 manual-wlan-mapping

Wireless Configuration Commands

Use this CLI command to manually map/un-map the wlans configured on a radio.

Syntax

    manual-wlan-mapping

Parameters

| enable | Enable support for manual-wlan-mapping |

Usage Guidelines

Example

    WS5100(config-wireless)#manual-wlan-mapping enable
    WS5100(config-wireless)#
17.1.17 mobility

Wireless Configuration Commands

Use this CLI command to configure mobility parameters

Syntax

mobility (enable|local-address|max-roam-period|peer)
mobility local-address (IP Address)
mobility max-roam-period<1-15>
mobility peer (IP Address)

Parameters

<table>
<thead>
<tr>
<th>enable</th>
<th>Enable Mobility Globally</th>
</tr>
</thead>
<tbody>
<tr>
<td>local-address</td>
<td>Set Local Addr for Mobility</td>
</tr>
<tr>
<td>A.B.C.D</td>
<td>IP Address of A.B.C.D format</td>
</tr>
<tr>
<td>max-roam-period&lt;1-15&gt;</td>
<td>Set Max Roam Period for an MU (in seconds)</td>
</tr>
<tr>
<td>peer</td>
<td>Add a Peer to this mobility region</td>
</tr>
<tr>
<td>A.B.C.D</td>
<td>IP address of the Peer</td>
</tr>
</tbody>
</table>

Usage Guidelines

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)#
17.1.18 no

Wireless Configuration Commands

Use this CLI command to negate a command or set its defaults.

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 17.1 on page 17-1 for the parameters that can be negated using no command.

Usage Guidelines

Example

WS5100(config-wireless)#no mobility enable
WS5100(config-wireless)#
17.1.19 oversized-frames

Wireless Configuration Commands

Use this CLI command to use oversized frames for data traffic.

Syntax

oversized-frames

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Enable support for oversized frames</td>
</tr>
</tbody>
</table>

Usage Guidelines

Example

```
WS5100(config-wireless)#oversized-frames enable
WS5100(config-wireless)#
```
17.20 proxy-arp

Wireless Configuration Commands

Use the CLI command respond to ARP requests from the RON to WLAN on behalf of mobile-units.

**Syntax**

```
proxy-arp
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Enable support for proxy arp</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

**Example**

```
WS5100(config-wireless)#proxy-arp enable
WS5100(config-wireless)#
```
17.1.21 qos-mapping

Wireless Configuration Commands

Use this CLI command to configure and setup 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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>wired-to-wireless</td>
<td>Mappings used while switching wired traffic over the air.</td>
</tr>
<tr>
<td>dot1p &lt;0-7&gt;</td>
<td>Configure mappings of 802.1p tags to access categories. You can specify</td>
</tr>
<tr>
<td></td>
<td>more than one 802.1p tag (0-7) to be configured.</td>
</tr>
<tr>
<td>dscp &lt;0-63&gt;</td>
<td>Configure mappings of DSCP values to access categories. You can specify</td>
</tr>
<tr>
<td></td>
<td>more than one DSCP value (0-63) to be configured.</td>
</tr>
<tr>
<td>background</td>
<td>background category traffic.</td>
</tr>
<tr>
<td>best-effort</td>
<td>best effort category traffic.</td>
</tr>
<tr>
<td>video</td>
<td>video traffic category traffic.</td>
</tr>
<tr>
<td>voice</td>
<td>voice traffic category traffic.</td>
</tr>
<tr>
<td>wireless-to-wired</td>
<td>Mappings used while switching wireless traffic to the RON side.</td>
</tr>
<tr>
<td>dot1p &lt;0-7&gt;</td>
<td>Configure the 802.1p tags that corresponds to selected access category.</td>
</tr>
</tbody>
</table>

Usage Guidelines

Example

WS5100(config-wireless)# qos-mapping wireless-to-wired background dot1p 5
WS5100(config-wireless)#
17.1.22 radio

Wireless Configuration Commands

Use this CLI command to configure radio related settings.

Syntax

```plaintext
radio (<1-1000>|RADIO|add|all-11a|all-11b|all-11bg|
configure-8021X|default-11a|default-11b|default-11bg|dns-name)

radio<1-1000>{<1-1000>|<1-200>|<4-20>}
radio configure-8021X|default-11a|default-11b|default-11bg|dns-name)

copy-config-from|description|detector|dtim-period|enforce-spec-mgmt|
image-name|location-message|mac|max-mobile-units|
on-channel-scan|reset|reset-ap|rts-threshold|run-acs|
self-heal-offset|short-preamble|speed|wmm}

radio bss((<1-4>|auto)>WLAN

radio channel-power(indoor|outdoor) (<1-200>|acs|random) 4-20>
radio coordinates (x coordinates) (y coordinates) (z coordinates)
radio copy-config-from(<1-1000>-<1-1000>|default-11a|default-11b|default-11bg)
radio dtim-period<1-50> bss<1-4>
radio range(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 wmm(background|best-effort|video|voice) (aifsn<1-15>|burst<0-65535>|cw<0-15>)
radio add<1-1000>(MAC Address) (11a|ap300)|11b(ap100|ap4131)|11bg(ap300))
```

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;1-1000&gt;</td>
<td>A single radio index.</td>
</tr>
<tr>
<td>RADIO</td>
<td>A list (eg: 1,3,7) or range (eg: 3-7) of radio indices.</td>
</tr>
<tr>
<td>all-11a</td>
<td>all 11a radios currently in configuration.</td>
</tr>
<tr>
<td>all-11b</td>
<td>all 11b radios currently in configuration.</td>
</tr>
<tr>
<td>all-11bg</td>
<td>all 11bg radios currently in configuration.</td>
</tr>
<tr>
<td>configure-8021X</td>
<td>Configure 802.1X username and password on adopted access-ports.</td>
</tr>
<tr>
<td>default-11a</td>
<td>default 11a configuration template.</td>
</tr>
<tr>
<td>default-11b</td>
<td>default 11b configuration template.</td>
</tr>
<tr>
<td>default-11bg</td>
<td>default 11bg configuration template.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>adoption-pref-id &lt;0-65535&gt;</td>
<td>A preference identifier for this radio port. The radio port is more likely to be adopted by a wireless switch that is its preferred wireless switch.</td>
</tr>
</tbody>
</table>
| antenna-mode <diversity|primary|secondary> | Antenna diversity mode. You can select from the following options:  
- diversity—Full Diversity (both antennas).  
- primary—Primary Antenna only.  
- secondary—Secondary Antenna only.  
**NOTE** Before executing this command please ensure that the radio is present and is of type AP300. |
| beacon-interval <50-200> | Beacon interval in K-uSec. |
| bss (<1-4>|auto) WLAN | map wireless lans to radio bssids.  
- <1-4>—The bss where wireless lans will be mapped.  
- auto—Automatic assignment of bss. The user selects wireless lans, and the system assigns them to a bss automatically.  
- WLAN—A list (eg: 1,3,7) or range (eg: 3-7) of wlan indices. When a bss is also specified, the first wlan will be used as the primary wlan. When the auto option is used, the system will automatically assign the first four wlans as primaries on their respective bss |
| cca-level <1-31> | CCA level value. |
| cca-mode <0-3> | CCA mode value. |
| channel-power <indoor|outdoor|<1-2000>|acs|random> <4-20> | Location, channel and transmit power level.  
- indoor — Indoor location  
- outdoor — Outdoor location  
- <1-2000> — Channel number  
- acs — Auto channel selection (radio will scan for the least congested channel at startup or reconfiguration)  
- random — Random channel selection  
- <4-20> — Power in dBm |
<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>coordinates (X,Y,Z coordinates)</td>
<td>Configure the location of this radio in terms of x,y,z coordinates.</td>
</tr>
<tr>
<td></td>
<td>• <code>&lt;-65535-65535&gt;</code> – X Coordinate</td>
</tr>
<tr>
<td></td>
<td>• <code>&lt;-65535-65535&gt;</code> – Y Coordinate</td>
</tr>
<tr>
<td></td>
<td>• <code>&lt;-65535-65535&gt;</code> – Z Coordinate</td>
</tr>
<tr>
<td>copy-config-from</td>
<td>Copy the configuration from a previously configured radio.</td>
</tr>
<tr>
<td>(&lt;1-1000&gt;</td>
<td>default-11a</td>
</tr>
<tr>
<td></td>
<td>• default-11a – default 11a configuration template</td>
</tr>
<tr>
<td></td>
<td>• default-11b – default 11b configuration template</td>
</tr>
<tr>
<td></td>
<td>• default-11bg – default 11bg configuration template</td>
</tr>
<tr>
<td>description</td>
<td>Configure a description for this radio. Should not exceed 20 characters.</td>
</tr>
<tr>
<td>detector</td>
<td>Dedicate this radio as a detector. No mobile-units can associate to a detector.</td>
</tr>
<tr>
<td>dtim-period&lt;1-50&gt; bss&lt;1-4&gt;</td>
<td>DTIM period (number of beacons between successive DTIMs)</td>
</tr>
<tr>
<td>radio dtim-period&lt;1-50&gt; bss&lt;1-4&gt;</td>
<td>• <code>&lt;1-50&gt;</code> – DTIM period.</td>
</tr>
<tr>
<td></td>
<td>• bss – BSS</td>
</tr>
<tr>
<td></td>
<td>• <code>&lt;1-4&gt;</code> – BSS index</td>
</tr>
<tr>
<td>enforce-spec-mgmt (enable)</td>
<td>Enforce spectrum management checks on specified radios. Only mobile-units that advertise spectrum management capabilities will be allowed to associate on this radio</td>
</tr>
<tr>
<td>image-name</td>
<td>Image Name, should not exceed more than 20 characters.</td>
</tr>
<tr>
<td>location-message</td>
<td>Specify message that would be sent to all mobile-units that associate with these radios. This message should not exceed more than 80 characters.</td>
</tr>
<tr>
<td>mac (AA-BB-CC-DD-EE-FF)</td>
<td>Change the parent (access-port) MAC address of the radio.</td>
</tr>
<tr>
<td>max-mobile-units &lt;1-256&gt;</td>
<td>Maximum number of mobile-units allowed to associate.</td>
</tr>
<tr>
<td>on-channel-scan</td>
<td>Enable rogue scanning on this radio.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>reset</td>
<td>reset a radio (this will only reset the specified radio, not the complete access-port)</td>
</tr>
<tr>
<td>reset-ap</td>
<td>reset the parent ap (this will reset all radios on that access-port)</td>
</tr>
<tr>
<td>rts-threshold&lt;0-2347&gt;</td>
<td>RTS threshold in bytes.</td>
</tr>
<tr>
<td>run-acss</td>
<td>Run auto-channel-selection on a radio. The radio should already have been configured for ACS</td>
</tr>
<tr>
<td>self-heal-offset &lt;0-30&gt;</td>
<td>Configure the self-healing offset, measured in dBm, for regulatory.</td>
</tr>
<tr>
<td>NOTE</td>
<td>This offset is based off the regulatory maximum power for the specified channel (the command &quot;show wireless regulatory&quot; shows the max power allowed)</td>
</tr>
<tr>
<td>short-preamble</td>
<td>Enable support for Short preamble</td>
</tr>
<tr>
<td>NOTE</td>
<td>This will disable support for long preamble and mobile-units that only support long preamble wont be able to associate.</td>
</tr>
<tr>
<td>speed</td>
<td>Configure the basic and supported data rates / speed.</td>
</tr>
<tr>
<td>--------</td>
<td>------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>• 1 1-Mbps</td>
</tr>
<tr>
<td></td>
<td>• 11 11-Mbps</td>
</tr>
<tr>
<td></td>
<td>• 12 12-Mbps</td>
</tr>
<tr>
<td></td>
<td>• 18 18-Mbps</td>
</tr>
<tr>
<td></td>
<td>• 2 2-Mbps</td>
</tr>
<tr>
<td></td>
<td>• 24 24-Mbps</td>
</tr>
<tr>
<td></td>
<td>• 36 36-Mbps</td>
</tr>
<tr>
<td></td>
<td>• 48 48-Mbps</td>
</tr>
<tr>
<td></td>
<td>• 54 54-Mbps</td>
</tr>
<tr>
<td></td>
<td>• 5p5 5.5-Mbps</td>
</tr>
<tr>
<td></td>
<td>• 6 6-Mbps</td>
</tr>
<tr>
<td></td>
<td>• 9 9-Mbps</td>
</tr>
<tr>
<td></td>
<td>• basic1 basic 1-Mbps</td>
</tr>
<tr>
<td></td>
<td>• basic11 basic 11-Mbps</td>
</tr>
<tr>
<td></td>
<td>• basic12 basic 12-Mbps</td>
</tr>
<tr>
<td></td>
<td>• basic18 basic 18-Mbps</td>
</tr>
<tr>
<td></td>
<td>• basic2 basic 2-Mbps</td>
</tr>
<tr>
<td></td>
<td>• basic24 basic 24-Mbps</td>
</tr>
<tr>
<td></td>
<td>• basic36 basic 36-Mbps</td>
</tr>
<tr>
<td></td>
<td>• basic48 basic 48-Mbps</td>
</tr>
<tr>
<td></td>
<td>• basic54 basic 54-Mbps</td>
</tr>
<tr>
<td></td>
<td>• basic5p5 basic 5.5-Mbps</td>
</tr>
<tr>
<td></td>
<td>• default factory default rates based on radio-type</td>
</tr>
<tr>
<td></td>
<td>• range all rates enabled, the lowest one set to basic</td>
</tr>
<tr>
<td></td>
<td>• throughput all rates basic (note: only g clients allowed on 11bg radios)</td>
</tr>
</tbody>
</table>
### 802.11e / Wireless MultiMedia (WMM) parameters (supported only on AP300)

```plaintext
radio wmm\{background\|best-effort\|video\|voice\}(aifsn<1-15>|burst<0-65535>|cw<0-15>)
```

- **background** – background category traffic
- **best-effort** – best effort category traffic
- **video** – video traffic category traffic
- **voice** – voice traffic category traffic
- **aifsn<1-15>** – (Arbitration Inter Frame Spacing Number)
  The wait time in milliSeconds between data frames is derived using AIFSN and the slot-time.
- **burst<0-65535>** – (transmit-opportunity) An interval of time 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 retrying transmission. Stations then double their wait time on a collision, until it reaches the maximum contention window

### Add a new radio

```plaintext
radio add<1-1000>(MAC Address)
\{11a(ap300)|11b(ap100|ap4131)|11bg(ap300)\}
```

- **<1-1000>** – Index where this radio is to be added
- **MAC** – 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 type access-port (default for 11a and 11bg)
- **ap100** – ap100 type access-port (default for 11b)
- **ap4131** – ap4131 type access-port
| **dns-name** WORD (MAC Address) | Configure *dns-name* to be used in L3-Discovery on adopted access-ports.  
  - AA-BB-CC-DD-EE-FF – Change the *dns-name* only on the access-port with a specified MAC address. If not specified, the *dns-name* update is sent to all currently adopted access-ports. |

**Usage Guidelines**

**Example**

```bash
WS5100(config-wireless)#radio 250 bss auto 3-5
WS5100(config-wireless)#
```
17.1.23 self-heal

Wireless Configuration Commands

Use this CLI command to configure Self Healing.

Syntax

```
self-heal
self-heal interference-avoidance
self-heal interference-avoidance enable
self-heal interference-avoidance hold-time
self-heal interference-avoidance retries
self-heal neighbor-recovery
self-heal neighbor-recovery action
self-heal neighbor-recovery neighbors
```

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interference-avoidance</td>
<td>Interference Avoidance configuration</td>
</tr>
<tr>
<td>enable</td>
<td>enable/disable interference avoidance</td>
</tr>
<tr>
<td>hold-time&lt;0-65535&gt;</td>
<td>The number of seconds to disable interference avoidance after a detection.</td>
</tr>
<tr>
<td></td>
<td>This prevents a radio from changing channels continuously. Set the hold-time</td>
</tr>
<tr>
<td></td>
<td>between 0-65535 seconds.</td>
</tr>
<tr>
<td>retries&lt;0.0-15.0&gt;</td>
<td>The average number retries to cause a radio to re-run auto channel selection.</td>
</tr>
<tr>
<td></td>
<td>Set a value between 0-15.</td>
</tr>
<tr>
<td>neighbor-recovery</td>
<td>Neighbor Recovery configuration commands</td>
</tr>
<tr>
<td>action</td>
<td>Radio self healing action when neighbors are detected down.</td>
</tr>
<tr>
<td>(both</td>
<td>none</td>
</tr>
<tr>
<td>radio (&lt;1-1000&gt;</td>
<td>RADIO)</td>
</tr>
<tr>
<td></td>
<td>• open-rates – open all rates.</td>
</tr>
<tr>
<td></td>
<td>• raise-power – raise the power to max.</td>
</tr>
<tr>
<td></td>
<td>• radio – modify the action for specified radio(s).</td>
</tr>
<tr>
<td></td>
<td>• &lt;1-1000&gt; – A single radio index.</td>
</tr>
<tr>
<td></td>
<td>• RADIO – A list (eg: 1,3,7) or range (eg: 3-7) of radio indices.</td>
</tr>
<tr>
<td>enable</td>
<td>Monitor access-ports and attempt to increase coverage on failure.</td>
</tr>
</tbody>
</table>
### Usage Guidelines

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>neighbors&lt;1-1000&gt;</td>
<td>Add radios as neighbors.</td>
</tr>
<tr>
<td>(&lt;1-1000&gt;</td>
<td>RADIO)</td>
</tr>
<tr>
<td>run-neighbor-detect</td>
<td>Disassociate all mobile-units, clear current neighbors and run neighbor detection.</td>
</tr>
</tbody>
</table>

### Example

EXAMPLE OUTPUT HERE
17.1.24 sensor

Wireless Configuration Commands

Use this CLI command to configure Wireless Intrusion Protection System parameters.

Syntax

```plaintext
sensor(default-config|vlan)
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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>default-config</td>
<td>default configuration sent to sensors when they are configured.</td>
</tr>
<tr>
<td>ip-mode</td>
<td>configure the IP address mode of the sensors.</td>
</tr>
<tr>
<td>dhcp</td>
<td>sensor should use DHCP to obtain an IP address.</td>
</tr>
<tr>
<td>static (A.B.C.D/M)(A.B.C.D)</td>
<td>sensor must use the specific static IP address.</td>
</tr>
<tr>
<td>wips-server-ip</td>
<td>specify IP addresses of the WIPS server.</td>
</tr>
<tr>
<td>primary (A.B.C.D)</td>
<td>specify the primary IP address of the WIPS server.</td>
</tr>
<tr>
<td>secondary (A.B.C.D)</td>
<td>specify the secondary IP address of the WIPS server.</td>
</tr>
<tr>
<td>vlan&lt;1-4094&gt;</td>
<td>Configure vlans where sensors are to be discovered.</td>
</tr>
</tbody>
</table>

Usage Guidelines

Example

```plaintext
WS5100(config-wireless)#sensor vlan 268 500
WS5100(config-wireless)#
```
17.1.25 service

Wireless Configuration Commands

Use this CLI command to invoke the service commands to troubleshoot or debug the (config-wireless) instance configurations.

Syntax

```
service(ap|clear|diag-shell|save-cli|show|
    start-shell|tethereal|wireless)

service ap(force-dump))
service clear(all|cores|dumps|panics)

service show(ap|cli|command-history|crash-info|info|last-passwd|reboothistory|startup-log|upgrade-history|wireless)
service show ap beacon-count
```

Parameters

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ap</td>
<td>access-port serviceability parameters.</td>
</tr>
<tr>
<td>force-dump</td>
<td>trigger the access-port to send a crash-dump to the wireless-switch.</td>
</tr>
<tr>
<td>clear</td>
<td>Remove specified support information</td>
</tr>
<tr>
<td>all</td>
<td>Remove all core, dump and panic files</td>
</tr>
<tr>
<td>cores</td>
<td>Remove all core files</td>
</tr>
<tr>
<td>dumps</td>
<td>Remove all dump files</td>
</tr>
<tr>
<td>panics</td>
<td>Remove all kernel panic files</td>
</tr>
<tr>
<td>diag-shell</td>
<td>Provide diag shell access.</td>
</tr>
<tr>
<td>save-cli</td>
<td>Save CLI tree for all modes in html format.</td>
</tr>
<tr>
<td>show</td>
<td>Show running system information.</td>
</tr>
<tr>
<td>start-shell</td>
<td>Provide shell access.</td>
</tr>
<tr>
<td>tethereal</td>
<td>Dump and analyze network traffic.</td>
</tr>
<tr>
<td>wireless</td>
<td>Wireless parameters.</td>
</tr>
</tbody>
</table>

Usage Guidelines
Example

WS5100(config-wireless)#service clear all
WS5100(config-wireless)#

WS5100(config-wireless)#service clear cores
WS5100(config-wireless)#

WS5100(config-wireless)#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-wireless)#

WS5100(config-wireless)#service show ?
ap access-port serviceability parameters
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
wireless Wireless parameters
WS5100(config-wireless)#

WS5100(config-wireless)#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 3 13:43
snmpd.log 316 Oct 3 13:43
startup.log 16.6k Oct 3 13:43
command.history 2.0k Oct 7 02:24
reboot.history 3.3k Oct 3 13:43
upgrade.history 782 Aug 29 18:32
Please export these files or delete them for more space.
WS5100(config-wireless)#

WS5100(config-wireless)#service start-shell
Last password used: password with MAC 00:a0:f8:65:ea:8e
Password:
WS5100(config-wireless)#
Wireless Instance

WS5100(config-wireless)#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-wireless)#service wireless ?
dump-core    Create a core file of the ccsrvr process
dump-state   Create a ccsrvr.dump file in nvram with internal state information
mu-history  Enable mu association history
mu-history-clear Delete all mu association history files
rate-scale   Enable wireless rate scaling (default)
request-ap-log Request ap Log

WS5100(config-wireless)#service wireless
17.1.26 show

Wireless Configuration Commands

Use this CLI command to view the current system information that is running on the WS5100 Series Wireless Switch.

Syntax

```
show<parameter>
```

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>?</td>
<td>Displays all the parameters for which the information can be viewed using the show command.</td>
</tr>
</tbody>
</table>

Usage Guidelines

Example

```
WS5100(config-wireless)#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
cmd                  Display 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 Management 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-wireless)#show
17.1.27 smart-scan-channels

Wireless Configuration Commands

Use this CLI command to configure a list of channels that are used on the network. This list will be provided to mobile-units that can support partial scanning.

Syntax

```
smart-scan-channels(11a|11bg)<1-200>
```

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>11a</td>
<td>Specify channel list for the 5Ghz band used by 802.11a mobile-units.</td>
</tr>
<tr>
<td>11bg</td>
<td>Specify channel list for the 2.4Ghz band used by 802.11bg mobile-units.</td>
</tr>
<tr>
<td>&lt;1-200&gt;</td>
<td>List of channels.</td>
</tr>
</tbody>
</table>

Usage Guidelines

Example

EXAMPLE OUTPUT HERE
17.1.28 terminal

Wireless Configuration Commands

Use this command to set the length /number of lines to be displayed on the terminal window.

**Syntax**

```
terminal (monitor|no)
terminal no (monitor)
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>monitor</td>
<td>Copy debug output to the current terminal line</td>
</tr>
<tr>
<td>no</td>
<td>Negate a command or set its defaults</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

**Example**

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

WS5100(config-wireless)#terminal no monitor
WS5100(config-wireless)#
```
17.1.29 wlan

Wireless Configuration Commands

Use this CLI command to configure Wireless LAN related commands.

Syntax

```plaintext
wlan(<1-32>|WLAN) (accounting|answer-bcast-ess|authentication-type|description
dot11i|enable|encryption-type|hotspot|inactivity-timeout|kdc|mobility|
umu-mu-disallow|qos|radius|secure-beacon|ssid|symbol-extensions
|syslog|tunnel|vlan|wep128|wep64)

wlan<1-32>(none|radius|ssyslog)
wlan<1-32> authentication-type(eap|hotspot|kerberos|mac-auth|none)

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> 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> qos(classification|mcast1|mcast2|prioritize-voice|svp|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)
<br60-3600>|start-stop|stop-only))
wlan<1-32> radius accounting timeout<1-60> retransmit<1-100>

wlan<1-32> radius authentication-protocol(chap|pap)
```
wireless_instance

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> syslog (accounting) server<IP Address> port<Port Number>

wlan<1-32> tunnel<1-32> gateway<IP Address and mask>

wlan<1-32> wep128 (key<1-4> (ascii|hex[0|2|WORD]) | phrase (LINE) | wep-default-key<1-4>)

## Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;1-32&gt;</td>
<td>A single wlan index.</td>
</tr>
<tr>
<td>WLAN</td>
<td>A list (eg: 1,3,7) or range (eg: 3-7) of wlan indices.</td>
</tr>
<tr>
<td>accounting</td>
<td>Accounting on this WLAN.</td>
</tr>
<tr>
<td>(none</td>
<td>radius</td>
</tr>
<tr>
<td></td>
<td>• radius – Use RADIUS accounting on this WLAN</td>
</tr>
<tr>
<td></td>
<td>• syslog – Use Syslog accounting on this WLAN</td>
</tr>
<tr>
<td>answer-bcast-ess</td>
<td>Allow this WLAN to respond to probes for broadcast ESS.</td>
</tr>
<tr>
<td>authentication-type</td>
<td>The authentication type of this WLAN.</td>
</tr>
<tr>
<td>(eap</td>
<td>hotspot</td>
</tr>
<tr>
<td></td>
<td>• hotspot – Web based authentication</td>
</tr>
<tr>
<td></td>
<td>• kerberos – Kerberos authentication (Note: encryption type will change to wep128 if its not already wep128/keyguard)</td>
</tr>
<tr>
<td></td>
<td>• mac-auth – MAC authentication (Radius lookup of MAC address)</td>
</tr>
<tr>
<td></td>
<td>• none – None / pre-shared keys</td>
</tr>
<tr>
<td>description</td>
<td>The description of this WLAN</td>
</tr>
<tr>
<td>dot11i ( )</td>
<td>Modify tkip/ccmp (802.11i) related parameters</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td><code>handshake</code></td>
<td>Use handshake to configure the timeout and retransmission.</td>
</tr>
<tr>
<td><code>timeout&lt;100-5000&gt;</code></td>
<td>The timeout in milliseconds, between retries.</td>
</tr>
<tr>
<td><code>retransmit&lt;1-10&gt;</code></td>
<td>The number of retransmission attempts.</td>
</tr>
<tr>
<td>`key(0</td>
<td>2</td>
</tr>
<tr>
<td><code>0</code></td>
<td>Password is specified UNENCRYPTED.</td>
</tr>
<tr>
<td><code>2</code></td>
<td>Password is encrypted with password-encryption secret.</td>
</tr>
<tr>
<td><code>WORD</code></td>
<td>The 256bit (64 hex characters) long key.</td>
</tr>
<tr>
<td><code>key-rotation(enable)</code></td>
<td>Control the periodic update of the broadcast keys of all associated mobile-units.</td>
</tr>
<tr>
<td><code>key-rotation-interval&lt;1800-86400&gt;</code></td>
<td>Configure the broadcast key rotation interval.</td>
</tr>
<tr>
<td><code>opp-pmk-caching</code></td>
<td>Enable the opportunistic use of cached pairwise master keys (fast roaming with eap/802.1X).</td>
</tr>
<tr>
<td>`phrase(0</td>
<td>2</td>
</tr>
<tr>
<td><code>0</code></td>
<td>Password is specified UNENCRYPTED.</td>
</tr>
<tr>
<td><code>2</code></td>
<td>Password is encrypted with password-encryption secret.</td>
</tr>
<tr>
<td><code>LINE</code></td>
<td>A passphrase between 8 and 63 characters long.</td>
</tr>
<tr>
<td><code>pmk-caching</code></td>
<td>Enable the use of cached pairwise master keys (fast roaming with eap/802.1X).</td>
</tr>
<tr>
<td><code>preauthentication</code></td>
<td>Enable support for 802.11i preauthentication.</td>
</tr>
<tr>
<td>`second-key(enable</td>
<td>key</td>
</tr>
<tr>
<td><code>enable</code></td>
<td>Enable the use of a secondary key/passphrase.</td>
</tr>
<tr>
<td><code>key</code></td>
<td>Configure the key (PMK).</td>
</tr>
<tr>
<td><code>phrase</code></td>
<td>Configure the passphrase.</td>
</tr>
<tr>
<td><code>0</code></td>
<td>Password is specified UNENCRYPTED</td>
</tr>
<tr>
<td><code>2</code></td>
<td>Password is encrypted with password-encryption secret</td>
</tr>
<tr>
<td><code>WORD</code></td>
<td>The 256bit (64 hex characters) long key</td>
</tr>
<tr>
<td>Wireless Instance</td>
<td>17-49</td>
</tr>
<tr>
<td>-------------------</td>
<td>-------</td>
</tr>
<tr>
<td><strong>tkip-cntrmeas-hold-time</strong>&lt;0-65535&gt;</td>
<td>Configure the hold-time in seconds for which clients are blocked when tkip countermeasures are taken. Default is 60 seconds.</td>
</tr>
<tr>
<td><strong>enable()</strong></td>
<td>enable specified wireless lan(s).</td>
</tr>
<tr>
<td><strong>encryption-type()</strong></td>
<td>The encryption type for this WLAN.</td>
</tr>
<tr>
<td><strong>ccmp</strong></td>
<td>AES Counter Mode CBC-MAC Protocol (AES-CCM/CCMP)</td>
</tr>
<tr>
<td><strong>keyguard</strong></td>
<td>Keyguard-MCM (Mobile Computing Mode)</td>
</tr>
<tr>
<td><strong>none</strong></td>
<td>no encryption</td>
</tr>
<tr>
<td><strong>tkip</strong></td>
<td>Enable Temporal Key Integrity Protocol (TKIP)</td>
</tr>
<tr>
<td><strong>tkip-ccmp</strong></td>
<td>Enable both tkip and ccmp on this WLAN</td>
</tr>
<tr>
<td><strong>wep128</strong></td>
<td>Enable Wired Equivalence Privacy (WEP) with 128 bit keys</td>
</tr>
<tr>
<td><strong>wep128-keyguard</strong></td>
<td>Enable both WEP128 as well as Keyguard-MCM on this WLAN</td>
</tr>
<tr>
<td><strong>wep64</strong></td>
<td>Enable Wired Equivalence Privacy (WEP) with 64 bit keys.</td>
</tr>
</tbody>
</table>

**NOTE**  A configuration where two WLANs are mapped to the same VLAN, and one of them is configured with no encryption and the other with WEP, is insecure. It can lead to a compromise of the WEP key.

<table>
<thead>
<tr>
<th><strong>hotspot()</strong></th>
<th>Modify hotspot related parameters.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>allow</strong>&lt;br&gt;(Rule index) (IP address)</td>
<td>Modify hotspot allow-list parameters. Users who have not yet authenticated will be allowed access to these IP addresses.</td>
</tr>
<tr>
<td></td>
<td>• Rule index – Allow-list Rule index. Should be between (1-10).</td>
</tr>
<tr>
<td></td>
<td>• IP address – allow-list IP address</td>
</tr>
</tbody>
</table>
### webpage(external|internal) (failure|login|welcome)
Modify hotspot page parameters.
- **external** – Modify hotspot External page.
- **internal** – Modify hotspot Internal page.
- **failure** – Users are redirected to this webpage if they fail authentication.
- **login** – Users are prompted for their username and password on this webpage.
- **welcome** – Users are redirected to this webpage after they authenticate successfully.

### webpage-location (advanced|external|internal)
The location of the webpages to be used for authentication. These pages can either be hosted on the wireless switch or on an external web server.
- **advanced** – use login/welcome/failure web pages created by the user on the wireless switch.
- **external** – use login/welcome/failure web pages on an external server.
- **internal** – use login/welcome/failure web pages created automatically on the wireless switch.

### inactivity-timeout
<60-86400>
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()
Modify KDC related parameters.

### password(0|2|LINE)
Kdc server password, upto 127 characters.
- 0 – Password is specified UNENCRYPTED.
- 2 – Password is encrypted with password-encryption secret.
- LINE – Kdc server password, upto 127 characters.

### realm(LINE)
Kdc realm 127 characters.
- LINE – Kdc realm, upto 127 characters.
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
</table>
| server (primary|secondary) (IP address) auth-port <1-65535> | Modify KDC server parameters.  
  - primary – Primary kdc server  
  - secondary – Secondary kdc server  
  - IP address – Kdc server IP address  
  - auth-port <1-65535> – Kdc server authentication port. Default is 88. |
| server(timeout)<1-60> | Modify KDC server parameters.  
  - timeout – Time the wireless switch waits for a response from the kdc server before retrying. |
| mobility (enable) | Enable L3 Mobility on WLAN(s). |
| mu-mu-disallow (switch-to-wired) | Disallow frames from one mu to another mu on this WLAN.  
  - switch-to-wired – Disallow by switching the frame out on the wired side (to allow an externalswitch to decide whether this frame is to be allowed or dropped). |
| qos() | Quality of Service commands. |
| classification (background|best-effort|video|voice|wmm) | Select how traffic on this WLAN must be classified (relative prioritization on the access-port).  
  - background – All traffic on this wlan is treated as background traffic.  
  - best-effort – All traffic on this wlan is treated as Best-Effort.  
  - video – All traffic on this wlan is treated as Video.  
  - voice – All traffic on this wlan is treated as Voice.  
  - wmm – Use WMM based classification, using DSCP or 802.1p tags to classify traffic into different queues. |
| mcast1|mcast2 (AA-BB-CC-DD-EE-FF) | The Egress prioritization multicast mask.  
| prioritize-voice | Prioritize voice frames over general data frames (applies non-WMM mobile-unit). |
| svp(enable) | Enable Spectralink Voice Prioritization support on this WLAN. |
| wmm (8021p|background|best-effort|dscp|video|voice) {aifsn|cw|txop-limit|acm} | 802.11e / Wireless MultiMedia (WMM) parameters (supported only on AP300). |
|-------------------------------------------------|-------------------------------------------------|
| • 8021p – Use 802.1p frame priority (field in the VLAN tag) to determine packet priority. |
| • background – background category traffic. |
| • best-effort – best effort category traffic. |
| • dscp – Use DSCP (Differentiated Services Code Point) bits in the IP header to determine packet priority. |
| • video – video traffic category traffic. |
| • voice – voice traffic category traffic. |
| • aifsn – (Arbitration Inter Frame Spacing Number) the wait time in milliseconds between data frames is derived using AIFSN and the slot-time. |
| • cw – (Contention Window parameters): wireless stations pick a number between 0 and the minimum contention window to wait before retrying transmission. Stations then double their wait time on a collision, until it reaches the maximum contention window. |
| • txop-limit – (transmit-opportunity): an interval of time when a particular WMM STA has the right to initiate transmissions onto the wireless medium. |
| • acm – admission control parameters |
### radius (accounting|authentication-protocol|dscp|dynamic-authorization|dynamic-vlan-assignment|mobile-unit|reauth|server)

Modify Radius/802.1X related parameters.
- **accounting** – Accounting Parameters
- **authentication-protocol** – Authentication protocol to use in the radius requests
- **dscp** – Specify a DSCP (Differentiated Services Code Point) value to provide QoS to Radius packets.
- **dynamic-authorization** – Configure support for Radius dynamic authorization extensions such as Disconnect Message, and Change-Of-Authorization, as described in RFC 3576.
- **dynamic-vlan-assignment** – Allow users to be assigned to Radius server specified VLANs, instead of only the vlan that is mapped to this wlan.
- **mobile-unit** – Modify Radius/802.1X supplicant related parameters.
- **reauth** – Enable periodic reauthentication of all associated mobile-units.
- **server** – Modify Radius/802.1X server parameters.

### accounting mode(start-interim-stop(interval)<60-3600>|start-stop|stop-only)

Use this to configure the radius accounting parameters.
- **mode** – Accounting Mode on this WLAN
- **start-interim-stop** – Accounting Start-Interim-Stop
- **interval <60-3600>** – Time Interval between successive accounting updates.
- **start-stop** – Send Accounting Start-Stop
- **stop-only** – Send Accounting Stop only

### accounting timeout<1-60> retransmit<1-100>

Use this to configure the radius accounting parameters.
- **timeout <1-60>** – Time in seconds that the wireless switch waits for a response from the radius server before retrying Accounting.
- **retransmit <1-100>** – Number of retries before the wireless switch will give up Accounting.
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>authentication-protocol</strong> (chap</td>
<td>pap)</td>
</tr>
<tr>
<td></td>
<td>• chap – Challenge Handshake Authentication Protocol</td>
</tr>
<tr>
<td></td>
<td>• pap – Password Authentication Protocol</td>
</tr>
<tr>
<td><strong>dscp&lt;0-63&gt;</strong></td>
<td>Specify a DSCP (Differentiated Services Code Point) value to provide QoS to Radius packets. The DSCP value should be between 0-63.</td>
</tr>
<tr>
<td><strong>dynamic-authorization (enable)</strong></td>
<td>Configure support for Radius dynamic authorization extensions such as Disconnect Message, and Change-Of-Authorization, as described in RFC 3576.</td>
</tr>
<tr>
<td></td>
<td>• enable – Enable support for Radius dynamic authorization.</td>
</tr>
<tr>
<td><strong>dynamic-vlan-assignment</strong></td>
<td>Allow users to be assigned to Radius server specified VLANs, instead of only the vlan that is mapped to this wlan.</td>
</tr>
<tr>
<td></td>
<td>• enable – Enable dynamic/radius-assigned vlan assignment.</td>
</tr>
<tr>
<td><strong>mobile-unit timeout&lt;1-60&gt; retransmit&lt;1-10&gt;</strong></td>
<td>Modify Radius/802.1X supplicant related parameters.</td>
</tr>
<tr>
<td></td>
<td>• timeout&lt;1-60&gt; – Time in seconds that the wireless switch waits for a response from the mobile-unit before retrying</td>
</tr>
<tr>
<td></td>
<td>• retransmit&lt;1-10&gt; – Number of retries before the wireless switch will give up and disassociate the mobile-unit.</td>
</tr>
<tr>
<td><strong>reauth&lt;30-65535&gt;</strong></td>
<td>Enable periodic reauthentication of all associated mobile-units.</td>
</tr>
<tr>
<td></td>
<td>• &lt;30-65535&gt; – Reauthentication period in seconds.</td>
</tr>
<tr>
<td>**server(primary</td>
<td>secondary) (ip-address &lt;1024-65535&gt;) (auth-port &lt;1024-65535&gt;) (radius-key 0</td>
</tr>
<tr>
<td></td>
<td>• primary – Primary radius server</td>
</tr>
<tr>
<td></td>
<td>• secondary – Secondary radius server</td>
</tr>
<tr>
<td></td>
<td>• ip-address – Radius server IP address</td>
</tr>
<tr>
<td></td>
<td>• auth-port&lt;1024-65535&gt; – Radius server authentication port (default:1812)</td>
</tr>
<tr>
<td></td>
<td>• radius-key – Radius server shared secret, upto 127 characters</td>
</tr>
<tr>
<td></td>
<td>• 0 – Password is specified UNENCRYPTED</td>
</tr>
<tr>
<td></td>
<td>• 2 – Password is encrypted with password-encryption secret</td>
</tr>
<tr>
<td></td>
<td>• LINE – Radius server shared secret, upto 127 characters</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>server timeout</td>
<td>Modify Radius/802.1X server parameters.</td>
</tr>
<tr>
<td>retransmit</td>
<td>- timeout&lt;1-60&gt; – Time, in seconds, the wireless switch waits for a response from the radius server before retrying.</td>
</tr>
<tr>
<td></td>
<td>- retransmit&lt;1-10&gt; – Number of retries before the wireless switch will give up and disassociate the mobile-unit.</td>
</tr>
<tr>
<td>secure-beacon</td>
<td>dont include the SSID of this WLAN in Beacon frames.</td>
</tr>
<tr>
<td>ssid</td>
<td>The SSID of this WLAN.</td>
</tr>
<tr>
<td>symbol-extensions</td>
<td>Enable support for Symbol extensions</td>
</tr>
<tr>
<td>fast-roaming</td>
<td>- fast-roaming(enable) – Enable support for Symbol fast roaming.</td>
</tr>
<tr>
<td>syslog</td>
<td>Syslog Accounting.</td>
</tr>
<tr>
<td>accounting</td>
<td>- accounting – Modify Accounting Parameters</td>
</tr>
<tr>
<td>server&lt;IP Address&gt;</td>
<td>- server&lt;IP Address&gt; – Modify Syslog Accounting Server IP Address.</td>
</tr>
<tr>
<td>port&lt;Port number&gt;</td>
<td>- port&lt;Port Number&gt; – Syslog Server Port. Default port number is 514.</td>
</tr>
<tr>
<td>tunnel</td>
<td>- tunnel&lt;1-32&gt; – The tunnel index mapping for this WLAN</td>
</tr>
<tr>
<td>gateway&lt;IP Address and mask&gt;</td>
<td>- gateway&lt;IP address&gt; – The gateway IP address and mask</td>
</tr>
<tr>
<td>vlan</td>
<td>The VLAN assignment of this WLAN.</td>
</tr>
</tbody>
</table>
### Usage Guidelines

**Example**

```bash
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)#
```

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>wep128</strong></td>
<td>Configure WEP128 parameters.</td>
</tr>
<tr>
<td>key&lt;1-4&gt;</td>
<td>Configure pre-shared hex keys</td>
</tr>
<tr>
<td>ascii</td>
<td>Keys as ASCII characters (5 characters for wep64, 13 for wep128)</td>
</tr>
<tr>
<td>hex</td>
<td>Keys as hexadecimal characters (10 characters for wep64, 26 for wep128)</td>
</tr>
<tr>
<td>0</td>
<td>Password is specified UNENCRYPTED</td>
</tr>
<tr>
<td>2</td>
<td>Password is encrypted with password-encryption secret</td>
</tr>
<tr>
<td>WORD</td>
<td>Key (10 hex or 5 ascii characters for wep64, 26 hex or 13 ascii characters for wep128)</td>
</tr>
<tr>
<td>phrase</td>
<td>Specify a passphrase from which the keys are to be derived</td>
</tr>
<tr>
<td>LINE</td>
<td>The passphrase (between 4 and 32 characters)</td>
</tr>
<tr>
<td>wep-default-key&lt;1-4&gt;</td>
<td>The key index to be used for transmission from AP to MU</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>wep64</strong></td>
<td>Configure WEP64 parameters.</td>
</tr>
</tbody>
</table>
Wireless Instance

```
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)#

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)#
```