Version 3.5
Part No. 311645-A Rev 00
December 2000

600 Technology Park Drive
Billerica, MA 01821-4130

Reference for the Contivity VPN Switch Command Line Interface

NORTEL NETWORKS™

Copyright © 2000 Nortel Networks

All rights reserved. December 2000.

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Nortel Networks NA Inc.

Trademarks

NORTEL NETWORKS is a trademark of Nortel Networks.

Bay Networks, Nortel Networks Extranet Switch 1500, Contivity, Extranet Ready, Personal Extranets, and Infrastructure for Extranets are trademarks of Nortel Networks.

Microsoft, MS, MS-DOS, Win32, Windows, and Windows NT are registered trademarks of Microsoft Corporation.

All other trademarks and registered trademarks are the property of their respective owners.

Restricted Rights Legend

Use, duplication, or disclosure by the United States Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013.

Notwithstanding any other license agreement that may pertain to, or accompany the delivery of, this computer software, the rights of the United States Government regarding its use, reproduction, and disclosure are as set forth in the Commercial Computer Software-Restricted Rights clause at FAR 52.227-19.

Statement of Conditions

In the interest of improving internal design, operational function, and/or reliability, Nortel Networks NA Inc. reserves the right to make changes to the products described in this document without notice.

Nortel Networks NA Inc. does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein.

Portions of the code in this software product may be Copyright © 1988, Regents of the University of California. All rights reserved. Redistribution and use in source and binary forms of such portions are permitted, provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that such portions of the software were developed by the University of California, Berkeley. The name of the University may not be used to endorse or promote products derived from such portions of the software without specific prior written permission.

SUCH PORTIONS OF THE SOFTWARE ARE PROVIDED “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

In addition, the program and information contained herein are licensed only pursuant to a license agreement that contains restrictions on use and disclosure (that may incorporate by reference certain limitations and notices imposed by third parties).

USA Requirements Only

Federal Communications Commission (FCC) Compliance Notice: Radio Frequency Notice

Note: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy. If it is not installed and used in accordance with the instruction manual, it may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to take whatever measures may be necessary to correct the interference at their own expense.

European Requirements Only

EN 55 022 Statement

This is to certify that the Nortel Networks Contivity Extranet Switch is shielded against the generation of radio interference in accordance with the application of Council Directive 89/336/EEC, Article 4a. Conformity is declared by the application of EN 55 022 Class A (CISPR 22).

Warning: This is a Class A product. In a domestic environment, this product may cause radio interference, in which case, the user may be required to take appropriate measures.

Achtung: Dieses ist ein Gerät der Funkstörgrenzwertklasse A. In Wohnbereichen können bei Betrieb dieses Gerätes Rundfunkstörungen auftreten, in welchen Fällen der Benutzer für entsprechende Gegenmaßnahmen verantwortlich ist.

Attention: Ceci est un produit de Classe A. Dans un environnement domestique, ce produit risque de créer des interférences radioélectriques, il appartiendra alors à l’utilisateur de prendre les mesures spécifiques appropriées.

EC Declaration of Conformity

This product conforms (or these products conform) to the provisions of Council Directive 89/336/EEC and 73/23/EEC. Go to *http://libra2.corpwest.baynetworks.com/cgi-bin/ndCGI.exe/DocView/* on the Nortel Networks World Wide Web site for a copy of the Declaration of Conformity.

Japan/Nippon Requirements Only

Voluntary Control Council for Interference (VCCI) Statement

この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

Canada Requirements Only

Canadian Department of Communications Radio Interference Regulations

This digital apparatus (Contivity Extranet Switch) does not exceed the Class A limits for radio-noise emissions from digital apparatus as set out in the Radio Interference Regulations of the Canadian Department of Communications.

Règlement sur le brouillage radioélectrique du ministère des Communications

Cet appareil numérique (Contivity Extranet Switch) respecte les limites de bruits radioélectriques visant les appareils numériques de classe A prescrites dans le Règlement sur le brouillage radioélectrique du ministère des Communications du Canada.

Nortel Networks NA Inc. Software License Agreement

NOTICE: Please carefully read this license agreement before copying or using the accompanying software or installing the hardware unit with pre-enabled software (each of which is referred to as “Software” in this Agreement). BY COPYING OR USING THE SOFTWARE, YOU ACCEPT ALL OF THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT. THE TERMS EXPRESSED IN THIS AGREEMENT ARE THE ONLY TERMS UNDER WHICH NORTEL NETWORKS WILL PERMIT YOU TO USE THE SOFTWARE. If you do not accept these terms and conditions, return the product, unused and in the original shipping container, within 30 days of purchase to obtain a credit for the full purchase price.

1. License grant. Nortel Networks NA Inc. (“Nortel Networks”) grants the end user of the Software (“Licensee”) a personal, nonexclusive, nontransferable license: a) to use the Software either on a single computer or, if applicable, on a single authorized device identified by host ID, for which it was originally acquired; b) to copy the Software solely for backup purposes in support of authorized use of the Software; and c) to use and copy the associated user manual solely in support of authorized use of the Software by Licensee. This license applies to the Software only and does not extend to Nortel Networks Agent software or other Nortel Networks software products. Nortel Networks Agent software or other Nortel Networks software products are licensed for use under the terms of the applicable Nortel Networks NA Inc. Software License Agreement that accompanies such software and upon payment by the end user of the applicable license fees for such software.

2. Restrictions on use; reservation of rights. The Software and user manuals are protected under copyright laws. Nortel Networks and/or its licensors retain all title and ownership in both the Software and user manuals, including any revisions made by Nortel Networks or its licensors. The copyright notice must be reproduced and included with any copy of any portion of the Software or user manuals. Licensee may not modify, translate, decompile, disassemble, use for any competitive analysis, reverse engineer, distribute, or create derivative works from the Software or user manuals or any copy, in whole or in part. Except as expressly provided in this Agreement, Licensee may not copy or transfer the Software or user manuals, in whole or in part. The Software and user manuals embody Nortel Networks’ and its licensors’ confidential and proprietary intellectual property. Licensee shall not sublicense, assign, or otherwise disclose to any third party the Software, or any information about the operation, design, performance, or implementation of the Software and user manuals that is confidential to Nortel Networks and its licensors; however, Licensee may grant permission to its consultants, subcontractors, and agents to use the Software at Licensee’s facility, provided they have agreed to use the Software only in accordance with the terms of this license.

3. Limited warranty. Nortel Networks warrants each item of Software, as delivered by Nortel Networks and properly installed and operated on Nortel Networks hardware or other equipment it is originally licensed for, to function substantially as described in its accompanying user manual during its warranty period, which begins on the date Software is first shipped to Licensee. If any item of Software fails to so function during its warranty period, as the sole remedy Nortel Networks will at its discretion provide a suitable fix, patch, or workaround for the problem that may be included in a future Software release. Nortel Networks further warrants to Licensee that the media on which the Software is provided will be free from defects in materials and workmanship under normal use for a period of 90 days from the date Software is first shipped to Licensee. Nortel Networks will replace defective media at no charge if it is returned to Nortel Networks during the warranty period along with proof of the date of shipment. This warranty does not apply if the media has been damaged as a result of accident, misuse, or abuse. The Licensee assumes all responsibility for selection of the Software to achieve Licensee’s intended results and for the installation, use, and results obtained from the Software. Nortel Networks does not warrant a) that the functions contained in the software will meet the Licensee’s requirements, b) that the Software will operate in the hardware or software combinations that the Licensee may select, c) that the operation of the Software will be uninterrupted or error free, or d) that all defects in the operation of the Software will be corrected. Nortel Networks is not obligated to remedy any Software defect that cannot be reproduced with the latest Software release. These warranties do not apply to the Software if it has been (i) altered, except by Nortel Networks or in accordance with its instructions; (ii) used in conjunction with another vendor’s product, resulting in the defect; or (iii) damaged by improper environment, abuse, misuse, accident, or negligence. THE FOREGOING WARRANTIES AND LIMITATIONS ARE EXCLUSIVE REMEDIES AND ARE IN LIEU OF ALL OTHER WARRANTIES EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Licensee is responsible for the security of its own data and information and for maintaining adequate procedures apart from the Software to reconstruct lost or altered files, data, or programs.

4. Limitation of liability. IN NO EVENT WILL NORTEL NETWORKS OR ITS LICENSORS BE LIABLE FOR ANY COST OF SUBSTITUTE PROCUREMENT; SPECIAL, INDIRECT, INCIDENTAL, OR CONSEQUENTIAL DAMAGES; OR ANY DAMAGES RESULTING FROM INACCURATE OR LOST DATA OR LOSS OF USE OR PROFITS ARISING OUT OF OR IN CONNECTION WITH THE PERFORMANCE OF THE SOFTWARE, EVEN IF NORTEL NETWORKS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT SHALL THE LIABILITY OF NORTEL NETWORKS RELATING TO THE SOFTWARE OR THIS AGREEMENT EXCEED THE PRICE PAID TO NORTEL NETWORKS FOR THE SOFTWARE LICENSE.

5. Government licensees. This provision applies to all Software and documentation acquired directly or indirectly by or on behalf of the United States Government. The Software and documentation are commercial products, licensed on the open market at market prices, and were developed entirely at private expense and without the use of any U.S. Government funds. The license to the U.S. Government is granted only with restricted rights, and use, duplication, or disclosure by the U.S. Government is subject to the restrictions set forth in subparagraph (c)(1) of the Commercial Computer Software—Restricted Rights clause of FAR 52.227-19 and the limitations set out in this license for civilian agencies, and subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause of DFARS 252.227-7013, for agencies of the Department of Defense or their successors, whichever is applicable.

6. Use of software in the European Community. This provision applies to all Software acquired for use within the European Community. If Licensee uses the Software within a country in the European Community, the Software Directive enacted by the Council of European Communities Directive dated 14 May, 1991, will apply to the examination of the Software to facilitate interoperability. Licensee agrees to notify Nortel Networks of any such intended examination of the Software and may procure support and assistance from Nortel Networks.

7. Term and termination. This license is effective until terminated; however, all of the restrictions with respect to Nortel Networks’ copyright in the Software and user manuals will cease being effective at the date of expiration of the Nortel Networks copyright; those restrictions relating to use and disclosure of Nortel Networks’ confidential information shall continue in effect. Licensee may terminate this license at any time. The license will automatically terminate if Licensee fails to comply with any of the terms and conditions of the license. Upon termination for any reason, Licensee will immediately destroy or return to Nortel Networks the Software, user manuals, and all copies. Nortel Networks is not liable to Licensee for damages in any form solely by reason of the termination of this license.

8. Export and re-export. Licensee agrees not to export, directly or indirectly, the Software or related technical data or information without first obtaining any required export licenses or other governmental approvals. Without limiting the foregoing, Licensee, on behalf of itself and its subsidiaries and affiliates, agrees that it will not, without first obtaining all export licenses and approvals required by the U.S. Government: (i) export, re-export, transfer, or divert any such Software or technical data, or any direct product thereof, to any country to which such exports or re-exports are restricted or embargoed under United States export control laws and regulations, or to any national or resident of such restricted or embargoed countries; or (ii) provide the Software or related technical data or information to any military end user or for any military end use, including the design, development, or production of any chemical, nuclear, or biological weapons.

9. General. If any provision of this Agreement is held to be invalid or unenforceable by a court of competent jurisdiction, the remainder of the provisions of this Agreement shall remain in full force and effect. This Agreement will be governed by the laws of the state of California.

Should you have any questions concerning this Agreement, contact Nortel Networks, 4401 Great America Parkway, P.O. Box 58185, Santa Clara, California 95054-8185.

LICENSEE ACKNOWLEDGES THAT LICENSEE HAS READ THIS AGREEMENT, UNDERSTANDS IT, AND AGREES TO BE BOUND BY ITS TERMS AND CONDITIONS. LICENSEE FURTHER AGREES THAT THIS AGREEMENT IS THE ENTIRE AND EXCLUSIVE AGREEMENT BETWEEN NORTEL NETWORKS AND LICENSEE, WHICH SUPERSEDES ALL PRIOR ORAL AND WRITTEN AGREEMENTS AND COMMUNICATIONS BETWEEN THE PARTIES PERTAINING TO THE SUBJECT MATTER OF THIS AGREEMENT. NO DIFFERENT OR ADDITIONAL TERMS WILL BE ENFORCEABLE AGAINST NORTEL NETWORKS UNLESS NORTEL NETWORKS GIVES ITS EXPRESS WRITTEN CONSENT, INCLUDING AN EXPRESS WAIVER OF THE TERMS OF THIS AGREEMENT.

Contents

Preface 27

Conventions 27
Documentation 27
Related publications 28
Text 28
Acronyms 30
Hard-copy technical manuals 31
User interface help button 31
Nortel Networks Customer Service 32

Chapter 1
Introduction 33

Accessing the CLI 33
Access from a Telnet session 33
Access from the serial port menu 34
Command modes 34
User Exec Mode 35
Privileged Exec Mode 37
Global Configuration Mode 38
Key bindings 39

Chapter 2
CLI Command Summary 41

arp 41
Syntax 41
Parameters 41
Default 41
Command mode 41
Next command mode 42
Related commands 42
audible alarm 43
Syntax 43

Parameters 43
Default 43
Command mode 43
Next command mode 43
Related commands 43
Example 43
clear arp-cache 44
Syntax 44
Parameters 44
Default 44
Command mode 44
Next command mode 44
Related commands 44
clear ip route 45
Syntax 45
Parameters 45
Default 45
Command mode 45
Next command mode 45
Warnings 45
Related commands 46
Example 46
clear logging events 47
Syntax 47
Parameters 47
Default 47
Command mode 47
Next command mode 47
Related commands 47
Example 47
configure 48
Syntax 48
Parameters 48
Default 48
Command mode 48

Next command mode 48
Related commands 48
Examples 48
console mode 49
Syntax 49
Parameters 50
Default 50
Command mode 50
Next command mode 50
Related commands 50
Examples 50
control 52
Syntax 52
Parameters 52
Command mode 52
Next command mode 52
Related commands 52
Examples 53
disable 54
Syntax 54
Parameters 54
Default 54
Command mode 54
Next command mode 54
Related commands 55
Example 55
enable 56
Syntax 56
Parameters 56
Default 56
Command mode 56
Next command mode 56
Warnings 56
Related commands 57
Example 57

enable password 58
Syntax 58
Parameters 58
Default 58
Command mode 58
Next command mode 58
Warnings 58
Related commands 59
Examples 59
exception backup 60
Syntax 60
Parameters 60
Default 60
Command mode 61
Next command mode 61
Related commands 61
Example 61
exit 62
Syntax 62
Parameters 62
Default 62
Command mode 62
Next command mode 62
Related commands 63
Example 63
help 64
Syntax 64
Parameters 64
Command mode 64
Related commands 64
Example 64
host address 65
Syntax 65
Parameters 65
Default 66

- Command mode . . . 66
- Next command mode . . . 66
- Prerequisites . . . 66
- Related commands . . . 66
- Example . . . 66

hostname . . . 67

- Syntax . . . 67
- Parameters . . . 67
- Default . . . 67
- Command mode . . . 67
- Next command mode . . . 67
- Prerequisites . . . 67
- Warnings . . . 67
- Related commands . . . 68
- Example . . . 68

interface management . . . 69

- Syntax . . . 69
- Parameters . . . 69
- Command mode . . . 69
- Next command mode . . . 69
- Warnings . . . 69
- Related commands . . . 70
- Example . . . 70

ip http server . . . 71

- Syntax . . . 71
- Parameters . . . 71
- Default . . . 71
- Command mode . . . 71
- Next command mode . . . 71
- Related commands . . . 72
- Example . . . 72

kill . . . 73

- Syntax . . . 73
- Parameters . . . 73
- Command mode . . . 73

Next command mode 73
Warnings 73
Related commands 74
Example 74
ldap 75
Syntax 75
Parameters 75
Default 76
Command mode 76
Next command mode 76
Warnings 76
Example 76
ldap-server 77
Syntax 77
Parameters 77
Default 77
Command mode 77
Next command mode 77
Related commands 78
Example 78
ldap-server source 79
Syntax 79
Parameters 79
Default 79
Command mode 79
Next command mode 79
Prerequisites 79
Warnings 80
Related commands 80
Example 80
load 81
Syntax 81
Parameters 81
Default 81
Command mode 81

Next command mode 81
Prerequisites 82
Related commands 82
Example 82
logging history 83
Syntax 83
Parameters 83
Default 83
Command mode 84
Next command mode 84
Warnings 84
Related commands 84
Example 84
logout 85
Syntax 85
Parameters 85
Command mode 85
Next command mode 85
Related commands 85
Example 85
more 86
Syntax 86
Parameters 86
Default 86
Command mode 87
Next command mode 87
Warnings 87
Example 88
ping 89
Syntax 89
Parameters 89
Default 89
Command mode 89
Next command mode 89
Warnings 90

Related commands 90
Examples 90
reload 91
Syntax 91
Parameters 91
Default 92
Command mode 92
Next command mode 93
Prerequisites 93
Warnings 93
Related commands 93
Example 94
Comments 94
reload at 95
Syntax 95
Parameters 95
Default 96
Command mode 96
Next command mode 96
Prerequisites 97
Warnings 97
Related commands 97
Example 98
Comments 98
reload cancel 99
Syntax 99
Parameters 99
Default 99
Command mode 99
Response 99
Next command mode 100
Warnings 100
Related commands 100
Example 101
reload in 102

Syntax 102
Parameters 102
Default 103
Command mode 103
Next command mode 103
Prerequisites 104
Warnings 104
Related commands 104
Example 105
Comments 105
reload no-sessions 106
Syntax 106
Parameters 106
Default 107
Command mode 107
Next command mode 107
Prerequisites 108
Warnings 108
Related commands 108
Example 109
Comments 109
server backup 110
Syntax 110
Parameters 110
Default 110
Command mode 110
Response 110
Next command mode 111
Prerequisites 111
Warnings 111
Related commands 111
Example 112
server restore 113
Syntax 113
Parameters 113

Default 113
Command mode 113
Response 113
Next command mode 114
Prerequisites 114
Warnings 114
Related commands 114
Example 115
server start 116
Syntax 116
Parameters 116
Default 116
Command mode 116
Response 116
Next command mode 116
Prerequisites 116
Warnings 117
Related commands 117
Example 117
Comments 117
server stop 117
Syntax 118
Parameters 118
Default 118
Command mode 118
Response 118
Next command mode 118
Prerequisites 118
Warnings 118
Related commands 119
Example 119
Comments 119
show arp 120
Syntax 120
Parameters 120

Default 120
Command mode 120
Next command mode 120
Related commands 120
Example 120
show exception backup 121
Syntax 121
Parameters 121
Default 121
Command mode 121
Response 121
Next command mode 122
Warnings 122
Related commands 122
Example 123
show file systems 124
Syntax 124
Parameters 124
Default 124
Command mode 124
Next command mode 124
Example 124
show flash: contents 125
Syntax 125
Parameters 125
Default 125
Command mode 126
Next command mode 126
Related commands 126
xample 127
show health 128
Syntax 128
Parameters 128
Default 129
Command mode 129

Response 129
Next command mode 129
Related commands 129
Example 129
show ip access-list 130
Syntax 130
Parameters 130
Default 130
Command mode 130
Response 130
Next command mode 131
Example 131
show ip ospf 132
Syntax 132
Parameters 132
Default 132
Command mode 132
Response 132
Next command mode 132
Related commands 132
Example 133
show ip ospf database 134
Syntax 134
Parameters 134
Default 134
Command mode 134
Response 134
Next command mode 134
Related commands 134
Example 135
show ip ospf interface 136
Syntax 136
Parameters 136
Default 136
Command mode 136

Response 136
Next command mode 136
Related commands 137
Example 137
show ip ospf neighbor 138
Syntax 138
Parameters 138
Default 138
Command mode 138
Response 138
Next command mode 138
Related commands 138
Example 139
show ip rip 140
Syntax 140
Parameters 140
Default 140
Command mode 140
Response 140
Next command mode 141
Related commands 141
show ip rip database 142
Syntax 142
Parameters 142
Default 142
Command mode 142
Response 142
Next command mode 143
Related commands 143
Example 143
show ip rip interface 144
Syntax 144
Parameters 144
Default 144
Command mode 144

Response 144
Next command mode 144
Related commands 144
Example 145
show ip route 146
Syntax 147
Parameters 147
Default 147
Command mode 147
Response 148
Next command mode 148
Related commands 148
Example 148
show ip route-policies 149
Syntax 149
Parameters 149
Default 149
Command mode 149
Response 149
Next command mode 150
Related commands 150
Example 150
show ip traffic 151
Syntax 151
Parameters 151
Default 151
Command mode 151
Response 151
Next command mode 151
Example 152
show ip vrrp 154
Syntax 154
Parameters 154
Default 154
Command mode 154

Response 154
Next command mode 154
Example 155
show ldap-server 156
Syntax 156
Parameters 156
Default 156
Command mode 156
Response 156
Next command mode 156
Warnings 157
Related commands 157
Example 157
show logging config 158
Syntax 158
Parameters 158
Default 159
Command mode 159
Response 159
Next command mode 159
Related commands 159
Example 160
Comments 160
show logging events 161
Syntax 161
Parameters 161
Default 162
Command mode 162
Response 162
Next command mode 162
Warnings 162
Related commands 162
Example 163
Comments 165
show logging history 165

Syntax 165
Parameters 165
Default 165
Command mode 166
Response 166
Next command mode 166
Related commands 166
Example 166
show logging security 166
Syntax 166
Parameters 167
Default 167
Command mode 167
Response 168
Next command mode 168
Related commands 168
Example 168
Comments 169
show logging syslog 169
Syntax 169
Parameters 169
Default 170
Command mode 170
Response 170
Next command mode 170
Related commands 171
Example 171
Comments 172
show reload 172
Syntax 172
Parameters 172
Default 172
Command mode 172
Response 172
Next command mode 173

- Warnings 173
- Related commands 173
- Example 173

show sessions 173

- Syntax 174
- Parameters 174
- Default 174
- Command mode 174
- Response 175
- Next command mode 175
- Related commands 175
- Example 175

show version 175

- Syntax 175
- Parameters 175
- Default 176
- Command mode 176
- Next command mode 176
- Related commands 176
- Example 176

snmp-server contact 177

- Syntax 177
- Parameters 177
- Default 177
- Command mode 177
- Next command mode 177
- Warnings 178
- Related commands 178
- Example 178

snmp-server location 179

- Syntax 179
- Parameters 179
- Default 179
- Command mode 179
- Next command mode 179

- Warnings 179
- Related commands 180
- Example 180

snmp-server name 181

- Syntax 181
- Parameters 181
- Default 181
- Command mode 181
- Next command mode 182
- Warnings 182
- Related commands 182
- Example 182

suffix remove 183

- Syntax 183
- Parameters 183
- Default 183
- Command mode 183
- Next command mode 183
- Related commands 183
- Example 184

trace 185

- Syntax 185
- Parameters 185
- Default 185
- Command mode 185
- Next command mode 185
- Warnings 186
- Related commands 186
- Example 186

who 187

- Syntax 187
- Parameters 187
- Default 187
- Command mode 187
- Next command mode 187

Warnings 187

Related commands 188

Chapter 3
Bulk Load Command 189

Components 190

Load command 190

Command file 190

File format 191

User commands 192

Add User 193

Delete User 194

Add Group 194

Modify Group 194

Purge Group 197

Delete Group 197

Delete All 198

Branch office commands 198

Add branch office connection 199

Modify branch office connection 202

Delete branch office connection 202

Add branch office group 203

Modify branch office group 203

Contivity VPN Switch configuration commands 206

Network definitions 206

NAT 207

Address pools 209

Filters 210

Automatic backup 213

SYSLOG forwarding 214

SNMP 215

DHCP 217

Licensing commands 218

Usage notes 219

Deletion of groups 219

Required fields for user and branch records 219
Group name syntax 220
Certificate Distinguished Name order 220
Index 221

Preface

This book is intended for Nortel Networks™ Contivity™ VPN Switch managers and administrators. It provides reference information for each of the Web browser configuration screens.

Conventions

This guide refers to the Contivity VPN Switch as the switch.. This guide assumes that you are familiar with Web browsers and their general operation.

Documentation

This document uses the following conventions to distinguish among notes of varying importance.

Note: *Take notice*. Notes contain helpful suggestions or references to materials contained in this document.

Caution: *Be careful*. In this situation, you might do something that could result in damage to the equipment or loss of data.

Warning: *Danger.* You are in a situation that could cause bodily injury. Before working on equipment, beware of the hazards involved with electrical circuitry and standard practices for preventing accidents, such as disconnecting equipment from its power source.

Related publications

The following list shows the associated documentation that you will need to configure and manage the switch and describes the document's objectives.

- *Contivity VPN Switch Release Notes* provide the latest information, including known problems, workarounds, and special considerations.
- *Configuring the Contivity VPN Switch* (included on the CD) provides complete details to configure, monitor, and troubleshoot the switch.
- *Reference for the Contivity VPN Switch* provides reference information for each of the Web browser configuration screens.

Text

This guide uses the following text conventions:

angle brackets (< >)

Indicate that you choose the text to enter based on the description inside the brackets. Do not type the brackets when entering the command.

Example: If the command syntax is `ping <`*`ip_address`*`>`, you enter `ping 192.32.10.12`

`bold Courier text`

Indicates command names, options, and text that you need to enter.

Example: Use the **`dinfo`** command.

Example: Enter **`show ip`** {**`alerts|routes`**}.

braces ({})

Indicate required elements in syntax descriptions where there is more than one option. You must choose only one of the options. Do not type the braces when entering the command.

Example: If the command syntax is `show ip {alerts|routes}`, you must enter either `show ip alerts` or `show ip routes`, but not both.

brackets ([ ])

Indicate optional elements in syntax descriptions. Do not type the brackets when entering the command.

Example: If the command syntax is `show ip interface [-alerts]`, you can enter either `show ip interface` or `show ip interface -alerts`.

ellipsis points (. . .)

Indicate that you repeat the last element of the command as needed.

Example: If the command syntax is `ethernet/2/1 [<parameter> <value>]...`, you enter `ethernet/2/1` and as many parameter-value pairs as needed.

italic text

Indicates new terms, book titles, and variables in command syntax descriptions. Where a variable is two or more words, the words are connected by an underscore.

Example: If the command syntax is `show at <valid_route>`, `valid_route` is one variable and you substitute one value for it.

`plain Courier text`

Indicates command syntax and system output, for example, prompts and system messages.

Example: `Set Trap Monitor Filters`

separator (->)

Shows menu paths.

Example: Protocols -> IP identifies the IP option on the Protocols menu.

vertical line (|)

Separates choices for command keywords and arguments. Enter only one of the choices. Do not type the vertical line when entering the command.

Example: If the command syntax is `show ip {alerts|routes}`, you enter either `show ip alerts` or `show ip routes`, but not both.

Acronyms

This guide uses the following acronyms:

AUI	attachment unit interface
BootP	Bootstrap Protocol
BRI	basic rate interface
CSMA/CD	carrier sense multiple access/collision detection
DLCMI	Data Link Control Management Interface
HDLC	High-level Data Link Control
IP	Internet Protocol
ISDN	Integrated Services Digital Network
ISO	International Organization for Standardization
ITU-T	International Telecommunication Union-Telecommunication Standardization Sector (formerly CCITT)
MAC	media accountants control
MAU	media access unit
MDI-X	medium dependent interface crossover
NBMA	nonbroadcast multi-access
OSPF	Open Shortest Path First
PPP	Point-to-Point Protocol
SMDS	Switched Multimegabit Data Service
SNMP	Simple Network Management Protocol
STP	shielded twisted pair
TPE	twisted pair Ethernet

Hard-copy technical manuals

You can print selected technical manuals and release notes free, directly from the Internet. Go to the www25.nortelnetworks.com/library/tpubs/ URL. Find the product for which you need documentation. Then locate the specific category and model or version for your hardware or software product. Use Adobe Acrobat Reader to open the manuals and release notes, search for the sections you need, and print them on most standard printers. Go to Adobe Systems at the www.adobe.com URL to download a free copy of the Adobe Acrobat Reader.

You can purchase selected documentation sets, CDs, and technical publications through the Internet at the www1.fatbrain.com/documentation/nortel/ URL.

You can purchase Nortel Networks documentation sets, CDs, and selected technical publications through the Nortel Networks Collateral Catalog. The catalog is located at support.baynetworks.com/catalog.html:

- The “CD ROMs” section lists available CDs.
- The “Guides/Books” section lists books on technical topics.
- The “Technical Manuals” section lists available printed documentation sets.

Make a note of the part numbers and prices of the items that you want to order. Use the “Marketing Collateral Catalog description” link to place an order and to print the order form.

User interface help button

Click the Help button that is located in the upper right of displays to learn about fields on a given page. Where appropriate, the information provides cause and effect of an action; otherwise, it might offer troubleshoot

Nortel Networks Customer Service

If you purchased a service contract for your Nortel Networks product from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller for assistance.

If you purchased a Nortel Networks service program, contact one of the following Nortel Networks Technical Solutions Centers:

Technical Solutions Center	**Telephone**
EMEA	(33) (4) 92-966-968
North America	(800) 2LANWAN or (800) 252-6926
Asia Pacific	(61) (2) 9927-8800
China	(800) 810-5000

An Express Routing Code (ERC) is available for many Nortel Networks products and services. When you use an ERC, your call is routed to a technical support person who specializes in supporting that product or service. To locate an ERC for your product or service, go to the www12.nortelnetworks.com/ URL and click ERC at the bottom of the page.

Chapter 1
Introduction

This chapter provides an introduction to the Contivity VPN Switch Command Line Interface (CLI).

Accessing the CLI

Access from a Telnet session

You access the CLI by starting a Telnet session to the switch’s Management IP Address, for example:

```
telnet 10.0.16.247
```

You then log into the switch using an account with administrator privileges, for example:

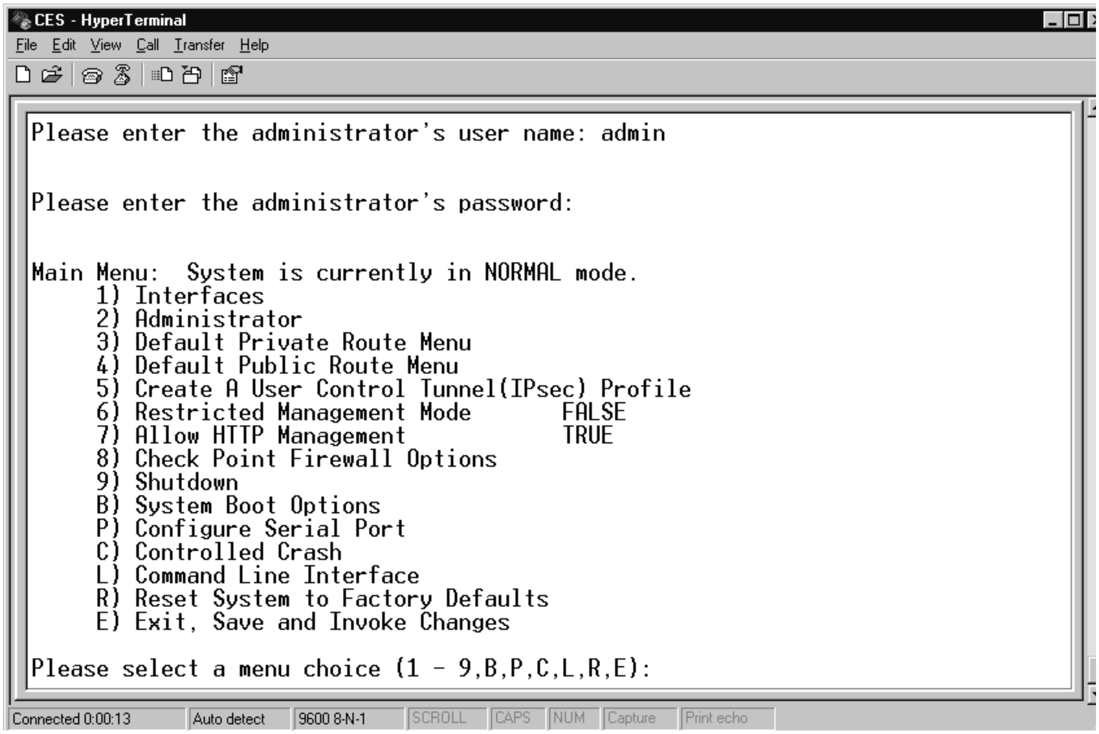
```
Login: admin
Password: *******
%%
```

Upon login, the CLI prompt appears (%%), indicating that you are in the CLI User Exec Mode. You can execute any User Exec Mode commands or change the command mode in order to execute other commands.

Note: The Telnet protocol must be enabled on the switch in order to use the CLI via a Telnet connection. Use the Services->Available screen to enable the Telnet management protocol.

Access from the serial port menu

You can access the CLI through the Serial Port menu if you have a serial port connection to the switch. Select L from the Serial Port menu, shown below, to access the CLI.



```
Please enter the administrator's user name: admin


Please enter the administrator's password:


Main Menu:  System is currently in NORMAL mode.
     1) Interfaces
     2) Administrator
     3) Default Private Route Menu
     4) Default Public Route Menu
     5) Create A User Control Tunnel(IPsec) Profile
     6) Restricted Management Mode       FALSE
     7) Allow HTTP Management            TRUE
     8) Check Point Firewall Options
     9) Shutdown
     B) System Boot Options
     P) Configure Serial Port
     C) Controlled Crash
     L) Command Line Interface
     R) Reset System to Factory Defaults
     E) Exit, Save and Invoke Changes

Please select a menu choice (1 - 9,B,P,C,L,R,E):
```

Figure 1 Serial Port Menu

Command modes

The switch CLI has three command modes.

- User Exec Mode
- Privileged Exec Mode
- Global Configuration Mode

Table 1 CLI Modes, Prompts and Access

Mode	Prompt	Access
User Exec Mode	CES>	Login via **Telnet** with **administrator name** and **password**.
Privileged Exec Mode	CES#	Enter the command **enable** at the User Exec Mode prompt.
Global Config Mode	CES(config)#	Enter the command **configure terminal** at the Privileged Exec Mode prompt.

User Exec Mode

This is the initial command mode when the administrator first establishes a Telnet connection to the switch. It is also called Exec mode.

This is a limited display mode. You cannot modify configuration parameters or view the configuration file.

User Exec Mode prompt

```
CES>
```

User Exec Mode commands

The following table summarizes the User Exec Mode commands.

Table 2 User Exec Mode Commands

Command	Description
clear ip route	Remove a route from the route table
enable	Enable privileged commands
exit	Exit the Telnet session
help	Display message about using help
ping	Send ping message to a destination
show file systems	List available file systems
show flash: contents	Display flash settings

Table 2 User Exec Mode Commands

Command	Description
show ip access-list	Display IP access lists
show ip ospf	Display IP OSPF routing details
show ip ospf database	Display IP OSPF database summary
show ip ospf interface	Display IP OSPF interfaces
show ip ospf neighbor	Display IP OSPF neighbor list
show ip rip	Display IP RIP details
show ip rip database	Display info about routes owned and imported by RIP
show ip rip interface	Display info about interfaces configured for RIP
show ip route	Display IP routing table
show ip route-policies	Display IP route policies
show ip traffic	Display information on IP traffic to/ from switch
show ip vrrp	Display IP VRRP settings
show reload	Show details of pending switch reboot
show sessions	Show current switch sessions
show version	Show switch configuration and hardware
trace	Trace the route to a destination
who	Display active Telnet sessions on switch

Privileged Exec Mode

This command mode is entered from User Exec mode with the enable command. The administrator can exit from this mode with the disable command, they will be returned to User Exec mode.

This is a full display and configuration mode; it enables additional commands to those in User Exec mode. Exec commands are typically one-time commands, for example, show commands and clear commands.

Privileged Exec Mode prompt

```
CES#
```

Privileged Exec Mode commands

The following table summarizes the Privileged Exec Mode commands

Table 3 Privileged Exec Mode commands

Command	Description
clear arp-cache	Clear ARP cache
clear logging events	Clear event log
configure	Enter configuration mode
disable	Turn off privileged commands
help	Display message about using help
kill	Terminate a Telnet session
more	Display the contents of a named file
reload	Reboot switch immediately
reload at	Schedule a switch reboot
reload cancel	Cancel pending reboot
reload in	Schedule a switch reboot
reload no-sessions	Schedule switch reboot when no more sessions
show arp	Show ARP cache contents
show health	Show overall system health
show logging config	Show configuration log contents

Table 3 Privileged Exec Mode commands

Command	Description
show logging events	Show event log contents
show logging history	Show the logging history setting
show logging security	Show security log contents
show logging syslog	Show system log contents

Global Configuration Mode

This mode allows the administrator to make changes to the switch running configuration. These changes are saved across reboots. This mode is also used to access other configuration modes (Router, and so on, to be supported in subsequent releases). The administrator enters this mode from Privileged Exec mode using the configure command. To leave this mode and return to Privileged Exec mode, the user enters Ctrl-Z.

Global Configuration Mode prompt

```
CES(config)#
```

Global Configuration Mode commands

The following table summarizes the Global Configuration Mode commands.

Table 4 Global Configuration Mode commands

Command	Description
arp	Delete ARP cache entries
audible alarm	Enable audible alarm
console mode	Set administration console mode (Mini-CLI)
control	Maintain control tunnel connections (Mini-CLI)
default logging history	Set logging history level to default value
enable password	Assign privileged level password
end	Exit from configure mode

Table 4 Global Configuration Mode commands

Command	**Description**
exit	Exit from configure mode
help	Display message about using help
ip http server	Enable/disable HTTP management
ldap	Control LDAP server (Mini-CLI)
load	Bulk load configuration commands (Mini-CLI)
logging history	Control system logging level
logout	Exit the Telnet session (Mini-CLI)
reset	Set switch system boot mode (Mini-CLI)
restore flash	Restore factory default switch flash settings
restore system	Restore factory default switch configuration
restrict	Restrict management access to (Mini-CLI)
save current_boot	Save current boot config (Mini-CLI)
shutdown	Shutdown the switch (Mini-CLI)
snmp-server contact	Set the contact details for the switch
snmp-server location	Set the locations details for the switch
snmp-server name	Set the administrative name for the switch

Key bindings

You can use the Nortel Networks CLI (NNCLI) commands to edit command line text entries. Table 2 describes key bindings for NNCLI.

Table 5 NNCLI key bindings

Keys	**Function**
control-A	start of line
control-B	back 1 character
control-C	abort command

Table 5 NNCLI key bindings

Keys	**Function**
control-D	delete 1 character
control-E	end of line
control-F	forward 1 character
control-H &	delete character left of cursor
control-I &	command/parameter completion
control-K	delete all characters after cursor
control-L & control-R	re-display line
control-N or down arrow	next history command
control-P or up arrow	previous history command
control-Q	escape sequence for unprintables
control-T	transpose characters
control-U	delete entire line
control-W	delete word left of cursor
control-X	delete all characters before cursor delete character at cursor
control-z	“end” out of config mode
?	context-sensitive help
esc-c & esc-u	capitalize character at cursor
esc-l	convert character at cursor to lowercase
esc-b	backward 1 word
esc-d	delete 1 word to the right
esc-f	forward 1 word

Chapter 2
CLI Command Summary

This chapter provides a summary of all CLI commands. The Commands are listed in alphabetical order.

arp

This command modifies the contents of the Address Resolution Protocol (ARP) cache. On the Contivity VPN Switch, only the no form of the de facto command is supported. There is no command to add a permanent entry to the ARP cache.

Syntax

```
no arp ip-address
```

Parameters

ip-address	The IP address to be removed from the ARP cache.

Default

None

Command mode

Global Configuration

Next command mode

Global Configuration

Related commands

```
show arp
clear arp-cache
```

audible alarm

This command enables and disables the audible alarm on the switch that is sounded under certain error conditions.

Syntax

```
audible alarm
no audible alarm
```

Parameters

None

Default

Audible alarm is enabled.

Command mode

Global Configuration

Next command mode

Global Configuration

Related commands

```
show health
```

Example

```
CES(config)#no audible alarm
```

This example shows the audible alarm being switched off for the switch.

clear arp-cache

This command deletes all dynamic entries from the ARP cache, to clear the fast-switching cache, and to clear the IP route cache

Syntax

This command has no arguments or keywords.

clear arp-cache

Parameters

None

Default

None

Command mode

Privileged Exec

Next command mode

```
Privileged Exec
```

Related commands

```
arp
show arp
```

clear ip route

This command removes a route from the route table. Note that Static Routes are not removed from the switch browser interface by this command. This command is intended as a troubleshooting tool for use when routing problems are being caused by the presence of a wrong route.

Syntax

```
clear ip route address [mask]
```

Parameters

address	The address of the network to remove from route table.
mask	The mask associated with the address to remove.

Default

The mask defaults to 255.255.255.255.

Command mode

User Exec

Next command mode

User Exec

Warnings

Address not found in route table.

Related commands

```
show ip route
```

Example

```
CES>clear ip route 10.11.0.12
```

clear logging events

This command is used to clear the contents of the system events log.

Syntax

clear logging events

Parameters

None

Default

None

Command mode

Privileged Exec

Next command mode

```
Privileged Exec
```

Related commands

```
show logging events
```

Example

```
CES>clear logging events
```

The example shows the command in use. This command does not give any feedback to the user.

configure

This command puts the CLI into global configuration mode. This allows the administrator to access global configuration mode commands. To exit this mode, the user can enter [control]-Z, the exit command, or the end command.

All global configuration commands are entered from the terminal.

Syntax

```
configure terminal
```

Parameters

None

Default

None

Command mode

```
Privileged Exec
```

Next command mode

```
Global configuration
```

Related commands

```
disable
enable
end
```

Examples

```
CES#configure

CES(config)#end
```

console mode

Note: You must have a control tunnel established before you can set this command.

This is a mini-CLI command that allows emulation of CLI commands available in earlier versions of the Contivity VPN Switch software.

This command controls which menu items are visible on the serial port console for the switch, and what CLI commands can be used.

When this command is used to set the switch in one of the two restricted modes, the only CLI commands that are available are:

```
disable
enable
exit
reload
reload at
reload in
reload no-sessions
```

Because none of the Global Configuration mode commands are allowed, setting the switch into a restricted mode causes the CLI to return to Privileged Exec mode on the Telnet session where the command is issued. Other Telnet sessions will not be forced back to Privileged Exec mode, but they will only support the above CLI command set.

The switch can be set back to an unrestricted mode on the System->Settings Web management page.

Syntax

console mode {*restricted1*|*restricted2*|*show*}

Parameters

restricted1	The system reset and reload commands to change the IP interface address and mask are enabled.
restricted2	Only the system reload commands are enabled. The reload command in the CLI only supports the boot-safe and boot-normal parameters.
show	Display the current console mode setting.

Default

The system boots in unrestricted mode, where all commands are enabled.

Command mode

Global configuration

Next command mode

Global configuration (console mode show) or Privileged Exec

Related commands

```
reload
reload at
reload in
reload no-sessions
```

Examples

CES(config)#console mode show

```
CONSOLE MODE is set to UNRESTRICTED
```

```
CES(config)#console mode restricted1

CONSOLE MODE has been set to RESTRICTED1.

CES#?

Exec commands:

disable          Turn off privileged commands.

enable           Turn on privileged commands.

exit             Exit the Telnet session.

reload           Stop and perform a cold restart.
```

These examples show the default console mode setting, and how setting the console mode to restricted forces the user back to Privileged Exec mode and limits the available CLI commands.

control

This command allows emulation of CLI commands available in earlier versions of the switch software.

This command allows the administrator to create or delete control tunnels and to display the currently existing control tunnels.

Control tunnels provide a secure means to manage the switch.

Syntax

control [*help*] {*create*|*delete*|*show*}

Parameters

help	If present, the control command is not Executed, but some Help about the command is displayed..
create	Create control tunnels.
delete	Delete control tunnels.
show	Display the current control tunnels.

Command mode

Global configuration

Next command mode

Global configuration

Related commands

None

Examples

```
CES(config)#control Help delete

CES(config)#control create

CES(config)#control show
```

disable

This command makes the CLI parser exit from Privileged Exec mode and return to user Exec mode.

Syntax

```
disable
```

Parameters

None

Default

None

Command mode

Privileged Exec

Next command mode

User Exec

Related commands

```
configure

enable

end
```

Example

```
CES#disable

CES>
```

enable

This command puts the CLI parser into Privileged Exec mode, allowing the administrator to use additional CLI commands.

The administrator is prompted for a case-sensitive password before they can enter privileged Exec mode. This password is created when the administrator user account is set up using the Web management pages.

The user gets three attempts to enter the password. After the third incorrect attempt an error message is displayed (Bad secrets) and the User Exec prompt is redisplayed.

Syntax

enable

Parameters

None

Default

None

Command mode

User Exec

Next command mode

Privileged Exec

Warnings

%Bad secrets

Related commands

```
configure

disable

enable password
```

Example

```
CES>enable

Password: fred (The password does not display.)

CES#disable

CES>
```

enable password

This command allows the user to change the password used by the enable command to get into privileged Exec mode. This is the same password as set on the Profiles->Users Web page for the administator (user admin) account.

If the new password is not different from the existing password, a warning message is generated.

Syntax

enable password *password*

Parameters

password	The password is defined that the administrator types to enter enable mode. This password is case sensitive.

Default

The default password is defined when the (administrator) user admin account is created on the Profiles->Users Web management page.

Command mode

Global configuration

Next command mode

Global configuration

Warnings

New password is same as current one.

Related commands

```
configure

disable

enable
```

Examples

```
CES(config)#enable password fred
CES(config)#exit
CES#disable

CES>enable
Password: fred
CES#configure
CES(config)#enable password jane
CES(config)#exit
CES#disable

CES>enable
Password: fred
Password: joan
Password: charles
% Bad secrets

CES>enable
Password: jane
CES#configure
CES(config)#enable password jane

The enable password you have chosen is the same as your current
password.

This is not recommended.  reenter the enable password.
```

This first example shows the password being set in global configuration mode and then asked for when the administrator tries to go from user Exec mode back to privileged Exec mode. The administrator then changes the enable password and enters an incorrect one three times.

The last example shows the error message displayed when the administrator tries to reuse the existing password.

exception backup

This command allows the administrator to define backup FTP servers for the Contivity VPN Switch. A backup FTP server receives a copy of the LDAP database, configuration file, and other system files that have changed since the last backup. A switch supports up to three backup FTP servers.

Syntax

exception backup {*1|2|3*} backup-ip-add [*backup-filepath*] [*interval hours*] username user_name password userpassword

no exception backup {*1|2|3*}

default exception backup

Parameters

1|2|3	The number of backup FTP servers being modified (defined/undefined)
backup_ip_add	The IP address for backup server
backup_file_path	If present, specifies the file path on the backup server where the files should be written.
hours	The time interval in hours between backups; range is 1 to 8064 hours.
user_name	The user name that the switch uses to establish the FTP connection to the backup server
user_password	The user password that the switch uses to establish the FTP connection to the backup server

Default

Defaults to 5 hours, if the interval is omitted.

Command mode

Global configuration

Next command mode

Global configuration

Related commands

show exception backup

Example

```
CES(config)#exception backup 1 12.0.44.129 interval 4 username
BackupLogon password BackupPassword
```

exit

This command allows the administrator to exit any configuration mode or to close an active Telnet session if they use the command when in User Exec mode.

Syntax

```
exit
```

Parameters

None

Default

None

Command mode

Available in all command modes

Next command mode

Either the lower level command mode, or none because the Telnet session is terminated

Related commands

end

Example

```
CES(config)#exit

CES#exit

CES>
```

This example shows a user starting in Global configuration mode and using the exit command twice to end in User Exec mode.

help

This command displays a message about how to use the Help system.

Syntax

help

Parameters

None

Command mode

Available in all command modes

Related commands

None

Example

CES#help

Help may be requested at any point in a command by entering a question mark (?). If nothing matches, the Help list is empty and you must back up until entering a question mark (?) shows the available options.

Two styles of Help are provided:

1. Full Help is available when you are ready to enter a command argument (for example, 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 (for example, show arp?).

host address

This command establishes the IP address, port, bind DN, and bind password settings for the external master and slave LDAP servers. The master server is the primary server to process queries. If the master server becomes unavailable, the switch attempts to use the slave LDAP servers. The switch reattempts connection to the master server every 15 minutes or upon a configuration change. The switch has read/write access to the master LDAP server. The slave servers are read-only.

Syntax

```
host address {master|slave1|slave2} [{port|ssl-port} [port_number]] [bind-dn bind_dn_value] bind-password bind_password

no host {master|slave1|slave2}
```

Parameters

address	The IP address for the LDAP server. Can be a dotted IP address or a host name. The host name does not have to be fully qualified if it is in the same domain as the switch.
master	The settings for the master LDAP server
slave1	The settings for the slave 1 LDAP server
slave2	The settings are for the slave 2 LDAP server
port	The port number that connects to the LDAP server
ssl-port	The port number to connect to the LDAP server when using SSL. In addition, the SSL encryption settings must be se.
port_number	The port number to connect to on the LDAP server
bind-dn	If present, the distinguished name used to connect to the LDAP server

bind_dn_value The bind distinguished name (DN) used to connect to the LDAP server. This is the equivalent of a user ID for an LDAP server. It can be omitted for an LDAP server that allows anonymous access.

bind-password A password must be used during connection to the FTP server.

Default

Defaults to a non-SSL connection made to port 389. If ssl-port is specified without providing a port number value, the SSL connection attempt is made to port 636.

Command mode

Global configuration

Next command mode

Global configuration

Prerequisites

None

Related commands

ldap-server

show ldap-server

Example

See the example for the ldap-server command.

hostname

This command allows the administrator to specify the DNS host name for the switch. This name should correspond to the name in the DNS server to identify the management address of the switch that is located on the private network.

Syntax

```
hostname string
```

Parameters

string	The DNS name to assign to the switch. This name can have up to 64 characters.

Default

None

Command mode

Global configuration

Next command mode

Global configuration

Prerequisites

At least one DNS server should be specified.

Warnings

Validate against DNS server?

Related commands

```
no hostname
```

```
ip domain-name
```

```
ip name-server
```

interface management

Example

CES(config)#hostname MarketingCES

This example assigns the name MarketingCES to the switch.

interface management

This command is used to specify the IP address that is used to connect to systemfor the services such as HTTP, FTP, SNMP, and Telnet. The IP address cannot be used for any other purpose.

Syntax

```
interface management

ip address address

exit
```

Parameters

address	The IP address that is used to connect to system services on the switch

Command mode

Global configuration

Next command mode

Interface configuration

Warnings

IP Address is already in use on switch for other purposes.

Related commands

```
ip http server
```

Example

```
CES(config)#interface management

Router(config-if)#ip address 10.0.3.33

Router(config-if)#exit
```

This command assigns the IP address 10.0.3.33 to the switch for HTTP, FTP, Telnet, and SNMP connections.

ip http server

This command allows the administrator to enable or disable management of the switch using a Web browser. If HTTP management is disabled, the switch can still be managed using the Nortel Networks CLI.

Syntax

```
ip http server
```

```
no ip http server
```

Parameters

None

Default

This feature is enabled by default on the switch.

Command mode

Global configuration

Next command mode

Global configuration

Related commands

interface loopback

Example

```
CES(config)#no ip http server
```

This command disables management of the switch using a Web browser. The switch can still be configured using the CLI.

kill

This command terminates an identified Telnet session. The Telnet session ID can be obtained using the who command.

Any in-progress session commands are completed and the session is then terminated without any warning or message to the Telnet user.

If the session ID given by the administrator is not valid, or is not for a Telnet session, the command displays an error message and does nothing.

Syntax

```
kill telnet_id
```

Parameters

telnet_id	Session ID of Telnet session to be terminated

Command mode

Privileged Exec

Next command mode

Privileged Exec

Warnings

Invalid session ID.

Session is not a Telnet session.

Related commands

who

show sessions

Example

CES# who

```
121: From 116.102.4.45
213: From 116.102.12.23
217: From 116.102.12.23
CES# kill 213
```

CES# who

```
121: From 116.102.4.45
217: From 116.102.12.23
```

This example shows a series of Telnet sessions active on the switch. One is terminated using kill and the results are shown in the subsequent who command.

ldap

This is a mini-CLI command to allow emulation of CLI commands available in versions of the switch software earlier than Release 3.0.

This command allows the administrator to:

- Start or stop the switch internal LDAP server
- Export the LDAP database to an LDIF file on the switch
- Import the LDAP database from an LDIF file on the switch
- Show the current LDAP server status

Syntax

ldap [*help*] {*export*|*import*|*show*|*start*|*stop*}

Parameters

help
If present, the ldap command is not Executed, but some Help about the command is displayed on the terminal.

export
Export the contents of the LDAP database to the named LDIF file. The LDAP server must be stopped before an ldap export can be performed.

import
Import the contents of the LDAP database from the named LDIF file. The current LDAP database contents are replaced. The LDAP server must be stopped before an ldap import can be performed.

show
Display the status of the LDAP server.

start
Start the LDAP server running. This command cannot be performed while the LDAP server is performing an export or import command. This command cannot be Executed unless the LDAP server is actually stopped.

stop	Stop the LDAP server running. This command cannot be Executed unless the LDAP server is actually running.

Default

None

Command mode

Global configuration

Next command mode

Global configuration

Warnings

LDAP server is currently running.

LDAP server is already running.

LDAP server is already stopped.

Invalid LDIF file name.

LDIF file does not exist.

Example

```
CES(config)#ldap show

CES(config)#ldap stop

CES(config)#ldap export

CES(config)#ldap start
```

ldap-server

This command is used to configure the settings for the LDAP server used by the switch to store the configuration settings that are not specific to an individual switch. The LDAP server can be internal to the switch being administered, or can be an external server that is shared by one or more Contivities.

Syntax

```
ldap-server {internal|external}
```

Parameters

internal	Enter LDAP server configuration mode for the internal LDAP server.
external	Enter LDAP server configuration mode for an external LDAP server.

Default

When initially configured, the switch has an internal LDAP server.

Command mode

Global configuration

Next command mode

LDAP server configuration

Related commands

ldap-server source

show ldap-server

Example

```
CES(config)#ldap-server source internal

CES(config)#ldap-server internal

Router(config-ldap)#server stop

Router(config-ldap)#server backup bk0901

Router(config-ldap)#server start

Router(config-ldap)#exit
```

This example sets the switch to use the internal LDAP server, stops the server, and backs up the current server database to an LDIF file named /ide0/system/slapd/ldif/bk0901. The prompt returns after the backup is completed, then the administrator restarts the LDAP server.

CES(config)#ldap-server external

```
Router(config-ldap)#domain-delimiter @ suffix
Router(config-ldap)#suffix remove
Router(config-ldap)#host 122.33.102.44 master bind-dn cn=Management
bind-password myPas4wd
Router(config-ldap)#base-dn ou=engineering, o=Nortel Networks, c=US
Router(config-ldap)#exit
CES(config)#ldap-server source external
```

This example specifies the settings for a master LDAP server at IP address 122.33.102.44 port number nnn, with a bind DN and base DN. The domain delimiter is the character @ and the domain suffix is removed. The switch is set to use the external LDAP server.

ldap-server source

This command sets the source of the LDAP server used by the switch to either the internal LDAP server on the switch itself, or an external LDAP server that can be shared by one or more Contivities.

Syntax

ldap-server source {*internal*|*external*}

Parameters

internal	Use the internal LDAP server for switch configuration data.
external	Use the external LDAP server for switch configuration data.

Default

When initially configured, the switch has an internal LDAP server.

Command mode

Global configuration

Next command mode

Global configuration

Prerequisites

If setting to an external LDAP server, the settings must already have been configured for the LDAP server.

Warnings

External LDAP server not configured.

Cannot reach external LDAP server.

Related commands

```
ldap-server
```

```
show ldap-server
```

Example

See the example for the ldap-server command.

load

This is a mini-CLI command to allow emulation of CLI commands available in earlier versions of the switch software.

This command allows the administrator to use the Bulk Load facility to Execute a command file that has been previously copied to the switch using FTP. The commands in the file can configure various settings on the switch. This facility is used to bulk configure the switch.

Syntax

```
load filename
```

Parameters

filename	The name of the file on the switch that contains the bulk load commands.

Default

None

Command mode

Global configuration

Next command mode

Global configuration

Prerequisites

The LDAP server must be running.

Related commands

ldap

Example

```
CES(config)#load /ide0/system/test.cmd
```

logging history

This command determines what types of messages are stored in the system logs. Once the message type level has been established, future messages stored in the system logs must be at or above this level for them to be saved.

This is different from the IOS implementation, where this command only affects syslog messages.

On the switch a warning is displayed if the level set with this command does not agree with the level required for syslog message forwarding (as set in the logging facility syslog command).

Syntax

```
logging history {alerts|errors|notifications|debugging}

default logging history
```

Parameters

alerts	Log all emergency and alert messages.
errors	Previous level plus critical and error conditions.
notifications	Previous level and warnings and notifications.
debugging	All message levels.
default	Sets logging level back to alerts for future messages.

Default

Defaults to a logging level of alerts.

The default logging history command sets the level to errors for future messages.

Command mode

Global configuration

Next command mode

Global configuration

Warnings

Does not agree with syslog forwarding settings.

Related commands

```
show logging history
```

```
logging facility syslog
```

```
show logging syslog
```

Example

```
CES(config)#logging history errors
```

This command sets the system logging on the switch to store emergency, alert, critical, and error condition messages in the system log.

logout

This is a mini-CLI command to allow emulation of CLI commands available in earlier versions of the switch software.

This command logs the administrator off the switch and terminates the Telnet session. It is equivalent to using the exit command in User Exec mode.

Syntax

```
logout
```

Parameters

None

Command mode

Global configuration

Next command mode

Global configuration

Related commands

```
exit
```

Example

```
CES(config)#logout
```

This example disconnects the session.

more

This command displays a readable file on the switch. The file is displayed on Telnet screen at a time. The user can use the pagination keys to see the next screen or line in the file, or to quit from the display.

It differs from the de facto standard in that it cannot be used to display a file on a remote file system. It also does not support the /ebcdic output switch that causes the file to be printed in EBCDIC mode.

On the switch, this command is limited to files that are 10KB or smaller. If the user tries to use more on a file that is larger than 10KB, an error message is displayed.

Syntax

```
more [/ascii|/binary] file
```

Parameters

/ascii	Display file in ASCII.
/binary	Display file in binary.
file	Fully qualified name of the switch file to display. The name has the format: diskn:[directory/]file.ext where: diskn is either disk0 or disk1, there are zero or more directory names and there is a file name.

Default

The default depends on the type of file. If the file contains non-printable characters, it defaults to binary output, otherwise it defaults to ASCII output. You cannot print a binary file in ASCII format output. If you attempt to print a binary file in ASCII output format, the switch is ignored.

Printable characters are characters whose character codes are in the range decimal 32 (space) to decimal 126 (~) inclusive, plus the characters \t (decimal 9), \n (decimal 10), and \r (decimal 13). Non-printable characters are represented by a period (.) in the ASCII part if the binary output format.

Command mode

Privileged Exec

Next command mode

Privileged Exec

Warnings

File not found.

Cannot display a file that is larger that 10KB.

Example

```
CES#more disk0:system/config/CFG01022.DAT

+AccessLst[abc]
AccessLst[abc].Name=abc
+AccessLst[abc].Rule[11.4.1.6:1.1.1.1:DENY]
AccessLst[abc].Rule[11.4.1.6:1.1.1.1:DENY].Key=11.4.1.6:1.1.1.1:DENY
AccessLst[abc].Rule[11.4.1.6:1.1.1.1:DENY].Protocol=IP
AccessLst[abc].Rule[11.4.1.6:1.1.1.1:DENY].SourceAddr=11.4.1.6
AccessLst[abc].Rule[11.4.1.6:1.1.1.1:DENY].SourceWildcard=1.1.1.1
+AccessLst[abc].Rule[abdguiwfeh:255.255.0.0:Permit]
AccessLst[abc].Rule[abdguiwfeh:255.255.0.0:Permit].Action=PERMIT
AccessLst[abc].Rule[abdguiwfeh:255.255.0.0:Permit].Key=abdguiwfeh:255.255.0.0:Permit
AccessLst[abc].Rule[abdguiwfeh:255.255.0.0:Permit].SourceWildcard=255.255.0.0
+AccessLst[abc].Rule[2.0.0.0:255.0.0.:Permit]
AccessLst[abc].Rule[2.0.0.0:255.0.0.:Permit].Action=PERMIT
AccessLst[abc].Rule[2.0.0.0:255.0.0.:Permit].Key=2.0.0.0:255.0.0.:Permit
AccessLst[abc].Rule[2.0.0.0:255.0.0.:Permit].SourceAddr=2.0.0.0
+AccessLst[bar]
AccessLst[bar].Name=bar
+AccessLst[bar].Rule[1.2.0.0:255.255.0.0:0]
AccessLst[bar].Rule[1.2.0.0:255.255.0.0:0].Key=1.2.0.0:255.255.0.0:0

CES#

CES#more /binary disk0:system/config/CFG01022.DAT

00000000:  0A210A21 204C6173 7420636F 6E666967    .!.!  Las t co nfig
00000010:  75726174 696F6E20 6368616E 67652061    urat ion  chan ge a
00000020:  74203134 3A30333A 32322070 73742046    t 14 :03: 22 p st F
00000030:  72692041 75672032 37203139 39390A21    ri A ug 2 7 19 99.!
00000040:  204E5652 414D2063 6F6E6669 67206C61     NVR AM c onfi g la
00000050:  73742075 70646174 65642061 74203134    st u pdat ed a t 14
00000060:  3A30393A 30392070 73742046 72692041    :09: 09 p st F ri A
00000070:  75672032 37203139 39390A21 0A766572    ug 2 7 19 99.! .ver
00000080:  73696F6E 2031322E 300A7365 72766963    sion  12. 0.se rvic
```

This first example of using more to display the contents of a config file in ASCII mode. The second example (with bogus file contents) of the binary output format.

ping

The ping (packet internet groper function) command provides a basic ping facility. It sends three 100-byte ping packets.

The ping command does not recognize DNS names with hyphens.

Syntax

ping {*host* | *address*} [*scr_host* | *scr_address*]

Parameters

address	The IP address of system to ping
host	The host name of system to ping
scr_host	The source host name
scr_address	The source IP address

Default

None

Command mode

User Exec

Next command mode

User Exec

Warnings

If the system cannot map an address for a host name, it returns a "%Unknown Host" error message.

Related commands

trace ip {*host* | *address*}

Examples

```
CES>ping 122.104.11.112

  PING 122.104.11.112: 56 data bytes

  64 bytes from 122.104.11.112: icmp_seq=0. time= 16 ms

  64 bytes from 122.104.11.112: icmp_seq=1. time=<16 ms

  64 bytes from 122.104.11.112: icmp_seq=2. time=<16 ms

  ----122.104.11.112 PING Statistics----

  3 packets transmitted, 3 packets received, 0% packet loss

  round-trip (ms)  min/avg/max = <16/<16/16

CES>ping badaddress.com

  ping: unknown host baddaddress.com

CES>ping 10.0.4.44

  PING 10.0.4.44: 56 data bytes

  ping: timeout

  no answer from 10.0.4.44
```

The examples show a successful ping command, an attempt to ping an unknown host address, and an attempt to ping an unreachable IP address.

reload

This command forces the switch to reboot immediately. Options can be specified to determine whether the switch turns off or reboots, which configuration to use after a reboot, and other settings.

The user is prompted to confirm that they want to continue with the reload. If they say yes and if the reload command is valid, the system reload commences in approximately 10 seconds.

The Safe and Normal boot modes are used for secure management of the switch. In Normal mode, the switch operates normally. In Safe mode, the HTTP, or FTP traffic is allowed. No other VPN traffic is allowed through the secure management tunnel or the switch.

Syntax

reload [power-off|restart] [boot-safe|boot-normal] [boot-drive {ide0|ide1}] [config-file {latest|factory|config-name}] [disable-logins] [disable-after-restart] [text]

Parameters

power-off	If present, the switch powers down after it has completed shutdown.
restart	If present, the switch restarts after it has completed shutdown.
boot-safe	If present, switch restarts in safe boot mode.
boot-normal	If present, switch restarts in normal boot mode.
boot-drive	Specify the drive from which the switch will reboot.
ide0|ide1	Disk drive from which bootable image will be loaded.
config-file	Specify which configuration should be used after a reboot.

latest The switch should be rebooted with the latest configuration file.

factory The switch should be rebooted with the reset configuration file. This file sets the switch to basic defaults. The contents of the LDAP database and other settings are still maintained.

config-name Name of previously saved configuration to use on reboot.

disable-logins No more logins should be permitted before the reboot occurs.

disable-after-restart Logins should not be permitted after the reboot. This is intended to support system maintenance tasks after a reboot.

text If present, this explains the reason for a reload command. This reason will be displayed on the Admin->Shutdown and Status->System Web management pages.

If the value for the text parameter contains spaces, it may be enclosed in double quotes so that it has a single parameter value.

Default

The default settings for this command are determined by any previous reload command. For the first reload command, the following defaults apply:

```
restart

boot-drive ide0

config-file latest
```

Command mode

Privileged Exec

Next command mode

Privileged Exec

Prerequisites

A named configuration file can only be used after it has been created.

Warnings

Any warnings cause the command to fail. The user must reenter the command after correcting the parameters in error.

Configuration file does not exist.

Related commands

```
reload at
```

```
reload cancel
```

```
reload in
```

```
reload no-sessions
```

```
show reload
```

Example

```
CES#reload restart boot-drive ide0 config-file factory
disable-after-restart Upgrade software

 Reload Scheduled Shutdown

 Reload Explanation: Upgrade software

 After Shutdown: Restart

 Disable New Logins: No

 Disable Logins after Restart: Yes

 Boot Mode: Normal

 Config File: Reset Config File

 Boot Drive: /ide0/

 Proceed with reload? [confirm]y
```

This reboots the switch from ide0, using the factory installed defaults and disabling logins after the reboot to allow for system maintenance. Reason is to "Upgrade software." The user must press [CR], or any subset of the string “yes”, to confirm that they want the reload to proceed.

Comments

After a successful reload command, the switch will reboot in approximately 10 seconds. For most Telnet client software, the reboot will cause the Telnet client to close the connection to the switch.

If there are any outstanding reboot commands, they will be canceled. There can only be one reboot scheduled at any time.

reload at

This command sets a time in the future at which the switch will reboot. Options can be specified to determine whether the switch turns off or reboots, which configuration to use after a reboot, and other settings.

The user is prompted to confirm that they want to continue with the reload. If they say yes and if the reload command is valid, the system reload will start at the specified time.

Syntax

```
reload at hh:mm [power-off|restart] [boot-safe|boot-normal]
[boot-drive {ide0|ide1}]

[config-file {latest|factory|config-name}] [disable-logins]
[disable-after-restart] [text]
```

Parameters

hh:mm	The time at which the shutdown will commence. Values are based on a 24 hour clock. If this time has already passed today, then the reload will occur at this time tomorrow.
power-off	If present, the switch will power down after it has completed shutdown.
restart	If present, the switch restarts after it has completed shutdown.
boot-safe	If present, switch restarts in safe boot mode.
boot-normal	If present, switch restarts in normal boot mode.
boot-drive	Specify the drive from which the switch will reboot.
ide0|ide1	Disk drive from which bootable image will be loaded.
config-file	Specify which configuration should be used after a reboot.
latest	The switch should be rebooted with the latest configuration file.

factory The switch should be rebooted with the reset configuration file. This file sets the switch to basic defaults, the contents of the LDAP database and other settings are still maintained.

config-name Name of previously saved configuration to use on reboot.

disable-logins No more logins should be permitted before the reboot occurs.

disable-after-restart Logins should not be permitted after the reboot. This is intended to support system maintenance tasks after a reboot.

text If present, this gives the reason for a reload command. This reason will be displayed on the Admin->Shutdown and Status->System Web management pages.

If the value for the text parameter contains spaces, it may be enclosed in double quotes so that it has a single parameter value.

Default

The default settings for this command are determined by any previous reload command. For the first reload command, the following defaults apply:

```
restart
```

```
boot-drive ide0
```

```
config-file latest
```

Command mode

Privileged Exec

Next command mode

Privileged Exec

Prerequisites

A named configuration file can only be used after it has been created.

Warnings

Any warnings cause the command to fail. The user must reenter the command after correcting the parameters in error.

Configuration file does not exist.

Related commands

```
reload
```

```
reload cancel
```

```
reload in
```

```
reload no-sessions
```

```
show reload
```

Example

```
CES#reload at 22:00 restart boot-drive ide0

disable-after-restart Backup LDAP database

 Reload Scheduled Shutdown at 22:00:00

 Reload Explanation: Backup LDAP database

 After Shutdown: Restart

 Disable New Logins: No

 Disable Logins after Restart: Yes

 Boot Mode: Normal

 Config File: latest

 Boot Drive: /ide0/

Proceed with reload? [confirm]y
```

This reboots the switch from ide0, using the latest configuration and disabling logins after the reboot to allow for system maintenance. Reason is to "Backup LDAP database."

Comments

After a successful reload at command, the switch will reboot at the time specified based on internal clock settings. For most Telnet client software, the reboot will cause the Telnet client to close the connection to the switch.

If there are any outstanding reboot commands, they will be canceled. There can be only be one reboot scheduled at any time.

reload cancel

This command cancels any pending reload command. There can only be one pending reload at any given time.

When a reload has been canceled the details for the pending reload are displayed.

Syntax

```
reload cancel
```

Parameters

None

Default

None

Command mode

Privileged Exec

Response

The command will output a message giving details about the type of reload command that was canceled.

Next command mode

Privileged ExecPrerequisites

A reload must already have been scheduled.

Warnings

No currently scheduled reload operation.

Related commands

reload

reload at

reload in

reload no-sessions

show reload

Example

```
CES#reload at 22:00 restart boot-drive ide0

disable-after-restart Backup LDAP database

CES#reload cancel

Reload Scheduled Shutdown at 22:00:00 has been canceled

Reload Explanation: Backup LDAP database

After Shutdown: Restart

Disable New Logins: No

Disable Logins after Restart: Yes

Boot Mode: Normal

Config File: latest

Boot Drive: /ide0/
```

This example schedules a reload command that would reboot the switch from ide0, using the latest configuration and disabling logins after the reboot to allow for system maintenance. Reason is to "Backup LDAP database." The reload is then canceled and the resulting output shows the original reload command.

reload in

This command sets a timer that causes the switch to reboot after a certain time has passed. Options can be specified to determine whether the switch turns off or reboots, which configuration to use after a reboot, and other settings.

The user is prompted to confirm that they want to continue with the reload. If they say yes and if the reload command is valid, the system reload will start at the specified time.

Syntax

```
reload in [hh:]mm [power-off|restart] [boot-safe|boot-normal]
[boot-drive {ide0|ide1}]

[config-file {latest|factory|config-name}] [disable-logins]
[disable-after-restart] [text]
```

Parameters

[*hh*|mm]	The hours and minutes that must pass before the shutdown will start. The allowed range is 00:01 to 24:00.
power-off	If present, the switch will power down after it has completed shutdown.
restart	If present, the switch restarts after it has completed shutdown.
boot-safe	If present, switch restarts in safe boot mode.
boot-normal	If present, switch restarts in normal boot mode.
boot-drive	Specify the drive from which the switch will reboot.
ide0|ide1	Disk drive from which that bootable image will be loaded.
config-file	Specify which configuration should be used after a reboot.
latest	The switch should be rebooted with the latest configuration file.

factory The switch should be rebooted with the reset configuration file. This file sets the switch to basic defaults; the contents of the LDAP database and other settings are still maintained.

config-name Name of the previously saved configuration to use on reboot.

disable-logins No more logins should be permitted before the reboot occurs.

disable-after-restart Logins should not be permitted after the reboot. This is intended to support system maintenance tasks after a reboot.

text If present, this explains the reason for a reload command. This reason will be displayed on the Admin->Shutdown and Status->System Web management pages.

If the value for the text parameter contains spaces, it may be enclosed in double quotes so that it has a single parameter value.

Default

The default settings for this command are determined by any previous reload command. For the first reload command, the following defaults apply:

```
restart

boot-drive ide0

config-file latest
```

Command mode

Privileged Exec

Next command mode

Privileged Exec

Prerequisites

A named configuration file can only be used after it has been created.

Warnings

Any warnings cause the command to fail. The user must reenter the command after correcting the parameters in error.

Configuration file does not exist.

Related commands

```
reload

reload cancel

reload at

reload no-sessions

show reload
```

Example

```
CES#reload in 8:00 restart boot-drive ide1 power-off
   disable-logins
 Reload Scheduled Shutdown in 480 minutes
 Reload Explanation: Scheduled Shutdown in 480 minutes
 After Shutdown: Powerdown
 Disable New Logins: Yes
 Disable Logins after Restart: No
 Boot Mode: Normal
 Config File: latest
 Boot Drive: /ide1/
 Proceed with reload? [confirm]y
```

This example command powers down the switch in eight hours time. When the switch is powered up again it will reboot from ide1. Further logins are disabled until the switch has rebooted.

Comments

After a successful reload in command, the switch will reboot after the time specified has elapsed. For most Telnet client software, the reboot will cause the Telnet client to close the connection to the switch.

If there are any outstanding reboot commands, they will be canceled. There can be only be one reboot scheduled at any time.

reload no-sessions

This command causes the switch to reboot after there are no further logins. The reboot will start after all tunnels into the box, and all management sessions (Telnet, Web, etc.) have been closed. Options can be specified to determine whether the switch turns off or reboots, which configuration to use after a reboot and other settings.

The user is prompted to confirm that they want to continue with the reload. If they say yes and if the reload command is valid, the system reload will start a short time after all sessions (tunnels and administrative) have disconnected.

Syntax

```
reload no-sessions [power-off|restart] [boot-safe|boot-safe]
[boot-drive {ide0|ide1}]
[config-file {latest|factory|config-name}] [disable-logins]
[disable-after-restart] [text]
```

Parameters

no-sessions	Indicates the reboot will start once there are no more sessions connected to the switch.
power-off	If present, the switch will power down after it has completed shutdown.
restart	If present, the switch restarts after it has completed shutdown.
boot-safe	If present, switch restarts in safe boot mode.
boot-normal	If present, switch restarts in normal boot mode.
boot-drive	Specify the drive from which the switch will reboot.
ide0|ide1	Disk drive from which the bootable image will be loaded.
config-file	Specify which configuration should be used after a reboot.
latest	The switch should be rebooted with the latest configuration file.

factory The switch should be rebooted with the reset configuration file. This file sets the switch to basic defaults; the contents of the LDAP database and other settings are still maintained.

config-name Name of previously saved configuration to use on reboot.

disable-logins No more logins should be permitted before the reboot occurs.

disable-after-restart Logins should not be permitted after the reboot. This is intended to support system maintenance tasks after a reboot.

text If present, this explains the reason for a reload command. This reason will be displayed on the Admin->Shutdown and Status->System Web management pages.

If the value for the text parameter contains spaces, it may be enclosed in double quotes so that it has a single parameter value.

Default

The default settings for this command are determined by any previous reload command. For the first reload command, the following defaults apply:

restart

boot-drive ide0

config-file latest

Command mode

Privileged Exec

Next command mode

Privileged Exec

Prerequisites

A named configuration file can only be used after it has been created.

Warnings

Any warnings cause the command to fail. The user must reenter the command after correcting the parameters in error.

Configuration file does not exist.

Related commands

```
reload
```

```
reload cancel
```

```
reload at
```

```
reload in
```

```
show reload
```

Example

```
CES#reload no-sessions restart disable-logins

 Reload Shutdown after all users log off

 Reload Explanation: Shutdown after all users log off

 After Shutdown: Restart

 Disable New Logins: Yes

 Disable Logins after Restart: No

 Boot Mode: Normal

 Config File: latest

 Boot Drive: /ide0/

 Proceed with reload? [confirm]y
```

This example reboots the switch from ide0, using the latest configuration when there are no sessions connected to the switch. New session connections have been disabled.

Comments

After a successful reload no-sessions the command, the switch reboots once all sessions on the switch have terminated. This includes Web and CLI management sessions.

If there are any outstanding reboot commands, they will be canceled. There can be only be one reboot scheduled at any time.

server backup

This command copies the current contents of the internal switch LDAP database into an LDIF file. The LDIF file can be saved off the switch for backup purposes. The internal LDAP server must be stopped before a backup command can be performed.

Syntax

```
server backup filename
```

Parameters

filename	The filename to which the LDAP database will be backed up. The filename can have a maximum of 8 characters. The file is stored in the directory /ide0/system/slapd/ldif on the switch.

Default

None

Command mode

LDAP server configuration

Response

The backup can take a considerable amount of time to complete, depending on the size of the LDAP database. The user sees a message once the backup task has been completed.

Next command mode

LDAP server configuration

Prerequisites

The internal LDAP server must be stopped before a backup command can be performed.

Warnings

LDIF File xxxxxxxx already exists.

The LDAP server must be stopped before performing a backup.

Cannot backup LDAP server, backup in progress.

Cannot backup LDAP server, restore in progress.

Related commands

```
ldap-server internal
```

```
server restore
```

```
server start
```

```
server stop
```

Example

```
CES(config)#ldap-server internal

Router(config-ldap)#server stop

Router(config-ldap)#server backup jan102000

Server backup started to file /ide0/system/slapd/ldif/jan102000

  Server backup completed

Router(config-ldap)#server start

Router(config-ldap)#exit
```

This example shows the internal LDAP server being stopped and the contents being backed up to a file called jan102000. After the backup has completed, the LDAP server is started again.

server restore

This command replaces the current contents of the internal LDAP database with an LDIF file, possibly created by a server backup operation, or some script. The internal LDAP server must be stopped before a restore command can be performed. The previous contents of the LDAP database is lost.

Syntax

server restore filename

Parameters

filename	The name of the LDIF file that should be restored into the LDAP database. The filename can have a maximum of 8 characters. The file is restored from the directory /ide0/system/slapd/ldif on the switch.

Default

None

Command mode

LDAP server configuration

Response

The restore can take a considerable amount of time to complete, depending on the size of the LDIF file. The user sees a message once the restore task has been completed.

Next command mode

LDAP server configuration

Prerequisites

The internal LDAP server must be stopped before a restore command can be performed.

Warnings

LDIF file “*filename*” not found.

The LDAP server must be stopped before performing a restore.

Cannot restore LDAP server, backup in progress.

Cannot restore LDAP server, restore in progress.

Related commands

ldap-server internal

server backup

server start

server stop

Example

```
CES(config)#ldap-server internal

Router(config-ldap)#server stop

Router(config-ldap)#server restore jan031999

  Server restore started from file /ide0/system/slapd/ldif/
jan031999

  Server restore completed

Router(config-ldap)#server start

Router(config-ldap)#exit
```

This example shows the internal LDAP server being stopped and the contents being restored from the LDIF file called jan031999. After the restore has completed, the LDAP server is started again.

server start

This command starts the internal switch LDAP server after it has been stopped.

Syntax

```
server start
```

Parameters

None

Default

None

Command mode

LDAP server configuration

Response

The switch outputs a confirmation message once the LDAP server has been restarted.

Next command mode

LDAP server configuration

Prerequisites

The internal LDAP server must have been previously stopped.

Warnings

The LDAP server is already started.

Cannot start LDAP server, backup in progress.

Cannot start LDAP server, restore in progress.

Related commands

```
ldap-server internal

server backup

server restore

server stop
```

Example

```
CES(config)#ldap-server internal

Router(config-ldap)#server start

  The LDAP server has started

Router(config-ldap)#exit
```

This example shows the internal LDAP server being started.

Comments

For a large LDAP database, the start command can take some time to complete.

server stop

This command stops the internal switch LDAP server.

Syntax

server stop

Parameters

None

Default

None

Command mode

LDAP server configuration

Response

The switch outputs a confirmation message when the LDAP server has stopped.

Next command mode

LDAP server configuration

Prerequisites

The internal LDAP server must be running.

Warnings

The LDAP server is already stopped.

Related commands

```
ldap-server internal

server backup

server restore

server start
```

Example

```
CES(config)#ldap-server internal

Router(config-ldap)#server stop

  The LDAP server has stopped

Router(config-ldap)#exit
```

This example shows the internal LDAP server being stopped.

Comments

Once the internal LDAP server has been stopped, the switch will not allow further login attempts to the switch because it cannot validate the user credentials.

show arp

This command displays the entries in the ARP table.

Syntax

```
show arp
```

Parameters

None

Default

None

Command mode

Privileged Exec

Next command mode

Privileged Exec

Related commands

clear arp-cache

Example

```
CES# show arp

LINK LEVEL ARP TABLE

destination gateway flags Refcn Use  Interface
```

show exception backup

This command shows the current backup FTP servers that are defined for the switch.

Syntax

```
show exception backup
```

Parameters

None

Default

None

Command mode

Global configuration

Response

This command outputs details of the current backup FTP servers that have been defined for the switch, if any.

Next command mode

Global configuration

Warnings

No backup FTP servers defined

Related commands

exception backup

Example

```
CES(config)#show exception backup

  Backup FTP Server 1.

  Server Address:  12.230.111.10

  Backup Filepath: /dev1/CES/Backup

  Backup Interval: 12 hours

  Server Username: ContivityAdmin

  Backup FTP Server 3.

  Server Address:  backupCES.internal.com

  Backup Interval: 168 hours

  Server Username: ContivityMainAdmin

CES(config)#no exception backup 3

CES(config)#show exception backup

  Backup FTP Server 1.

  Server Address:  12.230.111.10

  Backup Filepath: /dev1/CES/Backup

  Backup Interval: 12 hours

  Server Username: ContivityAdmin
```

This example shows the output when two backup FTP servers have been defined. There is no backup file path defined for the second server. The second server (number 3) is removed from the list of available backup FTP servers and the second show exception command shows that details for this server have been removed from the switch configuration.

show file systems

This command shows the available file systems on the switch, including device size, and details of available space remaining.

Syntax

```
show file systems
```

Parameters

None

Default

None

Command mode

User Exec

Next command mode

User Exec

Example

```
CES>show file systems

 File Systems:

      Size(b)       Free(b)   Type    Flags  Prefixes

      1249280     262752      disk       rw    ide0:

      1269760    1241752      disk       rw    ide1:
```

This example shows the output for a switch that has two hard disk drives.

show flash: contents

This command shows the current settings that are in flash for the switch.

This is equivalent to the Flash Contents button display on the Status->Statistics Web management page.

Syntax

```
show flash: contents
```

Parameters

None

Default

None

Command mode

User Exec

Next command mode

User Exec

Related commands

show version

xample

```
CES>show file: contents

Flash Header - copyright: Nortel Networks, Copyright 1999, 2000
               tag:       NOC
               version:   1
               length:    711
               count:     15
Flash Data -
model number: Contivity1510D
MAC address: 00-E0-7B-00-0D-30
serial number: 12192
feature keys:
     Maximum Ethernet ports: 2
     Maximum T-1 ports: 1
     Maximum T-3 ports: 0
     Allow PPTP tunnels: True
     Allow L2F tunnels: True
     Allow L2TP tunnels: True
     Allow IPsec tunnels: True
     Allow QoS internal: True
     Allow QoS admission: True
     Allow RSVP: True
     Allow RADIUS authentication: True
     Allow LDAP authentication: True
     Allow NT Domain authentication: True
     Allow RSA encryption: True
     Allow SSL: True
     Allow X.509 certificates: True
     Allow RADIUS accounting: True
     CPU clock rate 400 MHz
     CPU cache size 0 KB
     Number of CPUs supported: 1
     Allow IPX: True
     Allow NAT: True
     Allow FW-1: True
     Require FW-1: False
     Firewall: Disabled
     Maximum Hifn 7751 Accelerators: 0
     FIPS Mode: False
     Allow Safe Mode Boot: False
feature mask
Flash Revision: 1
key length: 128
Boot Device: /ide0/
maximum concurrent sessions: 100
```

```
system IP address: 10.211.4.42
system IP netmask: 255.255.0.0
system default gateway: 10.0.0.10
checksum: 56091
```

This example shows the flash settings for a Contivity VPN Switch1510D. The output differs depending on the type of switch being using.

show health

This command displays information about the overall health of the switch. It allows the administrator to check on areas that may cause problems in the future, as well as see where problems have been detected already.

Syntax

show health [alerts|warnings|disabled|all]

Parameters

alerts	Causes conditions to be shown that require immediate administrator attention.
warnings	Causes conditions to be shown that need to be fixed to avoid an alert condition. It also shows alert conditions.
disabled	Causes conditions to be shown that need to be fixed to avoid an alert condition. It also shows warning and alert conditions.
all	Causes all conditions to be shown, including those that are operating correctly.

Default

If a warning level is not given, then only alert and warning problems are shown, equivalent to:

show health warnings

Command mode

Privileged Exec

Response

See the example for output from this command.

Next command mode

Privileged Exec

Related commands

audible alarm

Example

CES#show health warnings

```
Alert:   LAN on slot 2 Interface 1.   Device fei1 down
Alert:   Auto backup servers.   Can't backup to 12.33.44.123
Alert:   Voltage 2.5 VA.   Voltage out of range
Alert:   Chassis Fan.   Fan not functioning
Warning: Hard Disk 1.   Device /ide1/ not available
Warning: SNMP Servers.   Server not configured
```

This example shows the type of output that is displayed when alerts and warning messages are requested by the show health command.

show ip access-list

This command displays the contents of all current IP access lists. The CLI accepts names up to 50 characters long. The maximum length of the CLI name is 50 characters, not 64 as it is in the browser-based GUI.

Syntax

```
show ip access-list
```

Parameters

access-list	The access-list.
name	Optional parameter.

Default

None

Command mode

User Exec

Response

See the example for output from this command.

Next command mode

User Exec

Example

```
CES>show ip access-list name
Standard IP access list TEST
    permit 2.2.0.0, wildcard bits 255.255.0.0, exact
Standard IP access list TEST1
    deny   3.3.0.0, wildcard bits 255.255.0.0, exact
```

This example shows the lists of all access lists created and the contents of it.

show ip ospf

This command displays general information about OSPF routing and the state of OSPF routing processes.

Syntax

show ip ospf

Parameters

None

Default

None

Command mode

User Exec

Response

See the example for output from this command.

Next command mode

User Exec

Related commands

show ip ospf database

show ip ospf interface

show ip ospf neighbor

Example

CES>show ip ospf

```
Router id is 10.254.1.36
Router State is Up
Supports TOS 0 route
SPF schedule delay 3 secs, Hold time between two SPFs 3 secs
Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
Number of external LSA = 0
Link State Update Interval is 00H:30M  (Same for all areas)
Link State Age    Interval is 01H:00M  (Same for all areas)
Number of Areas in this router is 3. 3 Normal 0 Stub 0 nssa

Area 0.0.0.0
    Number of interfaces in this area = 2
    SPF algorithm has Executed 37 times

Area 1.1.1.1
    Number of interfaces in this area = 0
    SPF algorithm has Executed 37 times

Area 2.2.2.2
    Number of interfaces in this area = 0
    SPF algorithm has Executed 37 times
```

This example shows the state of OSPF routing process.

show ip ospf database

This command displays information related to the OSPF database for the switch. It also delivers information about OSPF link state advertisements.

Syntax

show ip ospf database

Parameters

None

Default

None

Command mode

User Exec

Response

See the example for output from this command.

Next command mode

User Exec

Related commands

show ip ospf

show ip ospf interface

show ip ospf neighbor

Example

```
CES>show ip ospf database
```

```
CES>show ip ospf database


Displaying Router Link States (Area 0.0.0.0)

Link State ID   Adv Router      Age   Seq Nbr    CheckSum Links
--------------- --------------- ----- ---------- -------- -----
15.62.250.250   15.62.250.250   1041  0x80000011 0xecf5   3
10.254.1.36     10.254.1.36     1001  0x8000001d 0xf39a   6

Displaying Summary Link States (Area 0.0.0.0)

Link State ID   Adv Router      Age   Seq Nbr    CheckSum
--------------- --------------- ----- ---------- --------
15.62.0.0       15.62.250.250   798   0x80000006 0xdede
```

This example lists the information related to the OSPF database.

show ip ospf interface

This command displays information about interfaces that are configured for OSPF routing.

Syntax

```
show ip ospf interface
```

Parameters

None

Default

None

Command mode

User Exec

Response

See the example for output from this command.

Next command mode

User Exec

Related commands

```
show ip ospf

show ip ospf database

show ip ospf neighbor
```

Example

```
CES>show ip ospf interface

IP Address-CId Area ID   Type     State    Cost   Priority   Router

15.60.150.150-17  0.0.0.0   BCAST    DR          1      1  10.254.1.36

15.63.150.150-74  0.0.0.0   PTPT     Other      100      1   0.0.0.0
```

This example displays OSPF related interface information.

show ip ospf neighbor

This command displays information about OSPF neighbors on a per interface basis.

Syntax

show ip ospf neighbor

Parameters

None

Default

None

Command mode

User Exec

Response

See the example for output from this command.

Next command mode

User Exec

Related commands

```
show ip ospf
```

```
show ip ospf database
```

```
show ip ospf interface
```

Example

```
CES>show ip ospf neighbor
```

```
OSPF Dynamic Neighbors

RouterID       Pri  State          Dead Time      Address         Interface
-------------- ---  -------------  -------------  --------------  -----------
10.0.62.182    1    FULL/DR        00:00:20       10.0.62.182     10.0.4.41
10.0.16.36     1    2WAY           00:00:34       10.0.16.36      10.0.4.41
10.0.7.184     1    FULL/BDR       00:00:37       10.0.60.182     10.0.4.41
10.0.7.182     1    2WAY           00:00:40       10.0.61.182     10.0.4.41
```

This example shows the IP address, router-id, and state of the neighbors.

show ip rip

This command displays general information about RIP routing and the state of RIP routing process and status.

Syntax

```
show ip rip
```

Parameters

None

Default

None

Command mode

User Exec

Response

See the example for output from this command.

Next command mode

User Exec

Related commands

Example

```
CES>show ip rip
Global Rip Status: Enabled
Trusted Neighbor: Disabled, Rip Domain: 0
Triggered Update: Off, RouteChange: 0x0, Query: 0x0
Local [Net: 0x00000000, Mask: 0x00000000, ClassMask: 0x00000000]
LocalCircuit: 1
Node Wide Stats:
rn_rtid: 0x00000000
rn_tics: 0, rn_num_circ: 0, rn_routes: 0
rn_udpInDatagrams: 0, rn_udpOutDatagrams: 1
rn_udpInErrors: 0, rn_udpNoPorts: 0
```

This example shows the state of RIP and the associated status information.

show ip rip database

This command provides information related to the RIP database for the switch. It also delivers information about routes owned and imported by RIP.

Syntax

show ip rip database

Parameters

None

Default

None

Command mode

User Exec

Response

See the example for output from this command.

Next command mode

User Exec

Related commands

show ip rip

show ip rip interface

show ip rip database

Example

```
CES>show ip rip database
```

Table 6

Circuit	Address	Mask	Owner	Cost	Metric	GW
1	192.32.0.0	255.255.0.0	RIP	5	5	10.0.234.230
1	192.168.0.0	255.255.0.0	RIP	5	5	10.0.234.230
1	9.1.10.18	255.255.255.255	RIP	5	5	10.0.234.230

This example shows routes owned by an RIP database.

show ip rip interface

This command displays information about interfaces that are configured for RIP routing

Syntax

show ip rip interface

Parameters

None

Default

None

Command mode

User Exec

Response

See the example for output from this command.

Next command mode

User Exec

Related commands

```
show ip rip
```

```
show ip rip database
```

```
show ip rip interface
```

Example

```
CES>show ip rip interface

Ip: 10.0.15.146             Subnet: 255.255.0.0         RipEnabled: Yes
IntfState: UP               Auth: None                  Type: ETH
Cid: 1                      RxMode: V2                  TxMode: V2
PoisonRev: Enabled          ImpDRoute: Disabled         ExpTSMetric: 1
ExpSMetric: 1               ExpDMetric: 0               ExpOspfMetric: 0
```

This example shows the state of the configured interface.

show ip route

This command displays the current contents of the RTM routing table.

```
Each line of the output has the following format:
```

```
P   TT a.a.a.a/n [ad/rm] via nh.nh.nh.nh, d hh:mm:ss, CircId nFormat CodeUsage
```

P Authoring protocol

TT Type

a.a.a.a Address

n Number of bits in the network mask

ad Administrative distance (route preference)

rm Route metric

nh.nh.nh.nh Next hop address

The meaning of the authoring protocol codes shown for each line of the output is shown below.

Table 7

Code	Meaning
BBGP	Derived
D	Direct
OOSPF	Derived
RRIP	Derived
S	Static
IAOSPF	inter area route
E1OSPF	external type 1 route
E2OSPF	external type 2 route

Syntax

```
show ip route [address [mask]]
```

Parameters

If no parameters are specified all of the current contents are displayed.

address	Display a specific host a.a.a.a
mask	Display a specific route to address a.a.a.a net mask m.m.m.m

Default

None

Command mode

User Exec

Response

See the example for output from this command.

Next command mode

User Exec

Related commands

clear ip route

Example

CES>show ip route

```
 S    0.0.0.0/0 [6/10] via 10.0.0.10, 0 00:58:36, CircId 1
 D    10.0.0.0/16 [0/0] via 10.0.4.41, 0 00:58:36, CircId 1
 D    10.0.3.41/32 [0/0] via 127.0.0.1, 0 00:58:36, CircId 1
 D    10.0.4.41/32 [0/0] via 127.0.0.1, 0 00:58:36, CircId 1
 D    11.0.0.0/16 [0/0] via 11.0.4.41, 0 00:58:36, CircId 9
 D    11.0.4.41/32 [0/0] via 127.0.0.1, 0 00:58:36, CircId 9
```

CES>show ip route 10.0.3.41

Routing Entry for 10.0.3.41 (mask 255.255.255.255)

Known via 'Direct', distance 0, metric 0

Last update from 127.0.0.1 on CircId 1, 0 01:09:52

CES>show ip route 10.0.0.0 255.255.0.0

Routing Entry for 10.0.0.0 (mask 255.255.0.0)

Known via 'Direct', distance 0, metric 0

Last update from 10.0.4.41 on CircId 1, 0 01:15:28

show ip route-policies

This command displays the contents of route policies in the routing protocol.

Syntax

show ip route-policies

Parameters

None

Default

None

Command mode

User Exec

Response

See the example for output from this command.

Next command mode

User Exec

Related commands

show ip route

Example

```
CES>show ip route-policies

ospf, 0, interface 10.0.3.41, distribute list in TEST
```

This example shows the accept route policy in OSPF on the interface where TEST stands for the name of the access list.

show ip traffic

This command displays statistics about IP traffic including packets sent and received, and various errors.

Syntax

show ip traffic

Parameters

None

Default

None

Command mode

User Exec

Response

See the example for output from this command.

Next command mode

User Exec

Example

```
CES>show ip traffic
IP statistics:
               total 282511
              badsum    0
            tooshort    0
            toosmall    0
             badhlen    0
              badlen    0
         infragments    0
         fragdropped    0
         fragtimeout    0
             forward    0
         cantforward    3
        redirectsent    0
     unknownprotocol    6
           nobuffers   18
         reassembled    0
        outfragments    0
             noroute  125
          badoptions    0
          badversion    0
       zero src addr    3
        src=dst addr    0
      src addr error    0
     dest addr error    0
    mgmt filterdrops 6127
    intf filterdrops    0
   route filterdrops    0
            qosdrops    0

ICMP:
        27 calls to icmp_error
        0 error not generated because old message was icmp
        Output histogram:
                echo reply: 3
                destination unreachable: 27
        0 message with bad code fields
        0 message < minimum length
        0 bad checksum
        0 message with bad length
        Input histogram:
                echo reply: 10
                echo: 3
        3 message responses generated
UDP:
        49825 total packets
        49807 input packets
        18 output packets
        0 incomplete header
        0 bad data length field
        0 bad checksum
        22277 broadcasts received with no ports
        0 full socket
        59 pcb cache lookups failed
        27 pcb hash lookups failed
TCP:
        16085 packets sent
                15226 data packets (2336894 bytes)
                0 data packet (0 byte) retransmitted
                778 ack-only packets (504 delayed)
                0 URG only packet
                0 window probe packet
                3 window update packets
                78 control packets
        15898 packets received
                11943 acks (for 2334342 bytes)
                124 duplicate acks
                0 ack for unsent data
    14578 packets (1713926 bytes) received in sequence
                0 completely duplicate packet (0 byte)
                0 packet with some dup. data (0 byte duped)
                117 out-of-order packets (0 byte)
                0 packet (0 byte) of data after window
                0 window probe
                8 window update packets
                0 packet received after close
                0 discarded for bad checksum
                0 discarded for bad header offset field
                0 discarded because packet too short
        4 connection requests
        138 connection accepts
        142 connections established (including accepts)
        140 connections closed (including 14 drops)
        0 embryonic connection dropped
        11825 segments updated rtt (of 11835 attempts)
        0 retransmit timeout
                0 connection dropped by rexmit timeout
        0 persist timeout
        0 keepalive timeout
                0 keepalive probe sent
                0 connection dropped by keepalive
        0 pcb cache lookup failed
```

show ip vrrp

This command displays information about VRRP status.

Syntax

show ip vrrp [interface]

Parameters

interface	Displays information about VRRP status of the specified interface.

Default

None

Command mode

User Exec

Response

See the example for output from this command.

Next command mode

User Exec

Example

```
CES>show ip vrrp

  Slot Intf VRID Prio State  Address

  0    1    1    255  Master 10.0.20.186

  0    1    2    100  Backup 10.0.21.186

CES>show ip vrrp interface
  Slot 0 Interface 1
    Virtual router 1
      Current state is Master, priority 255, may not preempt
      Advertisement interval 1
      IP Address 10.0.20.186
      Became master 1 times, sent 0 Zero prio pkts, recv'd 0
      Sent 436 advertisements, recv'd 0
      No errors
    Virtual router 2
      Current state is Backup, priority 100, may not preempt
      Advertisement interval 1
      IP Address 10.0.21.186
      Became master 1 times, sent 0 Zero prio pkts, recv'd 0
      Sent 7 advertisements, recv'd 426
      No errors
```

This example shows the command displaying the interfaces configured for VRRP, and then the more detailed output available with the optional interface parameter.

show ldap-server

This command displays the configuration settings and state for the internal and external LDAP servers.

Syntax

show ldap-server [*all|external|internal*]

Parameters

all	Displays configuration and state for the internal and the external LDAP servers.
external	Displays configuration and state for the external LDAP servers.
internal	Displays configuration and state for the internal LDAP server.

Default

If no parameters are specified, then the configuration and state for all LDAP servers are displayed. This is equivalent to:

show ldap-server all

Command mode

Global configuration

Response

See the example for output from this command.

Next command mode

Global configuration

Warnings

No external LDAP servers configured.

Related commands

ldap-server

ldap-server source

Example

```
CES(config)#show ldap-server
  Current LDAP server is Internal
  LDAP server is started
  Internal LDAP Server settings
Suffix-remove:            Yes
  External LDAP Server settings
Suffix-remove:            No
  Master Host Address:      11.122.12.200
  Master Host Port:         389
  Master Host Bind DN:      cn=Marketing Base
  Master Host Base DN:      ou=Marketing, o=Nortel, c=US
  Master Host SSL Encrypt:  None
  Slave1 Host Address:      16.211.17.100
  Slave1 Host SSL Port:     636
  Slave1 Host Bind DN:      cn=Marketing
  Slave1 Host Base DN:      ou=Marketing, o=Nortel, c=US
  Slave1 Host SSL Encrypt:  DES-56, RC4-40
  Warning Slave1 cannot be reached
```

This example shows the output where the internal LDAP server is being used. There is configuration information for an external master and slave1 LDAP server. The master server is being accessed using a non-encrypted connection. The slave1 server is being accessed via SSL with DES-56 and RC4-40 encryption. The slave1 server is not accessible.

show logging config

This command displays the contents of the configuration log. This log tracks all changes to the configuration of the switch.

Syntax

```
show logging config [date {day month [year]|month day [year]}]
[normal|urgent|detailed|all]
```

Parameters

date
: The date for which the configuration log is to be displayed.

day
: The day of the month for which the configuration log is to be displayed.

month
: The month for which the configuration log is to be displayed.

year
: The year for which the configuration log is to be displayed. A four-digit value.

normal
: Display normal events, including user and system interactions, that indicate switch activity.

urgent
: Display events that an administrator should be aware of immediately.In the output, these events are marked with an asterisk. Could indicate potential security or access problems. Also display normal events.

detailed
: Display events for use of Nortel Networks support personnel. Also display normal and urgent events.

all
: Display events for use of Nortel support personnel used for troubleshooting the switch. Includes every event that the switch generates. Also display detailed, normal, and urgent events.

Default

The date value defaults to today. If the year portion of the date is omitted it defaults to the current year. The display level defaults to normal.

Command mode

Privileged Exec

Response

See the example for output from this command.

Next command mode

Privileged Exec

Related commands

show logging events

show logging security

show logging syslog

Example

```
CES#show logging config level urgent
  Config Log contents for Friday, July 30, 2000
  *09:54:15 tRootTask 0 : Error in cfg file setting 'IpxIntfOmCls.IpxPrivateLANS[256].$
  *09:54:15 tRootTask 0 : Error in cfg file setting 'IpxIntfOmCls.IPXPublicAddress=N/A$
CES#
CES#show logging config
  Config Log contents for Friday, July 30, 2000
   09:52:31 tHttpdTask 0 : Shutdown.Mode changed from 'NONE' to 'NOW' by user 'admin' $
   09:52:31 tHttpdTask 0 : Reboot[Scheduled Shutdown] created by user 'admin' @ '132.2$
  *09:54:15 tRootTask 0 : Error in cfg file setting 'IpxIntfOmCls.IpxPrivateLANS[256].$
  *09:54:15 tRootTask 0 : Error in cfg file setting 'IpxIntfOmCls.IPXPublicAddress=N/A$
   09:54:31 tSerialConfig 0 : Flash.AdminUid changed from 'admin' to 'sysadmin' by use$
   09:54:31 tSerialConfig 0 : Flash.AdminPassword changed by user '' @ ''
   09:54:31 tSerialConfig 0 : DirBackup.PrimaryHost changed from '11.33.55.66' to '11.$
   09:54:31 tSerialConfig 0 : DirBackup.PrimaryUsername changed from 'bernard' to 'sys$
   09:54:50 tObjMgr 0 : ObjMgrCls::WriteConfigFile() new configuration file config/CFG$
```

This example shows the output from the configuration log with the urgent messages displayed, followed by example where the normal messages are displayed.

Comments

The amount of output from this command can be substantial. It is automatically paginated on display so that the user can see one page of output at a time. The user can go through the output one screen at a time, or quit and abandon the remainder of the output.

show logging events

This command displays the contents of the event log. The event log is a detailed recording of all events that take place on the system. The event log is maintained in switch memory with significant events being saved in the system log and written to disk. The event log retains approximately 2000 entries and discards old entries when it is refreshed.

This command also allows the administrator to log details about packets that have been dropped by the switch, including packets that are dropped due to filtering rules. These options should only be used for troubleshooting as using them can significantly impact performance of the switch. Once you set these options, they remain on until cleared by a subsequent show logging events command.

Syntax

```
show logging events [ip-drops {all [filtered]|filtered|none}]

    [ipx-drops {all|none}]
```

Parameters

ip-drops	Specify the type of dropped IP packets to track in the events log.
all	Specify that all dropped IP packets are to be tracked. For each dropped packet the source and destination address are kept in the event log for display.
filtered	Specify that IP packets dropped due to filter rules are to be tracked. For each packet dropped due to filtering the packet contents are kept in the event log for display.
none	Specify that dropped IP packets are not to be tracked.
ipx-drops	Specify the type of dropped IPX packets to track in the events log.

Default

Dropped IP and IPX packets are not tracked.

Command mode

Privileged Exec

Response

See the example for output from this command.

Next command mode

Privileged Exec

Warnings

If the user chooses to track dropped IP or IPX packets, a confirmation is requested due to the performance impact.

Related commands

```
clear logging events
```

```
show logging config
```

```
show logging security
```

```
show logging syslog
```

Example

```
CES#show logging events
  09/02/1999 11:57:12 0 PaceJob{0} [00] Calling 0x00ca012c, passing 011b7e88, 00000000$
  09/02/1999 12:01:52 0 FTP Backup [13] Redundant Disk is not available
  09/02/1999 12:01:52 0 FTP Backup [13] Update completed
  09/02/1999 12:02:00 0 DCLog [00] DCManager flushing data to stat file '19990902.DC'
  09/02/1999 12:02:20 0 PaceJob{0} [00] Calling 0x00ca012c, passing 011b7b24, 00000000$
  09/02/1999 12:02:20 0 PaceJob{0} [00] Calling 0x00ca012c, passing 011b7e88, 00000000$
  09/02/1999 12:03:59 0 Security [13] Management: Forced Admin User Off Due to Timeout$
  09/02/1999 12:04:00 0 Security [12] Session: LOCAL[admin]:2876 logged out
  09/02/1999 12:04:00 0 Security [13] Management: Forcing admin to re-supply userid
  09/02/1999 12:04:03 0 Security [11] Session: LOCAL[admin] attempting login
  09/02/1999 12:04:03 0 Security [01] Session: LOCAL[admin] has no active sessions
  09/02/1999 12:04:03 0 Security [01] Session: LOCAL[admin] admin has no active accoun$
  09/02/1999 12:04:03 0 Security [12] Session: LOCAL[admin]:2877 master admin authenti$
  09/02/1999 12:04:03 0 Security [11] Session: LOCAL[admin]:2877 server right: MANAGE
  09/02/1999 12:04:03 0 Security [11] Session: LOCAL[admin]:2877 user/group right: MAN$
  09/02/1999 12:04:04 0 Security [12] Session: LOCAL[admin]:2877 Management: logged in$
  09/02/1999 12:07:36 0 PaceJob{0} [00] Calling 0x00ca012c, passing 011b7b24, 00000000$
  09/02/1999 12:07:36 0 PaceJob{0} [00] Calling 0x00ca012c, passing 011b7e88, 00000000$
  09/02/1999 12:12:44 0 PaceJob{0} [00] Calling 0x00ca012c, passing 011b7b24, 00000000$
  09/02/1999 12:12:44 0 PaceJob{0} [00] Calling 0x00ca012c, passing 011b7e88, 00000000$
  09/02/1999 12:17:00 0 DCLog [00] DCManager flushing data to stat file '19990902.DC'
CES#
CES#show logging events ip-drops all
  09/02/1999 11:57:12 0 PaceJob{0} [00] Calling 0x00ca012c, passing 011b7e88, 00000000$
  09/02/1999 12:01:52 0 FTP Backup [13] Redundant Disk is not available
  09/02/1999 12:01:52 0 FTP Backup [13] Update completed
  09/02/1999 12:02:00 0 DCLog [00] DCManager flushing data to stat file '19990902.DC'
  09/02/1999 12:02:20 0 PaceJob{0} [00] Calling 0x00ca012c, passing 011b7b24, 00000000$
  09/02/1999 12:02:20 0 PaceJob{0} [00] Calling 0x00ca012c, passing 011b7e88, 00000000$
  09/02/1999 12:03:59 0 Security [13] Management: Forced Admin User Off Due to Timeout$
  09/02/1999 12:04:00 0 Security [12] Session: LOCAL[admin]:2876 logged out
  09/02/1999 12:04:00 0 Security [13] Management: Forcing admin to re-supply userid
  09/02/1999 12:04:03 0 Security [11] Session: LOCAL[admin] attempting login
  09/02/1999 12:04:03 0 Security [01] Session: LOCAL[admin] has no active sessions
  09/02/1999 12:04:03 0 Security [01] Session: LOCAL[admin] admin has no active accoun$
  09/02/1999 12:04:03 0 Security [12] Session: LOCAL[admin]:2877 master admin authenti$
  09/02/1999 12:04:03 0 Security [11] Session: LOCAL[admin]:2877 server right: MANAGE
  09/02/1999 12:04:03 0 Security [11] Session: LOCAL[admin]:2877 user/group right: MAN$
  09/02/1999 12:04:04 0 Security [12] Session: LOCAL[admin]:2877 Management: logged in$
  09/02/1999 12:07:36 0 PaceJob{0} [00] Calling 0x00ca012c, passing 011b7b24, 00000000$
  09/02/1999 12:07:36 0 PaceJob{0} [00] Calling 0x00ca012c, passing 011b7e88, 00000000$
  09/02/1999 12:12:44 0 PaceJob{0} [00] Calling 0x00ca012c, passing 011b7b24, 00000000$
  09/02/1999 12:12:44 0 PaceJob{0} [00] Calling 0x00ca012c, passing 011b7e88, 00000000$
  09/02/1999 12:17:00 0 DCLog [00] DCManager flushing data to stat file '19990902.DC'
  09/02/1999 12:17:50 0 tHttpdTask [35] DbEventLog.IpVerbose changed from 'FALSE' to '$
  09/02/1999 12:17:52 0 IPvfy.03739424{Prv} [00] Mgmt filter drop, src 0x8f0f010a dst $
  09/02/1999 12:17:54 0 IPvfy.03739424{Prv} [00] Mgmt filter drop, src 0x8c10000a dst $
  09/02/1999 12:17:57 0 PaceJob{0} [00] Calling 0x00ca012c, passing 011b7b24, 00000000$
  09/02/1999 12:17:57 0 PaceJob{0} [00] Calling 0x00ca012c, passing 011b7e88, 00000000$
  09/02/1999 12:17:59 0 IPvfy.03739424{Prv} [00] Mgmt filter drop, src 0xe6ea000a dst $
CES#
CES#show logging events ip-drops all filtered
  09/02/1999 12:26:17 0 IPvfy.03739424{Prv} [00] Mgmt filter drop, src 0x2810000a dst $
  09/02/1999 12:26:17 0 IPvfy.03739424{Prv} [00] Mgmt filter drop, src 0x2810000a dst $
  09/02/1999 12:26:18 0 IPvfy.03739424{Prv} [00] Mgmt filter drop, src 0x850a090a dst $
  09/02/1999 12:26:19 0 tHttpdTask [35] DbEventLog.FltVerbose changed from 'FALSE' to $
  09/02/1999 12:26:20 0 IPvfy.03739424{Prv} [00] Mgmt filter drop, src 0x841c090a dst $
  09/02/1999 12:26:20 0 IPvfy.03739424{Prv} [00] Pkt(01-20) 45 00 00 ca b4 59 00 00 05$
  09/02/1999 12:26:20 0 IPvfy.03739424{Prv} [00] Pkt(21-40) 00 8a 00 8a 00 b6 52 31 11$
  09/02/1999 12:26:21 0 IPvfy.03739424{Prv} [00] Mgmt filter drop, src 0x841c090a dst $
  09/02/1999 12:26:21 0 IPvfy.03739424{Prv} [00] Pkt(01-20) 45 00 00 4e b4 5d 00 00 05$
  09/02/1999 12:26:21 0 IPvfy.03739424{Prv} [00] Pkt(21-40) 00 89 00 89 00 3a 80 78 d7$
  09/02/1999 12:26:22 0 IPvfy.03739424{Prv} [00] Mgmt filter drop, src 0x841c090a dst $
  09/02/1999 12:26:22 0 IPvfy.03739424{Prv} [00] Pkt(01-20) 45 00 00 4e b4 5f 00 00 05$
  09/02/1999 12:26:22 0 IPvfy.03739424{Prv} [00] Pkt(21-40) 00 89 00 89 00 3a 80 78 d7$
  09/02/1999 12:26:23 0 IPvfy.03739424{Prv} [00] Mgmt filter drop, src 0x841c090a dst $
  09/02/1999 12:26:23 0 IPvfy.03739424{Prv} [00] Pkt(01-20) 45 00 00 4e b4 66 00 00 05$
  09/02/1999 12:26:23 0 IPvfy.03739424{Prv} [00] Pkt(21-40) 00 89 00 89 00 3a 80 78 d7$
CES#
CES#show logging events ip-drops none clear
```

This long example shows the amount of detail that is output by this command depending on the options chosen. The second to last command disables tracking of IP drops and clears the event log so that no output results from the final command.

Comments

The amount of output from this command can be substantial. It is automatically paginated on display so that the user can see one page of output at a time. The user can go through the output one screen at a time, or quit and abandon the remainder of the output.

show logging history

This command displays the current logging history setting that is being used by the switch.

Syntax

```
show logging history
```

Parameters

None

Default

None

Command mode

Privileged Exec

Response

See the example for output from this command.

Next command mode

Privileged Exec

Related commands

logging history

Example

```
CES#show logging history

  Logging history level is errors
```

This example shows the output for a switch where the logging history is still the default value.

show logging security

This command displays the contents of the security log. The security log records all events concerned with system or user security, including failures and successes.

Syntax

```
show logging security [date {day month [year]|month day [year]}] [normal|urgent|detailed|all]
```

Parameters

date	Specify the date for which the security log is to be displayed.
day	The day of the month for which the security log is to be displayed.
month	The month for which the security log is to be displayed.
year	The year for which the security log is to be displayed. A four-digit value.
normal	Display normal events, including user and system interactions, that indicate switch activity.
urgent	Display events that an administrator should be aware of immediately. In the output, these events are marked with an asterisk. Could indicate potential security or access problems. Also, display normal events.
detailed	Display events for use of Nortel Networks support personnel. Also, display normal and urgent events.
all	Display events for use of Nortel Networks support personnel used for troubleshooting the switch. Includes every event that the switch generates. In addition, display detailed, normal, and urgent events.

Default

The date value defaults to today. If the year portion of the date is omitted it defaults to the current year. The display level defaults to normal.

Command mode

Privileged Exec

Response

See the example below for output from this command.

Next command mode

Privileged Exec

Related commands

```
show logging config

show logging events

show logging syslog
```

Example

```
CES#show logging security
  *09:54:26 tEvtLgMgr 0 : Security [13] Management: Request for manager.htm denied, re$
   09:54:29 tEvtLgMgr 0 : Security [12] Session: LOCAL[admin]:2873 master admin authen$
   09:54:30 tEvtLgMgr 0 : Security [12] Session: LOCAL[admin]:2873 Management: logged $
  *11:05:38 tEvtLgMgr 0 : Security [13] Management: Forced Admin User Off Due to Timeo$
   11:05:39 tEvtLgMgr 0 : Security [12] Session: LOCAL[admin]:2873 logged out
  *11:05:39 tEvtLgMgr 0 : Security [13] Management: Forcing admin to re-supply userid
   11:05:40 tEvtLgMgr 0 : Security [12] Session: LOCAL[admin]:2874 master admin authen$
   11:05:41 tEvtLgMgr 0 : Security [12] Session: LOCAL[admin]:2874 Management: logged $
  *11:26:08 tEvtLgMgr 0 : Security [13] Management: Forced Admin User Off Due to Timeo$
   11:26:09 tEvtLgMgr 0 : Security [12] Session: LOCAL[admin]:2874 logged out
  *11:26:09 tEvtLgMgr 0 : Security [13] Management: Forcing admin to re-supply userid
   11:26:11 tEvtLgMgr 0 : Security [12] Session: LOCAL[admin]:2875 master admin authen$
   11:26:11 tEvtLgMgr 0 : Security [12] Session: LOCAL[admin]:2875 Management: logged $
  *11:48:39 tEvtLgMgr 0 : Security [13] Management: Forced Admin User Off Due to Timeo$
   11:48:40 tEvtLgMgr 0 : Security [12] Session: LOCAL[admin]:2875 logged out
  *11:48:40 tEvtLgMgr 0 : Security [13] Management: Forcing admin to re-supply userid
   11:48:41 tEvtLgMgr 0 : Security [12] Session: LOCAL[admin]:2876 master admin authen$
   11:48:42 tEvtLgMgr 0 : Security [12] Session: LOCAL[admin]:2876 Management: logged $
  *12:03:59 tEvtLgMgr 0 : Security [13] Management: Forced Admin User Off Due to Timeo$
   12:04:00 tEvtLgMgr 0 : Security [12] Session: LOCAL[admin]:2876 logged out
  *12:04:00 tEvtLgMgr 0 : Security [13] Management: Forcing admin to re-supply userid
   12:04:03 tEvtLgMgr 0 : Security [12] Session: LOCAL[admin]:2877 master admin authen$
   12:04:04 tEvtLgMgr 0 : Security [12] Session: LOCAL[admin]:2877 Management: logged $
   12:18:15 tEvtLgMgr 0 : Security [12] Session: LOCAL[admin]:2878 master admin authen$
   12:18:16 tEvtLgMgr 0 : Security [12] Session: LOCAL[admin]:2878 FTP: logged in from$

   12:19:06 tEvtLgMgr 0 : Security [12] Session: LOCAL[admin]:2878 FTP Get filename /s$

   12:19:49 tEvtLgMgr 0 : Security [12] Session: LOCAL[admin]:2878 FTP Get filename /s$
```

This example shows the security log output for normal messages. The urgent messages are marked with an asterisk (*) character.

Comments

The amount of output from this command can be substantial. It is automatically paginated on display so that the user can see one page of output at a time. The user can go through the output one screen at a time, or quit and abandon the remainder of the output.

show logging syslog

This command displays the contents of the system log. The system log contains all system events that are considered significant enough to be written to disk, including those displayed in the security and configuration logs.

Syntax

show logging syslog [*date* {*day month* [*year*]|*month day* [*year*]}]
[*normal*|*urgent*|*detailed*|*all*]

Parameters

date — Specify the date for which the system log is to be displayed.

day — The day of the month for which the system log is to be displayed.

month — The month for which the system log is to be displayed.

year — The year for which the system log is to be displayed. A four-digit value.

normal — Display normal events, including user and system interactions, that indicate switch activity.

urgent Display events that an administrator should be aware of immediately. In the output, these events are marked with an asterisk. Could indicate potential security or access problems. Also display normal events.

detailed Display events for use of Nortel Networks support personnel. Also display normal and urgent events.

all Display events for use of Nortel Networks support personnel used for troubleshooting the switch. Includes every event that the switch generates. Also display detailed, normal, and urgent events.

Default

The date value defaults to today. If the year portion of the date is omitted, it defaults to the current year. The display level defaults to normal.

Command mode

Privileged Exec

Response

See the example for output from this command.

Next command mode

Privileged Exec

Related commands

```
logging history

logging facility syslog

show logging config

show logging events

show logging security
```

Example

```
CES#show logging syslog

  *14:01:52 tEvtLgMgr 0 : FTP Backup [13] Update completed

  *15:01:52 tEvtLgMgr 0 : FTP Backup [13] Redundant Disk is not available

  *15:01:52 tEvtLgMgr 0 : FTP Backup [13] Update completed

  *15:09:09 tEvtLgMgr 0 : Security [13] Management: Forced Admin User Off Due to Timeo$

   15:09:09 tEvtLgMgr 0 : Security [12] Session: LOCAL[admin]:2879 logged out

  *15:09:09 tEvtLgMgr 0 : Security [13] Management: Forcing admin to re-supply userid

   15:09:11 tEvtLgMgr 0 : Security [12] Session: LOCAL[admin]:2880 master admin authen$

   15:09:12 tEvtLgMgr 0 : Security [12] Session: LOCAL[admin]:2880 Management: logged $

  *15:27:33 tEvtLgMgr 0 : Security [13] Management: Forced Admin User Off Due to Timeo$

   15:27:33 tEvtLgMgr 0 : Security [12] Session: LOCAL[admin]:2880 logged out

  *15:27:37 tEvtLgMgr 0 : Security [13] Management: Request for manager.htm denied, re$

   15:27:39 tEvtLgMgr 0 : Security [12] Session: LOCAL[admin]:2881 master admin authen$

   15:27:40 tEvtLgMgr 0 : Security [12] Session: LOCAL[admin]:2881 Management: logged $

   15:27:57 tHttpdTask 0 : DbSysLog.CaptureLevel changed from 'NORMAL' to 'ALL' by use$

   15:28:54 tHttpdTask 0 : DbSysLog.CaptureLevel changed from 'URGENT' to 'NORMAL' by $

   15:29:04 tEvtLgMgr 0 : Security [12] Session: LOCAL[admin]:2882 logged out
```

This first example shows the system log output for normal messages. The second example shows the normal messages. The urgent messages are marked with an asterisk (*).

Comments

The amount of output from this command can be substantial. It is automatically paginated on display so that the user can see one page of output at a time. The user can go through the output one screen at a time, or quit and abandon the remainder of the output.

show reload

This command displays information about any pending shutdowns that are scheduled on the switch.

This is the same information that is displayed on the Admin->Shutdown and Status->System Web management pages.

Syntax

```
show reload
```

Parameters

None

Default

None

Command mode

User Exec

Response

See the example for output from this command.

Next command mode

User Exec

Warnings

No reload currently scheduled.

Related commands

```
reload cancel

reload

reload at

reload in

reload no-sessions
```

Example

```
CES>show reload
  Reload scheduled in 1 hour 45 minutes
  Explanation:     Load latest software patches
  After shutdown:  Restart
  Current logins:  Enabled
  Reboot logins:   Disabled
  Boot drive:      /ide0
  Config file:     latest
```

This example shows details about the currently scheduled reload.

show sessions

This command displays information about the current sessions connected to the switch.

Syntax

```
show [branch-office] [ipsec] [pptp] [l2tp] [l2f] [admin] [all]
sessions [detail]
```

Parameters

admin	Show information for administrator connections.
all	Show information for all connection types.
branch-office	Show information for branch office connections.
details	Show detailed information for the connections.
ipsec	Show information for IPSec connections.
l2f	Show information for L2F connections.
l2tp	Show information for L2TP connections.
pptp	Show information for PPTP connections.
detail	Give detailed output for the specified session types.

Default

If no options are selected, this command shows summary and detailed information for all session types. This is the equivalent of the user entering:

```
show all sessions detail
```

Command mode

User Exec

Response

See the example for output from this command.

Next command mode

User Exec

Related commands

```
who
```

```
kill
```

Example

```
CES>show sessions
```

This command shows the administrator connections currently made to the switch. Details include the number of current sessions as well as who is currently logged in to each session.

show version

This command displays the configuration of the system hardware, the software version, the names and locations of the config file, and the system up time.

Syntax

```
show version
```

Parameters

None

Default

None

Command mode

User Exec

Next command mode

User Exec

Related commands

show flash: contents

Example

```
CES>show version
  Contivity VPN Client Software
  Software Version: V01_00.00
  Software Build Date: Nov 18 2000, 11:31:50
  System Serial Number: 12012
  MAC Address: 00-E0-7B-00-00-C0
  BIOS: 1.00.02.DI0 11/05/9612:40:54
  bftarget uptime: 016 days, 01 hours, 14 minutes
  Current Configuration File: /ide0/system/config/CFG01022.DAT
Processor: 1 Pentium Pro 200 Mhz, L1D Cache: 8K, L1I Cache: 8K, L2
Cache:512K
  Memory: 23 MB Free, 64 MB Total.
  Hard Disk: 1 198 MB Free, 1220 MB Total
  Diskette: 3.5 Inch
```

This example displays the basic information for this system.

snmp-server contact

This command sets, or clears, the SysContact field in the MIB-II MIB. This field contains the name and contact information of the contact person for this switch.

Syntax

snmp-server contact text

no snmp-server contact

Parameters

text	String containing the contact name and the location

Default

None

Command mode

Global configuration

Next command mode

Global configuration

Warnings

Contact string too long (must be 255 characters or less).

Related commands

snmp-server location text

snmp-server name text

Example

```
CES(config)#snmp-server contact Dial John Connolly at
1-800-555-1212, x 123
```

This example sets the contact string to dial John Connolly at 1-800-555-1212, x 123.

snmp-server location

This command sets, or clears, the SysLocation field in the MIB-II MIB. This field contains the physical location for this switch.

Syntax

```
snmp-server location text
no snmp-server location
```

Parameters

text	String containing the physical location of the switch

Default

None

Command mode

Global configuration

Next command mode

Global configuration

Warnings

Location string too long (must be 255 characters or less).

Related commands

snmp-server contact text

snmp-server name text

Example

```
CS(config)#snmp-server location Building 400,4th Floor Closet A122
```

This example sets the location string to Building 400, 4th Floor Closet A122.

snmp-server name

This command sets, or clears, the SysName field in the MIB-II MIB. This field contains an administratively assigned name for this switch.

Syntax

```
snmp-server name text

no snmp-server name
```

Parameters

text	String containing the switch name

Default

None

Command mode

Global configuration

Next command mode

Global configuration

Warnings

Name string too long (must be 255 characters or less).

Related commands

snmp-server contact text

snmp-server location text

Example

```
CES(config)#snmp-server name Contivity Chester, Group 1
```

This example sets the name string to Contivity Chester, Group 1.

suffix remove

This command is used when configuring the LDAP server for the switch. It allows the administrator to remove the domain name suffix from the user ID before sending the user ID to the LDAP server for authentication.

Syntax

```
suffix remove
```

```
no suffix remove
```

Parameters

None

Default

suffix remove

Command mode

LDAP server configuration

Next command mode

LDAP server configuration

Related commands

ldap server

show ldap server

Example

```
CES(config)#ldap-server internal

Router(config-ldap)#no suffix remove
Router(config-ldap)#domain-delimiter # suffix
Router(config-ldap)#exit
```

In this example the delimiter between the user ID and the domain name is set to the # character and the suffix is not removed before sending the user ID value to the LDAP server for authentication.

trace

The trace command allows the administrator to determine the route that packets use when traveling to their destination. It is commonly used as a diagnostic command (traceroute on most systems).

The trace command does not recognize DNS names with hyphens.

Syntax

trace ip {*host* | *address*} [hops *number*] [wait *timeout*]

Parameters

host	The trace packets to the system identified by this host name.
address	The trace packets to the system identified by this dotted IP address.
hops number	Specify the maximum hops.
wait timeout	Specify the wait timeout in seconds.

Default

The wait timeout defaults to 5 seconds.

The maximum hops defaults to 30.

Command mode

User Exec

Next command mode

User Exec

Warnings

If the system cannot map an address for a host name, it returns an "%Unknown Host" error message.

Related commands

ping {*host*|*address*}

Example

```
CES>trace 208.216.182.15

Tracing the route to amazon.com (208.216.182.15)

1 router-a.fred.corp.com (195.120.1.6) 1000 msec 8 msec 4 msec
2 filter-1.jane.fred.com (195.120.16.2) 8 msec 8 msec 8 msec
3 core2.seattle.cw.net (204.70.9.120) 8 msec 4 msec 4 msec
4 internap.seattle.cw.net (204.70.233.6) 8 msec 8 msec 8 msec
6 amazon.com (208.216.182.15) 216 msec 120 msec 132 msec

CES> trace badaddress.com

trace: unknown host baddaddress.com
```

The examples show a successful trace command, and an attempt to trace the path to an unknown host address.

who

This command shows the active Telnet administration sessions on the switch with the IP address from which they are connected. The sessions are listed by session ID.

The session ID values are fixed for the life of a session.

Syntax

```
who [ip_address]
```

Parameters

ip_address	A dotted IP address. If present, limits the output to Telnet sessions that are connected from the specified IP address, if any. If this argument is not specified, then all Telnet sessions are displayed.

Default

None

Command mode

User Exec

Next command mode

User Exec

Warnings

No Telnet sessions from specified IP address.

Illegal IP address.

Related commands

kill

show sessions

Chapter 3
Bulk Load Command

The bulk load command allows an administrator to send a list of commands and parameters to a Contivity VPN Switch and have them executed in series. This command allows an administrator with many switches to configure them in bulk from a list of settings instead of having to configure each switch manually through the browser interface.

The bulk load command allows an administrator to configure several different aspects of the switch such as users, branch office connections, tunnel types, and so forth.

The bulk load command is executed via the telnet interface by using the LOAD command. The LOAD command has the following syntax:

%% LOAD [`name of file`]

As the command executes, any errors encountered will be displayed on the screen. Most errors are reported in the following format:

Error: [`error message`] at line number [`line number`]: END

The line number refers to the END label of the command in error.

If errors occur during the execution of a command, they are displayed. Non-error status information is not displayed during the execution of the commands. Once a command has been executed, its results can be verified by viewing the command's corresponding UI page.

> **Note:** A Bulk load file can contain a maximum of 40,000 lines, including blank lines.

Components

The bulk loading feature has two main components: the command file and the LOAD command.

Load command

The Load command is available only through the Telnet interface. Once executed, the command will load the specified command file, and execute the instructions it contains. When completed, the command file will be deleted. Following is the syntax of the Load command:

%% LOAD [*`command file`*]

Command file

The command file is a text file containing a sequence of commands that are to be executed. The file is located in /SYSTEM/COMMAND directory on the boot disk. The command file has the following characteristics:

- The command file must conform to the 8.3 (eight character prefix.the character suffix) naming convention.
- Each command file begins with the string FILE_FORMAT: [*`format`*].
- Each command is initiated with the string "COMMAND: xxxx".
- Each command is terminated with the string "END".
- Each command accepts a number of qualifiers. Each qualifier is defined by TYPE: VALUE pairs; for example "NAME" is the field type, and "Joe" is the field value.
- The comment character is "//".
- The command file must end with a blank line.
- A command file may contain an unlimited number of commands.
- When all commands have been executed, the command file is automatically deleted.

File format

The FILE_FORMAT command defines what versions of the bulk load commands are contained in the command file. In this release, bulk loading file formats 1.0, 2.0, and 3.0 are supported. The FILE_FORMAT command is useful if a bulk load script is to be used on several switches with different releases installed. For example, the following command file may be executed on a switch installed with versions 2.50, 2.60, and 3.00:

```
FILE_FORMAT: 1.0
COMMAND: ONE
[...]
END
FILE_FORMAT: 2.0
COMMAND: TWO
[...]
END
FILE_FORMAT: 3.0
COMMAND: THREE
[...]
END
```

The 2.50 switch will recognize and execute command ONE and ignore command TWO and command THREE. The 2.60 switch will recognize both command ONE and command TWO, but ignore command THREE. The 3.0 switch will recognize all three commands. If the command file is only being used on a 3.00 switch, the file format may be set to 1.0, 2.0, or 3.0.

User commands

User commands allow an administrator to add or delete user records. They also allow an administrator to add or delete user groups. The supported user commands are:

```
ADD_USER

DELETE_USER

RESET_USER_CERTS

ADD_GROUP

MODIFY_GROUP

PURGE_GROUP

DELETE_GROUP

DELETE_ALL
```

Add User

ADD_USER adds a user or user group. A user record must contain authentication credentials (such as UID and Password, DN, and so forth.) before the user is added to the database.

```
COMMAND: ADD_USER

GROUP: [Group name]

NAME: [User name - Required]

STATIC_ADDR_IP: [Static IP address]

STATIC_ADDR_MASK: [Static IP address mask]

IPSEC_UID: [IPSec User ID - Required if not using
certificates]

IPSEC_PSW: [IPSec password - Required if not using
certificates]

IPSEC_SUBJECTDN: [Subject distinguished name - Required if
using certificates and not IPSEC_ALTNAME]

IPSEC_ALTNAME: [Subject alternative name - Required if using
certificates and not IPSEC_SUBJECTDN]

IPSEC_TYPE: [Subject name type {Email/DNS/IP} - Required
with certificates and IPSEC_ALTNAME]

IPSEC_ISSUERCA: [Issuer certificate authority - Required
with certificates]

SERVER_CERT: [Server Certificate - Default: Inherit from
group]

RESTRICTED: [Control User Tunnel {True/False} -
Default:False]

END
```

Delete User

```
The DELETE_USER command is used to delete a specified user record
from the database. You must include a user name, and if you do not
specify a group, then the /Base group is assumed.
COMMAND: DELETE_USER

GROUP: [Group name]
NAME: [User name - Required]
END
```

Add Group

The ADD_GROUP command is used to add a group to the switch database.

```
COMMAND: ADD_GROUP

GROUP: [Group name - Required]

END
```

Modify Group

The MODIFY_GROUP command is used to modify existing user groups. Any set of these attributes may be included in this command. Any attribute not specified will inherit the value from its parent group.

Note: All attributes accept the "inherited" value, which for switch that attribute to inherit the values of its parent.

```
COMMAND: MODIFY_GROUP

GROUP: [Group name - Required]

// Connectivity Attributes

FILT_NAME: [Name of existing filter]

CALL_PRI: [Call admission priority {Low/Medium/High/Highest}]

FORWARD_PRI: [Forwarding priority {Low/Medium/High/Highest}]

NUM_LOGINS: [Number of logins]

STATIC_ADDR: [Static addresses {Enable/Disable}]

IDLE_TO: [Idle timeout period (hh:mm:ss format)]

FORCED_LO_TIME: [Forced logout timeout (hh:mm:ss format)]

SPLIT_TUN: [Split tunneling {Enable/Disable}]

SPLIT_TUN_NET: [Split tunnel network name]

ADDR_POOL: [Address pool name or 'Default' for default pool]

// Bandwidth Policy

BW_COMMIT_RATE: [Committed Bandwidth Rate (bps)]

BW_EXCESS_RATE: [EXCESS Bandwidth Rate (bps)]

BW_EXCESS_ACTION: [EXCESS Rate Action {Drop/Mark}]

// IPSEC Attributes

DIG_SIG: [RSA Digital Signature {Enable/Disable}]

UNAMEPW: [User Name/Password Authentication {Enable/Disable}]

SERVER_CERT: [Default server certificate]

ESP_3SHA1: [ESP - Triple DES with SHA1 Integrity

{Enable/Disable}]
```

```
ESP_3MD5: [ESP - Triple DES with MD5 Integrity

          {Enable/Disable}]

ESP_56SHA1: [ESP - 56-bit DES with SHA1 Integrity

          {Enable/Disable}]

ESP_56MD5: [ESP - 56-bit DES with MD5 Integrity

{Enable/Disable}]

ESP_40SHA1: [ESP - 40-bit DES with SHA1 Integrity

          {Enable/Disable}]

ESP_40MD5: [ESP - 40-bit DES with MD5 Integrity

{Enable/Disable}]

ESP_NULLSHA1: [ESP - NULL (Authentication Only) with SHA1

Integrity {Enable/Disable}]

ESP_NULLMD5: [ESP - NULL (Authentication Only) with MD5

Integrity {Enable/Disable}]

AH_SHA1: [AH - Authentication Only (HMAC-SHA1)

{Enable/Disable}]

AH_MD5: [AH - Authentication Only (HMAC-MD5) {Enable/Disable}]

SCRSVR_PSW: [Client screen saver password required

Enable/Disable}]

SCRSVR_INT: [Client screen saver interval]

PSW_ON_CLI: [Allow password storage on client {Enable/Disable}]

PFS: [Perfect forward security {Enable/Disable}]

COMPRESSION: [Compression {Enable/Disable}]

REKEY_TO: [Rekey timeout (hh:mm:ss format)]
```

```
REKEY_DATACNT: [Rekey datacount (in KB)]

DOMAIN: [Domain name]

PRI_DNS: [Primary DNS address]

PRI_WINS: [Primary WINS address]

SEC_DNS: [Secondary DNS address]

SEC_WINS: [Secondary WINS address]

END
```

Purge Group

The PURGE_GROUP command is used to delete all users in a specified group. If you do not specify a group, the command purges all users in the /Base group.

```
COMMAND: PURGE_GROUP

GROUP: [Group name - Required]

END
```

Delete Group

The DELETE_GROUP command is used to delete a specified group and its users.

```
COMMAND: DELETE_GROUP

GROUP: [Group name - Required]

END
```

Delete All

The DELETE_ALL command deletes all users in the database.

Caution: This command should only be executed by the switch administrator because all other accounts are removed.

```
COMMAND: DELETE_ALL

END
```

Branch office commands

Branch office commands allow an administrator to add or delete branch office connections, including control tunnel connections. These commands also allow administrators to add and delete branch office groups. The supported branch office commands are:

```
ADD_CONNECTION

DELETE_CONNECTION

ADD_BRANCHGROUP

MODIFY_BRANCHGROUP

PURGE_BRANCHGROUP

DELETE_BRANCHGROUP

DELETE_ALLBRANCH
```

Add branch office connection

The ADD_CONNECTION command defines a branch office control connection with specific attributes. The connection must contain authentication information before it is created. Once a connection is created with the required attributes, it is automatically enabled. This command has been modified for the Contivity VPN Switch Version 3.0

```
COMMAND: ADD_CONNECTION

GROUP: [Group name]

NAME: [Connection name - Required]

SYSTEM_IP: [Contivity management IP address - Required for
Restricted tunnel]
```

Note: Using a SYSTEM _IP value other than the actual management IP address, will create a NAT SET for the Management IP.

```
LOCAL_ENDPOINT: [Local interface IP address - Required]

REMOTE_ENDPOINT: [Remote interface IP address - Required]

RESTRICTED: [Control Tunnel {True/False} - Default:False]

FILT_NAME: [Tunnel filter name - Required]

ROUTING: [Routing type {Static/Dynamic} - Default:Static]

TUNNEL: [Tunnel type {IPSEC,PPTP,L2TP} - Default:IPSEC]

// Static Routing

NET_NAME: [Local accessible network - Required for Static
Routing]

NAT_NAME: [NAT Translation (Optional for Static Routing)]

SUBNET: [Remote Accessible Net Subnet - Required for Static
Routing]
```

```
MASK: [Remote Accessible Net Subnet mask - Required for
Static Routing]

REM_NET_COST: [Remote network cost - Default:10]

REM_NET_STATE: [Remote network state - {Enable/Disable}
Default: Enable]

// Dynamic Routing

OSPF_STATE: [OSPF state {Enable/Disable} (Dynamic Routing)

Default:Disable]

AREA_ID: [Area ID (Dynamic Routing) - Default:0.0.0.0]

OSPF_COST: [OSPF cost (Dynamic Routing) - Default:10]

RIP_STATE: [Rip state {Enable/Disable} (Dynamic Routing) -
Default: Disable]

// IPSec Authentication

IPSEC_PSW: [IPSec password - Required if not using
certificates]

IPSEC_SUBJECTDN: [Subject distinguished name - Required if
using certificates and not IPSEC_ALTNAME]

IPSEC_ALTNAME: [Subject alternative name - Required if using
certificates and not IPSEC_SUBJECTDN]

IPSEC_TYPE: [Subject name type {Email/DNS/IP} - Required with
certificates and IPSEC_ALTNAME]

IPSEC_ISSUERCA: [Issuer certificate authority - Required with
certificates]

SERVER_CERT: [Server Certificate - Required with certificates]

SERVER_ALTNAME: [Server Certificate Alternate name]

// PPTP/L2TP Authentication

TUNNEL_AUTH: [MSChap V2 Authentication {RC4-128,RC4-40,
Unencrypt} - (PPTP & L2TP tunnel types)]
```

```
LOCAL_UID: [Tunnel authentication - local user ID - (PPTP &
L2TP tunnel types) - Required for PPTP/L2TP]

PEER_UID: [Tunnel authentication - peer user ID - (PPTP &
L2TP tunnel types) - Required for PPTP/L2TP]

PEER_PSW: [Tunnel authentication - peer password - (PPTP &
L2TP tunnel types)]

COMPRESSION: [PPTP & L2TP compression {Enable/Disable} -
(PPTP & L2TP tunnel types)]

ENC_STATE_MODE: [PPTP & L2TP Compression/Encryption
stateless mode {Enable/Disable} - (PPTP & L2TP tunnel
types)]

// L2TP specific authentication parameters

CONCENTRATOR: [L2TP Concentrator (L2TP tunnel type)]

L2TP_IPSEC_XPORT: [L2TP IPSEC Transport {None, 3DES, 56DES,
40DES, AH} - (L2TP tunnel type only)]

END
```

Modify branch office connection

The MODIFY_CONNECTION command is used to add a new remote accessible network entry to an existing branch office connection.

```
COMMAND: MODIFY_CONNECTION

GROUP: [Branch Office group - Default:/Base]

NAME: [Name of existing Branch Office connection to modify -
Required]

SUBNET: [Remote Network subnet - Required]

MASK: [Remote Network subnet mask - Required]

REM_NET_COST: [Remote network cost - Default:10]

REM_NET_STATE: [Remote network state - {Enable/Disable}
Default:Enable]

END
```

Delete branch office connection

The DELETE_CONNECTION command deletes the specified connection from the branch office group.

```
COMMAND: DELETE_CONNECTION

NAME: [Connection name - Required]

GROUP: [Group name - Default:/Base]

END
```

Add branch office group

The ADD_BRANCHGROUP command creates a branch office group as specified. A group name is required.

```
COMMAND: ADD_BRANCHGROUP

GROUP: [Group name - Required]

END
```

Modify branch office group

The MODIFY_BRANCHGROUP command is used to modify existing branch office groups. All values that are not specified will inherit values from its parent group.

Note: All attributes accept the "inherited" value, which forces that attribute to inherit its value from its parent.

NOTE: COMMAND: MODIFY_BRANCHGROUP

```
GROUP: [Name of existing Branch Office group to modify -Required]

//Connectivity Attributes

CALL_PRI: [Call admission priority {Low/Medium/High/Highest}]

FORWARD_PRI: [Forwarding priority {Low/Medium/High/Highest}]

IDLE_TO: [Idle timeout period (hh:mm:ss format)]

// Bandwidth Policy

BW_COMMIT_RATE: [Committed Bandwidth Rate (bps)]

BW_EXCESS_RATE: [EXCESS Bandwidth Rate (bps)]

BW_EXCESS_ACTION: [EXCESS Rate Action {Drop/Mark}]

// IPSEC Attributes

ESP_3SHA1: [ESP - Triple DES with SHA1 Integrity {Enable/Disable}]

ESP_3MD5: [ESP - Triple DES with MD5 Integrity {Enable/Disable}]

ESP_56SHA1: [ESP - 56-bit DES with SHA1 Integrity {Enable/Disable}]

ESP_56MD5: [ESP - 56-bit DES with MD5 Integrity {Enable/Disable}]

ESP_40SHA1: [ESP - 40-bit DES with SHA1 Integrity {Enable/Disable}]

ESP_40MD5: [ESP - 40-bit DES with MD5 Integrity {Enable/Disable}]

ESP_NULLSHA1: [ESP - NULL (Authentication Only) with SHA1 Integrity {Enable/Disable}]

ESP_NULLMD5: [ESP - NULL (Authentication Only) with MD5 Integrity {Enable/Disable}]

AH_SHA1: [AH - Authentication Only (HMAC-SHA1) {Enable/Disable}]

AH_MD5: [AH - Authentication Only (HMAC-MD5) {Enable/Disable}]

VEND_ID: [Vendor ID {Enable/Disable}]
```

```
PFS: [Perfect forward security {Enable/Disable}]

COMPRESSION: [Compression {Enable/Disable}]

REKEY_TO: [Rekey timeout (hh:mm:ss format)]

REKEY_DATACNT: [Rekey datacount (in KB)]

// RIP Attributes

RIP_TRANSMIT: [Rip Transmit {OFF,V1,V2}]

RIP_RECEIVE: [Rip Receive {OFF,V1,V2}]

IMPORT_DEF_ROUTE: [Import Default Route {Enable/Disable}]

EXPORT_DEF_ROUTE: [Export default routes metric {Enable/Disable}]

EXPORT_STATIC_ROUTE: [Export static routes metric {Enable/Disable}]

EXPORT_BO_STATIC_ROUTE: [Export branch office static routes metric
(Enable/Disable}]

EXPORT_OSPF_ROUTE: [Export OSPF e static routes metric (Disable,
1-15}]

POISON_REV: [Poison Reverse {Enable/Disable}]

RIP_AUTH: [Rip Authentication {None/Simple/MD5}]

//
```

Note: The following value does not accept the "INHERITED"keyword. The RIP_AUTH value will controlthe inheritance of this value.

```
//

RIP_PASS: [RIP authentication password]

// OSPF Attributes

OSPF_PRI: [OSPF Priority]

OSPF_DEAD_INT: [OSPF dead interval]

OSPF_HELLO_INT: [OSPF hello interval]
```

```
OSPF_REXMIT_INT: [OSPF retransmit interval]

OSPF_XMIT_DELAY: [OSPF transmission delay]

OSPF_AUTH: [OSPF Authentication {None/Simple/MD5}]

// NOTE: The following values do not accept the "INHERITED"

//       keyword. The OSPF_AUTH value will control the

//       inheritance of these values.

OSPF_PASS: [OSPF Authentication Password]

MD5_PASS: [OSPF MD5 password]

MD5_KEY: [OSPF MD5 Key]

END
```

Contivity VPN Switch configuration commands

Switch configuration commands allow the administrator to configure switch attributes such as network definitions, NAT, address pools, filters, automatic backup, syslog forwarding, SNMP settings, and DHCP servers.

Network definitions

Three bulk load commands are used to manage network definitions:

```
CREATE_NETWORK

DELETE_NETWORK

MODIFY_NETWORK
```

The CREATE_NETWORK command is used to add a new network definition.

```
COMMAND: CREATE_NETWORK

NET_NAME: [Name of new network definition - Required]

SUBNET: [New IP address - Required]

MASK: [New subnet mask - Required]

END
```

The DELETE_NETWORK command is used to delete an existing network definition.

```
COMMAND: DELETE_NETWORK

NET_NAME: [Name of existing network to delete - Required]

END
```

The MODIFY_NETWORK command is used to add new subnets to an existing network definition.

```
COMMAND: MODIFY_NETWORK

NET_NAME: [Name of existing network to modify - Required]

SUBNET: [New IP address - Required]

MASK: [New subnet mask - Required]

END
```

NAT

Three bulk load commands are used to configure NAT settings: CREATE_NAT, DELETE_NAT, and MODIFY_NAT.

The CREATE_NAT command is used to create a new NAT set.

```
COMMAND: CREATE_NAT

NAT_NAME: [Name of new NAT set - Required]

NAT_TYPE: [Translation Type {Static/Pooled/Port} - Required]

IN_START_IP: [Internal starting IP address - Required]

IN_END_IP: [Internal ending IP address - Required]

EX_START_IP: [External starting IP address - Required]

EX_END_IP: [External ending IP address - Required for Pooled

NAT type]

END
```

The DELETE_NAT command is used to delete an existing NAT set.

```
COMMAND: DELETE_NAT

NAT_NAME: [Name of existing NAT set to delete - Required]

END
```

The MODIFY_NAT command is used to add a new rule to an existing NAT set.

```
COMMAND: MODIFY_NAT

NAT_NAME: [Name of existing NAT set to modify - Required]

NAT_TYPE: [Translation Type {Static/Pooled/Port} - Required]

IN_START_IP: [Internal starting IP address - Required]

IN_END_IP: [Internal ending IP address - Required]

EX_START_IP: [External starting IP address - Required]

EX_END_IP: [External ending IP address - Required for Pooled
NAT type]

END
```

Address pools

Two bulk load commands are used to configure address pools: CREATE_POOL and DELETE_POOL.

The CREATE_POOL command is used to create a new address pool.

```
COMMAND: CREATE_POOL

NAME: [Name of new address pool]

IP_START: [Starting IP address - Required]

IP_END: [Ending IP address - Required]

MASK: [Subnet mask]

END
```

The DELETE_POOL command is used to delete an existing address pool.

```
COMMAND: DELETE_POOL

IP_START: [Starting IP address - Required]

IP_END: [Ending IP address - Required]

END
```

Filters

Several bulk load commands are used to create and configure filters and filter rules:

```
CREATE_FILTER

DELETE_FILTER

ADD_RULE

CREATE_RULE

DELETE_RULE

CREATE_ADDRESS

CREATE_PORT
```

The CREATE_FILTER command allows for the creation of a new named filter. The filter may be created to allow or disallow certain management traffic. These fields are not required.

```
COMMAND: CREATE_FILTER

FILT_NAME: [Filter name - Required]

// Allow management traffic for…

HTTP_SVC: [HTTP local service {Enable/Disable}]

SNMP_SVC: [SNMP local service {Enable/Disable}]

FTP_SVC: [FTP local service {Enable/Disable}]

TELNET_SVC: [TELNET local service {Enable/Disable}]

PING_SVC: [Ping local service {Enable/Disable}]

RADIUS_SVC: [Radius local service {Enable/Disable}]

FIREWALL_SVC: [Firewall local service {Enable/Disable}]

FTP_SVR: [FTP remote server {Enable/Disable}]

DHCP_SVR: [DHCP remote server {Enable/Disable}]

RADIUS_SVR: [Radius remote server {Enable/Disable}]

DNS_SVR: [DNS remote server {Enable/Disable}]

END
```

The DELETE_FILTER command allows for the deletion of an existing filter.

```
COMMAND: DELETE_FILTER

FILT_NAME: [Filter name - Required]

END
```

The ADD_RULE command allows an existing rule to be added to an existing filter.

```
COMMAND: ADD_RULE

FILT_NAME: [Filter name - Required]

RULE_NAME: [Rule name - Required]

END
```

The CREATE_RULE command allows for the creation of a new rule definition.

```
COMMAND: CREATE_RULE

RULE_NAME: [Rule name - Required]

ADDR_NAME: [Address Name- Default:Any]

ACTION: [Rule action {Permit/Deny} - Default:Deny]

DIRECTION: [Direction {Inbound/Outbound} - Default:Inbound]

PROTOCOL: [Protocol Name - Default:Ip]

SRC_PORT: [Source Port Name - Default:Any]

DEST_PORT: [Destination Port Name - Default:Any]

END
```

The DELETE_RULE command deletes an existing rule definition. This command will fail if the rule is being used by a filter.

```
COMMAND: DELETE_RULE

RULE_NAME: [Rule name - Required]

END
```

The CREATE_ADDRESS command creates a new address definition to be used by a filter rule.

```
COMMAND: CREATE_ADDRESS

ADDR_NAME: [Address Name - Required]

IP_ADDR: [IP Address - Required]

MASK: [Address mask - Required]

END
```

The CREATE_PORT command creates a new port definition to be used by a filter rule.

```
COMMAND: CREATE_PORT

PORT_NAME: [Port Name - Required]

PORT: [Port number - Required]

END
```

Automatic backup

Two bulk load commands are available to configure the automatic backup feature:

```
ADD_FTPSERVER

DELETE_FTPSERVER.
```

The ADD_FTPSERVER command is used to configure a new automatic backup server.

```
COMMAND: ADD_FTPSERVER

FTP_IP: [FTP host IP address - Required]

FTP_UID: [User ID for FTP host - Required]

FTP_ENABLE: [Enable Auto-backup Host - Default:Enable]

FTP_PSW: [Password for FTP host - Default: "" ]

FTP_INTERVAL: [Time between backups (hours) - Default: 5]

FTP_PATH: [Path where files are stored - Default: \]

FTP_SERVER: [FTP Server {1/2/3} - Default: 1]

END
```

The DELETE_FTPSERVER command is used to remote an existing automatic backup server.

```
COMMAND: DELETE_FTPSERVER

FTP_SERVER: [Existing FTP Server {1/2/3} - Required]

END
```

SYSLOG forwarding

Two bulk load commands are available to configure the syslog forwarding feature:

```
ADD_SYSLOG

DELETE_SYSLOG
```

The ADD_SYSLOG command is used to setup a system log forwarding server.

```
COMMAND: ADD_SYSLOG

SLOG_IP [Host IP address - Required]

SLOG_MSGLEVEL: [Urgent/Normal/Detailed/All - Default:
Normal]

SLOG_FACILITY: [Syslog Facility {KERN/LOCAL[0-7]} -
Default:KERN]

SLOG_PORT: [Syslog port - Default: 514]

SLOG_ENABLE: [Enable Syslog Server - Default:Enable]

SLOG_SERVER: [Syslog Server {1/2/3/4} - Default: 1]

END
```

The DELETE_SYSLOG command is used to remove an existing system log forwarding server.

```
COMMAND: DELETE_SYSLOG

SLOG_SERVER: [Existing Syslog Server {1/2/3/4} - Required]

END
```

SNMP

Three bulk load commands are used to configure SNMP: ADD_SNMPHOST, DELETE_SNMPHOST, and CONFIG_TRAP.

The ADD_SNMPHOST command is used to add and configure either SNMP-Get or Trap hosts.

```
COMMAND: ADD_SNMPHOST

SNMP_TYPE: [Get/Trap - Required]

SNMP_IP: [SNMP host IP address - Required]
```

```
SNMP_COMMUNITY: [SNMP Community name]

SNMP_ENABLE: [Enable SNMP Host - Default:Enable]

END
```

The DELETE_SNMPHOST command is used to remove an existing SNMP-Get or Trap host.

```
COMMAND: DELETE_SNMPHOST

SNMP_TYPE: [Get/Trap - Required]

SNMP_IP: [SNMP host IP address - Required]

END
```

The CONFIG_TRAP command is used to configure which conditions will cause traps.

```
COMMAND: CONFIG_TRAP

TRAP_DESCRIPTION: [Trap Description - Required]

TRAP_INTERVAL: [Time between trap checks (hh:mm:ss)]

TRAP_ENABLE: [Enable SNMP Trap - Default:Enable]

END
```

DHCP

Three bulk load commands are used to configure DHCP:

- CONFIG_REMOTE_POOL
- CONFIG_DHCP
- DELETE_DHCP

The CONFIG_REMOTE_POOL command is used to set the type of remote pool used by the switch, either DHCP or Address Pools.

```
COMMAND: CONFIG_REMOTE_POOL

POOL_TYPE: [Pool type to use {DHCP/Address Pool} - Required]

END
```

The CONFIG_DHCP command is used to setup the DHCP servers on the switch.

```
COMMAND: CONFIG_DHCP

DHCP_TYPE: [DHCP servers to use {Any/Specified}]

DHCP_IP: [DHCP server IP address - Required if DHCP_SERVER
is specified]

DHCP_SERVER: [Specified DHCP server to modify {Primary/
Secondary/Tertiary} - Default:Primary]
```

```
CACHE_SIZE: [DHCP cache size]

IMMEDIATE_ADDR_REL: [Immediate address release {Enable/
Disable}]

END
```

The DELETE_DHCP command is used to remote an existing DHCP server.

```
COMMAND: DELETE_DHCP

DHCP_SERVER: [Existing DHCP server to remove {Primary/
Secondary/Tertiary} - Required]

END
```

Licensing commands

Licensing of certain features will be supported in bulkload version 3.0. The following two commands allow the user to enable and disable a paid feature on the CES:

ENABLE_PAID_FEATURE

```
DISABLE_PAID_FEATURE
```

The ENABLE_PAID_FEATURE command allows a user to specify the licensing key to enable a paid feature on the CES.

```
COMMAND: ENABLE_PAID_FEATURE

PAID_KEY: [Licensing key for the feature to be enabled]

END
```

The DISABLE_PAID_FEATURE command allows a user to specify the licensing key to disable a paid feature on the CES.

COMMAND: DISABLE_PAID_FEATURE

PAID_KEY: [Licensing key for the feature to be disabled]

END

Usage notes

Deletion of groups

The DELETE_GROUP and DELETE_BRANCHGROUP commands can cause the LDAP server in use by the switch to become unreachable while the group is being deleted. This can happen if the group being deleted has a large number of users or Branch Office connections defined (for example, more than 50). Deleting each user or Branch Office connection individually, using the DELETE_USER or DELETE_CONNECTION command lessens the load on the LDAP server, but it may increase the time required to execute the commands.

Required fields for user and branch records

You must specify an authentication method and details when using the ADD_CONNECTION and ADD_USER commands. Valid authentication information can be specified using any one of the following combinations of attributes:

- Text Password
- Subject Distinguished Name (DN), a valid issuer certificate authority (CA), and a valid server certificate
- Subject Alternative Name, Subject Alternative Name Type, a valid issuer certificate authority (CA), and a valid server certificate

Note: Server certificates may be inherited from a user’s group for ADD_USER.

Group name syntax

For many of the User and Branch Office commands, you must specify the name of the group that you are manipulating. The syntax of the group name is very important. Group names are specified in Relative Distinguished Name (RDN) format, leaving out the '/Base' specifier.

For example:

/Base/Engineering' is specified as:

Group: ou=Engineering

/Base/Engineering/Software' is specified as:

Group: ou=Software, ou=Engineering

/Base/Field/Boston/Sales' is specified as:

Group: ou=Sales, ou=Boston, ou=Field

Certificate Distinguished Name order

The Distinguished Name for certificates must be entered in the same order as they appear in the certificate. For Example:

cn=Joe, ou=My Org Unit, o=Some Org, c=US

is not the same as:

cn=Joe, o=Some Org, ou=My Org Unit, c=US

Index

A

acronyms 30
administrator privileges 33
arp 41

C

clear arp-cache 44
clear ip route 45
clear logging events 47
configure 48
console mode 49
control 52
conventions 28
conventions, text 28
customer support 32

D

DHCP 217
disable 54
documentation map 28

E

enable 56
enable password 58
exception backup 60
exit 62

H

help 64
host address 65
hostname 67

I

interface management 69
ip http server 71

K

kill 71

L

ldap 75
ldap-server 77
ldap-server source 79
load 81
logging history 83
logout 85

M

Management IP Address 33
more 86

P

ping 89
product support 32
publications
  hard copy 31

R

reload 91
reload at 95
reload cancel 99
reload in 102
reload no-sessions 106

S

Serial Port 34
server backup 110

server restore 113

server start 116

server stop 117

show arp 120

show exception backup 121

show file systems 124

show flash
contents 125

show health 128

show ip access-list 130

show ip ospf 132

show ip ospf database 134

show ip ospf interface 136

show ip ospf neighbor 138

show ip rip 140

show ip rip database 142

show ip rip interface 144

show ip route 146

show ip route-policies 149

show ip traffic 151

show ip vrrp 154

show ldap-server 156

show logging config 158

show logging events 161

show logging history 165

show logging security 166

show logging syslog 169

show reload 172

show sessions 173

show version 175

snmp-server contact 177

snmp-server location 179

snmp-server name 181

suffix remove 183

support, Nortel Networks 32

T

technical publications 31

technical support 32

Telnet 33

text conventions 28

trace 185

U

user interface 31