

Alteon EMS 3.1.1.0

Help

part number: 216515-B, September 2004

4655 Great America Parkway
Santa Clara, CA 95054
Phone 1-800-4Nortel
http://www.nortelnetworks.com

Copyright 2004 Nortel Networks, Inc.,4655 Great America Parkway, Santa Clara, California 95054, USA. All rights reserved. Part Number: 216515-B.

This document is protected by copyright and distributed under licenses restricting its use, copying, distribution, and decompilation. No part of this document may be reproduced in any form by any means without prior written authorization of Nortel Networks, Inc. Documentation is provided “as is” without warranty of any kind, either express or implied, including any kind of implied or express warranty of non-infringement or the implied warranties of merchantability or fitness for a particular purpose.

U.S. Government End Users: This document is provided with a “commercial item” as defined by FAR 2.101 (Oct 1995) and contains “commercial technical data” and “commercial software documentation” as those terms are used in FAR 12.211-12.212 (Oct 1995). Government End Users are authorized to use this documentation only in accordance with those rights and restrictions set forth herein, consistent with FAR 12.211- 12.212 (Oct 1995), DFARS 227.7202 (JUN 1995) and DFARS 252.227-7015 (Nov 1995).

Nortel Networks, Inc. reserves the right to change any products described herein at any time, and without notice. Nortel Networks, Inc. assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by Nortel Networks, Inc. The use and purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of Nortel Networks, Inc.

Alteon OS, Alteon 2424, Alteon 2424-SSL, Alteon 2224, 2216, 2208, 3408, Alteon 180, Alteon 180e, Alteon 184, Alteon AD3, Alteon AD4, and ACEswitch are trademarks of Nortel Networks, Inc. in the United States and certain other countries. Cisco® and EtherChannel® are registered trademarks of Cisco Systems, Inc. in the United States and certain other countries. Check Point® and FireWall-1® are trademarks or registered trademarks of Check Point Software Technologies Ltd. Any other trademarks appearing in this manual are owned by their respective companies.

Originated in the U.S.A.

Contents

Alteon: Properties 14
Configuring the Switch 16
Selection Dialog windows 17
Enabling Special Software Features on the Switch 18
Configuring General properties on Alteon 180 or AD series 19
Configuring General properties on Alteon Application Switches 21
Configuring the Management Port on Alteon Application Switches 25
Configuring Software Images on the Switch 27
Configuring a TFTP server 28
Configuring Syslog 30
Configuring Trap Hosts on Web OS 10.x and lower and Alteon OS 21.0 and lower 32
Configuring Trap Hosts on Alteon Application Switches 33
Configuring Syslog Traps 34
Configuring a RADIUS Server 35
Configuring TACACS+ Server 36
Configuring Network Time Protocol 38
Configuring Reboot 39
Configuring SONMP 40
Configuring Trunk Groups 41
Configuring a Management Network 43
Link Aggregation Control Protocol 44
Link Aggregation Control Protocol Ports 46
Aggregators 47
Link Aggregation Control 49
Configuring Port Mirroring on Alteon 180 or AD series running Web OS 9.0.34 or lower 52
Configuring Port Mirroring 53
Configuring the Bridge 55
General Bridge Properties 56

Configuring Spanning Tree Protocol on the Bridge 57
Configuring STP Groups on the Bridge 59
Configuring Spanning Tree Group Ports on the Bridge 61
Configuring Spanning Tree Protocol on Individual Ports 62
Configuring Virtual LANs 63
Configuring VLAN Membership 64
Configuring Security 65
Configuring Security: General 66
Configuring Security: UDP Blast Defaults 67
Configuring Security: UDP Blast 68
Configuring Security: Pattern Match Group 69
Configuring Security: Ports 70
Configuring Security: IP ACL 71
Configuring IP Routing Protocols 72
Configuring General IP settings 73
Configuring IP Interfaces 75
Configuring IP Gateways 76
Configuring DNS 77
Configuring the Local Route Cache 78
Configuring Routing Information Protocol (RIP1) 79
Configuring IP Forwarding on Ports 81
Configuring IP Static Routes 82
Configuring Route Maps on Alteon Application Switches 83
Configuring the Route Map Access List on Alteon Application Switches 85
Configuring IP Network Filters on Alteon Application Switches 86
Configuring AS Paths on Alteon Application Switches 87
Configuring Static ARP 88
Configuring OSPF 89
Configuring OSPF Administration 91
Configuring OSPF General Settings 92
Configuring OSPF Areas 93
Configuring OSPF Area SPF 95
Configuring OSPF Stub Areas 96
Configuring OSPF Hosts 97
Configuring OSPF Host Areas on Alteon Application Switches 98
Configuring OSPF Interfaces 99

Configuring OSPF Interface Metrics . . . 101
Configuring OSPF Virtual Interfaces . . . 102
Configuring OSPF Area Aggregates . . . 103
Configuring OSPF Fixed Routes on Alteon Application Switches . . . 104
Configuring OSPF Static Routes on Alteon Application Switches . . . 105
Configuring OSPF External BGP on Alteon Application Switches . . . 106
Configuring OSPF: Internal BGP on Alteon Application Switches . . . 107
Configuring OSPF: MD5 on Alteon Application Switches . . . 108
Configuring OSPF MD5-Interface on Alteon Application Switches . . . 109
Configuring OSPF MD5-Virtual Interface on Alteon Application Switches . . . 110
Configuring Border Gateway Protocol (BGP) . . . 111
Configuring BGP Administration on Alteon Application Switches . . . 112
Configuring General BGP Information . . . 114
Configuring BGP Peers on Alteon Application Switches . . . 115
Configuring BGP Aggregations on Alteon Application Switches . . . 117
Configuring Peers Information on Alteon Application Switches . . . 118
Configuring Layer 4 on the Switch . . . 119
Configuring Layer 4 Filters . . . 120
Configuring Advanced Layer 4 Filters . . . 125
ICMP Message Types . . . 127
Configuring TCP Filters . . . 129
Configuring IP Filters . . . 130
Configuring Layer 7 Deny Filters . . . 131
Configuring Layer 7 Lookup . . . 132
Configuring Security . . . 133
Configuring HTTP Redirection . . . 135
Configuring URL BWM Filtering . . . 136
Configuring Server Load Balancing . . . 137
Configuring General Server Load Balancing . . . 139
Configuring Layer 4 SLB: Real Servers . . . 142
Configuring Layer 4 SLB: Real Server Ports . . . 146
Configuring Layer 4 SLB: Real Server Groups . . . 147
Configuring Layer 4 SLB: Real Server Group State . . . 150
Configuring Layer 4 SLB: Real Server Group Operation . . . 151
Configuring Layer 4 SLB: Virtual Servers on Alteon 180 or AD series . . . 152
Configuring Virtual Server Services on Alteon 180 or AD series . . . 154

Configuring Layer 4 SLB: Virtual Servers on Alteon Application Switches 158
Configuring Virtual Server Services on Alteon Application Switches 160
Configuring Ports for Server Load Balancing 165
Configuring Layer 4 SLB: Proxy IP Addresses on Alteon Application Switches in Alteon OS 21.0 and Lower 167
Configuring Layer 4 SLB: Proxy IP Addresses on Alteon Application Switches in Alteon OS 22.0 and Above 170
Configuring Layer 4 SLB: Real Time Streaming Protocol (RTSP) Load Balancing on Alteon 180 or AD series 171
Configuring Layer 4 SLB: Health Scripts on Alteon Application Switches 172
Configuring SNMP Health Scripts on Alteon Application Switches 175
Configuring Layer 4 SLB: Syn Attack 176
Configuring Layer 4 SLB: Inbound Link Load Balancing 177
Configuring Layer 4 SLB: Domain Records 178
Configuring Layer 4 SLB: Domain Mapping 179
Configuring Layer 4 SLB: Service Mapping 180
Configuring Layer 4 SLB: URL-Based BWM 181
Configuring Layer 4 SLB: Remote URL General settings on Alteon 180 or AD series 182
Configuring Layer 4 SLB: Remote URL Destination Port on Alteon 180 or AD series 183
Configuring Layer 4 Global SLB 184
Configuring Layer 4 Global SLB: General 185
Configuring Layer 4 Global SLB: Remote Sites 188
Configuring Layer 4 Global SLB: Lookups 189
Configuring Layer 4 Global SLB: Network Lookups 190
Configuring Layer 4 Global SLB: Network Preferences 191
Configuring Layer 4 Global SLB: Rules 192
Configuring Layer 4 Global SLB: Rules Metric 193
Configuring Layer 4: WAP 194
Configuring Layer 4: WAP General Properties 195
Configuring Layer 7 on the Switch 197
Configuring Layer 7 URL Parsing: Expressions on Alteon 180 or AD series 198
Configuring Layer 7 URL Parsing: WCR Redirect 199
Configuring Layer 7 URL Parsing: SLB Strings 201
Configuring Layer 7 URL Parsing: HTTP Methods 203
Configuring Virtual Routing 204
Configuring Virtual Routing: General 205

Configuring Virtual Routing: Routers 207
Configuring Virtual Routing: Interfaces 209
Configuring Virtual Routing: Groups 210
Configuring Virtual Routing: VIR Group 212
Configuring Virtual Routing: Synchronizing to a Peer Switch 214
Configuring Virtual Routing: Peers 215
Configuring Bandwidth Management 216
Configuring General Bandwidth Management 217
Configuring BWM Policies on Alteon 180 or AD series 218
Configuring BWM Policies on Alteon Application Switches 220
Configuring BWM Contracts 222
Configuring BWM Contracts: Time Policies 224
Configuring BWM Contract Group 225
Configuring SNMP version 3 226
Configuring SNMPv3: User-based Security Model Table 227
Configuring SNMPv3: View-based Access Control Model Table: Group Membership 228
Configuring SNMPv3: View-based Access Control Model Table: Group Access Right 229
Configuring SNMPv3: View-based Access Control Model Table: MIB View 230
Configuring SNMPv3: Community Table 231
Configuring SNMPv3: Target Table 232
Configuring SNMPv3: Target Params Table 233
Configuring SNMPv3: Notify Table 234
Configuring Ports 235
Configuring General Properties for Ports 236
Configuring Port Properties 237
Configuring Spanning Tree Protocol on Ports 239
Configuring Filtering on Ports 240
Configuring Filter Membership on Ports 241
Monitoring Summary 244
Switch Summary View 245
Switch Summary View 248
GUI Front Panel View 250
Monitoring the switch 251
Monitoring Simple Network Management Protocol (SNMP) 252
Monitoring Web OS Statistics on Alteon 180 or AD series 254
Monitoring Alteon OS Statistics on ALO and on Alteon Application Switches 255

Monitoring Switch MP CPU Stats on ALO and on Alteon 180 or AD series 256
Monitoring Switch MP CPU Stats on Alteon Application Switches 257
Monitoring MP Memory Statistics 258
Monitoring SP CPU Statistics on Alteon Application Switches 259
Monitoring SP Maintenance on Alteon Application Switches 260
Monitoring SP Maintenance Received on Alteon Application Switches 261
Monitoring SP Maintenance Send on Alteon Application Switches 262
Monitoring the Management Port on Alteon Application Switches 263
Monitoring SONMP 264
Monitoring Aggregated Ports 265
Monitoring Link Aggregation Information 266
Monitoring Link Aggregation Control Protocol Ports 267
Monitoring NTP 268
Monitoring Spanning Tree Group Information 269
Monitoring Bridge 270
Monitoring Bridge: Forwarding Database on ALO and on Alteon 180 or AD series 271
Monitoring Bridge: Forwarding Database on Alteon Application Switches 272
Monitoring Bridge: Forwarding Statistics on Alteon Application Switches 273
Monitoring Bridge: Base Ports 274
Monitoring Bridge: Base Ports on Alteon Application Switches 275
Monitoring Bridge: TP Ports 276
Monitoring Security 277
Monitoring Security: Port Denial of Service 278
Monitoring Security: Pattern Match Group 279
Monitoring Security: UDB Blast 280
Monitoring Security: IP ACL 281
Monitoring IP 282
Monitoring IP: Routes 283
Monitoring IP: Routes on ALO and on Alteon 180 or AD series 284
Monitoring IP: Routes on Alteon Application Switches 285
Monitoring IP: Routes - Standard 286
Monitoring IP: Route Statistics 287
Monitoring IP: Address Resolution Protocol (ARP) 288
Monitoring IP: ARP Statistics 289
Monitoring IP: Interfaces 290
Monitoring IP: Interface Statistics 291

Monitoring IP: IP Addresses 293
Monitoring IP: TCP 294
Monitoring IP: TCP Connection 295
Monitoring IP: UDP 296
Monitoring IP: UDP Local 297
Monitoring IP: Switch IP Properties on Alteon 180 or AD series 298
Monitoring IP: Switch IP Properties on Alteon Application Switches 300
Monitoring IP: ICMP In 302
Monitoring IP: ICMP Out 303
Monitoring IP: Routing Information Protocol (RIP) 304
Monitoring IP: Gateways 305
Monitoring OSPF 306
Monitoring OSPF: Administrative Status 307
Monitoring OSPF: Area 308
Monitoring OSPF: Area Nbr on Alteon 180 or AD series 309
Monitoring OSPF: Area Nbr on Alteon Application Switches 310
Monitoring OSPF: Area Interface 311
Monitoring OSPF: Interface Transmissions 312
Monitoring OSPF: Interface Nbr 313
Monitoring OSPF: Interfaces 314
Monitoring OSPF: Stats on Alteon 180 or AD series 315
Monitoring OSPF: Stats on Alteon Application Switches 318
Monitoring OSPF: Stats 2 321
Monitoring OSPF: Area Information 322
Monitoring OSPF: Interface Information 323
Monitoring OSPF: Link-State DB 324
Monitoring OSPF: External Link-State DB 325
Monitoring OSPF: Area Receive Error Statistics on Alteon Application Switches . 326
Monitoring OSPF: Area Interface Receive Error Statistics on Alteon Application Switches 327
Monitoring OSPF: Neighbor Interface 328
Monitoring BGP 329
Monitoring BGP: Administration on Alteon Application Switches 330
Monitoring BGP: Peers Summary on Alteon Application Switches 331
Monitoring Layer 4 333
SLB Summary View 335

Monitoring Layer 4 Filters: Statistics 338
Monitoring Layer 4 Filters: Rate Limit 339
Monitoring Layer 4 Filters: SP Filters on Alteon Application Switches 341
Monitoring Layer 4 SLB: Real Servers 342
Monitoring Layer 4 SLB: Real Servers by SP 343
Monitoring Layer 4 SLB: Groups 344
Monitoring Layer 4 SLB: Virtual Servers 345
Monitoring Layer 4 SLB: Real Servers State 346
Monitoring Layer 4 SLB: FTP on Alteon 180 or AD series 347
Monitoring Layer 4 SLB: FTP on Alteon Application Switches 348
Monitoring Layer 4 SLB: DNS on Alteon 180/AD series 349
Monitoring Layer 4 SLB: DNS on Alteon Application Switches 350
Monitoring Layer 4 SLB: Stats on Alteon 180 or AD series 351
Monitoring Layer 4 SLB: Stats on Alteon Application Switches 352
Monitoring Layer 4 SLB: SP Maintenance on Alteon Application Switches 354
Monitoring Layer 4 SLB: SSL Statistics on Alteon Application Switches 357
Monitoring Layer 4 SLB: Virtual Server Service Status on Alteon Application Switches 358
Monitoring Layer 4 SLB: Virtual Server Service Statistics 359
Monitoring Layer 4 SLB: The Auxiliary Session Statistics on Alteon Application Switches 360
Monitoring Layer 4 SLB: The Auxiliary Session SP Statistics on Alteon Application Switches 361
Monitoring Layer 4 SLB: Sessions 362
Monitoring Layer 4 SLB: Formatted Sessions 364
Monitoring Layer 4 SLB: Session Filter Criteria 367
Monitoring Layer 4 SLB: SIP 368
Monitoring Layer 4: Global SLB: General 369
Monitoring Layer 4: Global SLB: Remote Real Servers on Alteon Application Switches 370
Monitoring Layer 4: Global SLB: Real Server Groups on Alteon Application Switches 371
Monitoring Layer 4: Global SLB: Virtual Servers on Alteon Application Switches . 372
Monitoring Layer 4: Global SLB: Remote Sites on Alteon Application Switches . . 373
Monitoring Layer 4: Global SLB: Remote Real Servers Information on Alteon Application Switches 374
Monitoring Layer 4: Global SLB: Virtual Server Information on Alteon Application Switches 375

Monitoring Layer 4: Global SLB: Remote Site Information on Alteon Application Switches 376
Monitoring Layer 4: Global SLB: Networks on Alteon Application Switches 377
Monitoring Layer 4: Global SLB: Rules on Alteon Application Switches 378
Monitoring Layer 4: Global SLB: Geographical Regions on Alteon Application Switches 379
Monitoring Layer 4: RTSP on Alteon 180 or AD series 380
Monitoring Layer 4: RTSP on Alteon Application Switches 381
Monitoring Layer 4 WAP: Add Sessions on Alteon 180 or AD series 382
Monitoring Layer 4 WAP: Add Sessions on Alteon Application Switches 383
Monitoring Layer 4: WAP: Delete Sessions on Alteon 180 or AD series 384
Monitoring Layer 4: WAP: Delete Sessions on Alteon Application Switches 385
Monitoring Layer 4: WAP: RADIUS Accounting on Alteon 180 or AD series 386
Monitoring Layer 4: WAP: RADIUS Accounting on Alteon Application Switches . . 387
Monitoring Layer 4: Remote URL Buffers 388
Monitoring Layer 4: Remote URL Errors 389
Monitoring Layer 4: Remote URL Maintenance 390
Monitor: Layer 4: Remote URL Miscellaneous 391
Monitor: Layer 4: Remote URL Sessions 392
Monitoring Layer 4: Remote URL Tables 393
Monitoring Layer 7 394
Monitoring Layer 7: URL Parsing: WCR Redirect on Alteon 180 or AD series . . . 395
Monitoring Layer 7: URL Parsing: WCR Redirect on Alteon Application Switches 396
Monitoring Layer 7: URL Parsing: SLB Strings 397
Monitoring Layer 7: URL Parsing: Maintenance on Alteon 180 or AD series 398
Monitoring Layer 7: URL Parsing: Maintenance on Alteon Application Switches . 400
Monitoring Layer 7: URL Parsing: Parsing Information 402
Monitoring VRRP 403
Monitoring Virtual Routing: Statistics 404
Monitoring Virtual Routing: State 405
Monitoring Bandwidth Management 406
Monitoring BWM: Contracts 407
Monitoring BWM: Contracts Per Port 408
Monitoring BWM: Contract Rates on Alteon 180 or AD series 410
Monitoring BWM: Contract Rate Per Port on Alteon 180 or AD series 411
Monitoring SNMPv3 412

Monitoring SNMPv3: Statistics 413
Monitoring Ports 415
Monitoring Port: Interfaces 416
Monitoring Port: Ethernet Errors 418
Monitoring Port: Bridge 420
Monitoring Port: Load Balancing on ALO and on Alteon 180 or AD series 421
Monitoring Port: CPU Statistics on ALO and on Alteon 180 or AD series 422
Monitoring Port: Statistics 423

Configuring the Switch

The following main topics about switch configuration are covered in this manual:

- “Alteon: Properties” on page 14
- “Configuring the Switch” on page 16
- “Configuring the Bridge” on page 55
- “Configuring Virtual LANs” on page 63
- “Configuring Security” on page 65
- “Configuring IP Routing Protocols” on page 72
- “Configuring OSPF” on page 89
- “Configuring Border Gateway Protocol (BGP)” on page 111
- “Configuring Layer 4 on the Switch” on page 119
- “Configuring Server Load Balancing” on page 137
- “Configuring Layer 4 Global SLB” on page 184
- “Configuring Layer 4: WAP” on page 194
- “Configuring Layer 7 on the Switch” on page 197
- “Configuring Virtual Routing” on page 204
- “Configuring Bandwidth Management” on page 216
- “Configuring SNMP version 3” on page 226
- “Configuring Ports” on page 235

Alteon: Properties

This tab is used to configure the general switch properties.

Field	Description
Status Interval	Interval at which statistics and status information are gathered.
(If Traps, Status Interval secs)	If the Register for Traps box is checked, interval, in seconds, at which statistics and status information are gathered.
Hotswap Detect every intervals	The multiples of polling intervals between the hotswap checks.
Enable	**Note:** If checked, Alteon EMS will poll the switch according to the settings listed above the Enable box.

SNMP Information

Field	Description
Retry Count	The number of times Alteon EMS will retransmit any SNMP message before reporting a `timeout` message.
Timeout	Length of time between each retry of each SNMP waiting period, from 3 to 30 seconds. If you set the retry count to 2 and the time-out value to 5 seconds, Alteon EMS will report a `timeout` (no response from the switch) after 10 seconds.
Trace	If checked, Alteon EMS sends detailed SNMP information to the log.
Register for Traps	If checked, Alteon EMS will attempt to register the client's IP address to one of the trap hosts' IP fields. You only need to `apply` if the changes are new.
Listen for Traps	If checked, Alteon EMS will listen for traps and will attempt to hook to the trap port 162.
Max Traps in Log	The specified number of traps that may exist in the trap log between 1 to 10,000. The default is 500.
Trap Port	The number of the port on which trap messages will be captured. The default is 162.

General Information

Field	Description
Listen for Syslogs	If checked, Alteon EMS will listen for syslogs and will attempt to hook to the syslog port 514.
Confirm row deletion	If checked, Alteon EMS will request that you confirm that you wish to delete a row.
Synchronize VRRP Peers on Apply	If checked, the switch will synchronize the SLB, filter, and VRRP configuration on a peer switch on `Apply`. To take effect, peers must be configured on the switches and the administrator password on the switches must be identical.

Configuring the Switch

Use this menu to configure switch properties. For more information on using Alteon EMS to configure a switch, choose the **Help>Contents** menu.

- "Selection Dialog windows" on page 17
- "Enabling Special Software Features on the Switch" on page 18
- "Configuring General properties on Alteon 180 or AD series" on page 19
- "Configuring General properties on Alteon Application Switches" on page 21
- "Configuring the Management Port on Alteon Application Switches" on page 25
- "Configuring Software Images on the Switch" on page 27
- "Configuring a TFTP server" on page 28
- "Configuring Syslog" on page 30
- "Configuring Trap Hosts on Web OS 10.x and lower and Alteon OS 21.0 and lower" on page 32
- "Configuring Trap Hosts on Alteon Application Switches" on page 33
- "Configuring Syslog Traps" on page 34
- "Configuring a RADIUS Server" on page 35
- "Configuring TACACS+ Server" on page 36
- "Configuring Network Time Protocol" on page 38
- "Configuring Reboot" on page 39
- "Configuring SONMP" on page 40
- "Configuring Trunk Groups" on page 41
- "Configuring a Management Network" on page 43
- "Link Aggregation Control Protocol" on page 44
- "Link Aggregation Control Protocol Ports" on page 46
- "Aggregators" on page 47
- "Link Aggregation Control" on page 49
- "Configuring Port Mirroring" on page 53

NORTEL NETWORKS
216515-B, September 2004

Selection Dialog windows

A Selection Dialog window appears when you click on a **Browse...** button anywhere in EMS.



The highlighted row(s) represent the current selection. Some Selection Dialog windows allow more than one row to be selected. Select one or more rows in the table, then click the **Modify...** button.



To view a subset of the items listed in the table, click the **Filter Table Rows** button. For more information, see *Using Alteon Element Management System.*

Enabling Special Software Features on the Switch

The Global Server Load Balancing, Inbound Link Load Balancing, Security, and Bandwidth Management features in Web OS or Alteon OS, each require purchase of an additional software license and password key. Instructions for obtaining a password key are provided with your software license certificate.

Once you have obtained the proper Password Key to enable the Web OS or Alteon OS feature, follow these instructions:

1. Connect to the switch command line interface via Telnet or the console port, and login as the Administrator, following the directions in the *Web OS Command Reference* or *Alteon OS Command Reference*.
2. From the command line prompt, type the `/oper/swkey` command. You will be prompted to enter the Password Key at this time. If the key is correct for this MAC address, the switch will accept the password, permanently record it in the switch's non-volatile RAM (NVRAM), and will then enable the feature.
3. Please read the Alteon EMS Help and the Web OS or Alteon OS documentation to understand the software feature you just enabled.

Configuring General properties on Alteon 180 or AD series

This screen is used to set general properties of your Alteon 180 series or Alteon AD series Web switch running Web OS versions up to 10.1.

Field	Description
System Description	Displays the product name of the switch.
MAC Address	MAC address of the switch.
System Up Since	Displays the date and time when the switch was last booted.
System Name	The administrative-assigned name for the managed node. You may enter the name of the device in this field to show up in the tool tip.
Location	The physical location of the node, such as *telephone closet, 3rd floor.*
Contact	Information about the contact person for this managed node.
Current Date	Displays the date on the real time clock.
Current Time	Displays the time on the real time clock.
Switch HTTP Server Port	Sets the TCP port number that the switch uses for any HTTP traffic. The default is HTTP port 80. If Global Server Load Balancing is to be used, set this to a different port (such as 8080). **Note:** You can use the **Browse..**. button to view other TCP port numbers for the server to listen to. To select another port, click in either the name or port number, and use the Modify button.
Login Banner	Displays the user-defined login banner. When using the Command Line Interface, the message will be displayed whenever someone logs into the switch.
Port Mirroring State	Enables or disables the port mirroring state of the switch. The mirroring and monitoring ports are configured under the Mirror tab.
Management Network [1]	Sets the base source IP address that allows access to switch management through Telnet, SNMP, RIP, or the Web OS browser-based interface. A range of IP addresses is produced when used with Management Mask (below). Specify an IP address in dotted-decimal notation.
Management Mask [1]	This IP address mask is used with Management Network (above) to set a range of source IP addresses allowed access to switch management functions. Specify the mask in dotted-decimal notation.
Part Number	The hardware part number of the opened device.

Field	Description
Hardware Revision	The hardware revision. If the revision is not available, the field will be blank.
Power Supply Status	The status of the internal power supply.
Rear Left Sensor Temperature	The temperature of the rear left sensor in degrees Celsius.
Rear Middle Sensor Temperature	The temperature of the rear middle sensor in degrees Celsius.
Front Middle Sensor Temperature	The temperature of the front middle sensor in degrees Celsius.
Front Right Sensor Temperature	The temperature of the Front Right sensor in degrees Celsius.

1. This is applicable on Web OS 10.1 and lower and 9.x and higher.

Configuring General properties on Alteon Application Switches

Field	Description
System Description	Displays the product name of the switch.
MAC Address	MAC address of the switch.
System Up Since	Displays the date and time when the switch was last booted.
System Name	The administrative-assigned name for the managed node. You may enter the name of the device in this field to show up in the tool tip.
Location	The physical location of the node, such as *telephone closet, 3rd floor.*
Contact	Information about the contact person for this managed node.
Current Date	Displays the date on the real time clock.
Current Time	Displays the time on the real time clock.
Switch HTTP Server Port	Sets the TCP port number that the switch uses for any HTTP traffic. The default is HTTP port 80. If Global Server Load Balancing is to be used, set this to a different port (such as 8080). **Note:** You can use the **Browse...** button to view other TCP port numbers for the server to listen to. To select another port, click in either the name or port number, and use the Modify button.
Switch HTTPS Server Port [4]	Sets the TCP port number that the switch uses for any HTTPS traffic. The default is HTTP port 443. **Note:** You can use the **Browse...** button to view other TCP port numbers for the server to listen to. To select another port, click in either the name or port number, and use the Modify button.
Switch Telnet Server Port [1]	Sets the TCP port number that the switch uses for Telnet traffic. The default is HTTP port 23. **Note:** You can use the **Browse...** button to view other TCP port numbers for the server to listen to. To select another port, click in either the name or port number, and use the Modify button.
Login Banner	Displays the user-defined login banner. When using the Command Line Interface, the message will be displayed whenever someone logs into the switch.
Port Mirroring State	Enables or disables the port mirroring state of the switch. The mirroring and monitoring ports are configured under the Mirror tab.
Management Network [1]	Sets the base source IP address that allows access to switch management through Telnet, SNMP, RIP, or the Web OS browser-based interface. A range of IP addresses is produced when used with Management Mask (below). Specify an IP address in dotted-decimal notation.

Field	Description
Management Mask [1]	This IP address mask is used with Management Network (above) to set a range of source IP addresses allowed access to switch management functions. Specify the mask in dotted-decimal notation.
Hardware Order Number [4]	Displays the hardware order number of the switch.
Main Board Number [4]	Displays the hardware part number of the main board of the opened device.
Main Board Revision [4]	Displays the hardware revision number of the main board of the opened device.
Chassis Serial Number [4]	Displays the serial number of the chasis.
Chassis Revision Number [4]	Displays the revision number of the chasis.
Management Processor Board Part Number [4]	Displays the hardware part number of the management processor board of the opened device.
Management Processor Board Revision [4]	Displays the hardware revision number of the management processor board of the opened device. If the revision is not available, the field will be blank.
Ethernet Board Number [4]	Displays the part number of the Ethernet board of the opened device.
Ethernet Board Revision [4]	Displays the revision number of the Ethernet board hardware of the opened device.
Temperature Status	Displays the status of the temperature sensor: *ok* or *exceed*.
Fan Status	Displays the status of the fan: *ok* or *fail.*
Maximum Rate MP-Destined ARP Packets	Displays the maximum allowed rate for MP-destined ARP packets.
Maximum Rate MP-destined ICMP packet [2]	Displays the maximum allowed rate for MP-destined ICMP packets.
Maximum Rate MP-destined TCP packet [2]	Displays the maximum allowed rate for MP-destined TCP packets.
Maximum Rate MP-destined UDP packet [2]	Displays the maximum allowed rate for MP-destined UDP packets.

Field	Description
SSL Cluster Management IP Address [3]	The management IP address of SSL processor. You need to configure this IP address (using CLI) to match the Management IP address (MIP) of the SSL processor to establish an HTTPs link. You can use this HTTPs link to access the SSL processor through Web UI or EMS. See “Setting up SSL Processor” on page 23 for information on how to set up the SSL processor.
SSL Cluster Management Port [3]	The SSL cluster management port number. This is the access port of SSL processor. You need to configure this port to match the HTTPs server port of the SSL processor. Do not use port 443 as it will conflict with the SSL processor.
RTS on Internal Port [3]	Enables or disables RTS (Return to Sender) on the internal port. You need to use RTS rather than redirect filter so that the response from the real server goes back to the SSL processor, the origin of the request.

1. This is applicable on Alteon OS 21.0 and lower.
2. This is applicable only on Alteon Application Switches and Alteon OS 21.0 and higher.
3. This is applicable only on Alteon 2424-SSL.
4. This is applicable only on Alteon OS 22.0.1.0 and higher.

Setting up SSL Processor

You need to use the CLI to enable the Web UI HTTPs access on the SSL Processor by performing the following:

1. Using the command line interface (CLI), select the `ssl` option from the main menu.
2. Login as admin and enter the password (for example, admin).
3. Select `cfg -> sys -> cluster -> mip` from `SSL` main menu and configure the Management IP address.

To configure the port, perform the following:

1. Select `cfg -> sys -> adm -> https` from `SSL` main menu.
2. Type `ena` to enable the server.
3. Type `port` and enter the port number (for example, 8443).

You need to use EMS to match the `mip` on the switch with the `mip` on the SSL processor as described below:

1. Open EMS.
2. Open the 2424-SSL switch. 
3. Select `Switch -> Configure -> Switch -> General`
4. Configure the SSL cluster Management Port to match the HTTPs server port of the Alteon SSL Accelerator (ASA).
5. Configure the SSL cluster Management IP address to match the HTTPs server Management IP address.
6. On the menu bar, select Actions -> Open SSL Page... or by clicking on this button:

Configuring the Management Port on Alteon Application Switches

The management port is a Fast Ethernet port on the Alteon Application Switch that is used exclusively for managing the switch. While the switch can be managed from any network port, the management port conserves data ports that could otherwise be used for processing requests.

The management port is isolated and does not participate in the switching and routing protocols that run on the network ports. This port manages the switch using either Telnet (CLI), SNMP (EMS), HTTP (Web OS Browser-Based Interface), or HTTPS (in Alteon OS).

Note: Telnet and HTTP access to the management port must be configured in the CLI. For more management port configuration commands and options, see the *Alteon OS Command Reference*, version 20.Alteon OS0 or higher.

Field	Description
Management Port State	Enables or disables the management port. • If the management port is *enabled*, the default for performing all the non-console management of the switch is set for the network ports—but you can individually specify whether to allow certain network protocol requests from the switch, through the management port or the data ports. • If the management port is *disabled*, the network ports must be used for performing all switch management functions.
Management Port IP Address	The IP address of the management port. A static IP address is required for the port to be operational.
Management Port Mask	The subnet mask of the management port.
Management Port Broadcast [1]	The broadcast address of the management port.
Management Port Gateway	The default gateway for the management port.
Management Port Auto Negotiation	Set auto-negotiation for the management port: *on* or *off*.
Management Port Speed	Configure the speed of the management port: *mbs10*, *mbs100*, or *any*.
Management Port Mode	Set the Management port flow control mode: *full* duplex, *half* duplex, or *any*.

Field	Description
NTP Through Port	Specify whether to allow Network Time Protocol (NTP) access through the *data* or *management* port.
Radius Through Port	Specify whether to allow RADIUS server access through *data* or *management* port.
SMTP Through Port	Specify whether to allow Simple Mail Transfer Protocol (SNMP) through *data* or *management* port.
SNMP through Port	Specify whether to allow Simple Network Management Protocol (SNMP) trap host access through *data* or *management* port.
Syslog through Port	Specify whether to allow syslog host access through *data* or *management* port.
TFTP through Port	Specify whether to allow Trivial File Transfer Protocol (TFTP) operation should be performed through *data* or *management* port.
DNS through Port	Specify whether to allow DNS server access through *data* or *management* port. This feature is available only on Alteon Application switches running Alteon OS 20.1.1.0 and higher.
Gateway Health Check Interval [2]	Sets the interval between gateway ping attempts.
Gateway Retries [2]	Sets the number of failed ping attempts before a gateway is declared DOWN.

1. This is applicable on Alteon Application Switches and Alteon OS below 21.0.
2. This is applicable only on Alteon Application Switches and Alteon OS and higher.

Configuring Software Images on the Switch

Field	Description
Running Software Version	The version of the software image that is currently running on the system.
Enabled Software Features	The enabled software features, such as *SLB, BWM, GSLB, WCR*, and so on.
Boot Code Version	The version of the boot code: *major.minor.bugfix.patch*.
Image1 Software Version	The version of the software image stored in image 1: *major.minor.bugfix.patch*. If there is no image, or if information is not valid, the field will be blank.
Image2 Software Version	The version of the software image stored in image 2: *major.minor.bugfix.patch*. If there is no image, or if information is not valid, the field will be blank.
Image For Next Reset	Choose the software image to boot for the next reset: *image1* or *image2*.
Configuration For Next Reset	Choose the configuration information to load for the next reset: *active*, *backup*, or *default*.
Use BOOTP	Enables or disables retrieving IP configuration through the Bootstrap Protocol.
Apply Pending	Indicates that apply action is necessary or that the configuration has been changed.
Save Pending	Indicates if an action listed in *Apply Pending* needs to be saved.
SNMP Free Resources Timeout [1]	The SNMP Free Resources Timeout indicates the number of minutes before the resources are freed and the state is set back to *idle*. Once SNMP operations that use the state machine are finished, the resources used by these operations need to be freed by setting the state back to *idle* so that other commands can be issued via SNMP. One such operation would be an SNMP *apply*. This setting normally would not require modification unless you are using a MIB browser or performing debugging operations that might require a shorter or longer timeout period for SNMP operations.

1. This field is applicable only on Alteon OS.

Configuring a TFTP server

Field	Description
TFTP Server	Enter the domain name or IP address of the TFTP server.
Configuration File Name	Defines the configuration file name. This text field is editable after selecting *get-configuration* or *put-configuration* as the Action.
Dump File Name	Defines the name of that file to store core dump. This text field is editable after selecting *put-dump* as the Action.
Image File Name	Defines the image file to download. This text field is editable after selecting *get-image* as the Action.
Image	Selects the image to download to the file: *image1*, or *image2*. This field is enabled after selecting *img-get Action*.
Action	Selects the desired TFTP *GET* or *PUT* action. *get-image:* Downloads the specified image file, *Image File Name*, from the TFTP server. *get-configuration:* Downloads switch configuration from a specified file, *Configuration File Name*, from the TFTP server. *put-configuration:* Uploads the active switch configuration to the specified file, *Configuration File Name*, on the TFTP server. *put-dump:* Downloads switch core dump to a specified file, *Dump File Name*, on the TFTP server. *put-bkupdump:* Downloads switch backup core dump to a specified file, *Dump File Name*, on the TFTP server. [1] *put-image:* Uploads specified switch image to a specified file, *Image File Name*, from the TFTP server. [1]
TFTP Through Port [1]	Allows you to choose between data or management port for TFTP.
Transfer Status	The transfer status of the selected *Action*.
Local TFTP Server [2]	This box displays the status of the TFTP server.
Local TFTP Server is: [2]	 Displays if local TFTP server is running or not. You can start the TFTP server using this button.
Start TFTP Server When EMS Starts [2]	Check this box if you want to start TFTP server when EMS starts.
TFTP Server File System Root [2]	Displays where the TFTP server's root system file resides.

1. This is applicable only to Alteon OS 22.0.1.0 and higher.

NORTEL NETWORKS
216515-B, September 2004

2. This is only applicable on Microsoft Windows.

Configuring Syslog

This tab is used to configure where syslog messages are sent, and the level of severity of the syslog messages to be sent.

Field	Description
1st Syslog Host IP Address	Enter the IP address of the first Syslog host. The Syslog host is where syslog messages are to be sent.
2nd Syslog Host IP Address	Enter the IP address of the first Syslog host. The Syslog host is where syslog messages are to be sent.
1st Syslog Host Facility [1]	Syslog Facility: Messages are dumped from the 1st Syslog Host to the selected bucket: local0 to local7.
2nd Syslog Host Facility [1]	Syslog Second Facility: Messages are dumped from the 2nd Syslog Host to the selected bucket: local0 to local7.
1st Syslog Host Severity	This option sets the severity level of the first syslog host displayed. The default is 7, which means log all the seven severity levels. For a detailed description of the seven levels of severity, see "Seven Levels of Severity" on page 30. **Note:** The severity levels of the 1st Syslog Host are separate from those of the 2nd Syslog Host.
2nd Syslog Host Severity	This option sets the severity level of the second syslog host displayed. The default is 7, which means, log all the seven severity levels. For a detailed description of the seven levels of severity, see "Seven Levels of Severity" on page 30. **Note:** The severity levels of the 2nd Syslog Host are separate from those of the 1st Syslog Host.
Console Output	Enables or disables the output of syslog messages to the console. When necessary, disabling console output ensures that the switch is not affected by syslog messages.

1. This is not applicable on Alteon Link Optimizer (ALO) and on Alteon Web OS 10.0.x and lower.

Seven Levels of Severity

Following is the description of the seven levels of severity:

0: Emergency. This means that the system is unusable.

1: Alert. This means that action must be taken immediately.

2: Critical. This means the condition of the system is critical.

3: Error. This means that the system has errors.

4: Warning. This means that the system is giving a warning.

5: Notice. This means that the condition of the system is normal but with significant conditions that need attention.

6: Informational. This means that the system is working but giving out information about certain conditions.

7. Debug. This means that the system is giving out debug-level messages.

Configuring Trap Hosts on Web OS 10.x and lower and Alteon OS 21.0 and lower

Note: This feature is applicable only on Web OS 10.x and lower and Alteon OS 21.0 and lower.

Field	Description
Trap Host IP Address 1	Defines the IP address of the host that will receive SNMP traps.
Trap Host Community String 1	Defines the SNMP community string to use with the first trap host. The default is *public*.
Trap Host IP Address 2	Defines the IP address of the second trap host that will receive SNMP traps.
Trap Host Community String 2	Sets the SNMP community string to use with the second trap host. The default is *public*.
Send Authentication Traps	Enables or disables the switch to generate authentication failure traps.

Configuring Trap Hosts on Alteon Application Switches

Note: This feature is applicable only to Alteon OS 22.0 and higher.

Field	Description
Send Authentication Traps	Enables or disables the switch to generate authentication failure traps.
Trap Source Interface Number [1]	Defines the interface number for SNMP trap source interface. Using this field, you can select one of the configured interfaces as the source interface using the interface number.

1. This command is applicable only to SNMPv1 traps because only the SNMPv1 trap packet contains the source IP address. The SNMPv2 and SNMPv3 packets do not contain the source IP address.

Configuring Syslog Traps

This tab is used to enable or disable syslog messages and SNMP traps on a per-feature basis.

Field	Description
Console	Enables or disables logging of messages to the console.
System	Enables or disables system level alerts.
Management	Enables or disables management (flash, config, login) alerts.
CLI	Enables or disables CLI generated error messages.
Spanning Tree	Enables or disables spanning tree-related alerts.
VLAN	Enables or disables VLAN-related alerts.
Server Load Balancing	Enables or disables SLB-related alerts.
Global Server Load Balancing	Enables or disables GSLB-related alerts.
Filter	Enables or disables filters-related alerts.
SSH/Radius	Enables or disables SSH, RADIUS-related alerts.
VRRP	Enables or disables VRRP-related alerts.
BGP	Enables or disables BGP-related alerts.
NTP	Enables or disables NTP-related alerts.
ISD	Enables or disables ISD-related alerts. **Note:** Available on Alteon 180 or AD series only.
IP	Enables or disables IP-related alerts.
Web UI	Enables or disables Web OS Browser-Based Interface-related alerts.
Syn Attack Detection	Enables or disables Syn Attack Detection-related alerts.
TCP Rate Limiting	Enables or disables TCP rate limiting-related alerts.
OSPF [1]	Enables or disables the OSPF-related alerts.

1. This feature is available only on Alteon Application Switches running Alteon OS 20.0 and higher.

Configuring a RADIUS Server

Field	Description
Primary RADIUS Server IP Address	Sets the IP address for the primary Remote Authentication Dial-In User Service (RADIUS) server.
Secondary RADIUS Server IP Address [1]	Sets the IP address for the secondary RADIUS server.
Port	Sets the user-configurable RADIUS application port. The default is RADIUS port number 1,645.
Timeout	Sets the time-out in seconds.
Retries	Sets the number of retries to the RADIUS server before timing out.
RADIUS Authentication	Enables or disables RADIUS authentication.
Secret	This is the shared secret password between the switch and the primary RADIUS server(s).
Second Secret [1]	This is the shared secret password between the switch and the secondary RADIUS server(s).
RADIUS Telnet Backdoor	Enables or disables access through the RADIUS backdoor. enable allows console access disable allows telnet access.

1. This is applicable only on Alteon OS 22.0.1.0 and higher.

Configuring TACACS+ Server

TACACS (Terminal Access Controller Access Control System) is an authentication protocol that allows a remote access server to forward a user's logon password to an authentication server to determine whether access can be allowed to a given system. TACACS is an encryption protocol and therefore less secure than TACACS+ and Remote Authentication Dial-In User Service (RADIUS) protocols. (Both TACACS and TACACS+ are described in Request for Comments 1492.)

TACACS+ protocol is seen as more reliable than RADIUS as TACACS+ uses the Transmission Control Protocol (TCP) whereas RADIUS uses the User Datagram Protocol (UDP). Also, RADIUS combines authentication and authorization in a user profile, whereas TACACS+ separates the two operations.

TACACS+ protocol has been implemented on Alteon EMS to support the customers that have Cisco's TACACS+ protocol as their network security feature. Apart from that, TACACS+ offers the following advantages over RADIUS as the authentication device:

- TACACS+ is TCP-based so it facilitates connection-oriented traffic.
- It supports full-packet encryption as against password-only in authentication requests.
- Supports decoupled authentication, authorization, and accounting.

Note: This feature is applicable only to Alteon OS 22.0 and higher.

Field	Description
TACACS+ Server Access	Allows you to choose port over data or management for TACACS+ traffic.
Primary Server	Defines the primary TACACS+ server address.
Secondary Server	Defines the secondary TACACS+ server address.
Port	Enter the number of the TCP port to be configured.
Timeout	Sets the amount of time, in seconds, before a TACACS+ server authentication attempt is considered to have failed.
Retries	Sets the number of failed authentication requests before switching to a different TACACS+ server.
State	Enables or disables the TACACS+ server.

Field	Description
Authentication	This is the shared password between the switch and the primary TACACS+ server(s).
Second Authentication	This is the shared password between the switch and the secondary TACACS+ server(s).
Telnet	Enables or disables the TACACS+ back door for telnet. Telnet also applies to SSH/SCP connections.

Configuring Network Time Protocol

Field	Description
NTP Service	Enables or disables the Network Time Protocol (NTP) switch.
Primary NTP Server IP Address	Sets the IP address of the primary NTP server.
Secondary NTP Server IP Address [1]	Sets the IP address of the secondary NTP server.
Server Resync Interval	Specifies how often to resynchronize the switch clock with the NTP server:
Server Timezone Offset from GMT [2]	The NTP Server timezone offset from GMT. The range is +12 hours to -12 hours.
Server Timezone Offset from GMT as (+/-)HH:MM [3]	The NTP Server timezone offset from Greenwich Mean Time (GMT) as (+/-)HH:MM. Only settings within the range of +12:59 and -12:59 are accepted. **Note:** You can use the spinner arrows to move the time settings up or down.
Daylight Savings Time	Enables or disables daylight savings time for the system clock.

1. This is applicable only to Alteon OS and higher.
2. This field is applicable only to Web OS or Alteon 2000 series 21.0 and lower.
3. This field is applicable only on Alteon OS 21.0 and higher.

Configuring Reboot

This feature allows the switch administrator to schedule a reboot to occur at a particular time in future. This feature is particularly helpful if the user needs to perform switch upgrades during off-peak hours. You can set the reboot time, cancel a previously scheduled reboot, and check the time of the currently set reboot schedule.



You can click on the **Cancel Reboot** button to cancel the currently set reboot schedule and reset the switch with the original settings.

Field	Description
Weekday	Defines the day of the week for the reboot to take place.
Hour	Sets time in terms of the hour of the day or night.
Minute	Sets time in terms of minute of the day or night.
Next Scheduled Reboot time	Defines the time for the next scheduled reboot of the switch.
Current Date	Displays the current date.
Current Time	Displays the current time.

Note: This feature is applicable only on Alteon OS 21.0 and higher.

Configuring SONMP

SynOptics Network Management Protocol (SONMP) is a proprietary network management protocol that is used by Nortel Networks Optivitiy Switch Manager (OSM) to discover Alteon Application Switches on the network. The following commands add support for the Ethernet Autotopology algorithm and the Bay Topology MIB. The topology algorithm is executed by each Alteon switch on which SONMP is enabled.

Field	Description
IP Address	The IP address of the agent that fills the IP address field of the transmitted SONMP packets.
Topology Status	Indicates the status of the agent participating in multi-segment topology as on or off.
Last known Topology Change	Indicates the last time the entry in the NMM table was added, deleted or modified. If the NMM topology table has not been changed since cold/warm start of the agent, then the value is zero.
Maximum Topology Entries	The maximum number of entries in the NMM topology table.
Topology Count	The current number of entries in the NMM topology table.
SONMP Source Interface	Indicates the IP address to be used in the hello packets. If the interface specified by this command is not up, then the first interface which is up and running is used in the hello packets.
SONMP Hello Address	Sets default IP address for SONMP hello packets. When this option is set to mgmt then the Management Port IP address is used in the SONMP hello packets transmitted by the switch. But if it is set to data, then the IP address of the data port interface specified by the source interface is used in the hello packets.

Note: This feature is applicable only on Alteon OS 21.0 and higher.

Configuring Trunk Groups

Trunk groups can provide super-bandwidth, multi-link connections between Alteon switches or other trunk-capable devices. A trunk group is a group of ports that act together, combining their bandwidth to create a single, larger virtual link. The number of trunk groups and ports per trunk group depends on your switch model and Alteon OS or Web OS software version. For details, see your *Application Guide*.

To create a trunk group:

1. Define a trunk group on the first switch and press the Insert button.
2. Assign ports to the trunk group. Click on the Add port button. This button allows you to add and remove ports to and from the selected trunk group. This selection will bring up the port selection browser where you can select ports for the trunk group.
3. Choose Enable in the **State** drop-down combo box.
4. Repeat steps 1-3 on the second switch. Make sure that trunk groups consist of the expected ports and that each port is in the expected state.

The following restrictions apply:

- Any physical switch port can belong to only one trunk group.
- Best performance is achieved when all ports in any given trunk group are configured for the same speed.
- Trunking from non-Alteon devices must comply with Cisco® EtherChannel® technology.



You can add ports to the trunk groups by using this button.

Field	Description
Trunk Group	The number of the trunk group.
Ports	The physical ports in the trunk group.

Field	Description
State	Enables or disables the trunk group.
Default BWM Contract [1]	Sets the Bandwidth Management (BWM) contract number that is assigned to this trunk group. Only one contract can be assigned to this trunk group. **Note:** To select another BWM contract for this port, select the **Browse..**. button. Select any one of the BWM contracts that appear in the list, then Select the Modify button. The BWM Contract will now display the new selection.

1. This is feature not applicable if Bandwidth Management has not been activated on the switch.

Configuring a Management Network

This table is used to define IP address ranges which are allowed to access the switch for management purposes using both the data and management ports. You can configure up to five management networks.

Field	Description
Index	The index for the Management Network.
IP Address	The IP address for the Management Network.
IP Mask	The IP Mask for the Management Network.

Note: This feature is not applicable to Web OS 10.0.x or below.

Link Aggregation Control Protocol

Alteon OS and higher supports IEEE 802.3ad standard on the Alteon EMS. At the core of the 802.3ad standard is Link Aggregation Control Protocol (LACP). This protocol allows the user to group several physical ports into one logical port (LACP trunk group) with any switch that supports IEEE 802.3ad standard (LACP). You can configure the trunk groups manually called the static trunks as well as you can configure trunk group using the IEEE 802.3ad standard called the LACP trunks. The maximum number of configurable trunk groups are 40:12 user configurable trunks and 28 LACP trunks. The maximum number of active physical ports in any trunk group is eight. If more than the maximum eight ports are configured in the LACP trunk, they will be put in the standby state to replace any ports that fail. The maximum number of standby ports is eight.

The 802.3ad standard allows standard Ethernet links to form a single Layer 2 link using the Link Aggregation Control Protocol (LACP). Link aggregation is a method of grouping physical link segments of the same media type and speed, and treating them as if they were part of a single, logical link segment. If a link in a LACP trunk group fails, traffic is reassigned dynamically to the remaining links of the LACP trunk group.

Note: Refer to IEEE 802.3ad-2000 for a detailed information about the standard.

LACP automatically determines which member links can be aggregated and then aggregates them. It provides for the controlled addition and removal of physical links for the link aggregation.

Each external port in the Alteon EMS can have one of the following LACP modes.

off (default)

The user can configure this port in to a regular static trunk group. When the system initializes, all ports are in `off` mode by default.

active

The port is capable of forming an LACP trunk. This port initiates negotiation with the partner system port by sending LACP packets.

passive

The port is capable of forming an LACP trunk. This port only responds to the negotiation requests sent from an LACP `active` port.

Each LACP `active` or `passive` port needs an admin key, an operational key, and an aggregator for LACP to start negotiation on these ports. You need to assign the same admin key to a group of ports to make them aggregatable. Link Aggregation ID (LAG ID) is generated internally based on the operational key. All the aggregatable ports must have the same LAG ID. You can form an active LACP trunk group with all the ports that have the same LAG ID.

Note: All ports are in `off` mode by default.

Field	Description
Actor System Priority	Defines the priority value (1 through 65535) for the Alteon EMS. Lower numbers provide higher priority. The default value is 32768.
LACPDU Timeout	Defines the timeout period before invalidating LACP data from a remote partner. You can choose between short (3 seconds) or long (90 seconds) timeout periods.
Link Aggregation Last Changed	The last time the Link Aggregation configuration was changed.

Link Aggregation Control Protocol Ports

You can configure Link Aggregation Control Protocol (LACP) on a selected port in Alteon OS and higher.

Field	Description
Port	The port number.
Mode	The ports can be in the following modes: **`off:`** Using this option, you can turn LACP off for this port. You can use this port to manually configure a static trunk. All ports are in `off` mode by default. **`active:`** Using this option, you can turn LACP on and set this port to `active`. Only active ports initiate negotiation with the partner system port by sending the LACP packets. **`passive:`** Using this option, you can turn LACP on and set this port to `passive` mode. Passive ports do not initiate negotiation, but only respond to the negotiation requests from active ports.
Port Priority	Sets the priority value for the selected port between 1-65535. Lower numbers provide higher priority. The default value is 128.
Actor Administrative Key	Sets the admin key for this port between 1-255. Only ports with the same `admin` key and `oper` key (operational state) can form an LACP trunk group.

Aggregators

This feature is applicable only on Alteon OS and higher.

Field	Description
Selected Aggregator	The unique identifier allocated to this Aggregator by the local System. This attribute identifies an Aggregator instance among the subordinate managed objects of the containing object. This value is read-only.
MAC Address	A 6-octet read-write MAC address value used as a unique identifier for the System that contains this Aggregator.
Actor System Priority	A 2-octet read-write value indicating the priority value associated with the Actor's System ID.
Actor System ID	A 6-octet read-write MAC address value used as a unique identifier for the System that contains this Aggregator. **Note:** From the perspective of the Link Aggregation mechanisms, only a single combination of Actor's System ID and System Priority are considered, and no distinction is made between the values of these parameters for an Aggregator and the port(s) that are associated with it; that is, the protocol is described in terms of the operation of aggregation within a single System. However, the managed objects provided for the Aggregator and the port both allow management of these parameters. The result of this is to permit a single piece of equipment to be configured by management to contain more than one System from the point of view of the operation of Link Aggregation. This may be of particular use in the configuration of equipment that has limited aggregation capability.
Is Aggregate?	A read-only Boolean value indicating whether the Aggregator represents an Aggregate ('TRUE') or an Individual link ('FALSE').
Actor Administrative Key	The current administrative value of the Key for the Aggregator. This is a 16-bit, read-write value. The meaning of particular Key values is of local significance.
Actor Operational Key	The current operational value of the Key for the Aggregator. This is a 16-bit read-only value. The meaning of particular Key values is of local significance.
Partner System Priority	A 2-octet read-only value that indicates the priority value associated with the Partner's System ID. If the aggregation is manually configured, this System Priority value will be a value assigned by the local System.

Field	Description
Partner System ID	A 6-octet read-only MAC address value consisting of the unique identifier for the current protocol Partner of this Aggregator. A value of zero indicates that there is no known Partner. If the aggregation is manually configured, this System ID value will be a value assigned by the local System.
Partner Operational Key	The current operational value of the Key for the Aggregator's current protocol Partner. This is a 16-bit read-only value. If the aggregation is manually configured, this Key value will be a value assigned by the local System.

Link Aggregation Control

This feature is applicable only on Alteon OS and higher.

Field	Description
Port	A list of the ports.
Actor System ID	A 6-octet read-only MAC address value that defines the value of the System ID for the System that contains this Aggregation Port.
Actor System Priority	A 2-octet read-write value used to define the priority value associated with the Actor's System ID.
Actor Administrative Key	The current administrative value of the Key for the Aggregation Port. This is a 16-bit read-write value. The meaning of particular Key value is of local significance.
Actor Operational Key	The current operational value of the Key for the Aggregation Port. This is a 16-bit read-only value. The meaning of particular Key value is of local significance.
Actor Port	The port number locally assigned to the Aggregation Port. The port number is communicated in LACPDUs as the `Actor_Port`. This value is read-only.
Actor Port Priority	The priority value assigned to this Aggregation Port. This 16-bit value is read-write.
Partner Administrative System Priority	A 2-octet read-write value used to define the administrative value of priority associated with the Partner's System ID. The assigned value is used, along with the value of `aAggPortPartnerAdminSystemID`, `aAggPortPartnerAdminKey`, `aAggPortPartnerAdminPort`, and `aAggPortPartnerAdminPortPriority`, in order to achieve manually configured aggregation.
Partner Operational System Priority	A 2-octet read-only value indicating the operational value of priority associated with the Partner's System ID. The value of this attribute may contain the manually configured value carried in `aAggPortPartnerAdminSystemPriority` if there is no protocol Partner.
Partner Administrative System ID	A 6-octet read-write `MACAddress` value representing the administrative value of the Aggregation Port's protocol Partner's System ID. The assigned value is used, along with the value of `aAggPortPartnerAdminSystemPriority`, `aAggPortPartnerAdminKey`, `aAggPortPartnerAdminPort`, and `aAggPortPartnerAdminPortPriority`, in order to achieve manually configured aggregation.

Field	Description
Partner Operational System ID	A 6-octet read-only MACAddress value representing the current value of the Aggregation Port's protocol Partner's System ID. A value of zero indicates that there is no known protocol Partner. The value of this attribute may contain the manually configured value carried in aAggPortPartnerAdminSystemID if there is no protocol Partner.
Partner Administrative Key	The current administrative value of the Key for the protocol Partner. This is a 16-bit read-write value. The assigned value is used, along with the value of aAggPortPartnerAdminSystemPriority, aAggPortPartnerAdminSystemID, aAggPortPartnerAdminPort, and aAggPortPartnerAdminPortPriority, in order to achieve manually configured aggregation.
Partner Operational Key	The current operational value of the Key for the protocol Partner. The value of this attribute may contain the manually configured value carried in aAggPortPartnerAdminKey if there is no protocol Partner. This is a 16-bit read-only value.
Partner Administrative Port	The current administrative value of the port number for the protocol Partner. This is a 16-bit read-write value. The assigned value is used, along with the value of aAggPortPartnerAdminSystemPriority, aAggPortPartnerAdminSystemID, aAggPortPartnerAdminKey, and aAggPortPartnerAdminPortPriority, in order to achieve manually configured aggregation.
Partner Administrative Port Priority	The current administrative value of the port priority for the protocol Partner. This is a 16-bit read-write value. The assigned value is used, along with the value of aAggPortPartnerAdminSystemPriority, aAggPortPartnerAdminSystemID, aAggPortPartnerAdminKey, and aAggPortPartnerAdminPort, in order to achieve manually configured aggregation.
Partner Operational Port	The operational port number assigned to this Aggregation Port by the Aggregation Port's protocol Partner. The value of this attribute may contain the manually configured value carried in aAggPortPartnerAdminPort if there is no protocol Partner. This 16-bit value is read-only.
Partner Operational Port Priority	The priority value assigned to this Aggregation Port by the Partner. The value of this attribute may contain the manually configured value carried in aAggPortPartnerAdminPortPriority if there is no protocol Partner. This 16-bit value is read-only.

Field	Description
Actor Administrative State	A string of 8 bits, corresponding to the administrative values of `Actor_State` as transmitted by the Actor in LACPDUs. The first bit corresponds to bit 0 of `Actor_State` (`LACP_Activity`), the second bit corresponds to bit 1 (`LACP_Timeout`), the third bit corresponds to bit 2 (Aggregation), the fourth bit corresponds to bit 3 (Synchronization), the fifth bit corresponds to bit 4 (Collecting), the sixth bit corresponds to bit 5 (Distributing), the seventh bit corresponds to bit 6 (Defaulted), and the eighth bit corresponds to bit 7 (Expired). These values allow administrative control over the values of `LACP_Activity`, `LACP_Timeout` and Aggregation. This attribute value is read-write.
Actor Operational State	A string of 8 bits, corresponding to the current operational values of Actor_State as transmitted by the Actor in LACPDUs. This attribute value is read-only.
Partner Administrative State	A string of 8 bits, corresponding to the current administrative value of Actor_State for the protocol Partner. This attribute value is read-write. The assigned value is used in order to achieve manually configured aggregation.
Partner Operational State	A string of 8 bits, corresponding to the current values of Actor_State in the most recently received LACPDU transmitted by the protocol Partner. In the absence of an active protocol Partner, this value may reflect the manually configured value `aAggPortPartnerAdminState`. This attribute value is read-only.
Is Port Aggregate?	A read-only Boolean value indicating whether the Aggregation Port is able to Aggregate (TRUE) or is only able to operate as an Individual link (FALSE).
Selected Aggregator ID	The identifier value of the Aggregator that this Aggregation Port has currently selected. Zero indicates that the Aggregation Port has not selected an Aggregator, either because it is in the process of detaching from an Aggregator or because there is no suitable Aggregator available for it to select. This value is read-only.
Attached Aggregator ID	The identifier value of the Aggregator that this Aggregation Port is currently attached to. Zero indicates that the Aggregation Port is not currently attached to an Aggregator. This value is read-only.

Configuring Port Mirroring on Alteon 180 or AD series running Web OS 9.0.34 or lower

The Port Mirroring Menu is used to configure, enable, and disable the monitored port. When port mirroring is enabled, network packets being sent and/or received on a target port are duplicated and sent to a monitor port. You can attach a network analyzer to the monitor port to collect detailed information about your network performance and usage.

Note: This port mirroring menu is for switches running Web OS 9.0.34 and lower.

Field	Description
State	Enables or disables port mirroring.
Timeout	Sets the time-out period to disable port mirroring after not being used for the specified time.
Monitoring Port	The selected physical port for monitoring: Receives the duplicated packets delivered by the Mirrored Port.
Mirrored Port	Sets the selected physical port for mirroring: Packets received by or delivered from this port are delivered to the Monitoring Port.
Traffic Direction	This field allows you to specify the direction in which packets are received by the monitoring Port: • *in*: Packets received by the mirrored port. • *out*: Packets transmitted from the mirrored port. • *both*: Packets received by or transmitted from the mirrored port. It is necessary to specify the direction because: • If the source port of the frame matches the mirrored port and the mirrored direction is *in* or *both* (in and out), the frame is sent to the mirrored port. • If the destination port of the frame matches the mirrored port and the mirrored direction is *out*, or the frame is sent to the monitoring port.

Configuring Port Mirroring

This tab is used to configure Port Mirroring. You can enable or disable the port mirroring state in the General tab.

The Port Mirroring Menu is used to configure, enable, and disable the monitored port. When port mirroring is enabled, network packets being sent and/or received on a target port are duplicated and sent to a monitoring port. You can attach a network analyzer to the monitoring port to collect detailed information about your network performance and usage.

Note: This port mirroring menu is for switches running Web OS 10.0 and higher on Alteon 180 or AD series, and Alteon OS 20.0 and higher on Alteon Application Switches.

Note: For the VLAN columns in Alteon OS 21.0 and higher. If no VLAN is assigned, then all VLANs are used. But if the user assigns a VLAN it will only use the VLANs specified, even if new VLANs are created.

Note: A VLAN must contain the mirrored port in order to associate the VLAN to port mirroring.



This button allows you to add or remove VLANs to or from the selected ports to be mirrored.

Field	Description
Monitoring Port	The selected physical port for monitoring: Receives the duplicated packets delivered by the Mirrored Port. Select the **Browse..**. button to choose a port.
Mirrored Port	Sets the selected physical port for mirroring: Packets received by or delivered from this port are delivered to the Monitoring Port. Select the **Browse..**. button to choose a port.

Field	Description
Direction Mirrored	This field also allows you to enter the direction in which packets are received by the Monitoring Port. *in:* Packets are received by the mirrored port. *out:* Packets are transmitted from the mirrored port. *both:* Packets are received by or transmitted from the mirrored port. It is necessary to specify the direction because: • If the source port of the frame matches the mirrored port and the mirrored direction is *in* or *both (in* and out), the frame is sent to the mirrored port. • If the destination port of the frame matches the mirrored port and the mirrored direction is *out*, or the frame is sent to the monitoring port.
VLAN Range 1-2048 [1]	The VLANs associated to Port Mirroring.
VLAN Range 2049-4090 [1]	The VLANs associated to Port Mirroring.
VLANs [2]	The VLANs associated with Port Mirroring.

1. This is applicable only on Alteon OS 21.0 and lower.
2. This is applicable only on Alteon OS and higher.

Configuring the Bridge

The Bridge directory is used to configure Layer 2 properties on the switch.

Alteon OS supports the IEEE 802.1d Spanning Tree Protocol (STP). STP is used to prevent loops in the network topology.

Note: When VRRP is used for active/active redundancy, STP must be enabled.Spanning Tree bridge parameters affect the global Spanning Tree Protocol operation of the switch.

The following bridge configuration topics are covered in this section:

- "General Bridge Properties" on page 56
- "Configuring Spanning Tree Protocol on the Bridge" on page 57
- "Configuring STP Groups on the Bridge" on page 59
- "Configuring Spanning Tree Group Ports on the Bridge" on page 61
- "Configuring Spanning Tree Protocol on Individual Ports" on page 62

General Bridge Properties

For switches running Web OS 10.0 and higher, this menu applies to the Spanning Tree Group that has been selected in the **STP Group**. You can configure up to 16 Spanning Tree Groups. For Web OS versions 9.0.x and lower, this menu applies to the default Spanning Tree Group.

Note: The **STP group** is not applicable to Alteon OS 21.0 and higher.

Field	Description
MAC Address	The MAC address used by the bridge. **Note:** It is recommended that the bridge address be the numerically smallest MAC address of all ports that belong to the bridge. The only requirement is that the MAC Address be unique.
Bridge Port Count	The number of ports controlled by this bridging entity.
Type	Indicates the type of bridging this bridge can perform.
Total Learned Discards	The total number of Forwarding Database entries that have been discarded because of insufficient storage space in the Forwarding Database.If the counter increases, it indicates that the Forwarding Database is regularly becoming full, which can degrade the performance of the subnetwork. If Total Learned Discards shows a significant value but does not increase, it indicates the problem has occurred but is not persistent.
Nortel Multiple STG Mode [1]	Enables or disables Nortel Multiple Spanning Tree Group Mode.

1. This is applicable only on Alteon OS 21.0 and higher.

NORTEL NETWORKS
216515-B, September 2004

Configuring Spanning Tree Protocol on the Bridge

For switches running Web OS 10.0 and higher, you can configure up to 16 Spanning Tree Groups. This menu applies to the Spanning Tree Group that has been selected in the **STP Group.**

Note: The **STP group** is not applicable to Alteon OS 21.0 and higher.

Note: For Web OS versions 9.0.x and lower, this menu applies only to the default Spanning Tree Group.

Field	Description
Protocol Type	The current operating version of the Spanning Tree Protocol.
Priority	Configures the bridge priority. The bridge priority parameter controls which bridge on the network is the STP root bridge. To make this switch the root bridge, configure the bridge priority lower than all other switches and bridges on your network. The lower the value, the higher the bridge priority.
Last Topology Change	The time since a topology change was last detected by the bridge. Time is displayed in days:hours:minutes:seconds.
Total Topology Changes	Displays total number of topology changes that were detected by the bridge.
Root Identifier	The bridge identifier of the root of the spanning tree. **Note:** This value is used as the Root Identifier parameter in all the configuration bridge protocol data units (PDU) that were originated by this node.
Root Cost	The cost of the path to the root as seen from this bridge.
Root Port	The number of the port that offers the lowest cost path from this bridge to the root bridge.
Maximum Age	Configures the bridge maximum age. The maximum age parameter specifies the maximum time the bridge waits without receiving a configuration bridge protocol data unit before it re-configures the STP network.
Hello Interval	Configures the bridge hello time. The hello time specifies how often the root bridge transmits a configuration bridge protocol data unit (BPDU). Any bridge that is not the root bridge uses the root bridge hello value. **Note:** The value is entered into this field in units of 1/100 of a second. Therefore, the default value of 2 seconds is displayed in this field as 200. The time is measured when the bridge is the root of the spanning tree (or trying to become so).

Field	Description
Forwarding Delay	The time for a port to change its spanning state when moving towards the Forwarding state. Forwarding Delay determines how long the port stays in each of the Listening and Learning states that precede the Forwarding state.This value is also used for aging all dynamic entries in the Forwarding Database, after a topology change has been initiated.Forwarding Delay is displayed in units of 1/100 of a second. **Note:** The bridge uses this value, unless the bridge becomes the root. In that case, Forwarding Delay becomes the value that all bridges, including this one, will start using when this bridge becomes the root.
Root Maximum Age	Sets the Maximum bridge age. When this bridge is acting as the root, all bridges use Root Maximum Age for Maximum Age: 6 to 40 seconds. **Note:** The value is entered into this field in units of 1/100 of a second. Therefore, the default value of 20 seconds is displayed in this field as 2000. Maximum Age is an integer: an error may be returned if the input value is not a whole number.
Root Hello Interval	Sets the value that all bridges use for Hello Interval when this bridge is acting as the root: 1 to 10 seconds. **Note:** The value is entered into this field in units of 1/100 of a second. Therefore, the default value of 2 seconds is displayed in this field as 200. Hello Root Interval is an integer: an error may be returned if the input value is not a whole number.
Root Forwarding Delay	Sets the state change delay. When this bridge is acting as the root, all bridges use Root Forwarding Delay for Forwarding Delay: 4 to 30 seconds. **Note:** The value is entered into this field in units of 1/100 of a second. Therefore, the default value of 15 seconds is displayed in this field as 1500. Root Forwarding Delay is an integer: an error may be returned if the input value is not a whole number.
Aging Timeout (sec)	Sets the time-out period for aging out the dynamically learned forwarding information.
Hold Interval	The time value that determines the interval length during which no more than two Configuration bridge PDUs shall be transmitted by this node, in units of 1/100 of a second.

Configuring STP Groups on the Bridge

This menu allows you to set the Spanning Tree state to on or off, for all Spanning Tree Groups.



This button allows you to add or remove VLANs to or from the selected Spanning Tree Groups.



This button allows you to restore the state and bridge parameters of the selected Spanning Tree Groups to their default settings.

Field	Description
Index	The Spanning Tree Group (STG) index number.
State	The current state (on or off) of Spanning Tree Protocol for the Spanning Tree Group.
Priority [1]	Configures the bridge priority. The bridge priority parameter controls which bridge on the network is the STP root bridge. To make this switch the root bridge, configure the bridge priority lower than all other switches and bridges on your network. The lower the value, the higher the bridge priority. The range is 0 to 65535, and the default is 32768.
Hello Time [1]	Configures the bridge hello time.The hello time specifies how often the root bridge transmits a configuration bridge protocol data unit (BPDU). Any bridge that is not the root bridge uses the root bridge hello value. The range is 1 to 10 seconds, and the default is 2 seconds.
Forward Delay [1]	Configures the bridge forward delay parameter. The forward delay parameter specifies the amount of time that a bridge port has to wait before it changes from the listening state to the learning state and from the learning state to the forwarding state. The range is 4 to 30 seconds, and the default is 15 seconds.
Maximum age [1]	Configures the bridge maximum age. The maximum age parameter specifies the maximum time the bridge waits without receiving a configuration bridge protocol data unit before it re configures the STP network. The range is 6 to 40 seconds, and the default is 20 seconds.
Aging Time [1]	Configures the forwarding database aging time. The aging time specifies the amount of time the bridge waits without receiving a packet from a station before removing the station from the forwarding database. The range is 1 to 65535 seconds, and the default is 300 seconds. To disable aging, set this parameter to 0.

Field	Description
VLAN Range 1-2048 [2]	Displays the VLANs in the range 1 to 2048 for the Spanning Tree Group. Click on the VLANs... button and select one or more VLANS in the Selection dialog. **Note:** Only the default Spanning Tree Group (STG 1) may contain more than one VLAN. All other Spanning Tree Groups may contain only one VLAN each. If you select more than one VLAN for Spanning Tree Groups 2-16, an error message will appear when you attempt to apply the configuration.
VLAN Range 2049-4094 [2]	Displays the VLANs in the range 2049 to 4094 for the Spanning Tree Group. Click on the VLANs... button and select one or more VLANS in the Selection dialog. **Note:** Only the default Spanning Tree Group (STG 1) may contain more than one VLAN. All other Spanning Tree Groups may contain only one VLAN each. If you select more than one VLAN for Spanning Tree Groups 2-16, an error message will appear when you attempt to apply the configuration.
VLANs [3]	Displays the VLANs in the Spanning Tree Group.

1. This is applicable only on Alteon OS 21.0 and higher.
2. This is applicable only on Alteon OS 21.0 and lower.
3. This is applicable only on Alteon OS and higher.

Configuring Spanning Tree Group Ports on the Bridge

Field	Description
Group Index	The spanning tree group number.
Port	The port number that is associated with the Spanning Tree Group.
Port State	Shows the STP port state information as either on or off.
Priority [1]	Configures the bridge priority. The bridge priority parameter controls which bridge on the network is the STP root bridge. To make this switch the root bridge, configure the bridge priority lower than all other switches and bridges on your network. The lower the value, the higher the bridge priority. The range is 0 to 65535, and the default is 32768.
Path Cost [1]	The contribution of this port to the path cost of paths towards the spanning tree root which include this port. The port path cost parameter is used to help determine the designated port for a segment. Generally speaking, the faster the port, the lower the path cost. A setting of 0 indicates that the cost will be set to the appropriate default after the link speed has been auto negotiated.

1. This is applicable only on Alteon Application Switches and Alteon OS 21.0 and higher.

Configuring Spanning Tree Protocol on Individual Ports

Spanning Tree port parameters are used to modify STP operation on an individual port basis. The port option of STP is turned on by default.

This menu applies to the Spanning Tree Protocol group that has been selected in the **STP Group**. You can configure up to 16 Spanning Tree Groups.

Note: This section is not applicable to Alteon OS 21.0 and above.

Field	Description
Port	The port number.
Priority	The value of priority that determines which bridge is the root bridge. The port priority helps determine which bridge port becomes the designated port. In a network topology that has multiple bridge ports connected to a single segment, the port with the lowest port priority becomes the designated port for the segment.
State	The port's current state as defined by application of the Spanning Tree Protocol. This state controls what action a port takes on reception of a frame. If the bridge has detected a port that is malfunctioning it will place that port into the broken(6) state. For ports which are disabled, this object will have a value of disabled(1).
Status [1]	The port's current state: *enabled* or *disabled*.
Path Cost	The port path cost is used to help determine the designated port for a segment. Generally speaking, the faster the port, the lower the path cost. The default path cost is 10 for 100Mbps ports, and 1 for Gigabit ports. A value of 0 indicates that the default cost will be computed for an auto-negotiated link speed.
Root	The unique identifier of the bridge that is recorded as the root bridge in the configuration bridge protocol data units (BPDU). This field is read-only.
Root Cost	The cost of the path to the root as seen from this bridge. This field is read-only.
Bridge	The Bridge Identifier of the bridge that this port considers to be the Designated Bridge for this port's segment. This field is read-only.
Bridge Port	The Port Identifier of the port on the Designated Bridge for this port's segment. This field is read-only.
Learn-Forward Transitions	The number of times this port has transitioned from the Learning state to the Forwarding state. This field is read-only.

1. This is applicable only on Alteon Application Switches.

Configuring Virtual LANs

VLANs are commonly used to split up groups of network users into manageable broadcast domains, to create logical segmentation of workgroups, and to enforce security policies among logical segments.

The following VLAN topics are covered in this section:

- "Configuring VLAN Membership" on page 64

Configuring VLAN Membership

Note: All ports must belong to at least one VLAN. Any port which is removed from a VLAN and which is not a member of any other VLAN is automatically added to default VLAN #1. You cannot remove a port from VLAN #1 if the port has no membership in any other VLAN.
Also, you cannot add a port to more than one VLAN unless the port is configured for VLAN tagging (page 237).



This button allows you to add or remove ports to or from the selected VLANs.

Field	Description
VLAN	The VLAN identification number. The number can be set when a VLAN is Inserted or Modified.
Name	The VLAN name. The default is none except for the first VLAN name -- that default name is Default VLAN.
Ports	The ports in the VLAN. The default is *none* except for VLAN 1. By default, all ports belong to VLAN 1. Select the ports belonging to the VLAN group by pressing the Ports... button or double-clicking on the ports column in the table. This will open the port browser window.
State	Enables or disables a VLAN.
Spanning Tree Group	The Spanning Tree Group (STG) assigned to the VLAN. To choose an STG, double-click on the field. Then right-click to select Browse...
Jumbo Frames [1]	Enables or disables Jumbo frame support for the VLAN.
Source MAC Address Learning on VLAN [2]	Enables or disables source MAC Address Learning on the VLAN.
Default BWM Contract [2]	Displays the default Bandwidth Management (BWM) Contract for the VLAN. To choose a BWM contract, double-click on the field. Then right-click to select Browse...

1. This is applicable only on Alteon 180 or AD series and on ALO.
2. This is applicable only on Alteon OS 21.0 and higher.

Configuring Security

The following topics are discussed in this section:

- "Configuring Security: General" on page 66
- "Configuring Security: UDP Blast Defaults" on page 67
- "Configuring Security: UDP Blast" on page 68
- "Configuring Security: Pattern Match Group" on page 69
- "Configuring Security: Ports" on page 70
- "Configuring Security: IP ACL" on page 71

Note: You need to purchase the license/key from Nortel Networks to be able to apply the security configurations on your switch.

Note: The security feature is available only on Alteon OS 21.0 and higher.

Configuring Security: General

Field	Description
Rate Threshold for Logging	Displays the threshold for the number of packets per second.
Out of Order IP Fragments	Displays the filter set for out-of-order IP fragment packets during filtering. When set to allow, the switch will let through all the out-of-order fragments in filtering. When set to deny, the switch will drop these packets. The default is allow.

Configuring Security: UDP Blast Defaults

This tab defines the default packet rate limit for UDP blast protection.

Field	Description
UDP Default Packet Limit	Allows you to define the UDP Default packet limit. In Alteon OS 21.0 and above, the default packet limit is set at 512.

Configuring Security: UDP Blast

Malicious attacks over UDP protocol ports are becoming a common way to bring down the real servers. Alteon OS can be configured to restrict the amount of traffic allowed on any UDP port, thus ensuring that backend servers are not flooded with data and disabled.

Field	Description
Low Port	Sets the low UDP port range for UDP blast protection.
High Port	Sets the high UDP port range for UDP blast protection.
Packet Limit	Sets the packet rate limit per second. If the number of packets on this port range exceeds the maximum packet rate per second, UDP traffic will be dropped.

Configuring Security: Pattern Match Group

This feature provides the capability to scan ingressing packets for patterns contained in some well-known TCP or UDP attacks on backend servers. The switch can be configured with one or more filters that scan the first IP packet, and drop the packet if it finds one or all of the configured patterns. If no match is found, the packets will be allowed through.

When a virus or other attack contains multiple patterns or strings, it is useful to combine them into one group and give the group a name that is easy to remember. When a pattern group is applied to a deny filter, the switch will match any of the strings or patterns within that group before denying and dropping the packet. Up to five patterns can be combined into a single pattern group. Configure the binary or ASCII pattern strings, group them into a pattern group, name the pattern group, and then apply the group to a filter.



You can add pattern matching groups by selecting a binary or ASCII pattern using this button.

Field	Description
Pattern Matching Group	The index of the pattern matching group.
Name	Specifies a descriptive name for this pattern group.
Pattern Matching Rules	Adds binary or ASCII strings to a pattern matching group. Up to five patterns can be combined into a single pattern group.

Configuring Security: Ports

Alteon OS can protect switch ports against a variety of Denial of Service (DOS) attacks including Port Smurf, LandAttack, Fraggle, Nullscan, Xmascan, PortZero, and ScanSynFin. Enable DOS protection on ports connected to any network that could be the source of an attack.

Field	Description
Port	Displays Security features on this port.
Denial of Service Attack	Enables or disables Denial of Service (DOS) protection on this port.
IP ACL	Enables or disables IP Access Control List denial on this port.
UDP Blast	Enables or disables UDP blast protection on this port.

Configuring Security: IP ACL

Alteon OS can be configured with IP access control lists (ACLs) composed of ranges of client IP addresses that are to be denied access to the switch. When traffic ingresses the switch, the client source IP address is checked against this pool of addresses. If a match is found, then the client traffic is blocked.

ACLs vs. Filters

Access control lists (ACLs) are used to control which IP addresses are allowed access to a network. The decision about whether to deny traffic is based solely on whether or not a match is found between the client IP and the ACL. The IP access control list (ipacl) commands can be used to configure a pool of up to 5000 blockable IP addresses.

While filters can perform the same function by blocking IP addresses ranges, they contain more information besides source IP address which also must be matched on ingress traffic before determining whether to allow, deny, or redirect traffic.

How it works

The IP ACL feature uses a hash table to effectively block a configured range of IP addresses. The access control list is a global list which is by default disabled on the switch; and then enabled on a per-port basis.

When a packet ingresses a port that has been enabled with IP access control list processing, the switch compares the client source IP address with internal hash tables containing the IP addresses. If a match is found, the packet is dropped. If no match on the address is found in any of the hash tables, the packet is allowed to pass.

Field	Description
Index	The index of the IP Access Control List.
Address	The client source IP address that is to be compared with the Access Control List.
Mask	The client IP mask address.

Configuring IP Routing Protocols

In addition to switching traffic at near line rates, the Web switch can perform multi-protocol routing.

The following IP routing topics are covered in this section:

- "Configuring General IP settings" on page 73
- "Configuring IP Interfaces" on page 75
- "Configuring IP Gateways" on page 76
- "Configuring DNS" on page 77
- "Configuring the Local Route Cache" on page 78
- "Configuring Routing Information Protocol (RIP1)" on page 79
- "Configuring IP Forwarding on Ports" on page 81
- "Configuring IP Static Routes" on page 82
- "Configuring Route Maps on Alteon Application Switches" on page 83
- "Configuring the Route Map Access List on Alteon Application Switches" on page 85
- "Configuring IP Network Filters on Alteon Application Switches" on page 86
- "Configuring AS Paths on Alteon Application Switches" on page 87
- "Configuring Static ARP" on page 88

Configuring General IP settings

This tab is for configuring general IP routing on Alteon 180 or AD series and on Alteon Application Switches.

Field	Description
IP Forwarding	Sets IP Forwarding: on or off.
Forward Directed Broadcasts	Enables or disables forward directed broadcasts.
Default Gateway Metric	Sets the metric: strict or roundrobin.
Re-ARP Period	Sets the Re-ARP period in minutes.
1st BOOTP Server IP Address	Sets the IP address of the primary BOOTP server.
2nd BOOTP Server IP Address	Sets the IP address of the secondary BOOTP server.
BOOTP Relay	Enables or disables the BOOTP relay. When enabled, the BOOTP relay allows obtaining configuration from the Dynamic Host Configuration Protocol (DHCP) server. The BOOTP configuration enables the switch to forward a client request for an IP address to two DHCP/BOOTP servers with IP addresses that have been configured on the Application switch.
Default TTL (Time To Live)	The default time-to-live, which is the number of router hops the IP datagram can make. This field is read-only.
Reassembly Timeout	The maximum number of seconds in which received fragments are held while they are awaiting reassembly at this entity. This field is read-only.
Timeout Algorithm	The algorithm used to determine the timeout value that is used for retransmitting unacknowledged octets. This field is read-only.
Minimum Retransmit Timeout	The maximum value permitted by a TCP implementation for the retransmission timeout, measured in milliseconds. This field is read-only.
Maximum Retransmit Timeout	The maximum value permitted by a TCP implementation for the retransmission timeout, measured in milliseconds. This field is read-only.
Maximum Connection Allowed	The limit on the total number of TCP connections that the entity can support. In entities where the maximum number of connections is dynamic, this object should contain the value of -1. This field is read-only.

Field	Description
Router ID [1]	The router ID number for the switch. Enter an IP address in dotted-decimal notation.
Autonomous System Number [1]	The autonomous system (AS) number.

1. This is applicable only on Alteon Application Switches.

Configuring IP Interfaces

IP interfaces are used to represent the Alteon switch on an IP subnet on your network. The Interface option is disabled by default.

Field	Description
Interface Number	The IP interface number. This number can be set when you Insert an IP interface.
IP Address	The IP address of the interface.
IP Subnet Mask	The subnet mask of the interface.
VLAN	The VLAN associated with the interface. Each interface can belong to one VLAN, though any VLAN can have multiple IP interfaces in it. Select the **Browse..**. button to choose a VLAN.
State	Enables or disables the state of the interface.
BOOTP Relay	Enables or disables the BOOTP relay.

Configuring IP Gateways

Field	Description
IP Gateway Index	The gateway index number. Default gateways 1 to 4 are reserved for default gateway load balancing. Gateways 5 and to 250 can be assigned to separate VLANS for load-balancing of VLAN-based gateways.
IP Address	Sets the IP address of the default gateway.
Ping Interval	Sets the interval between ping attempts.
Ping Retry Count	Sets the number of failed attempts to declare the default gateway down.
State	Enables or disables the default gateway.
ARP Only Health Check	Enables or disables the Address Resolution Protocol health checks.
Priority [1]	Allows you to change the priority of the default gateway route to either *high* or *low*, relative to learned default routes. If you set the priority to *high*, then the default gateway route will always be preferred over learned default routes (such as from OSPF, BGP, or RIP protocols). If you set the priority to *low*, then learned default routes will always be preferred over the default gateway route **Note:** By default, the learned default route has higher priority than the configured default gateway route.
Gateway VLAN	The VLAN number associated with this gateway. You cannot assign a gateway VLAN number to the default gateways 1-4. You can only assign a Gateway VLAN to any IP Gateway Index of 5 and higher. Select the **Browse...** button to choose a VLAN. **Note:** This feature is available in Web OS 10.0 and higher.

1. This is applicable only on Alteon OS and higher.

NORTEL NETWORKS
216515-B, September 2004

Configuring DNS

The Domain Name System (DNS) tab is used for defining the primary and secondary DNS servers on your local network, and for setting the default domain name served by the switch services. DNS parameters must be configured prior to using hostname parameters with Ping, Traceroute, and TFTP.

Field	Description
Primary DNS Server IP Address	Sets the DNS primary IP address.
Secondary DNS Server IP Address	Sets the DNS secondary IP address.
Domain Name	Sets the default DNS domain name served by the switch services.

Configuring the Local Route Cache

Defining IP Address Ranges for the Local Route Cache

The Local Route Cache lets you use switch resources more efficiently, by reducing the size of the ARP table on the Web switch. The parameters that you configure in this window define a range of addresses that will be cached on the Web switch.

By default, the local network address and mask are both set to 0.0.0.0. This produces a range that includes all Internet addresses for route caching: 0.0.0.0 through 255.255.255.255.

Addresses to be cached are subnets that are directly connected, and for which there is an interface that has been configured on the Web switch.

Field	Description
IP Forward Local	The index number of the local IP route which can be set when a new IP route is Inserted. The local network address is used to define the base IP address in the range that will be cached.
IP Subnet	Sets the subnet address of the local IP route.
IP Subnet Mask	Sets the mask of the local IP route. The local network mask is the mask that is applied to produce the range. To determine if a route should be added to the memory cache, the destination address is masked (bitwise AND) with the local network mask and checked against the local network address.

To limit the route cache to your local hosts, you could configure the parameters as shown in the examples in the following table.

Local Host Address Range	Address	Mask
0.0.0.0 - 127.255.255.255	0.0.0.0	128.0.0.0
128.0.0.0 - 255.255.255.255	128.0.0.0	128.0.0.0
205.32.0.0 - 205.32.255.255	205.32.0.0	255.255.0.0

Configuring Routing Information Protocol (RIP1)

The tab is used to configure Routing Information protocol, version 1. The Routing Information Protocol (RIP) is an interior gateway protocol (IGP). RIP is one of a class of algorithms known as distance vector algorithms. The distance or hop count is used as the metric to determine the best path to a remote network or host where the hop count does not exceed 15 hops assuming a cost of one for each network. RIP uses broadcast User Datagram protocol (UDP) data packets to exchange routing information.

RIP sends routing information updates every 30 seconds. This update contains known networks and the distances (hop count) associated with each one. For RIP1, no mask information is exchanged; the natural mask is always applied by the router receiving the update. This option is turned off by default.

Field	Description
RIP	Globally sets the Routing Information Protocol (RIP): *on* or *off*.
Listen to Route Updates	Enables or disables listening to route updates. When enabled, the switch learns routes from other routers. This command is disabled by default.
Supply Route Updates	Enables or disables supplying route updates. When enabled, the switch supplies routes to other routers. This command is disabled by default.
Listen to Default Routes	Enables or disables listening to default routes. When enabled, the switch accepts RIP default routes from other routers and gives them priority over configured default gateways. When disabled, the switch rejects RIP default routes.
Supply Static Route Updates	Enables or disables supplying static route updates. When enabled, the switch supplies static routes.
Poison Reverse	Enables or disables the RIP poison reverse. When enabled, the switch uses split horizon with poisoned reverse. When disabled, the switch uses only split horizon.

Field	Description
Update Period	Sets the update period in seconds. It is set at 30 seconds by default.
Advertise VIP Host Routes	Enables or disables the advertisement of virtual IP addresses as Host Routes. If a VIP route exists in a routing table, it will always be advertised except when it is included in another network route that is already being advertised. **Note:** If all real servers behind a VIP go down, the route will be removed from the routing table, and will not be advertised. If we disable all the real servers, the VIP route will not get eliminated from the routing table, and the switch will continue to advertise the route.

Configuring IP Forwarding on Ports

IP forwarding is used for VLAN-to-VLAN (non-BGP) routing. Make sure IP forwarding is enabled if the default gateways are on different subnets, or if the switch is connected to different subnets and those subnets need to communicate through the switch (which they almost always do).

The IP Port Menu allows you to turn IP forwarding on or off on a port-by-port basis. By default, the port forwarding option is turned on.

Field	Description
Port	The port number of the forwarding state information.
Forwarding	Enables or disables the forwarding state of the port.

Configuring IP Static Routes

Field	Description
Static Route	The index number of the static routing table.
Destination IP Address	Sets the destination IP address for this route.
IP Subnet Mask	Sets the subnet IP mask for this route. **Note:** If the destination IP address is 0.0.0.0, the mask is also 0.0.0.0.
Gateway IP Address	Sets the destination IP gateway for this route.
IP Interface	The IP interface number of the route that is used as the source IP for routing. Use the **Browse..**. button to set the IP interface number.

Configuring Route Maps on Alteon Application Switches

A route map is used to control and modify routing information. Route maps define conditions for redistributing routes from one routing protocol to another or controlling routing information when injecting it in and out of BGP. Route maps are used by OSPF only for redistributing routes. For example, a route map is used to set a preference value for a specific route from a peer router and another preference value for all other routes learned via the same peer router.

A route map allows you to match attributes, such as metric, network address, and Autonomous System (AS) number. It also allows users to overwrite the local preference metric and to append the AS number in the AS route.

Configuring Route Maps

1. Define a network filter.

   Enter a filter number from 1 to 256. Specify the IP address and subnet mask of the network that you want to match. Enable the network filter. You can distribute up to 256 network filters among 32 route maps each containing 8 access lists.

2. Set up the BGP attributes.

   If you want to overwrite the attributes that the peer router is sending, then define the following BGP attributes:

   - Specify the AS numbers that you want to prepend to a matched route and the local preference for the matched route.
   - Specify the metric [Multi Exit Discriminator (MED)] for the matched route.

3. Enable the route map in the **State** field in this tab.

4. Assign the route map to a peer router.

   Select the peer router and then add the route map to the inbound route map list, or to the outbound route map list.

Field	Description
Route Map	The route map number.
Local Preference	The local-preference of the route map. 4294967295 means *none*.
Metric	The metric of the route map. 4294967295 means *none*.

Field	Description
Metric Type	The OSPF metric-type of the matched route: *none, type1*, *type2*. Exports the routes of this protocol as external OSPF AS-external LSAs in which the metric and metric type are specified. To remove a previous configuration and stop exporting the routes of the protocol, choose *none*.
Precedence	The precedence of the route map. The smaller the value, the higher the precedence.
Weight	The weight of the route map. 65535 means *none*.
State	*Enable* or *disable* the route map.
AS Path Prepend	The as-path prepend of the matched route. Up to 3 AS number can be displayed for the string. The usage is: <AS number> [<AS number>][<AS number>]

Configuring the Route Map Access List on Alteon Application Switches

A route map access list consists of a network filter which defines an IP address and subnet mask of the network you wish to include in the filter. This screen is used to configure access lists and assign them to route maps.

Field	Description
Route Map	The route map number.
Access List	The access list number that is assigned to the route map.
Network Filter	The network filter number of the route map access list. 0 means *none*. Click the Browse... button to select a network filter. You can define network filters in the Configuring IP Network Filters tab.
Metric	The metric of the route map access list. 4294967295 means *none*
Action	Action of the route map access list.
State	Enable or disable the route map access list.

Configuring IP Network Filters on Alteon Application Switches

Field	Description
Filter	The network filter number.
IP Address	Sets the starting IP address for this filter.
Mask	The subnet mask of the network filter. Sets the IP subnet mask that is used with the IP Address field above, to define the range of IP addresses that will be accepted by the peer when the filter is enabled. The default value is 0.0.0.0. For Border Gateway Protocol (BGP), assign the network filter to a route map, then assign the route map to the peer.
State	Enable or disable the network filter.

Configuring AS Paths on Alteon Application Switches

Field	Description
Route Map	The route map number.
AS Path	Sets the Autonomous System filter's path number.
AS	The AS number of the route map access path. 0 means none
Action	Action of the route map access path.
State	Enable or disable the route map access path.

Configuring Static ARP

Static ARP entries are permanent in the ARP cache and do not age out like the ARP entries that are learnt dynamically. Static ARP entries enable the switch to reach the hosts without sending an ARP broadcast request to the network. Static ARPs are also useful in communicating with devices that do not respond to ARP requests. Static ARPs can also be configured for some gateways as a protection against malicious ARP cache corruption and possible DOS attacks.

Note: Alteon OS 21.0 allows the static ARP configuration to retain over reboots. Alteon OS 20.x and lower allow the user to configure the ARP information but that information cannot be retained over the switch reboot

Field	Description
ARP	The index of static ARP entries.
IP Address	The IP address of the static ARP entry.
MAC	The MAC address of the static ARP entry.
VLAN	The VLAN number of the static ARP entry.
Port	The port number of the static ARP entry.

Configuring OSPF

Open Shortest Path First (OSPF) is designed for routing traffic within a single IP domain called an Autonomous System (AS). The AS can be divided into smaller logical units known as areas.

All routing devices maintain link information in their own Link State Database (LSDB). The LSDB for all routing devices within an area is identical but is not exchanged between different areas. Only routing updates are exchanged between areas, thereby significantly reducing the overhead for maintaining routing information on a large, dynamic network.

For more information how OSPF is implemented in the Alteon OS and Web OS, read your *Application Guide*.

Note: OSPF is supported on Alteon 180 or AD series and on Alteon Application Switches.

The following topics are covered in this section:

- "Configuring OSPF Administration" on page 91
- "Configuring OSPF General Settings" on page 92
- "Configuring OSPF Areas" on page 93
- "Configuring OSPF Area SPF" on page 95
- "Configuring OSPF Stub Areas" on page 96
- "Configuring OSPF Hosts" on page 97
- "Configuring OSPF Interfaces" on page 99
- "Configuring OSPF Interface Metrics" on page 101
- "Configuring OSPF Virtual Interfaces" on page 102
- "Configuring OSPF Area Aggregates" on page 103
- "Configuring OSPF Fixed Routes on Alteon Application Switches" on page 104
- "Configuring OSPF Static Routes on Alteon Application Switches" on page 105
- "Configuring OSPF External BGP on Alteon Application Switches" on page 106
- "Configuring OSPF: Internal BGP on Alteon Application Switches" on page 107

- “Configuring OSPF: MD5 on Alteon Application Switches” on page 108
- “Configuring OSPF MD5-Interface on Alteon Application Switches” on page 109
- “Configuring OSPF MD5-Virtual Interface on Alteon Application Switches” on page 110

Configuring OSPF Administration

Note: The OSPF Administrative Status must be *enabled* before any other OSPF configuration tabs will appear in Alteon EMS.

Field	Description
OSPF Administrative Status	Enables or disables OSPF. The value *enabled* denotes that the OSPF Process is active on at least one interface; *disabled* disables it on all interfaces.
OSPF Default Route Metric	The AS External metric to be assigned.
OSPF Default Route Metric Type	Sets the AS External metric type: none, type 1, or type 2.

Configuring OSPF General Settings

Note: The General settings tab appears only when OSPF has been enabled in the OSPF Administration tab.

Field	Description
Router	Displays a 32-bit integer uniquely identifying the router in the Autonomous System. By default, this is the IP address of the Web switch, which functions as the OSPF router's IP interface address.
Version	Displays version 2, which is the current version number of the OSPF protocol.
Is Area Border Router?	This is a flag to note whether this router is an area border router.
Is Autonomous System Border Router?	This checkbox is used to note whether this router is configured as an Autonomous System border router.
Link-state advertisements	The number of external (LS type 5) link-state advertisements in the link-state database.
Link-state advertisement Checksum	The 32-bit unsigned sum of the Link State checksums of the external link-state advertisements that are contained in the link-state database. This sum can be used to determine if there has been a change in a router's link state database, and to compare the link-state database of two routers.
New link-state Advertisements	The number of new link-state advertisements that have been originated. This number is incremented each time the router originates a new LSA.
Received link-state Advertisements	The number of link-state advertisements that have been received, and are determined to be new instances. This number does not include newer instances of self-originated link-state advertisements.
Maximum Stored Link State Advertisements [1]	The maximum number of non-default Autonomous System external Link State Advertisement (LSA) entries that can be stored in the link-state database. If the value is -1, then there is no limit. Maximum stored Link State Advertisements limit MUST be set identically in all routers attached to the OSPF backbone and/or any OSPF area excluding OSPF stub areas and NSSAs.

1. This is applicable only on Alteon OS 22.0.1.0 and higher.

Configuring OSPF Areas

Note: The Area settings tab appears only when OSPF has been enabled in the OSPF Administration tab.

To modify an existing area, click the **Modify...** button.

To insert a new area, click the Insert... button and modify the Area number, Import Support type, and Status in the Insert Area window. All other fields in this window are read-only.

Field	Description
Area ID	The OSPF area ID. This is a 32-bit integer that uniquely identifies an area. Area ID 0.0.0.0 is used for the OSPF backbone. If you are attempting to delete the OSPF backbone area, make sure there are no configured Virtual Interfaces. **Note:** An Area cannot be deleted if you have associated an Interface, Virtual Interface, or Area Aggregate with an Area row.
Import Support	The area's support for importing AS external link-state advertisements (LSA's). The selectable options are *importExternal* (import external LSA's), *importNoExternal* (do not import external LSA's), *importNssa* (import LSA's from a Not-So-Stubby-Area). **Note:** You cannot change the type from ImportExternal if a Virtual Interface is associated with the Area row.
Intra-area Route Calculation Runs	The number of times that the intra-area route table has been calculated using this area's link-state database. This is typically done using Dijkstra's algorithm.
Area Border Routers Reachable Count	The total number of area border routers that are reachable within this area. This is initially zero, and is calculated in each SPF Pass.
Autonomous System Border Router Reachable Count	The total number of Autonomous System border routers reachable within this area. This is initially zero, and is calculated in each SPF Pass.
Link-state Advertisement Count	The total number of link-state advertisements in this area's link-state database, excluding AS External LSA's.

Field	Description
Link-state Checksum	Displays the 32-bit unsigned sum of the link-state advertisements' LS checksums that are contained in this area's link-state database. This sum excludes external (LS type 5) link-state advertisements. The sum can be used to determine if there has been a change in a router's link state database, and to compare the link-state database of two routers.
Status	This variable displays the status of the entry. Currently it is always in active state.

Configuring OSPF Area SPF

Note: The Area SPF tab appears only when OSPF has been enabled in the OSPF Administration tab.

Field	Description
Area Number	The OSPF area number for which the OSPF area table is related.
Area ID	The OSPF area ID. This is a 32-bit integer that uniquely identifies an area. Area ID 0.0.0.0 is used for the OSPF backbone.
Interval	The OSPF interval, which is the time interval between two successive SPF calculations of the shortest path tree using the Dijkstra's algorithm.
Authentication Type	Type of authentication being used. • *none*: No authentication required. • *password*: Authenticates simple passwords so that only trusted routing devices can participate.

Configuring OSPF Stub Areas

Note: The Stub Area tab appears only when OSPF has been enabled in the OSPF Administration tab.

Field	Description
Stub Area	The 32 bit identifier for the Stub Area, which is area that is connected to only one other area. External route information is not distributed into stub areas.
Type-of-Service	The Type of Service that is associated with the metric. On creation, this can be derived from the instance.
Metric	The metric value applied at the indicated type of service. By default, this equals the least metric at the type of service among the interfaces to other areas.

Configuring OSPF Hosts

Note: The Hosts settings tab appears only when OSPF has been enabled in the OSPF Administration tab.

Field	Description
Host	Enter a host entry number from 1-128. Host routes are used for advertising network device IP addresses to external networks, and allow for Server Load Balancing (SLB) within OSPF. For more information, see your *Application Guide.*
Type-of-service	The Type of Service of the route being configured.
Cost Metric	The metric to be advertised.
Status	The status of the entry. Currently it is always in active state.
Area ID	The Area that the Host Entry is to be found within. By default, this is the area that a subsuming OSPF interface is in, or 0.0.0.0.

Configuring OSPF Host Areas on Alteon Application Switches

Note: The Hosts settings tab appears only when OSPF has been enabled in the OSPF Administration tab.

Field	Description
Index	The index number for the OSPF host. Enter an index number from 1-128.
Host Address	The IP Address of the OSPF host.
Area Number	The OSPF area index number (0-2).

Configuring OSPF Interfaces

Note: The Interfaces tab appears only when OSPF has been enabled in the OSPF Administration tab.

Field	Description
IP Address	The IP address of this OSPF interface. Once an OSPF area has been defined, it must be associated with a network. To attach the area to a network, you must assign the OSPF area index to an existing IP interface that participates in the area. **Note:** An interface must already be defined and enabled for an OSPF interface to be created. The enabled interface must be in the switch's current configuration and operational in order to insert an OSPF interface. If the interface is disabled, deleted or becomes non-operational, the associated OSPF interface is removed.
Addressless Interface	For the purpose of easing the instancing of addressed and addressless interfaces, this variable takes the value of 0 on interfaces that have IP Addresses, and the corresponding value of the ifIndex for interfaces having no IP Address.
Area ID	The Area that the Host Entry is to be found within. By default, this is the area that a subsuming OSPF interface is in, or 0.0.0.0. In order to Insert or Modify an OSPF interface, this field must be associated with an existing area, which is configured in the OSPF Area tab. Select the **Browse..**. button to choose an area. **Note:** Once you have associated this field with an Area row, you cannot delete the Area row in the OSPF Area tab.
Administrative Status	The OSPF interface's administrative status. The value formed on the interface, and the interface will be advertised as an internal route to some area. The value 'disabled' denotes that the interface is external to OSPF.
Priority	The priority of this interface. Used in multi-access networks, this field is used in the designated router election algorithm. The value 0 signifies that the router is not eligible to become the designated router on this particular network. In the event of a tie in this value, routers will use their Router ID as a tie breaker.
Transmission Delay	The estimated number of seconds it takes to transmit a link state update packet over this interface.
Retransmission Interval	The number of seconds between link-state advertisement retransmissions, for adjacencies belonging to this interface. This value is also used when retransmitting database description and link-state request packets.
Hello Interval	The number of seconds between link-state advertisement retransmissions, for adjacencies belonging to this interface. This value is also used when retransmitting database description and link-state request packets.

Field	Description
Router Dead Interval	The number of seconds that a router's Hello packets have not been seen before its neighbors declare the router down. This should be some multiple of the Hello interval. This value must be the same for all routers attached to a common network.
State	The OSPF interface state.
Designated IP Address	The IP address of the designated router.
Backup Designated IP Address	The IP address of the backup designated router.
Event Count	The number of times this OSPF interface has changed its state, or the number of times an error has occurred.
Authentication Key	The Authentication Key. If the Area's Authorization Type is a simple password, and the key length is shorter than 8 octets, the agent will left adjust and zero fill to 8 octets.Note that unauthenticated interfaces need no authentication key, and simple password authentication cannot use a key of more than 8 octets. Larger keys are useful only with authentication mechanisms not specified in this document.When read, the Authentication key always returns an Octet String of length zero.
Status	The status of the entry. Currently it is always in active state.

Configuring OSPF Interface Metrics

Note: The Interface Metrics tab appears only when OSPF has been enabled in the OSPF Administration tab.

Field	Description
IP Address	The IP address of this OSPF interface.
Addressless Interface	For the purpose of easing the instancing of addressed and addressless interfaces, this variable takes the value of 0 on interfaces that have IP Addresses, and the corresponding value of the ifIndex for interfaces having no IP Address.
Type-of-service	The type of service metric that is being referenced. On row creation, this can be derived from the instance.
Value	The metric of using this type of service (TOS) on this interface. The default value of the TOS 0 Metric is 10^8 / ifSpeed.

Configuring OSPF Virtual Interfaces

Note: The Virtual Interfaces tab appears only when OSPF has been enabled in the OSPF Administration tab. A Backbone area (0.0.0.0) must exist before you can insert a Virtual Interface. If any Virtual Interfaces exist, the Backbone area cannot be deleted.

Field	Description
Transit Area	The transit area allows area summary information to be exchanged between routing devices by means of the virtual link. Select the **Browse...** button to choose an area. The transit area must be associated with an existing Area whose Import Support type is *ImportExternal*. By definition, this area is not the OSPF Backbone, 0.0.0.0. **Note:** Once you have associated this field with an Area row, you cannot delete the Area row in the OSPF Area tab.
Neighbor	The Router ID of the Virtual Neighbor.
Transmission Delay	The estimated number of seconds it takes to transmit a link-state update packet over this interface.
Retransmission Interval	The number of seconds between link-state advertisement retransmissions, for adjacencies that belong to this interface. This value is also used when retransmitting database description and link-state request packets. This value should be well over the expected round-trip time.
Hello Interval	The length of time, in seconds, between the Hello packets that the router sends on the interface. This value must be the same for the virtual neighbor.
Router Dead Interval	The number of seconds that a router's Hello packets have not been seen before it's neighbors declare the router down. This should be some multiple of the Hello interval. This value must be the same for the virtual neighbor.
State	Displays OSPF virtual interface states.
Events	The number of state changes or error events on this Virtual Link.
Authentication Type	The authentication type specified for a virtual interface. Authenticates passwords so that only trusted routing devices can participate.
Authentication Key	The Authentication type. If the Authentication Type is a simple password, the device will left-adjust and zero-fill to 8 octets. Simple password authentication cannot use a key of more than 8 octets. **Note:** Unauthenticated interfaces do not require an authentication key.
Status	The status of the entry. Currently it is always in active state.

Configuring OSPF Area Aggregates

The Area Aggregate window is used to insert OSPF area ranges.

Field	Description
Area ID	The area the Address Aggregate is to be found within. To insert an Area Aggregate, you must associate this field with an existing Area, which is configured in the OSPF Area tab. Select the **Browse..**. button to choose an area. **Note:** Once you have associated this field with an Area row, you cannot delete the Area row in the OSPF Area tab.
Type	The type of the Address Aggregate. This field specifies the Link-state database type to which this Address Aggregate applies: • *summaryLink* generates an aggregated summary. • *nssaExternalLink* generates a not so stubby area (NSSA) link summary.
IP Address	The IP Address of the Net or Subnet indicated by the range.
Mask	The Subnet Mask that pertains to the Net or Subnet.
Status	The status of the entry. Currently it is always in active state.
Effect	Select the effect you want. • *advertiseMatching* advertises the aggregate summary Link-State Advertisement with the same link-state ID. • *doNotAdvertiseMatching* prevents advertising the subnet outside of the area--suppressing all networks that fall within the range.

Configuring OSPF Fixed Routes on Alteon Application Switches



This button allows you to choose Route Maps Dialog.

Field	Description
Metric	The export metric for fixed routes. A value of 0 indicates none
Metric Type	The AS External metric type for fixed routes.
Route Maps	The route maps present in the route map list. The route maps are presented in a bitmap format.

Configuring OSPF Static Routes on Alteon Application Switches



This button allows you to choose Route Maps Dialog.

Field	Description
Metric	Specify the metric to be assigned to static routes. A value of 0 indicates none.
Metric Type	The AS External metric type for Static routes.
Route Maps	Double-click on the Route Maps: label to open a Browser window. You can select pre-defined route maps in this window. All route maps are defined in the Route Maps tab under the IP configuration menu.

Configuring OSPF External BGP on Alteon Application Switches



This button allows you to choose Route Maps Dialog.

Field	Description
Metric	The export metric to be assigned to External BGP routes. A value of 0 indicates none.
Metric Type	The AS External metric type for External BGP routes.
Route Maps	Double-click on the Route Maps: label to open a Browser window. You can select pre-defined route maps in this window. All route maps are defined in the Route Maps tab under the IP configuration menu.

Configuring OSPF: Internal BGP on Alteon Application Switches



This button allows you to choose Route Maps Dialog.

Field	Description
Metric	The export metric for Internal BGP routes. A value of 0 indicates none.
Metric Type	The AS External metric type for Internal BGP routes.
Route Maps	Double-click on the Route Maps: label to open a Browser window. You can select pre-defined route maps in this window. All route maps are defined in the Route Maps tab under the IP configuration menu.

Configuring OSPF: MD5 on Alteon Application Switches

Field	Description
Index	The key ID number that is assigned to a particular OSPF MD5 key.
Key	The character string representing the MD5 key.

Configuring OSPF MD5-Interface on Alteon Application Switches

Field	Description
Index	The OSPF Interface number for which the OSPF Interface table is related.
ID	The IP Address of the OSPF Interface.
Key	The MD5 key for the OSPF Interface. 0 (none) no MD5 authentication.

Configuring OSPF MD5-Virtual Interface on Alteon Application Switches

Field	Description
Index	The OSPF Virtual Interface number for which the OSPF Virtual Interface table is related.
Area ID	The IP Address of the OSPF area to which this virtual interface belongs.
Neighbor	The IP Address of the OSPF neighbor for this virtual interface.
Key	The MD5 key for the OSPF Virtual Interface. Zero (0) indicates no MD5 authentication.

Configuring Border Gateway Protocol (BGP)

The following BGP configuration topics are covered in this section:

- "Configuring BGP Administration on Alteon Application Switches" on page 112
- "Configuring General BGP Information" on page 114
- "Configuring BGP Peers on Alteon Application Switches" on page 115
- "Configuring BGP Aggregations on Alteon Application Switches" on page 117
- "Configuring Peers Information on Alteon Application Switches" on page 118

Configuring BGP Administration on Alteon Application Switches

Border Gateway Protocol (BGP) is an Internet protocol that enables routers on a network to share routing information with each other and advertise information about the segments of the IP address space they can access within their network with routers on external networks. BGP allows you to decide what is the “best” route for a packet to take from your network to a destination on another network, rather than simply setting a default route from your border router(s) to your upstream provider(s). BGP is defined in RFC 1771.

The BGP tabs allow you to configure the switch to receive routes and to advertise static routes, fixed routes and virtual server IP addresses with other internal and external routers. In the current implementation, the Alteon switch does not advertise BGP routes that are learned from other BGP “speakers”.

For more information, see your *Application Guide*.

Enabling BGP from Alteon EMS

Before you can configure BGP and view all BGP tabs, enable the feature by doing the following:

1. In the General IP Configuration tab, configure a Router ID and autonomous system (AS) number. In this tab, make sure to click on the **Set** button.
2. In the BGP Administration tab, set Pending Border Gateway Protocol (BGP) to *on*. In this tab, make sure to click on the **Set** and **Apply** buttons.

   The other BGP configuration tabs will now appear.

Field	Description
Pending Border Gateway Protocol (BGP)	Globally turn BGP on or off. Requires a Router ID and AS number to be configured first.

Field	Description
Local Preference	Sets the local preference. The path with the higher value is preferred. When multiple peers advertise the same route, use the route with the shortest AS path as the preferred route if external BGP, or use the local preference if internal BGP.
Current Border Gateway Protocol (BGP)	Current state of BGP: *on* or *off*.

Configuring General BGP Information

This tab is read-only. It displays BGP general information. To first configure BGP, go to the IP General tab and enter a Router ID and Autonomous System Number.

Field	Description
Local Autonomous System number	Displays the Autonomous System number.
Local BGP Identifier	Displays local BGP identifier.
Supported BGP Protocol Version Numbers	Displays a list of BGP supported protocols. Each peer negotiates the version from this vector. Versions are identified through the string of bits contained within this object.

Configuring BGP Peers on Alteon Application Switches



This button allows you to obtain an inbound Route Map.



This button allows you to obtain outbound Route Map.

Field	Description
Peer	The BGP peer number 1-16.
Remote Address	Defines the remote IP address for the specified peer (border router), using dotted decimal notation.
Remote AS	Sets the remote autonomous system number for the specified peer. 0 means *none*
Time-To-Live	The time-to-live value of the BGP peer IP datagram. Specifies the number of router hops that the IP datagram can make. This value is used to restrict the number of “hops” the advertisement makes. It is also used to support multi-hops, which allow BGP peers to talk across a routed network.
State	Enable or disable the peer.
Advertise OSPF Routes	Enable or disable advertising of OSPF routes.
Advertise Fixed Routes	Enable or disable advertising of fixed routes.
Advertise Static Routes	Enable or disable advertising of static routes.
Advertise VIP static Routes	Enable or disable VIP static routes.
Default Route Action	The value of default route action: *none*, *import*, *originate*, or *redistribute*.
Metric	The metric value of the BGP peer. A value of 0 or 4,294,967,295 means *none*

Field	Description
Inbound Route Map	The route maps present in the inbound route map list. The route maps are presented in a bitmap format. Double-click on the Route Maps: label to open a Browser window. You can select pre-defined route maps in this window. All route maps are defined in the Route Maps tab under the IP configuration menu.
Outbound Route Map	The route maps present in the outbound route map list. The route maps are presented in a bitmap format. Double-click on the Route Maps: label to open a Browser window. You can select pre-defined route maps in this window. All route maps are defined in the Route Maps tab under the IP configuration menu.

Configuring BGP Aggregations on Alteon Application Switches

This menu enables you to configure filters that specify the routes and range of IP destinations that a peer router will accept from other peers. A route must match a filter to be installed in the routing table. By default, the first filter is enabled and the rest of the filters are disabled.

Field	Description
Aggregation	The BGP aggregation number.
IP Address	Defines the starting IP address for this filter, using dotted decimal notation.
Subnet Mask	This IP address mask is used with addr to define the range of IP addresses that will be accepted by the peer when the filter is enabled.
State	Enable or disable the BGP aggregation filter.

Configuring Peers Information on Alteon Application Switches

Field	Description
Peer	The BGP number. Peers are border routers that exchange routing information with routers on internal and external networks.
State	The BGP peer connection state.
Administration State	The desired state of the BGP connection. A transition from 'stop' to 'start' will cause the BGP Start Event to be generated. A transition from 'start' to 'stop' will cause the BGP Stop Event to be generated. This parameter can be used to restart BGP peer connections. Care should be used in providing write access to this object without adequate authentication.
Version	The negotiated version of BGP running between the two peers.
Local Address	The local IP address of this entry's BGP connection.
Local Port	The local port for the TCP connection between the BGP peers.
Remote Address	The remote IP address of this entry's BGP peer.
Remote Port	The remote port for the TCP connection between the BGP peers.
Remote Autonomous System	The remote autonomous system number.
Retry Interval	The connection retry interval in seconds.
Hold Time	Sets the period of time, in seconds, that will elapse before the peer session is torn down because the switch hasn't received a "keep alive" message from the peer.
Keep Alive	Sets the keep-alive time for the specified peer in seconds.
Hold Time Interval	Time interval in seconds for the Hold Time configured for this BGP speaker with this peer.
Keep Alive Interval	Time interval in seconds for the *KeepAlive* timer configured for this BGP speaker with this peer.
Min AS Origination Interval	Time interval in seconds for the *MinASOriginationInterval* timer. The suggested value for this timer is 15 seconds.
Min Route Advertisement Interval	Time interval in seconds for the *MinRouteAdvertisementInterval* timer.

Configuring Layer 4 on the Switch

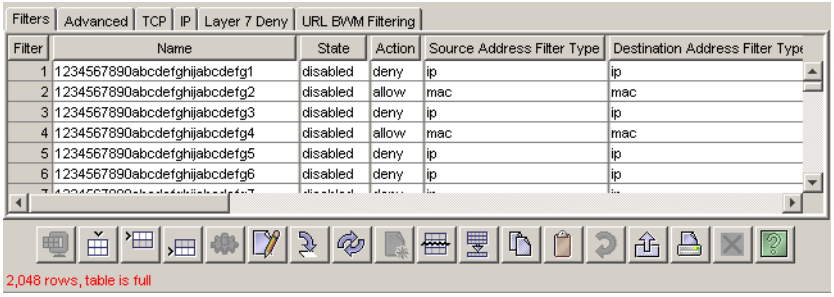
Internet traffic consists of myriad services and applications which use the Internet Protocol (IP) for data delivery. IP, however, is not optimized for all the various applications. Web switching goes beyond IP and makes intelligent switching decisions based on the application and its data.The following topics are covered in this section:

- “Configuring Layer 4 Filters” on page 120
- “Configuring Advanced Layer 4 Filters” on page 125
- “Configuring TCP Filters” on page 129
- “Configuring IP Filters” on page 130
- “Configuring Layer 7 Deny Filters” on page 131
- “Configuring Layer 7 Lookup” on page 132
- “Configuring Security” on page 133
- “Configuring HTTP Redirection” on page 135
- “Configuring URL BWM Filtering” on page 136
- “Configuring Server Load Balancing” on page 137

Configuring Layer 4 Filters

The switch can be configured with filters to allow, deny, redirect or perform Network Address Translation on traffic according to a variety of address and protocol specifications. Each physical switch port can be configured to use any combination of filters.

This tab is used to configure or modify existing filters on the switch. Alteon EMS provides a way to modify the block of filters without having to re-number the surrounding filters manually as you would using the CLI.



Compress



Select a block of non-consecutive filters. Then use the Compress button to renumber all non-consecutive filters to remove all empty spaces in the direction specified —up or down.

Move



Use the Move button to move the block of filters up or down by the specified interval.

Insert above



Use the Insert Above button to insert a filter above the selected filter. It moves and renumbers the existing filters to create a space to insert a new filter.

Insert below



Use the Insert Below button to insert a filter below the selected filter. It moves and renumbers the existing filters to create a space to insert a new filter. All filters are re-numbered to accommodate the new filter.

Delete Selected Rows



This button deletes the selected filter rows.

Note: If you have many filters configured and wish to view a subset of the items in this table, click on the Filter Table Rows… button.

Field	Description
Filter	The filter index number.
Name	The name of the filter.
State	The state of the filtering rule: disabled or enabled
Action	The action for the filtering rule: *allow, deny, redirect* or *NAT* • *allow*: Allow the frame to pass (by default). • *deny*: Discard frames that fit this filter's profile. This can be used for building basic security profiles. • *redirect*: Redirect frames that fit this filter's profile, such as for web cache redirection. In addition, Layer 4 processing must be activated. • *NAT*: Perform generic Network Address Translation (NAT). The *NAT* action can be used to map the source or destination IP address and port information of a private network scheme to/from the advertised network IP address and ports. This is used in conjunction with the nat option below and can also be combined with proxies.
Source Address Filter Type	The type of source address filter: IP address or MAC address.
Destination Address Filter Type	The type of destination address filter: IP address or MAC address.

Field	Description
Source IP Address	If defined, traffic with this source IP address will be affected by this filter. Specify an IP address in dotted decimal notation, or *any*. A range of IP addresses is produced when used with the Source IP Mask below. The default is any if the source MAC address is *any*. The source IP address to match. Enter an IP address in dotted decimal notation or enter *any* to filter on any source IP address. This option is enabled only when Source Address Filter Type is set to *IP*.
Source IP Mask	The source IP subnet mask used with the Source IP Address. Use with Destination IP Address to select traffic that this filter will affect. See "Defining IP Address Ranges for Filters" on page 124 for more information on producing address ranges.
Destination IP Address	The destination IP address to match. If defined, traffic with this destination IP address will be affected by this filter. Specify an IP address in dotted decimal notation, or *any*. A range of IP addresses is produced when used with the Destination IP Mask below. The default is *any* if the destination MAC address is any.
Destination IP Mask	The source IP subnet mask used with the Destination IP Address.
Source MAC Address	The source MAC address to match. This option is enabled only when Source Address Filter Type is set to MAC.
Destination MAC Address	The destination MAC address to match. This option is enabled only when Destination Address Filter Type is set to MAC.
Protocol	The selected filter protocol. Use the **Browse...** button to select a protocol.
Low Source Port Range	The lower source TCP/UDP port number in the range to filter. This applies only when the filter protocol is defined as TCP or UDP. A value of 0 (zero) indicates no source port filtering.
High Source Port Range	The higher source TCP/UDP port number in the range to filter. This applies only when the filter protocol is defined as TCP or UDP. A value of 0 (zero) indicates no source port filtering.
Low Destination Port Range	The lower destination TCP/UDP port number in the range to filter. This applies only when the filter protocol is defined as UDP or TCP. A value of 0 (zero) indicates no destination port filtering.
High Destination Port Range	The higher destination TCP/UDP port number in the range to filter. This applies only when the filter protocol is defined as UDP or TCP. A value of 0 (zero) indicates no destination port filtering.
Invert	Enables or disables the setting of the inverse logic for the filter entry.
VLAN	The VLAN on which to filter. Click the **Browse...** button to select a pre-defined VLAN.

Field	Description
Redirection Port	When *Redirect is set as* the filter Action, this field is used to define the real server TCP or UDP port to which redirected traffic will be sent. For valid Layer 4 health checks, this field must be configured whenever TCP protocol traffic is redirected. Also, if transparent proxies are used for Network Address Translation (NAT) on the Alteon switch, the Redirection Port must be configured for all Application Redirection filters. Click the **Browse..**. button to select a protocol port.
Redirection Group	When *Redirect is set as* the filter Action, this field is used to define a real server group to which redirected traffic will be sent.
Network Address Translation	When *NAT* is set as the filter action (see above), this field specifies whether Network Address Translation (NAT) is performed on the source IP address or on the destination IP address. If *source-address* is specified, the frame's source IP address and source port number are replaced with the destination IP address and destination port. If *destination-address* is specified, the frame's destination IP address (dip) and port number (dport) are replaced with the source IP and source port values.
Goto ID [1]	Allows the user to specify a target filter ID that the filter search should jump to when a match occurs. Filter searching will then continue from the designated filter ID. Use this tab to specify the new filter to go to.
Proxy IP Address [2]	Defines client proxy IP address. The switch uses the configured proxy IP address to replace the client's IP address. If the user does not configure the proxy IP address in the filter, the switch will use the proxy IP address configured in this tab.
PIP Selection Egress Port [2]	Enables or disables proxy IP selection based on egress port or VLAN. By default, the SP selects the proxy IP address based on ingress port or VLAN. Using this tab, you can enable or disable the SP to select proxy IP address based on the egress port or VLAN.

1. This is applicable only on Alteon OS 21.0 and higher.
2. This is applicable only on Alteon OS and higher.

Defining IP Address Ranges for Filters

You can specify a range of IP address for filtering both the source and/or destination IP address for traffic. When a range of IP addresses is needed, the source IP or destination IP address defines the base IP address in the desired range. The source mask or destination mask is applied to produce the range of addresses.

For example, to determine if a client request's destination IP address should be redirected to the cache servers attached to a particular switch, the destination IP address is masked (bitwise AND) with the destination mask, and then compared to the destination IP address.

As another example, you could configure the switch with two filters so that each would handle traffic filtering for one half of the Internet. To do this, you could define the following parameters:

Table 1 Filtering IP Address Ranges

Filter	Internet Address Range	Destination IP	Destination Mask
#1	0.0.0.0 - 127.255.255.255	0.0.0.0	128.0.0.0
#2	128.0.0.0 - 255.255.255.255	128.0.0.0	128.0.0.0

Configuring Advanced Layer 4 Filters

Field	Description
Filter	The filter index number.
Name	The name of the filter.
Logging	Enables or disables logging of filter messages.
Caching	Enables or disables caching sessions that match the filter. Caution: Exercise caution while applying cache-enabled and cache-disabled filters to the same switch port. A cache-enabled filter creates a session entry in the switch, so that the switch can bypass checking for subsequent frames that match the same criteria. Caching is enabled by default. **Note:** Caching should be disabled if applying a filter to virtual server IP address while performing UDP load balancing.
Client Proxy	Enables or disables client proxy. This option applies only when *redir* or *nat* is specified as the filter action. Enable or disable proxy IP address translation for traffic matching the filter criteria. By default, client proxy is enabled. If disabled, any proxy that has been defined for the switch port using the real server client proxy is not performed for traffic meeting the filter criteria. This is useful when certain traffic must retain original IP address information, or when other forms of translation (such as Application Redirection or NAT) are preferred.
URL Redirection [1]	Enables or disables URL redirection. By default, this option is disabled.
NAT Active FTP	Enables or disables active FTP Client Network Address Translation (NAT). When a client in active FTP mode sends a PORT command to a remote FTP server, the switch will look into the data part of the frame and replace the client 's private IP address with a proxy IP (PIP) address. The real server port (RPORT) will be replaced with a proxy port (PPORT), that is PIP:PPORT. By default, this option is disabled.
NAT Session Timeout	Sets the Network Address Translation (NAT) session timeout in an even number of minutes.
ICMP Type	Sets the ICMP message type. The default is set at *any*. For a detailed description of filtering and ICMP, see the *Application Guide*.
Firewall Redirect Hash	To ensure that the stateful inspection behavior of firewalls is maintained, a hashing algorithm is used to ensure that inbound packets and outbound packets for a pair of IP source address and destination address traverse through the same firewall. If the destination port (dport) is 80 or 21, enabling this option changes the hash of the filter from a Web cache-redirection hash to a FWLB hash. By default, this option is disabled.

Field	Description
WAN Link Load Balancing	Enables or disables WAN Link Load Balancing. By default, this option is disabled.
Intrusion Detection Hash	Sets the hash metric parameter for Intrusion Detection System Server Load Balancing: • The *sip* option hashes on the source IP address. • The *dip* option hashes on the destination IP address. • The *both* option hashes on both source and destination IP addresses.
Hash	Allows you to choose a tunable hash parameter to use for filter redirection. • The *Source-IP* option allows you to perform tunable hash on source IP address for this filter. • The *Destination-IP* option allows you to perform tunable hash on destination IP address for this filter. • The *Both-IP* option allows you to perform tunable hash on both source IP address and the destination IP address at the same time. • The *Source-IP&Port* option allows you to perform tunable hash on both source IP address and source port at the same time. • The *Automatic* option automatically chooses a tunable hash parameter.
RADIUS/WAP Persistence [2]	Enables or disables RADIUS/WAP persistence. When this command is enabled, the user can bind both RADIUS and WAP sessions to the same server. This command also enables the switch to continue to function in the same way, should the WAP traffic arrive before the RADIUS accounting start packet.
Persistent Binding [2]	Enables or disables persistent binding for a real server (disabled by default). This may be necessary for some server applications where state information about the client system is retained on the server over a series of sequential connections, such as with SSL (Secure Socket Layer, HTTPS), Web site search results, or multi-page Web forms. The disable option enables you to disable persistent binding, if it has previously been enabled for a particular application.
Match 802.1p Bits [3]	Allows you to add the optional capability to filter on the 802.1p value in the packet. When configured to filter on the 802.1p value, the filter will match whether the 802.1p value in the packet is the same as the value configured for the filter. If the values do not match or the packet does not have the 802.1p bits, the filter will not match.

Field	Description
802.1p Bits Value [3]	Allows you to filter IP packets based on the 802.1p bits in the packet's VLAN header. The 802.1p bits specify the priority that will be given to the packets while forwarding them. The packets with a higher (non-zero) priority bits will be given forwarding preference over the packets with lower priority bits value. You can classify the packets into different bandwidth management contracts and different contract limits (hard, soft and reserved) based on the 802.1p bits. You can also classify the packets based on the value of the 802.1p bits on the filter and assigning a contract for that filter.
Real Server Group IDS Load Balancing [3]	Sets the IDS server group for intrusion detection server load balancing. When filtering is used for IDSLB, each filter added to an IDSLB-enabled port can be assigned a unique IDS real server group.
Delayed Binding [3]	Enables or disables delayed binding for redirection on this filter.
BWM Contract [5]	Sets the Bandwidth Management Contract number for the selected filter.
WAP Radius Snooping [4]	Enables or disables WAP RADIUS Snooping capability of the selected filter. By default, this option is disabled.

1. This is not applicable on Alteon OS 22.0 and higher.
2. This is applicable only on Alteon OS 21.0 and higher.
3. This is applicable only on Alteon Application Switches and Alteon OS and higher.
4. This is not applicable on Alteon Link Optimizer (ALO) switch.
5. This field is applicable only if BWM software key is enabled.

ICMP Message Types

The following ICMP message types are used with the ICMP Type field.

Type #	Message Type	Description
0	`echorep`	ICMP echo reply
3	`destun`	ICMP destination unreachable
4	quench	ICMP source quench
5	redir	ICMP redirect

Type #	Message Type	Description
8	echoreq	ICMP echo request
9	rtradv	ICMP router advertisement
10	rtrsol	ICMP router solicitation
11	timex	ICMP time exceeded
12	param	ICMP parameter problem
13	timereq	ICMP timestamp request
14	timerep	ICMP timestamp reply
15	inforeq	ICMP information request
16	inforep	ICMP information reply
17	maskreq	ICMP address mask request
18	maskrep	ICMP address mask reply

Configuring TCP Filters

These fields can be used to configure packet filtering for specific TCP flags.

Field	Description
Filter	The filter number.
Name	The name assigned to the filter.
TCP ACK or RST Matching	Enables or disables the filtering on matching TCP ACK (acknowledgement) and RST (reset) flags.
TCP URG	Enables or disables TCP URG (urgent) flag matching.
TCP ACK	Enables or disables TCP ACK (acknowledgement) flag matching.</
TCP PSH	Enables or disables TCP PSH (push) flag matching.
TCP RST	Enables or disables TCP RST (reset) flag matching.
TCP SYN	Enables or disables TCP SYN (synchronize) flag matching.
TCP FIN	Enables or disables TCP FIN (finish) flag matching.
TCP Connection Rate Limit [1]	Enables or disables TCP connection rate limiting. By default, this option is disabled.
Maximum Connection for TCP Rate Limit [1]	Sets the maximum limit for new TCP connections in units of 10. To set the maximum number of connections (2,550), enter 255. To set the minimum number of connections (10), enter 1.

1. These features are applicable on Alteon OS 20.x and lower and Web OS 10.0 and higher.

Configuring IP Filters

Field	Description
Filter	The filter index number.
Name	The name of the filter
IP Option	Enables or disables the IP option.
IP TOS	Sets the IP Type of Service (TOS) value to filter: 0 to 255.
IP TOS Mask	Sets the IP TOS mask for filtering: 0 to 255.
New IP TOS	Overwrites the new IP TOS value when filtering: 0 to 255.
Maximum Packet Length [1]	Sets the IP maximum packet length in bytes. A value can be either 0 which indicates **any** length or between 64 and 65535.

1. This applies to Alteon OS 21.0.4.0 and above.

Configuring Layer 7 Deny Filters

You can secure your switch from virus attacks by configuring the switch with a list of potential offending string patterns (HTTP URL request). The switch examines the HTTP content of the incoming client request for the matching string pattern. If the matching virus pattern is found, then the packet is dropped and a reset frame is sent to the offending client.

Once configured, L7 Deny filters cause SYSLOG messages and SNMP traps to be generated, thus warning operators of a possible attack.

To associate URL Paths to a filter, select the **URL Paths..** button. This button is only active when the filter action is of type *deny*, and the filter row is selected.

Note: This feature is applicable only on Alteon OS 20.x and lower.

Field	Description
Filter	The filter index number.
Name	The name of the filter.
Action	The action for the filtering rule: *allow, deny, NAT*, or *redirect*.
Layer 7 State	Displays the Layer 7 Deny filtering state as enabled or disabled. This command replaces the urlp and l7deny commands found in earlier releases of Alteon OS. When enabled, the filter performs a lookup on layer 7 content such as HTTP strings or headers. When combined with a filter action (e.g. deny, redir), this feature enables content-intelligent redirection or content-intelligent deny filtering.
Layer 7 URLs	Displays the URL strings selected for Layer 7 deny filters. To select URL strings, click on the URL Paths... button to select pre-defined strings. To configure URL strings, go to the “Configuring Layer 7 URL Parsing: SLB Strings” on page 201 Configuring Layer 7 URL Parsing: SLB Strings tab.

Configuring Layer 7 Lookup

To associate URL Paths to a filter, select the **URL Paths..** button.



Field	Description
Filter	The filter index number.
Name	The name of the filter.
Action	The action for the filtering rule: *allow, deny, NAT*, or *redirect*.
Layer 7 State	Displays the Layer 7 lookup filtering state as enabled or disabled. This command replaces the urlp and l7deny commands found in earlier releases of Alteon OS. When enabled, the filter performs a lookup on layer 7 content such as HTTP strings or headers. When combined with a filter action (e.g. deny, redir), this feature enables content-intelligent redirection or content-intelligent deny filtering.
Layer 7 URL	Displays the URL strings selected for Layer 7 lookup filters. To select URL strings, click on the URL Paths... button to select pre-defined strings. To configure URL strings, go to the"Configuring Layer 7 URL Parsing: SLB Strings" on page 201 Configuring Layer 7 URL Parsing: SLB Strings tab.
Parse All	Enables or disables parsing of all packets in a session where layer 7 lookup is being performed. This command is enabled by default, and normally all data packets in a session are examined by the filter. However, some sessions may contain only one packet containing the layer 7 content. Once this packet is found, subsequent packets can be ignored. When parseall is disabled, layer 7 lookup is turned off for the remaining packets in the session.

Note: This feature is applicable only Alteon OS 21.0 and higher.

Configuring Security

Note: This feature is applicable only on Alteon Application Switches and on ALO 1.0 and higher.

Note: You need to purchase the license/key from Nortel Networks to be able to apply the security configurations on your switch.



You can add pattern matching groups using this button.

Field	Description
Filter	The filter index number.
Name	The name of the filter.
Protocol Rate Limiting	Enables or disables Rate Limiting Protocol for the filter.
Maximum Connections for Rate Limit	Defines maximum connections for rate limiting.
Rate Limiting Time Window	Defines time window for rate limiting. A time window is a configured period of time (in seconds) during which packets are allowed to be received. The time window can be configured per filter and not globally on all the filters.
Hold Duration	Defines hold down duration for rate limiting. When the number of new connections or packets exceeds the configured limit, any new TCP connection requests or UDP/ICMP packets from the client are blocked. When blocking occurs, the client is said to be held down. The client is held down for a specified number of minutes, after which new TCP connection requests or packets from the client are allowed once again to pass through. The hold-down duration can be configured per filter and not globally on all the filters.
Match All	The switch is capable of matching more than one UDP pattern and offset value pair before denying a packet. If these multiple patterns are specified with `matchall` enabled, all patterns must be matched before a UDP packet is denied and dropped. It is useful to combine these patterns into a group and assign a name to the group. When applied to a deny filter, the switch must match all strings or patterns within that group before denying and dropping the packet. Up to five patterns can be combined into a single pattern group.
Pattern Matching	Enables or disables pattern matching on this filter.

Field	Description
Parse All	Enables or disables pattern string lookup (parsing) of all packets in a session where pattern matching is being performed. This command is enabled by default, and normally all data packets in a session are examined by the filter. However, some sessions may contain only one packet containing the layer 7 content. Once this packet is found, subsequent packets can be ignored. When parseall is disabled, pattern matching is turned off for the remaining packets in the session.
Pattern Matching Group	When a pattern group is applied to a deny filter, the switch will match any of the strings or patterns within that group before denying and dropping the packet. The filtering commands in Alteon OS Security Pack allow the administrator to define groups of patterns and place them into groups. By applying the patterns and groups to a deny filter, the packet content can be detected and thus denied access to the network.

Configuring HTTP Redirection

Field	Description
Filter Index	Index of the filter
Original String	The original string of the packet. The SLB String pattern string type must be set to none.
Redirection String	Displays an HTTP redirection mapping string If the string on the filter matches with the first string id, then the switch will send back an HTTP redirection message back to the client that contains information in the second string ID. The SLB String pattern string type must be set to none.

Configuring URL BWM Filtering

Note: This feature is available only if the BWM software key is enabled.

Field	Description
Filter	The number of the filter. Select the **Browse..**. button to choose a Filter.
URL Path Number	The URL path for URL load balancing. Select the **Browse..**. button to choose a URL Path.
BWM Contract	The number of the Bandwidth Management contract. Select the **Browse..**. button to choose a contract.

See also:

- “Configuring Layer 4 SLB: URL-Based BWM” on page 181
- “Configuring Layer 7 URL Parsing: SLB Strings” on page 201

Configuring Server Load Balancing

The following topics are covered in this section:

- "Configuring General Server Load Balancing" on page 139
- "Configuring Layer 4 SLB: Real Servers" on page 142
- "Configuring Layer 4 SLB: Real Server Ports" on page 146
- "Configuring Layer 4 SLB: Real Server Groups" on page 147
- "Configuring Layer 4 SLB: Real Server Group State" on page 150
- "Configuring Layer 4 SLB: Real Server Group Operation" on page 151
- "Configuring Layer 4 SLB: Virtual Servers on Alteon 180 or AD series" on page 152
- "Configuring Layer 4 SLB: Virtual Servers on Alteon Application Switches" on page 158
- "Configuring Ports for Server Load Balancing" on page 165
- "Configuring Layer 4 SLB: Proxy IP Addresses on Alteon Application Switches in Alteon OS 21.0 and Lower" on page 167
- "Configuring Layer 4 SLB: Real Time Streaming Protocol (RTSP) Load Balancing on Alteon 180 or AD series" on page 171
- "Configuring Layer 4 SLB: Health Scripts on Alteon Application Switches" on page 172
- "Configuring SNMP Health Scripts on Alteon Application Switches" on page 175
- "Configuring Layer 4 SLB: Syn Attack" on page 176
- "Configuring Layer 4 SLB: Inbound Link Load Balancing" on page 177
- "Configuring Layer 4 SLB: Domain Records" on page 178
- "Configuring Layer 4 SLB: Domain Mapping" on page 179
- "Configuring Layer 4 SLB: Service Mapping" on page 180
- "Configuring Layer 4 SLB: URL-Based BWM" on page 181
- "Configuring Layer 4 SLB: Remote URL General settings on Alteon 180 or AD series" on page 182
- "Configuring Layer 4 SLB: Remote URL Destination Port on Alteon 180 or AD series" on page 183
- "Configuring Layer 4 Global SLB: General" on page 185
- "Configuring Layer 4 Global SLB: Remote Sites" on page 188

- “Configuring Layer 4: WAP General Properties” on page 195

Configuring General Server Load Balancing

Field	Description
Server Load Balance	Enables or disables Server Load Balancing.
Virtual Matrix Architecture	Enables or disables the Virtual Matrix Architecture (VMA). Enabling the virtual matrix allows the workload to be distributed among multiple processors.
Direct Access Mode	Enables or disables Direct Access Mode (DAM).When enabled, Direct Access Mode allows direct access to real servers and any combination of virtual and real servers.
IP Address Mask	Sets the virtual and real IP address mask.
Management Network	Displays the IP address of the Management Network. If defined, management traffic with this source IP address will be allowed direct (non-Layer 4) access to the real servers. Specify an IP address in dotted decimal notation. A range of IP addresses is produced when used with the Management Subnet Mask option.
Management Subnet Mask	Displays the subnet mask of the Management Network. This IP address mask is used with the Management Network to select management traffic which is allowed direct access to real servers. The default is 255.255.255.255.
Radius Secret	Sets the RADIUS authentication string. The string is used for generating an encrypted authentication string for the RADIUS health check.
Persistent Mask	Sets the persistent mask. Specify an IP mask address in dotted decimal notation
Graceful Failover	Enables or disables graceful server failure.When enabled, the connection to the failed real servers is maintained.
Session Table Fast-Age Period (seconds)	Sets the session fast-age period: 1, 2, 4, 8, 16, 32, 64, or 128.
Session Table Slow-Age Period (minutes)	Sets the session slow-age period: 2, 4, 8, 16, 32, 64, 128, 256, 512, 1024, 2048, 4096, 8192, 16384, 32768 or 65536. **Note:** Alteon OS and above supports only up to 32768 minutes as slow-age period.
Transparent Proxy Cache Protocol	Enables or disables TPCP.

Field	Description
Metric (Response & Bandwidth) Update Interval	Sets the interval of the response and bandwidth metric updates.
LDAP Version	Sets the version number for LDAP to version 2 or version 3.
Allow HTTP Health Check on any port?	Enable or disable allow HTTP health check on any port. If disabled, the non-HTTP virtual services will use TCP Health Checks, if enabled the HTTP Content Health Check will be sent to any port except HTTPS (443) if properly configured.
Time Window [1]	Sets the time window for TCP rate limiting.
Hold Duration [1]	Sets the hold down duration for TCP rate limiting. This is an integer from 1 to 65,535.
Substitute Mac	Enables or disables Source MAC address substitution.
SP Port Bind [1]	Enables or disables re-entrant session support for VMA. This option allows the user to check for multiple session entries on a VMA port.
Intrusion Detection Real Server Group [2]	Sets the hash parameter for intrusion detection server load balancing.
Source MAC address substitute [3, 6]	*Enables* or *disables* source MAC address substitution. Typically, the source MAC address is not modified for the packets going to the servers in an SLB environment. But if you enable this command, the switch will substitute the source MAC address (for the packets going to the server) with the MAC address of the switch.
Proxy IP Gratuitous ARP [5]	This feature is available only on Alteon Application switches running Alteon OS 20.1.1.0 and higher. Enable this command to send gratuitous ARPs for enabled proxy IP addresses (PIPs) every 30 seconds.
RTS Lookup per VLAN	Enables or disables the use of VLAN for Return to Sender information on the real server.
Virtual Server Service Statistics [3]	Enables or disables reporting of virtual service statistics.
SLB Session Attack Inspection Interval [4]	Allows you to configure the time interval (from one second to one hour) to specify how frequently you want to check the SLB sessions (attacks) the switch received. At the configured interval of time the switch will check if the number of sessions is within the configured limits. You can set the next field: SLB Session Attack Alert Allowable Limit.

Field	Description
SLB Session Attack Alert Allowable Limit [4]	Allows you to specify the maximum number of sessions the switch can receive at any given period of time. If the number of sessions exceeds this limit, the switch will generate a syslog and an SNMP trap to alert the administrator that the switch is under SLB attack.
Ingress Port Session Table Binding [4]	Enables or disables the inclusion of the ingress port number in the session table look up.

1. This feature is applicable on Alteon OS 20.x and lower.
2. This feature is applicable only on Alteon 180 or AD series.
3. This feature is applicable only on Alteon OS 21.0 and higher.
4. This is applicable only to Alteon OS and higher.
5. This is applicable to Alteon OS 21.0 and lower.
6. This is applicable only to Web OS 10.1 and higher.

Configuring Layer 4 SLB: Real Servers

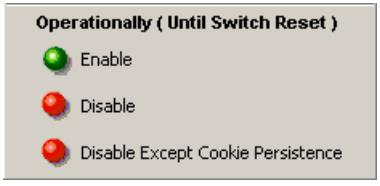
This menu is used for configuring information about real servers that participate in a server pool for Server Load Balancing or Application Redirection.

Right-Clicking for Operational Real Server Commands

You can right-click to operationally enable or disable a server in the Real Servers Configuration window.

The Disable Except Cookie Persistence option allows the switch to continue to send cookie persistent HTTP 1.0 sessions to the real server until that session ages out. Then the real server is disabled. If the real server is down, the switch will remove the persistent sessions and reassign to another real server.

The operational setting will remain in effect until the next reset of the switch. To configure the setting, right-click on the a real server index field, and select the desired command.





You can add URL path by using this button.

Field	Description
Real Server	The real server number.
IP Address	The IP address of the real server.
State	Enables or disables the real server.
Name	The name of the real server. This field is optional and may be left blank.

Field	Description
Weight	Sets the weighting value that this real server will be given in the load balancing algorithms. Higher weighting values force the server to receive more connections than the other servers configured in the same real server group. By default, each real server is given a weight setting of 1. A setting of 10 would assign the server roughly 10 times the number of connections as a server with a weight of 1. Weights are not applied when using the *hash* or *minmisses* metrics.
Max. Connections	Sets the maximum number of connections that this server should simultaneously support. This option sets a threshold as an artificial barrier, such that new connections will not be issued to this server if the Max. Connections limit is reached. New connections will be issued again to this server once the number of current connections has decreased below the Max. Connections setting. If all servers in a real server group for a virtual server reach their maxcon limit at the same time, client requests will be sent to the backup/overflow server or backup/overflow server group. If no backup servers/server groups are configured, client requests will be dropped by the virtual server.
Timeout	The maximum number of minutes that an inactive connection remains open. Every client-to-server session being load balanced is recorded in the switch's Session Table. When a client makes a request, the session is recorded in the table, the data is transferred until the client ends the session, and the session table entry is then removed. In certain circumstances, such as when a client application is abnormally terminated by the client's system, TCP/UDP connections will remain registered in the switch's binding table. In order to prevent table overflow, these orphaned entries must be aged out of the binding table. Using the Timeout option, you can set the number of minutes to wait before removing orphan table entries. Settings must be specified in even numbered increments between 2 and 30 minutes.
Backup	Sets the backup server number for this server. 0 indicates no backup server. To prevent loss of service if a particular real server fails, use this option to assign a backup real server number. Then, if the real server becomes inoperative, the switch will activate the backup real server until the original becomes operative again. The backup server is also used in overflow situations. If the real server reaches its maxcon (maximum connections) limit, the backup comes online to provide additional processing power until the original server becomes desaturated. The same backup/overflow server may be assigned to more than one real server at the same time.

Field	Description
Health Check Interval	Sets the interval between real server health verification attempts. 0 (zero) indicates *none*. Determining the health of each real server is a necessary function for Layer 4 switching. For TCP services, the switch verifies that real servers and their corresponding services are operational by opening a TCP connection to each service, using the defined service ports configured as part of each virtual service. For UDP services, the switch pings servers to determine their status.
Failure Retries	Sets the number of failed health check attempts required before declaring this real server inoperative.
Success Retries	Sets the number of successful health check attempts required before declaring a UDP service operational.
Type	Sets the server type: *local-server* or *remote-server*. The default is *local-server*. Type should be set to *remote-server* when the real IP address supplied above represents a remote server (real or virtual) that this switch will access as part of its Global Server Load Balancing network.
No Cookie Operation [1]	Enables or disables the real server to handle client requests that do not contain a URL cookie.
Exclude String Match [1]	Enables or disables the real server to handle requests that do not match the load balance string.
Substitute Source MAC	Enables or disables MAC source address substitution for Layer 4 traffic. **Note:** To substitute the MAC source address of client-to-server frames, Substitute Source MAC must be enabled.
Client Proxy	Enables or disables the client proxy. With this option enabled (default), a client request from any application can be proxied using a load-balancing Proxy IP address (PIP).
URL Paths [1]	**Note:** Sets the URL Paths selected for URL load balancing by the real server. This can be configured by selecting the URL button. In the URL Path Membership window, the available URL paths are listed.
Object ID [1]	Specifies the object identifier (OID). This OID overrides the OID for SNMP health checks.
Community String [1]	Overrides community string for SNMP health checks.
IDS VLAN [1]	Defines VLAN ID for the Intrusion Detection Server.
IDS Port [1]	Defines port for Intrusion Detection Server.

Field	Description
LDAP Write Sever [2]	Enables or disables LDAP write server. LDAP servers are of two types: read servers and write servers. You need to use read servers when you only want to browse the directory. You need to use the write servers when you want to modify the directory on the server. The write server can conduct both read and write operations.
Fast Health Check [2]	Enables or disables Fast Health Check operation.
Global SLB Availability [2, 3]	Displays the currently available real server for Global server load balancing and allows you to change to another real server for Global server load balancing.

1. This is applicable only on Alteon OS 21.0 and higher and on ALO 1.0 and higher.
2. This is applicable only on Alteon OS and higher.
3. This is applicable only when GSLB key is set.

Configuring Layer 4 SLB: Real Server Ports

Field	Description
Real Server	Sets the number of the real server. Select the **Browse..**. button to choose a configured Real Server.
Port Index	Sets the port index.
Port	Sets the number of the TCP/UDP real service port. Select the **Browse..**. button to choose a port.

Configuring Layer 4 SLB: Real Server Groups

This tab is used for combining real servers into real server groups. Each real server group should consist of all the real servers which provide a specific service for load balancing. Each group must consist of at least one real server. Each real server can belong to more than one group. Real server groups are used both for Server Load Balancing and Application Redirection.



You can add real servers by using this button.

Field	Description
Group	Sets the real server group number.
Name	Sets the name of the real server group. A maximum of 31 characters is allowed.
Real Servers	The numbers of the selected real servers that belong to the real server group. This can be modified by selecting the Servers button.
Metric	Sets the load balancing metric that is used to select the next server in the group. Use the drop-down combo box to view the available metrics. For a detailed description of the load balancing metrics that can be configured in this field, see the `/cfg/slb/group/metric` command description in your *Alteon OS Command Reference*.
Real Port Metric [1]	Sets the load balancing metric used for determining which port in the real server will be the target of the next client request.
Virtual Service Health Formula [1]	Defines an advanced health check formula expression for the real servers. This field allows you to create a boolean expression to health check the real server group based on the state of the virtual services. This field supports two boolean operators, AND or OR that are used to manipulate TRUE or FLALSE values. Using parenthesis with the boolean operators, you can create a boolean expression to state the health of the server group. This field also supports a string expression which is up to 128 characters long, or you can also set the formula expression as none.
Group Access for Operator [1]	Enables or disables the real server group operation.

Field	Description
Backup Server	Sets the real server to be used as the backup/overflow server for this real server group. To prevent loss of service if the entire real server group fails, use this option together with Backup Group below to assign a backup real server to a real server group number. Then, if the real server group becomes inoperative, the switch will activate the backup real server or backup real server group until one of the original real servers becomes operative again. The backup server/server group is also used in overflow situations. If all the servers in the real server group reach their maxcon (maximum connections) limit, the backup server/server group comes online to provide additional processing power until one of the original servers becomes desaturated. The same backup/overflow server/server group may be assigned to more than one real server group at the same time.
Backup Group	The backup real server group for this group. Only one type of Backup up is allowed, Backup Group or Backup Server. 0 means no Backup Group is configured.
Health Check	Sets the health check type. Use the drop-down combo box to view the health check types available for your switch. For a detailed description of the health check options that can be configured in this field, see the `/cfg/slb/group/health` command description in your *Alteon OS Command Reference*.
Health Check Content	This option defines the specific content that is examined during health checks. The content depends on the type of health check specified in the Health Check field.
Real Server Failure Threshold	The Real Server Failure Threshold specifies a minimum number of real servers that must be available in the specified real server group. If at any time the number of failed real servers in the real server group reaches this minimum limit, a syslog message is sent to the syslog servers.
VIP Health Checking	Enables or disables virtual server IP address (VIP) health checking in Direct Server Return (DSR) mode. Enables or disables VIP health checking in a service. This feature is enabled by default. However, it works only when the service has DSR (Direct Server Return) feature enabled. When VIP Health Checking is disabled, the switch uses the real server IP address (RIP) to perform all health checks, whether DSR is enabled or disabled.
Intrusion Detection State [1]	Enables or disables intrusion detection for the selected real server group. This feature is available in Alteon OS version 20.0 and higher. When enabled, the switch copies incoming traffic to a group of intrusion detection servers. Intrusion Detection must be enabled on client and server ports for this real server group.

Field	Description
Intrusion Detection Port [2]	The TCP port assigned to intrusion detection group. A value of 0 means that when intrusion detection is enabled, the switch will copy all ingress traffic from a port with IDS enabled and send it to one of the ids servers in the IDS group. **Example:** To configure the switch to copy only ingress HTTP traffic to a group of IDS servers, select the **Browse..**. button and select the service port 80.
Intrusion Detection Group Flood [2]	Enables or disables intrusion detection group flood. When *enabled*, will cause the IDS packets to be sent to all real servers in the group.
Hash Bits [3]	Defines the minmisses hash parameter for this real server as either 24 or 32 bits. By default the minmiss algorithm uses the upper 24-bits of the source IP address to calculate the real server that the traffic should be sent to when the minmiss metric is selected.You can also select all 32-bits of the source IP address to hash to the real server.
Persistent Hash Metric Mask [2]	The phash metric combines the best features of the hash and minmiss metrics. With phash enabled, the switch supports an even load distribution (hash) and stable server assignment (minmiss) even when a server in the group goes down. With the phash metric, the first hash will always be the same even if a real server is down. If the first hash hits a dead server, it will rehash for that request based on the actual number of servers that are up. This results in a request always being sent to a server that is up.

1. This is applicable only to Alteon OS and higher.
2. This is applicable only on Alteon Application Switches.
3. This is applicable only on Alteon Application Switches and on ALO 1.0 and higher.

Configuring Layer 4 SLB: Real Server Group State

This feature is used to enable or disable the real servers in a real server group.

Note: This feature is applicable only on Alteon OS 22.0 and higher.

Field	Description
Real Server Group	Allows you to place real servers into real server groups.
Real Server	Allows you to configure real servers.
State	Enables or disables the real server.

Configuring Layer 4 SLB: Real Server Group Operation

This feature is used to enable or disable the operation status of the real servers in a real server group.

Note: This feature is applicable only on Alteon OS 22.0 and higher.

Field	Description
Real Server Group	Allows you to place real servers into real server groups.
Real Server	Allows you to configure real servers.
State	Enables or disables the real server.

Configuring Layer 4 SLB: Virtual Servers on Alteon 180 or AD series

This tab is used for configuring the virtual servers which will be the target for client requests for Server Load Balancing. Configuring a virtual server requires the following parameters:

- Creating a virtual server IP address
- Adding a TCP/UDP port and real server group
- Enabling the virtual server (disabled by default)



To configure virtual services for a virtual server, select the row of the desired virtual server then select the **Services** button.

Note: All cookie-related parameters are shared by all configured virtual services.

Field	Description
Virtual Server	The number of the virtual server.
IP Address	IP address of the virtual server. Sets the IP address of the virtual server using dotted-decimal notation. The virtual server created within the switch will respond to ARPs and PINGs from network ports as if it was a normal server. Client requests directed to the virtual server's IP address will be balanced among the real servers available to it through real server group assignments.
State	Enables or disables the virtual server.
Layer 3 Only	Enables or disable Layer 3-only balancing: layer3Only or disable.
Domain Name	Sets the domain name for this virtual server. The domain name typically includes the name of the company or organization, and the Internet group code (.com, .edu, .gov, .org, and so forth). An example would be foocorp.com. This field should not include the Host Name portion (www, www2, ftp, and so forth).To clear the Domain Name, leave this field blank.
Cookie Name	Sets the cookie name of the virtual server used for cookie-based persistence. **Note:** If the Virtual Service parameter for Persistent Binding is not set to Cookie, this field is not used.

NORTEL NETWORKS
216515-B, September 2004

Field	Description
Cookie Offset	Sets the starting byte offset of the cookie value. This value is used in cookie-based persistence feature. If the Virtual Service parameter for Persistent Binding is not set to Cookie, or if Cookie Persistence Mode is not Passive, this field is not used. For more information on configuring cookie-based persistence, see the *Application Guide*.
Cookie Length	Sets the number of bytes to extract from the cookie value. If any Virtual Service parameter Cookie Persistence Mode is in Rewrite mode, the only valid lengths are 8 or 16. If the Virtual Service parameter Cookie Persistence Mode is not in Rewrite or Passive mode, or Persistent Binding is not set to cookie, this field is not used. For more information on configuring cookie-based persistence, see the *Application Guide*.
URI Cookie Search	Enables or disables cookie search in URI.
Hash Length	Sets the number of bytes to hash to the server. **Note:** 0 (zero) disables URL hashing.
HTTP Header Name	Sets the HTTP header name of the virtual server.
Cookie Search Response Count	Sets the maximum response count for cookie-based persistence. The switch will examine each server response until the cookie is found, or until the maximum count is reached.
Expire Cookie	The cookie expire of the virtual server used for insert cookie load balance depending on the mode it has the following format MM/dd/yy[@hh:mm] absolute mode or days[:hours[:minutes]] for relative mode. **Note:** If Virtual Service parameter for Cookie Persistence Mode is set to Insert, or if the Persistent Binding is not set to Cookie, this field is not used.
BWM Contract	Sets up to 1024 bandwidth management contracts on the Alteon AD4 and Alteon 184 Web switches. The Alteon AD3 and Alteon 180e Web switches do not support Bandwidth Management.

Note: You need to buy the software key to enable BWM on your switch.

Configuring Virtual Server Services on Alteon 180 or AD series

This tab is used for configuring the virtual server services which will be the target for client requests for Server Load Balancing. Configuring a virtual server requires the following parameters:

- Creating a virtual server IP address
- Adding a TCP/UDP port and real server group
- Enabling the virtual server (disabled by default)

To configure virtual services for a virtual server, first select the row of the desired virtual server in a Virtual Server window, then press the **Services** button.To configure virtual server services, select the **Insert** button to create a new configuration.

Note: To modify an existing configuration, click on the **Modify** button.

Field	Description
Virtual Server	The number of the Virtual Server. Select the **Browse..**. button to choose a Virtual Server.
Virtual Service	The number of the Virtual Service.
Virtual Port	The number of the Virtual Port. Select the **Browse..**. button to choose a Virtual Server.
Real Group	The number of the Real Group. The Real Group is the group of servers that will load balance this service. Select the **Browse..**. button to choose a Real Group.
Real Server Port Mapping	Defines the real server TCP or UDP port assigned to this service. By default, this is the same as the virtual port (service virtual port). If the real server port is configured to be different than the virtual port, the switch will map the virtual port to this real port.
UDP Balancing	Enables or disables UDP load balancing for a virtual port (disabled by default). You can configure this option if the service(s) to be load balanced include UDP and TCP: for example, DNS uses UDP and TCP. In those environments, you must activate UDP balancing for the particular virtual servers that clients will communicate with using UDP.

Field	Description
Cookie Persistence Mode	Sets cookie persistence mode: *rewrite*, *passive*, *insert*, or *disabled*. • *rewrite*: In active cookie mode (or cookie rewrite mode), the switch, and not the network administrator, generates the cookie value on behalf of the server. The switch intercepts this persistence cookie and rewrites the value to include server-specific information before sending it to the client. **Note:** In Rewrite mode, the Virtual Server parameter Cookie Length can only be 8 or 16. Also, the Virtual Server parameter Cookie Offset is invalid in rewrite mode. • *passive*: In this mode, the network administrator configures the Web server to embed a cookie in the server response that the switch looks for in sub-sequent requests from the same client. • *insert*: When a client sends a request without a cookie, the server responds with the data, and the switch inserts an Alteon persistence cookie into the data packet. The switch uses this cookie to bind to the appropriate server. **Note:** If set to Insert mode, the Virtual Server parameters Cookie Name, Cookie Offset, Cookie Length and Expire Cookie are invalid.
Persistent Binding	Sets persistent binding type: *disabled, clientip*, *sslid*, or *cookie*. **Note:** If persistent binding type is not set to *cookie*, the Virtual Server parameters *Cookie Name, Cookie Offset, Cookie Length* and *Expire Cookie* are invalid.
Host Name	Sets the hostname for a service added. This is used in conjunction with Domain Name to create a full host/domain name for individual services. For example, to add a hostname for Web services, you could specify `www` as the Host Name. If a domain name of “foocorp.com” was defined, “www.foocorp.com” would be the full host/domain name for the service.
HTTP SLB 1st	Sets the first HTTP SLB for load balancing on the following applications: • *urlslb*: Enable or disable URL SLB • *host*: Enable or disable for virtual hosting • *cookie*: Enable or disable cookie-based SLB for cookie-based preferential load balancing. You will be prompted for the following: Cookie name, starting point of the cookie value, number of bytes to be extracted, enable/disable checking for cookie in URI. • *browser*: Enable or disable SLB, based on browser type • *urlhash*: Enable or disable URL hashing based on URI • *headerhash*: Hashes on any HTTP header value. • *others*: Requires inputs for a particular header field

Field	Description
Operator	Sets the logical operator for the 1st HTTP SLB and the 2nd HTTP SLB: *and*, *or*, or *none*. You may choose to combine or select applications to load balance using the commands *and* and/or *or*. For example: • httpslb <application> • httpslb <application> and|or <application>
HTTP SLB 2nd	Sets the second HTTP SLB for load balancing on the following applications: • *urlslb*: Enable or disable URL SLB • *host*: Enable or disable for virtual hosting • *cookie*: Enable or disable cookie-based SLB for cookie-based preferential load balancing. You will be prompted for the following: Cookie name, starting point of the cookie value, number of bytes to be extracted, enable/disable checking for cookie in URI. • *browser*: Enable or disable SLB, based on browser type • *urlhash*: Enable or disable URL hashing based on URI • *headerhash*: Hashes on any HTTP header value. • *others*: Requires inputs for a particular header field
No NAT	Enables or disables substituting only the MAC address of the real server (disabled by default). This option does not substitute IP addresses. It is used for Direct Server Return (DSR) in an one-armed load balancing setup, so that frames returning from server to the client do not have to pass through the switch.
Remap UDP Fragments	Enables or disables remapping UDP Fragments.
RTSP URL SLB	Enables or disables Real Time Streaming Protocol (RTSP) URL balancing. RTSP Balancing can enable URL hashing using the entire URL except the extension (.xxx) at the end of the URL. • *hash*: URL hashing maintains persistency by enabling the client to hash to the same media server. • *patternMatch*: Matches a string pattern based on a configured server load balancing string.
Delayed Binding	Enables or disables Layer 4 Delayed Binding for TCP service and ports. Enabling this command protects the server from Denial of Service (DoS) attacks.
FTP Parsing	Enables or disables FTP SLB parsing for this virtual server. When this option is enabled, the switch modifies the appropriate FTP method/ command to support FTP servers on a private network for both active and passive FTP modes. To do this, the switch looks deeper into the packet and modifies the port command for active FTP or the “entering the passive mode” command for passive FTP.

Field	Description
DNS Query Load Balancing	Enables or disables DNS-based Layer 7 content load balancing.
BWM Contract	Sets the default BWM contract of the virtual server. Select the **Browse..**. button to choose a BWM contract.

Note: You need to buy the software key to enable BWM on your switch.

Configuring Layer 4 SLB: Virtual Servers on Alteon Application Switches

This tab is used for configuring the virtual servers which will be the target for client requests for Server Load Balancing. Configuring a virtual server requires the following parameters:

- Creating a virtual server IP address
- Adding a TCP/UDP port and real server group
- Enabling the virtual server (disabled by default)



To configure virtual services for a virtual server, first select the row of the desired virtual server in a Virtual Server window, then press the **Services** button.



To configure Global SLB rules for a virtual server, first select the row of the desired virtual server in a Virtual Server window, then press the **Add GSLB Rules**[1] button.

Note: All cookie-related parameters in Alteon OS 20.0 and higher, are configured in the Virtual Server Services window.

Field	Description
Virtual Server	The number of the virtual server.
IP Address	IP address of the virtual server.
State	Enables or disables the virtual server.
Layer 3 Only	Enables or disable Layer 3-only balancing: *layer3Only* or *disable*. Normally, the client IP address is used with the client Layer 4 port number to produce a session identifier. When the layr3 option is enabled (disabled by default), the switch uses only the client IP address as the session identifier. It associates all the connections from the same client with the same real server while any connection exists between them. This option is necessary for some server applications where state information about the client system is divided across different simultaneous connections, and also in applications where TCP fragments are generated. If the real server to which the client is assigned becomes unavailable, the Layer 4 software will allow the client to connect to a different server.

Field	Description
Domain Name	Sets the domain name for this virtual server. The domain name typically includes the name of the company or organization, and the Internet group code (.com, .edu, .gov, .org, and so forth). An example would be foocorp.com. It does not include the Host Name portion (www, www2, ftp, and so forth).To clear the Domain Name, leave this field blank.
Global SLB Weight [1]	Sets the Global server weight for the virtual server. The higher the weight value, the more connections that will be directed to the local site. The default is 1. The response time of this site is divided by this weight before the best site is assigned to a client. Remote site response times are divided by the real server weight before selection occurs.
Global SLB Availability [1]	Sets the Global SLB availability for the virtual server. The availability metric allows you to select the next server in a priority list when the capacity threshold of the previous servers has been reached.
GSLB Rules [1]	Allows you to select rule for this virtual server. Rules allow the GSLB selection to use different metric preferences based on time-of-day. You can configure one or more rules on each domain. Each rule has a metric preference list. The GSLB selection selects the first rule that matches the domain and starts with the first metric in the metric preference list of the rule.
BWM Contract	Sets the default BWM contract of the virtual server. Select the **Browse..**. button to choose a BWM contract.

1. This is applicable only on Alteon OS and higher. GSLB must be enabled.

Note: You need to buy the software key to enable BWM and/or GSLB on your switch.

Configuring Virtual Server Services on Alteon Application Switches



To open the Virtual Server Services window, press the **Services** button of the Virtual Servers window located at the bottom of the screen.

- To configure virtual server services, select the **Insert** button to create a new configuration.
- To modify an existing configuration, click on the **Modify** button.

Field	Description
Virtual Server	The number of the Virtual Server. Select the **Browse..**. button to choose a Virtual Server.
Virtual Service	The number of the Virtual Service.
Virtual Port	The number of the Virtual Port.
Real Group	The number of the Real Group. The Real Group is the group of servers that will load balance this service. Select the **Browse..**. button to choose a Real Group.
Real Server Port	Defines the real server TCP or UDP port assigned to this service. By default, this is the same as the virtual port (service virtual port). If the real server port is configured to be different than the virtual port, the switch will map the virtual port to this real port.
UDP Balancing	Enables or disables UDP load balancing for a virtual port (disabled by default). You can configure this option if the service(s) to be load balanced include UDP and TCP: for example, DNS uses UDP and TCP. In those environments, you must activate UDP balancing for the particular virtual servers that clients will communicate with using UDP. The options are enabled, disabled, or stateless.

Field	Description
Cookie Persistence Mode	Sets cookie persistence mode: *rewrite*, *passive*, *insert*, or *disabled*. • *rewrite*: In active cookie mode (or cookie rewrite mode), the switch, and not the network administrator, generates the cookie value on behalf of the server. The switch intercepts this persistence cookie and rewrites the value to include server-specific information before sending it to the client. **Note:** In Rewrite mode, the Virtual Server parameter Cookie Length can only be 8 or 16. Also, the Virtual Server parameter Cookie Offset is invalid in rewrite mode. • *passive*: In this mode, the network administrator configures the Web server to embed a cookie in the server response that the switch looks for in sub-sequent requests from the same client. • *insert*: When a client sends a request without a cookie, the server responds with the data, and the switch inserts an Alteon persistence cookie into the data packet. The switch uses this cookie to bind to the appropriate server. **Note:** If set to Insert mode, the Virtual Server parameters Cookie Name, Cookie Offset, Cookie Length and Expire Cookie are invalid.
Persistent Binding	Sets persistent binding type: *disabled, clientip*, *sslid*, or *cookie*. **Note:** If persistent binding type is not set to *cookie*, the Virtual Server parameters *Cookie Name, Cookie Offset, Cookie Length* and *Expire Cookie* are invalid.
Host Name	Sets the hostname for a service added. This is used in conjunction with Domain Name to create a full host/domain name for individual services. For example, to add a hostname for Web services, you could specify `www` as the Host Name. If a domain name of “foocorp.com” was defined, “www.foocorp.com” would be the full host/domain name for the service.
HTTP SLB 1st	Sets the first HTTP SLB for load balancing on the following applications: • *urlslb*: Enable or disable URL SLB • *host*: Enable or disable for virtual hosting • *cookie*: Enable or disable cookie-based SLB for cookie-based preferential load balancing. You will be prompted for the following: Cookie name, starting point of the cookie value, number of bytes to be extracted, enable/disable checking for cookie in URI. • *browser*: Enable or disable SLB, based on browser type • *urlhash*: Enable or disable URL hashing based on URI • *headerhash*: Hashes on any HTTP header value. • *others*: Requires inputs for a particular header field

Field	Description
Operator	Sets the logical operator for the 1st HTTP SLB and the 2nd HTTP SLB: *and*, *or*, or *none*. You may choose to combine or select applications to load balance using the commands *and* and/or *or*. For example: • httpslb <application> • httpslb <application> and|or <application>
HTTP SLB 2nd	Sets the second HTTP SLB for load balancing on the following applications: • *urlslb*: Enable or disable URL SLB • *host*: Enable or disable for virtual hosting • *cookie*: Enable or disable cookie-based SLB for cookie-based preferential load balancing. You will be prompted for the following: Cookie name, starting point of the cookie value, number of bytes to be extracted, enable/disable checking for cookie in URI. • *browser*: Enable or disable SLB, based on browser type • *urlhash*: Enable or disable URL hashing based on URI • *headerhash*: Hashes on any HTTP header value. • *others*: Requires inputs for a particular header field
No NAT	Enables or disables substituting only the MAC address of the real server (disabled by default). This option does not substitute IP addresses. It is used for Direct Server Return (DSR) in an one-armed load balancing setup, so that frames returning from server to the client do not have to pass through the switch.
Remap UDP Fragments	Enables or disables remapping UDP Fragments.
RTSP URL SLB	Enables or disables Real Time Streaming Protocol (RTSP) URL balancing. RTSP Balancing can enable URL hashing using the entire URL except the extension (.xxx) at the end of the URL. • *hash*: URL hashing maintains persistency by enabling the client to hash to the same media server. • *patternMatch*: Matches a string pattern based on a configured server load balancing string.
Delayed Binding	Enables or disables Layer 4 Delayed Binding for TCP service and ports. Enabling this command protects the server from Denial of Service (DoS) attacks.
FTP Parsing	Enables or disables FTP SLB parsing for this virtual server. When this option is enabled, the switch modifies the appropriate FTP method/ command to support FTP servers on a private network for both active and passive FTP modes. To do this, the switch looks deeper into the packet and modifies the port command for active FTP or the “entering the passive mode” command for passive FTP.
DNS Query Load Balancing	Enables or disables DNS-based Layer 7 content load balancing.

Field	Description
Cookie Name	Sets the cookie name of the virtual server used for cookie-based persistence. **Note:** If the Virtual Service parameter for Persistent Binding is not set to Cookie, this field is not used.
Cookie Offset	Sets the starting byte offset of the cookie value. This value is used in cookie-based persistence feature. If the Virtual Service parameter for Persistent Binding is not set to Cookie, or if Cookie Persistence Mode is not Passive, this field is not used. For more information on configuring cookie-based persistence, see the *Application Guide*.
Cookie Length	Sets the number of bytes to extract from the cookie value. If any Virtual Service parameter Cookie Persistence Mode is in Rewrite mode, the only valid lengths are 8 or 16. If the Virtual Service parameter Cookie Persistence Mode is not in Rewrite or Passive mode, or Persistent Binding is not set to cookie, this field is not used. For more information on configuring cookie-based persistence, see the *Application Guide*.
URI Cookie Search	Enables or disables cookie search in URI.
Expire Cookie	Enter the cookie expiration as either: • a date: <MM/dd/yy[@hh:mm]> (e.g. 12/31/01@23:59) • a duration: <days[:hours[:minutes]]> (e.g. 45:30:90)
HTTP Header Name	The HTTP header name of the virtual server. Enter a string from 0 to 32 characters.
Hash Length	Enter a value from 0 to 255. The hash length is the number of bytes to hash to a server for URL hashing. A value of zero disables URL hashing.
Cookie Search Response Count	Enter a value from 1-16. The response count is the number of server HTTP responses in which the switch should look for a persistence cookie. For example, if set to 2, the switch will look for the persistence cookie in two server responses.
Direct [1]	Enables or disables Direct Access Mode (DAM) on the selected virtual service. If you are using this field to enable/disable DAM, then you do not need to globally enable or disable DAM.
Hash [2]	Allows you to select the hash parameter for computing the hash value used by the hash, phash, and minmisses SLB metrics. For example, the source IP address, or both source IP address and source port. If the user does not select any, the switch will use default hash parameter, which is `sip`.
LDAP Server [2]	Enables or disables the LDAP server.
LDAP Server Load Balancing [2]	Enables or disables the LDAP server load balancing.

Field	Description
SIP Load Balancing [2]	Enables or disables Session Initiation Protocol (SIP) server load balancing on Alteon EMS. When enabled, you can configure SIP service on the service port 5060 for a virtual server. SIP is a UDP-based application-level control protocol for creating, modifying and terminating sessions with one or more participants (documented in RFC3261). The SIP processing occurs at application level in order to parse out messages coming from client side as well as the server side. Using SIP on your switch, you can load balance Nortel's MCS (Multimedia Communication Server) proxy servers. Nortel Networks' MCS is a SIP enabled application Server. When SIP is enabled, you can scan and hash calls based on a SIP Call-ID header to an MCS server. You need to turn Direct Access Mode (DAM) on to perform SIP load balancing. You can use only minmiss as the load balancing metric since the load balancing is performed based on the Call-ID.
X-Forward Proxy Mode [2]	Enables or disables inserting the X-Forward-For header into the client HTTP request to preserve the client IP information. X-Forward-For is a special header that stores and identifies the client IP information. This feature is applicable only on HTTP protocol.
HTTP Redirect [2]	Enables or disables HTTP Redirection for Global server load balancing on a per VIP basis. Disabling HTTP Redirection causes GSLB to use proxy IP address for HTTP.
Real Port Session Lookup [2]	Enables or disables parsing of all packets in a session where layer 7 lookup is being performed. This field is enabled by default, and normally all data packets in a session are examined by the filter. However, some sessions may contain only one packet containing the Layer 7 content. Once this packet is found, subsequent packets can be ignored. When this field is disabled, Layer 7 lookup is turned off for the remaining packets in the session.
PIP Based on Egress Port/ VLAN [2]	Enables or disables proxy IP selection based on egress port or VLAN. By default, the SP selects the proxy IP address based on ingress port or VLAN. Using the epip command, you can configure the SP to select proxy IP address based on the egress port or VLAN.
BWM Contract	The Bandwidth Management (BWM) contract number for this service. Select the **Browse...** button to choose a BWM contract.

1. This field is applicable only on Alteon Application Switches and on ALO 1.0 and higher.
2. This is applicable only on Alteon OS and higher.

Note: You need to buy the software key to enable BWM on your switch.

Configuring Ports for Server Load Balancing

On each port, you can enable or disable processing independently for each type of Layer 4 traffic (client and server), thus expanding your network topology options.



You can add filter to a port using this button. Select the desired virtual server then select the **Services** button.

Field	Description
Port	The port number.
Proxy IP Address [1]	The proxy IP address of the interface.
Load Balance State	The server load balancing (SLB) state of the port: none, client, server, or client-server. • *none*: No SLB port. • *client*: performs SLB on the client port. Ports configured to process client request traffic bind servers to clients and provide address translation from the virtual server IP address to the real server IP address, re-mapping virtual server IP addresses and port values to real server IP addresses and ports. Traffic not associated with virtual servers is switched normally. • *server*: performs SLB on the server port. Ports configured to provide real server responses to client requests require real servers to be connected to the Layer 4 switch, directly or through a hub, router, or another switch. When server processing is enabled, the switch port re-maps real server IP addresses and Layer 4 port values to virtual server IP addresses and Layer 4 ports. Traffic not associated with virtual servers is switched normally. • *client-server*: performs SLB on client and server ports.
Hot Standby	Enables or disables hot-standby processing on the switch port.
Inter-Switch	Enables or disables interswitch processing on the switch port.
Proxy IP State	Enables or disables a proxy for traffic that ingresses this port. When the PIP is defined, client address information in Layer 4 requests is replaced with this proxy IP address. In Server Load Balancing applications, this forces response traffic to return through the switch, rather than around it, as is possible in complex routing environments. Proxies are also useful for Application Redirection and Network Address Translation (NAT). When pip is used with Application Redirection filters, each filter's rport parameter must also be defined.
Filtering	Enables or disables filtering on this port. Enabling the filter sets up the Real Server to look into the VPN session table.

Field	Description
Filters Applied	The numbers of the applied filters.
Return to Sender State	Enables or disables Return to Sender (RTS) state on the specified port, to support applications such as VPN load balancing. The switch records state in a session table, for frames that enter the switch to and from the VPNs. This session table ensures that the same VPN server handles all the traffic between an inside host and an outside client for a particular session.
Intrusion Detection State	Enables or disables the Intrusion Detection state. Sets the real server group number for Intrusion Detection System server load balancing. The copied incoming sessions will be load-balanced across the servers in this real server group. Enable this feature when configuring Intrusion Detection Load Balancing.

1. This field is applicable only on Alteon 180 or AD series and on ALO.

Configuring Layer 4 SLB: Proxy IP Addresses on Alteon Application Switches in Alteon OS 21.0 and Lower

This tab lets you configure proxy IP (pip) addresses on an on Alteon Application Switches in Alteon OS 21.0 and lower.

In complex network topologies, SLB functions can be managed using a proxy IP addresses on the client switch ports.

When the client requests services from the switch's virtual server, the client sends its own IP address for use as a return address. If a proxy IP address is configured for the client port on the switch, the switch replaces the client's source IP address with the switch's own proxy IP address before sending the request to the real server. This creates the illusion that the switch originated the request.

The real server uses the switch's proxy IP address as the destination address for any response. SLB traffic is forced to return through the proper switch, regardless of alternate paths. Once the switch receives the proxied data, it puts the original client IP address into the destination address and sends the packet to the client. This process is transparent to the client.

Note: All proxy IP addresses must be configured if you wish to enable Virtual Matrix Architecture (VMA). (See "Configuring General Server Load Balancing" on page 139.)

Proxy IP addresses are assigned to ports as follows:

Proxy IP Address Assignment on Alteon 2224

Proxy IP Address	Assigned Ports
Proxy IP Address 1	Ports 1-12 and 25
Proxy IP Address 2	Ports 13-24
Proxy IP Address 3	Port 26
Proxy IP Address 4	This address is not assigned to any port, but must be configured with an address if you wish to enable Virtual Matrix Architecture (VMA). (See "Configuring General Server Load Balancing" on page 139)

Proxy IP Address Assignment on Alteon 2424

Proxy IP Address	Assigned Ports
Proxy IP Address 1	Ports 1-12 and 25
Proxy IP Address 2	Proxy IP address 2 for ports 13-24 and 27
Proxy IP Address 3	Proxy IP address 3 for ports 26
Proxy IP Address 4	Proxy IP address 4 for port 28

Proxy IP Address Assignment on Alteon 2208

Proxy IP Address	Assigned Ports
Proxy IP Address 1	Ports 1-8
Proxy IP Address 2	Ports 9 and 10
Proxy IP Address 3	None
Proxy IP Address 4	None

Proxy IP Address Assignment on Alteon 2216

Proxy IP Address	Assigned Ports
Proxy IP Address 1	Ports 1-8 and 17
Proxy IP Address 2	Ports 9-16 and 18
Proxy IP Address 3	None
Proxy IP Address 4	None

Proxy IP Address Assignment on Alteon 3408

Proxy IP Address	Assigned Port
Proxy IP Address 1	Ports 1, 5, and 9
Proxy IP Address 2	Ports 2, 6, and 10
Proxy IP Address 3	Ports, 3, 7, and 11
Proxy IP Address 4	Ports 4, 8, and 12

Configuring Layer 4 SLB: Proxy IP Addresses on Alteon Application Switches in Alteon OS 22.0 and Above

This tab lets you configure proxy IP (pip) addresses on an on Alteon Application Switches in Alteon OS 22.0 and above.

In complex network topologies, SLB functions can be managed using a proxy IP addresses on the client switch ports.

When the client requests services from the switch's virtual server, the client sends its own IP address for use as a return address. If a proxy IP address is configured for the client port on the switch, the switch replaces the client's source IP address with the switch's own proxy IP address before sending the request to the real server. This creates the illusion that the switch originated the request.

The real server uses the switch's proxy IP address as the destination address for any response. SLB traffic is forced to return through the proper switch, regardless of alternate paths. Once the switch receives the proxied data, it puts the original client IP address into the destination address and sends the packet to the client. This process is transparent to the client.

Note: All proxy IP addresses must be configured if you wish to enable Virtual Matrix Architecture (VMA) (See "Configuring General Server Load Balancing" on page 139.)

Field	Description
Proxy IP Address	This field is used to set the switch proxy IP address using dotted decimal notation. When the proxy IP address is defined, client address information in Layer 4 requests is replaced with this proxy IP address.
Port	Displays the port on which the proxy IP address is configured.
VLAN	Displays the VLAN on which the proxy IP address is configured.

Configuring Layer 4 SLB: Real Time Streaming Protocol (RTSP) Load Balancing on Alteon 180 or AD series

This menu displays virtual services configured on service port 554 for RTSP traffic.

Field	Description
Index	The index number that is assigned to each RTSP URL expression.
Expression	The non-cacheable RTSP URL expression.

Configuring Layer 4 SLB: Health Scripts on Alteon Application Switches

This tab lets you configure scriptable health checks by entering pre-defined commands. You can configure up to eight health check scripts, each not exceeding 1,024 characters. This feature is available on Alteon Application Switches running Alteon OS 20.x and higher.

Field	Description
Index	Health script index number.

Field	Description
Health Script	The health script string. To configure this field, click on the Insert... button • *Add Open*: This button sets the TCP port to be opened, such as http port 80. To select a port, click the **Browse..**. button to open the Protocol Port Selection Dialog. Select the desired protocol port and click the Modify button. • *Add Send*: This button opens the Health Script Send dialog. Enter an ASCII string to send through an open TCP port. For example, an HTTP request, such as, `"GET /default.asp HTTP/1.1\\r\\nHOST: www.alteon.com\\r\\n\\r\\n."` • *Add Binary Send Content:* [1] Sends a binary request string in hexadecimal format for the request packet through an open TCP or UDP port to the server. • *Add Additional Binary Send Content:* [1] Allows you to append additional content to the packet generated by the binary send command. The Alteon OS 22.0 allows a maximum of 256 bytes to be entered. Using one or more nsend commands allows you to generate a binary content of more than 256 bytes in length. • *Add Expect*: This button opens the Health Script Expect dialog. Enter an ASCII string that is expected back for successful health check on an open TCP port. An example would be an HTTP response such as: `HTTP/1.1 200` • *Add Binary Expect Content:* [1] Allows you to configure binary content request string (in hexadecimal format) that you can search in each server response packet for successful health check on an open TCP port. • *Add Additional Binary Expect Content:* [1] Allows you to append additional content to the original content of the response packet specified by the binary expect command.

Field	Description
Health Script *(cont.)*	• *Add Offset:* [1] Allows you to specify the offset from the beginning of the UDP data area to start matching the content specified in the expect command. If you need to specify offset, you must do it after executing the binary expect command. • *Add Depth:* [1] Allows you to specify the depth (the window) in bytes beginning from the start of the UDP data area, or beginning from offset if offset was specified, to search for the binary expect content. • *Add Wait:* [1] Allows the user to configure a wait window for the expected response. The wait window starts when the request is sent from the switch. If the expected response is received within the wait window, the health check passes, otherwise the health check fails. The wait command should follow the offset and depth commands in the script. The wait window is set in the units of milli-seconds. • *Add Close:* This button enters a command to close the TCP connection. • *Remove Last:* This button removes the last entered line from the script.

1. This is applicable only to Alteon OS 22.0 and higher.

Configuring SNMP Health Scripts on Alteon Application Switches

This tab lets you configure scriptable health checks using the SNMP protocol to check the health of real servers.

Note: This feature is available only on Alteon OS version 20.1.1.0 and higher.

Field	Description
Health Check	The index number of the SNMP health check.
Sent OID	The Object ID (OID) to be sent in the SNMP GET request packet; for example, 1.3.6.1.4.1.1872.2.5.7.11.
Community String	The community string (password) to be used in the SNMP get request packet.
Expected Response Content	The content expected in the SNMP response packet. The content specified can be either a string or an integer value.
Invert	When the invert option is enabled the health check will fail if the response packet contains the value specified in the receive content field.
Use Weight [1]	Enables or disables this feature. When enabled, the real server weights are dynamically adjusted based on SNMP health check response.

1. This field is applicable only on Alteon Application Switches and on ALO 1.0 and higher.

Configuring Layer 4 SLB: Syn Attack

This tab allows you to configure TCP SYN attack prevention on the switch.

Detecting SYN Attacks

In Alteon OS, SYN attack detection is enabled by default, whenever delayed binding is enabled.

The probability of a SYN attack is higher if excessive half-open sessions are being generated on the Alteon Application Switch. Half-opened sessions show an incomplete three-way handshake between the server and the client.

To detect SYN attacks, the Alteon Application Switch keeps track of the number of new half-open sessions for a set period of time. If the value exceeds the threshold, then a syslog message and an SNMP trap are generated.

Note: The Syn Attack requires you to enable Delayed Binding in the Virtual Server Services window.

Field	Description
Check Interval	The interval, specified in seconds, that determines how frequently the switch checks for SYN attacks.
Threshold	The threshold indicating the number of new half-open sessions per second.

See also:

- “Delayed Binding” on page 156 (on Alteon 180 or AD series)
- “Delayed Binding” on page 162 (on Alteon Application Switches)
- “Half Opened TCP Connections” on page 400 (only on Alteon Application Switches)

Configuring Layer 4 SLB: Inbound Link Load Balancing

Note: You need to obtain a software key for this feature.
Note: This feature is available only on ALO and Alteon OS 22.0 and higher.

Inbound traffic is data from an external client on the Internet that enters the Alteon Link Optimizer to access an internal service, such as corporate Web servers or FTP servers.

Alteon OS allows you to load balance the inbound traffic by providing access to the external client with the best available WAN link. This is implemented by configuring the Alteon Link Optimizer as an authoritative name server. The Alteon Link Optimizer dynamically determines the best ISP link to use at the time the request is generated. The best link is determined by the configured metric, the load on the ISP, and periodic health checks on the upstream routers. For more information on load balancing metrics, see your *Application Guide*.

Field	Description
State	Enables or disables inbound link load balancing.
Real Group	Sets the real server ISP group number.
Time to Live	Sets the time-to-live for DNS resource records.

Configuring Layer 4 SLB: Domain Records

Note: This feature is available only on ALO and Alteon OS 22.0 and higher.
Note: The Inbound Link Load Balancing software key must be installed for this feature to be displayed.



You can configure domain mapping by selecting a domain and clicking on the **Domain Mapping** button.

Field	Description
Domain	The number of the domain.
Name	Allows you to configure the domain name.
State	Enables or disables the domain records.

Configuring Layer 4 SLB: Domain Mapping

Note: This feature is available only on ALO and Alteon OS 22.0 and higher.
Note: The Inbound Link Load Balancing software key must be installed for this feature to be displayed.

Field	Description
Domain	The number of the domain.
Index	The index number of the domain mapping entry.
Virtual Server	The number of the virtual server associated with the domain mapping entry.
Real Server	The number of the real server associated with the domain mapping entry.
State	Enables or disables the domain mapping entry.

Configuring Layer 4 SLB: Service Mapping

Field	Description
Index	The index number of the service.
Real Port	The real port associated with the service.

Configuring Layer 4 SLB: URL-Based BWM

This feature assigns bandwidth based on URL paths. For URL-based server load balancing, first define the strings to monitor. Each of these strings is attached to real servers, and any URL with the string is load balanced across the assigned servers. The best way to achieve URL-based bandwidth management is to assign a contract to each defined string. This allocates a percentage of bandwidth to the string or URL containing the string.

Field	Description
Virtual Server	The number of the virtual server.
Service	The number of the virtual service.
URL Path	The number of the URL path.
BWM Contract	The number of the bandwidth management contract.

Note: This feature is available only if the BWM software key is enabled.

Configuring Layer 4 SLB: Remote URL General settings on Alteon 180 or AD series

Note: This tab is for switches running Web OS 9.0.34 and lower, with Remote URL (RURL) software enabled. Do not use the Remote URL configuration tab and the sub menus unless the Web switch is connected to an Alteon appliance, running an Remote URL application.

Field	Description
Deny L2 Pass-Through	Enables or disables the option to deny packets from passing through Layer 2 if the switch runs out of buffer resources. This option is disabled by default.

Configuring Layer 4 SLB: Remote URL Destination Port on Alteon 180 or AD series

Note: This tab is for switches running Web OS 9.0.34 and lower, with Remote URL (RURL) software enabled.

The following items can be configured through the Insert button or the Modify button.

Field	Description
RURL Destination Port Index	The index number.
Port Range Low	Sets the low port number, an integer between 0 to 65,534.
Port Range High	Sets the high port number, an integer between: 0 to 65,534.

Configuring Layer 4 Global SLB

The following topics are covered in this section:

- "Configuring Layer 4 Global SLB: General" on page 185
- "Configuring Layer 4 Global SLB: Remote Sites" on page 188
- "Configuring Layer 4 Global SLB: Network Preferences" on page 191
- "Configuring Layer 4 Global SLB: Rules" on page 192
- "Configuring Layer 4 Global SLB: Rules Metric" on page 193

Configuring Layer 4 Global SLB: General

GSLB allows balancing server traffic load across multiple physical sites. The Alteon GSLB implementation takes into account an individual site's health, response time, and geographic location to smoothly integrate the resources of the dispersed server sites for complete global performance.

For suggestions on configuring your network topology for GSLB, see your *Alteon OS Application Guide*.

Note: In order to use the GSLB feature, you must have purchased a GSLB software license. See your GSLB license certificate for information on obtaining the password key. See Enabling Special Software Features on the Switch for information on how to enable the feature.

Field	Description
Global Server Load Balancing	Sets the state of the global SLB: on or off.
DNS Handoffs [2]	Enables or disables DNS handoffs to peer sites by this switch. This should be enabled for proper GSLB operation. If disabled, whenever the switch receives a DNS request for a configured service, it will respond only with its own virtual server IP address, regardless of performance or load considerations.
DNS Time to Live [2]	Specifies the duration that the DNS response from the switch (indicating site of best service) will remain in the cache of DNS servers. • A lower value may increase the ability of the GSLB system to adjust to sudden changes in traffic load, but will generate more DNS traffic. • Higher numbers may reduce the amount of DNS traffic, but may slow GSLB's response to sudden traffic changes.
HTTP Redirect	Enables or disables HTTP redirects to peer sites by this switch. When enabled (default), this switch will redirect client requests to peer sites if its own real servers fail or have reached their maximum connection limits. If disabled, the switch will not perform HTTP Redirects, but will instead drop requests for new connections and cause the client's browser to eventually issue a new DNS request.

Field	Description
DNS Local Address Response Only [2]	Enables or disables switch responses to DNS queries with local virtual server IP addresses. When enabled, the switch will always respond to DNS queries by providing a local virtual server IP address, as long as the virtual server IP address has healthy real servers with an aggregate number of available connections equal to the total from each server's configured maxcons value, minus the server's current number of connections. When the real servers for the local virtual server IP addresses are unavailable or saturated, the switch will respond to DNS requests using normal GSLB rules.
DNS with at least one address [2]	Enables or disables DNS responses (with) at least one address. At least one IP address is included in each DNS response. Even if all remote sites cannot handle another request, the local VIP is returned in DNS response to eliminate long DNS time-outs caused by an empty response.
Local Weight [2]	Sets the local weight. The higher the weight value, the more connections that will be directed to the local site. The response time of this site is divided by this weight before the best site is assigned to a client. Remote site response times are divided by the real server weight before selection occurs.
Remote Site Update Interval	Sets the time between Distributed Site State Protocol (DSSP) updates between this switch and its peers.
Minimum Site Connections	Sets the minimum number of available site connections. If the site's available sessions fall below this value, traffic won't be redirected to the site. A site is not eligible for more requests (such as DNS or HTTP redirects) once the number of available connections at a site drops below this threshold.
Single Address Response [2]	Enables or disables DNS responses with only one address. At the most one IP address is included in each DNS response.
HTTP Redirect to Real Server Name	Enables or disables HTTP redirects to peer sites by this switch. When enabled (default), this switch will redirect client requests to peer sites if its own real servers fail or have reached their maximum connection limits. If disabled, the switch will not perform HTTP Redirects, but will instead drop requests for new connections and cause the client's browser to eventually issue a new DNS request.
Geographic Awareness [2]	Enables or disables geographic awareness, such as the IANA table. If this option is disabled, all clients and sites will be assumed to exist in the same geographic region, allowing all sites to be eligible for each client.
No Remote Real SLB [1]	Enables or disables no-remote real server load balancing. If enabled, the switch *will not* perform remote real server load balancing for non-HTTP protocols.

Field	Description
Encrypt Remote Site Update [1]	Enables or disables encryption of remote update DSSP messages. This feature should be enabled if your GSLB environment uses Alteon 180 or AD series Web switches versions 9.0 or 10.0. Or, upgrade your Web OS software to Web OS 9.0.41.11 and higher or Web OS 10.0.26.0 and higher.
Remote Site Update TCP Port [3]	Sets the TCP port number for remote site updates for Global server load balancing. The default TCP port is 80.
Session Utilization Capacity Threshold [3]	Sets the threshold for the CPU utilization capacity. The default configuration is 90%.
CPU Utilization Capacity Threshold [3]	Sets the threshold for the CPU utilization capacity. The default configuration is 90%.
Authoritative DNS Redirects [3]	Enables or disables DNS responses with only one address. At the most one IP address is included in each DNS response. This option is enabled by default.
DSSP Version [3]	Defines the version of Distributed Site State Protocol (DSSP) that is used to send out the remote site updates. DSSP is a proprietary protocol that resides above TCP.
Virtual Service HostName Matching [3]	Enables or disables lookups based on host or domain name in a GSLB configuration. When enabled, the hostname specified in the Virtual Service configuration, in addition to the domain name, will be used to resolve the IP address for the domain. When disabled, only the domain name will be used to match.
Remote Site Status Time Interval [3]	Sets the time interval in seconds for remote site updates. The range is between 10 and 7200 seconds.

1. This field is applicable on Alteon OS and Web OS 10.1.1.0 and higher.
2. This field is applicable on Alteon OS 21.x and lower.
3. This field is applicable on Alteon OS 22.0 and higher.

Configuring Layer 4 Global SLB: Remote Sites

Field	Description
GSLB Remote Site	The index number of the GSLB remote sites table.
Name	Sets the Name of the GSLB remote site.
Primary IP Address	Defines the IP address of the primary switch at the remote site used for Global Server Load Balancing. Use dotted decimal notation.
Secondary IP Address	If the remote site is configured with a redundant switch, enter the IP address of the IP interface for the remote secondary switch here. If the remote site primary switch fails, the local switch will address the remote site secondary switch instead.
State	Enables or disables GSLB of the remote site.
Status Update	Enables or disables remote site updates. If enabled (default), this switch will send regular Distributed Site State Protocol (DSSP) updates to its remote peers using HTTP port 80. If disabled, the switch will not send state updates. If your local firewall does not permit this traffic, disable the updates. **Note:** When update is enabled, Global Server Load Balancing uses service port 80 on the IP interface for DSSP updates. By default, the Web OS Web-based interface also uses port 80. Both services cannot use the same port. If both are enabled, configure the Web OS Browser-Based Interface (BBI) to use a different service port. To change the service port for the BBI, Telnet to the switch CLI and enter the `/cfg/sys/wport` command. You cannot change the service port using Alteon EMS.

Configuring Layer 4 Global SLB: Lookups

Note: This feature is applicable only on Alteon OS 21.0 and lower.

Field	Description
Network Preference Lookups [1]	Enables or disables network preference lookups.
Domain Name for Internal Lookup Table [1]	Sets the domain name for the internal lookup table. Note: This is not applicable to on Alteon 180 or AD series.
HostName Lookups [2]	Enables or disables hostname matching in lookups.

1. This field is applicable on Alteon OS 21.0 and lower, but does not exist in Web OS 10.0.30.5 and higher.
2. This field is applicable on Alteon OS 21.0 and lower and in Web OS 10.1.1.0 and higher.

Configuring Layer 4 Global SLB: Network Lookups

You can use the options in this tab to overwrite the IANA table by defining client networks. You should use regular GSLB to respond to a DNS request under the following conditions:

- Queried domain is not matched.
- Client IP address doesn't match address in the Network Preference Menu and no default entry is configured.
- There is an entry match in the Network Preference Menu. However, VIP1 and VIP2 are not healthy—they are down or over the minimum number of connections (mincon).

The default entry is one where the source IP address and mask are not configured (both are 0.0.0.0) and only the VIP1 and VIP 2 are configured. All client networks that are not in the Network Lookups Menu will use this entry to respond to a DNS request.

Note: This feature is applicable only on Alteon OS 21.0 and lower.

Field	Description
Internet Network	The index number of the Internet network preference table.
Source IP Address	Sets the source IP address. Specify an IP address in dotted decimal notation, or "none". A range of IP addresses is produced when used with the mask option.
IP Subnet Mask	Sets the IP Subnet mask of the network table. This IP address mask is used with the source IP address to find a correct virtual server IP address to respond to a DNS request.
First Virtual IP Address	Sets the address of the primary virtual IP. The address can either be a local or remote virtual server. The switch returns the VIP address with the least response time that is over the minimum number of available connections.
Second Virtual IP Address	Sets the address of the secondary virtual server IP address.

Configuring Layer 4 Global SLB: Network Preferences

Network preference selects a server based on the preferred network of the source IP address for a given domain. The preferred network contains a subset of the servers for the domain.

Up to 128 network preference numbers can be set.



You can add real servers by using this button.



You can add virtual servers by using this button.

Note: This feature is applicable only on Alteon OS 22.0 and higher.

Field	Description
Network Preference	Allows you to select the network preference.
State	Enables or disables the network.
Source IP	Defines the source (client) IP address. Specify an IP address in dotted decimal notation. A range of IP addresses is produced when used with the mask.
Network Mask	This IP address mask is used with the source IP (SIP) address to find a correct virtual server IP address to respond to a DNS request, such as 255.255.255.0.
Virtual Servers	Adds a virtual server to the network. No virtual server is added by default.
Remote Real Servers	Removes a virtual server from the network.

Configuring Layer 4 Global SLB: Rules

Rules allow the GSLB selection to use different metric preferences based on time-of-day. You can configure one or more rules on each domain. Each rule has a metric preference list. The GSLB selection selects the first rule that matches the domain and starts with the first metric in the metric preference list of the rule.

Note: This feature is applicable only on Alteon OS 22.0 and higher.

Field	Description
Rule	Displays the rule index.
State	Allows you to enable or disable the rule.
Start Hour	Defines the start hour for the rule.
Start Minute	Defines the start minute for the rule.
End Hour	Defines the end hour for the rule.
End Minute	Defines the end minute for the rule.
Time to Live	Specifies the duration (from 0 to 65535 seconds, with default at 60) that the DNS response from the switch (indicating site of best service) will remain in the cache of DNS servers. A lower value may increase the ability of the GSLB system to adjust to sudden changes in traffic load, but will generate more DNS traffic. Higher numbers may reduce the amount of DNS traffic, but may slow GSLB's response to sudden traffic changes.
DNS Resource Records	Sets the DNS resource records that how many DNS resource records will be returned in the DNS response.

Configuring Layer 4 Global SLB: Rules Metric

Note: This feature is applicable only on Alteon OS 22.0 and higher.

Field	Description
Rule	Displays the index of the rule.
Metric ID	Allows you to assign a metric ID.
Metric	Allows you to select the metric to select the next real server for GSLB out of: `leastconns|roundrobin|response|geographical|network|random|availability|qos|minmisses|hash|local|always|none.`

Configuring Layer 4: WAP

The following topic is covered in this section:

• “Configuring Layer 4: WAP General Properties” on page 195

Configuring Layer 4: WAP General Properties

Wireless Session Protocol (WSP) is used within the Wireless Application Protocol (WAP) suite to manage sessions between wireless devices and WAP content servers or WAP gateways. Alteon OS provides a content-based health check mechanism where customized WSP packets are sent to the WAP gateways, and the switch verifies the expected response, in a manner similar to scriptable health checks.

WSP content health checks can be configured in two modes: connectionless and connection-oriented. Connectionless WSP runs on UDP/IP protocol, ports 9200 and 9202 and connection-oriented (WTP) traffic runs on ports 9201 and 9203. Application switches can be used to load balance the gateways in both modes of operation.

Alteon OS allows you to configure three WAP gateway health check types for all four WAP services (WSP, WTP+WSP, WTLS+WSP, WTLS+WTP+WSP), deployed on WAP gateways/servers. For further details, refer to the Application Guide.

Field	Description
WAP Load Balancing	Enables or disables Wireless Application Protocol (WAP) load balancing.
WAP Debug Level	Sets the WAP debug level. The highest allowable number is the most verbose.
WSP Port to Health Check	Sets the Wireless Service Protocol (WSP) port number to health check. The default is WSP application port 9200.
WTLS Port to Health Check	Sets the Wireless Transport Layer Security (WTLS) port to health check. The default is WTLS application port 9203.
Offset into WSP Packet	Enter the receive offset value content of the received WSP packets. An offset value of 0 (default) sets the switch to start comparisons from the beginning of the content of the received packet.
Health Content to Send to WAP Gateway	Defines the content that is examined during health checks. Enter a hexidecimal string that represents a connectionless WSP request to a WSP gateway. This string will be delivered to the WSP gateway.
Expected Health Content from WAP Gateway	Enter a hexadecimal string that represents the content that the switch expects to receive from the WSP gateway. The string is the selected value for the gateway response to match.
Send Content [1]	Enter a hexadecimal string that represents a connectionless WSP request to a WSP gateway. This string will be delivered to the WSP gateway.
Receive Content [1]	Enter a hexadecimal string that represents the content that the switch expects to receive from the WSP gateway.

Field	Description
Connect Send Content [1]	Enter the content for the first switch-generated WSP session packet. This command allows you to customize the headers in the connect message.
WTP Port [1]	Defines the WTP port number to health check. The default port number is 9201.
WTLS WSP Port [1]	Defines the WTLS (Wireless Transport Layer Security) and WSP port number to health check. The connectionless encrypted WTLS traffic uses default port 9202.
Receive Offset [1]	Enter the offset value content of the received WSP packets. The offset value is the number of bytes from the beginning of the WSP PDU, at which the comparison begins to match with the expected receive content. An offset value of 0 (default) sets the switch to start comparisons from the beginning of WSP PDU of the received packet.
WAP RADIUS Coupling [1]	Enables or disables coupling together of all the four WAP services (WSP, WTP+WSP, WTLS+WSP, WTLS+WTP+WSP) with Radius Accounting Service. If the health check to any one of the four WAP services or Radius Accounting Service fails, then all of the four WAP services and Radius Accounting Service are disabled.

1. These fields are applicable only on Alteon Application Switches and on ALO 1.0 and higher.

Configuring Layer 7 on the Switch

This section discusses advanced load balancing solutions utilizing Layer 7 content switching such as inspecting HTTP headers, examining content identifiers such as URLs and cookies, and parsing content requests.

The following topics are discussed in this section:

- "Configuring Layer 7 URL Parsing: Expressions on Alteon 180 or AD series" on page 198
- "Configuring Layer 7 URL Parsing: WCR Redirect" on page 199
- "Configuring Layer 7 URL Parsing: SLB Strings" on page 201
- "Configuring Layer 7 URL Parsing: HTTP Methods" on page 203

Configuring Layer 7 URL Parsing: Expressions on Alteon 180 or AD series

This tab is used to configure the expressions file extensions that are *not cached* in a Web Cache Redirection scenario.

Noncacheable items:

The switch is preconfigured with a list of 12 noncacheable items:

- Dynamic content files: Common gateway interface files (.cgi), cold fusion files (.cfm), ASP files (.asp), BIN directory, CGI-BIN directory, SHTML (scripted html), Microsoft HTML extension files (.htx), executable files(.exe)
- Dynamic URL parameters: +, !, %, =, &

Field	Description
URL Path	The number of the URL Path. This number is used for making a URL-based switching decision. When you add URL paths to this table, make sure that the URL path numbering is consecutive; non-consecutive path numbers are not permitted.
String	The name of the noncacheable item. The first 12 string entries are preconfigured on the switch.

Configuring Layer 7 URL Parsing: WCR Redirect

This tab is used to configure Layer 7 properties for Web-cache redirection.

URL parsing for Web Cache Redirection operates in a manner similar to URL-based server load balancing except that in WCR a virtual server on the switch is the target of all IP/HTTP requests.

By separating static and dynamic content requests via URL parsing, Alteon OS enables you to send requests with specific URLs or URL strings to designated cache servers. The URL-based WCR option allows you to off load overhead processing from the cache servers by only sending appropriate requests to the cache server farm.

Field	Description
Redirect HTTP non-GETs to Origin Server	Enables or disables redirecting packets to the origin server when HTTP non-Gets are detected. • If this command is enabled, the switch will redirect all non-GET requests to the origin server. • If this command is disabled, the switch will compare the URI against the expression table to determine whether all non-GET requests should be redirected to a cache server or origin server.
Redirect Cookies to Origin Server	Enables or disables auto-ALLOW for cookie to origin servers. • If this command is enabled, the switch will redirect all requests that contain Cookie: in the HTTP header to the origin server. • If this command is disabled, the switch will compare the URI against the expression table to determine whether it should redirect all requests that contain Cookie: in the HTTP header to a cache server or origin server.
Redirect no-cache to Origin Server	Enables or disables redirecting packets to the origin server when no-cache headers are detected. • If this command is enabled, the switch will redirect all requests that contain Cache-Control: nocache in HTTP/1.1 header, or Pragma: no-cache in HTTP/1.0 header to the origin server. • If this command is disabled, the switch will compare the URI against the expression table to determine whether it should redirect requests that contain Cache-Control: no-cache in HTTP/1.1 header, or Pragma: no-cache in HTTP/1.0 header to a cache server or origin server.
URI Hash Length (bytes)	Specifies the number of bytes in the URI to hash on server.
Redirect Based on URI Header	Enables or disables URI header-based redirection.

Field	Description
HTTP Header Name	Sets the HTTP header name.
Error Message	User-defined message that is delivered to the client when the switch cannot bind the client's request to server.
String Case Sensitivity [1]	Enables or disables case sensitivity for string matching. Using this field you can do either case sensitive or case insensitive string comparison. If you disable case sensitive, all load balancing strings and all the request strings arriving on the switch will have to be converted to lower case before doing any string comparison.
Incomplete delayed binding timeout [1]	Sets the timeout for incomplete delayed binding connections.

1. This is applicable only on Alteon OS 22.0 and higher.

Configuring Layer 7 URL Parsing: SLB Strings

This tab is used to configure the strings for URL-based server load balancing (SLB).

SLB strings allow the switch to disperse content by making load-balancing decisions based on the entire path and filename of each URL.

Note: Both HTTP 1.0 and HTTP 1.1 requests are supported.

URL Matching

You can configure strings for URL matching. The number and length of the strings varies depending on your switch model and operating system. Each URL Web request is then examined against the URL strings that have been defined for each real server. URL requests are load balanced among multiple servers matching the URL, according to the load balancing metric that has been configured for the real server group.

Expressions Excluded from Web Cache Redirection

The SLB Strings tab can also be used to configure noncacheable expressions in a Web Cache Redirection scenario.

Field	Description
URL Path	The number of the URL Path. This number is used for making a URL-based switching decision.
String	The URL string.
HTTP Header [1, 2]	The HTTP header for URL load balancing.
HTTP Header Value [1, 2]	The HTTP header value for URL load balancing.
Pattern String Type [1]	Specifies the string type. The options are: ASCII, binary or none.
Offset [1, 3]	Specifies the offset value of a packet that comes in looking for a string. The default is 5.
Depth [1, 3]	Defines the maximum limit of how far a packet can go searching for a string.

Field	Description
Operator [1, 3]	Specifies an SLB string for load balancing. the options are: layer7 lookup or pattern matching. The pattern match can be set at: less than, equal to, or greater than.
BWM Contract [4]	Sets the Bandwidth Management (BWM) contract number. Select the **Browse..**. button to choose a BWM contract.

1. This is applicable only on Alteon OS 21.0 or higher and on ALO 1.0 and higher.
2. This is applicable when pattern string type is none.
3. This is applicable when pattern string type is not none.
4. This is applicable only when Bandwidth Management key is enabled on the switch.

Configuring Layer 7 URL Parsing: HTTP Methods

Note: This feature is applicable only on Alteon OS 22.0 and higher.

Field	Description
Index	HTTP method number.
HTTP Methods	Allows you to add HTTP request methods to your switch software. HTTP allows an open-ended set of methods to be used to indicate the purpose of a request. 22 request methods are supported. The methods GET and HEAD *must* be supported by all general-purpose servers. All other methods are optional. A method is case-sensitive. The software supports both HTTP 1.0 and HTTP 1.1 to perform HTTP request methods.

Configuring Virtual Routing

Alteon switches support high-availability network topologies through an enhanced implementation of the Virtual Router Redundancy Protocol (VRRP).

The following topics are discussed in this section:

- "Configuring Virtual Routing: General" on page 205
- "Configuring Virtual Routing: Routers" on page 207
- "Configuring Virtual Routing: Interfaces" on page 209
- "Configuring Virtual Routing: Groups" on page 210
- "Configuring Virtual Routing: Synchronizing to a Peer Switch" on page 214
- "Configuring Virtual Routing: Peers" on page 215

Configuring Virtual Routing: General

Virtual Router Redundancy Protocol (VRRP) support on Alteon switches provides redundancy between routers in a LAN. This is accomplished by configuring the same virtual router IP address and ID number on each participating VRRP-capable routing device. One of the virtual routers is then elected as the master, based on a number of priority criteria, and assumes control of the shared virtual router IP address. If the master fails, one of the backup virtual routers will assume routing authority and take control of the virtual router IP address. By default, VRRP is disabled.

Alteon has extended VRRP to include virtual servers as well, allowing for full active/active redundancy between its Layer 4 switches.

Tracking

Tracking used for setting weights for the various criteria used to modify priority levels during the master router election process. Each time one of the tracking criteria is met, the priority level for the virtual router is increased by an amount defined through this menu. In VRRP, tracking is a method that is used to increase the priority of a virtual router and thus its designation as Master. (with preemption enabled). Tracking can be very valuable in an active/active configuration. You can track the following:

- Virtual Routers in Master Mode (increments priority by 2 for each)
- Active IP interfaces on the Web switch (increments priority by 2 for each)
- Active ports on the same VLAN (increments priority by 2 for each)
- Active Layer 4 Ports, client or server designation (increments priority by 2 for each
- Healthy real servers (increments by 2 for each healthy real server)
- HSRP announcements heard on a client designated port (increments by 10 for each)

Field	Description
Virtual Routing	Globally enables or disables VRRP operation.
Track Virtual Router Increment	Sets the increment of VRRP virtual router priority. This priority is adjusted by tracking the state of other virtual routers. The value 254 provides maximum priority.

Field	Description
Track IP Interface Increment	Sets the increment of VRRP virtual router priority. This priority is adjusted by tracking the state of other virtual routers.
Track VLAN Ports Increment	Sets the increment of VRRP virtual router priority. The priority is adjusted by tracking the port state of those ports that belong to the same virtual LAN as the virtual router.
Track L4 Ports Increment	Sets the increment of VRRP virtual router priority. The priority is adjusted by tracking the Layer 4 port states. This is valid when a virtual server is configured as a VRRP virtual router.
Track Real Servers Increment	Sets the increment of VRRP virtual router priority. The priority is adjusted by tracking the state of real servers under the virtual server that is configured as a VRRP virtual router.
Track HSRP Advertisements Increment	Sets the increment of VRRP virtual router priority. The priority is adjusted by tracking the HSRP advertisements.
Hot Standby Processing	Enables or disables hot standby processing.
Track HSRP by VLAN Increment	Sets the priority increment value for VLAN port switch tracking.
Hold Time Before Changing State [1]	Suspends VRRP operation for the specified interval.

1. This is applicable only on Alteon Application Switches and on ALO 1.0 and higher.

Configuring Virtual Routing: Routers

This menu is used for configuring virtual routers for this switch. A virtual router is defined by its virtual router ID and an IP address. On each VRRP-capable routing device participating in redundancy for this virtual router, a virtual router will be configured to share the same virtual router ID and IP address.

Right-Clicking for Operational Virtual Router Commands



Click on the **Change to Backup** button (or right-click in the table row to select the command) to change a virtual router from Master to Backup. The setting will remain in effect until the next reset of the switch.

Field	Description
Virtual Router	The index number of the VRRP virtual router.
VRID	Defines the virtual router ID. This is used in conjunction with addr (below) to define a virtual router on this switch. To create a pool of VRRP-enabled routing devices which can provide redundancy to each other, each participating VRRP device must be configured with the same virtual router: one that shares the same VRID and addr combination. The VRID for standard virtual routers (where the virtual router IP address is not the same as any virtual server) can be any integer as defined on your particular switch model. The default value is 1. All VRID values must be unique within the VLAN to which the virtual router's IP interface belongs.
IP Address	Defines the IP address for this virtual router using dotted decimal notation. This is used in conjunction with the VRID (above) to configure the same virtual router on each participating VRRP device. The default address is 0.0.0.0.
IP Interface	Sets the IP interface that the VRRP virtual router represents. If the IP interface has the same IP address as the IP Address option above, this switch is considered the "owner" of the defined virtual router. An owner has a special priority of the highest available virtual router number, and will always assume the role of master router, even if it must preempt another virtual router which has assumed master routing authority. This preemption occurs even if the Preemption option below is disabled. The default value is 1.Select the **Browse..**. button to choose an IP interface.
State	Enables or disables the VRRP virtual router.

Field	Description
Priority	Defines the election priority bias for this virtual server. During the master router election process, the routing device with the highest virtual router priority number wins. If there is a tie, the device with the highest IP interface address wins. If this virtual router's IP address (addr) is the same as the one used by the IP interface, the priority for this virtual router will automatically be set to the highest available priority value.
Advertisement Interval	Sets the time interval between VRRP advertisements.
Preemption	Enables or disables a higher priority Backup VRRP virtual router to pre-empt a low-priority Master. When enabled, if this virtual router is in backup mode but has a higher priority than the current master, this virtual router will preempt the lower priority master and assume control. Note that even when Preemption is disabled, this virtual router will always preempt any other master if this switch is the owner. A switch is the owner when the IP interface address and virtual router address are the same.
Load Sharing	Enables or disables virtual router sharing, an Alteon-proprietary extension to VRRP. When enabled, this switch will process any traffic addressed to this virtual router, even when in backup mode. By default, this option is enabled.
Track VRs	Enables or disables tracking other virtual routers for priority adjustment.
Track IP Interfaces	Enables or disables tracking other virtual routers for priority adjustment.
Track VLAN Ports	Enables or disables tracking the states of VLAN ports for priority adjustment.
Track L4 Ports	Enables or disables tracking the state of Layer 4 ports for priority adjustment. This is applied when the virtual server is configured as a VRRP virtual router.
Track Real Servers	Enables or disables tracking the states of real servers for priority adjustment. This is applied when the virtual server is configured as a VRRP virtual router.
Track HSRP Advertisements	Enables or disables tracking HSRP advertisements for priority adjustment.
Track HSRP by VLAN	Enables or disables tracking VLANs for priority adjustment.

Configuring Virtual Routing: Interfaces

This menu is used for configuring VRRP authentication parameters for the IP interfaces that are used with the virtual routers. The interface-number (1 to 256) represents the IP interface on which authentication parameters must be configured.

Field	Description
Interface	The VRRP interface number.
Authentication Type	Sets the type of authentication in use. *none:* No authentication. *simple-text-password:* use the specified password for authentication.
Password	Sets the password for authentication.
IP Address	The IP address of the selected IP interface. This field is read-only.
State	The current VRRP state: enabled or disabled. This field is read-only.

Configuring Virtual Routing: Groups

The Virtual Router Group menu is used for associating all virtual routers into a single logical virtual router, which forces all virtual routers on the Alteon Switch to either be master or backup as a group. A virtual router is defined by its virtual router ID and an IP address.

On each VRRP-capable routing device participating in redundancy for this virtual router, a virtual router will be configured to share the same virtual router ID and IP address.

Note: This option is required to be configured only when using at least two Alteon Switches in a hot-standby failover configuration, where only one switch is active at any time.



Click on the **Change to Backup** button (or right-click in the table row to select the command) to change a virtual router group from Master to Backup. The setting will remain in effect until the next reset of the switch.

Field	Description
Virtual Router Group	The number of the VRRP virtual router.
VRID	The VRRP virtual group identifier.
IP Interface	Sets the IP Interface that the VRRP virtual group represents. Select the **Browse...** button to choose an IP Interface.
Advertisement Interval	Sets the time interval (in seconds) between VRRP advertisements.
Priority	Sets the priority value to be used by the specified VRRP virtual routers.
Preemption	Enables or disables a higher priority Backup VRRP virtual router to pre-empt a low priority Master.
State	Enables or disables the VRRP virtual router.
Load Sharing	Enables or disables load sharing a non-master virtual router.
Track VRs	Enables or disables tracking other virtual routers for priority adjustment. When enabled, the priority for this virtual router will be increased for each virtual router in master mode on this switch. This is useful for making sure that traffic for any particular client/server pairing are handled by the same switch, increasing routing and load balancing efficiency. This command is disabled by default.

Field	Description
Track IP Interfaces	Enables or disables tracking other router interfaces for priority adjustment. When enabled, the priority for this virtual router will be increased for each other IP interface active on this switch. An IP interface is considered active when there is at least one active port on the same VLAN. This helps elect the virtual routers with the most available routes as the master.
Track VLAN Ports	Enables or disables tracking port state of VLAN ports for priority adjustment. When enabled, the priority for this virtual router will be increased for each active port on the same VLAN. A port is considered “active” if it has a link and is forwarding traffic. This helps elect the virtual routers with the most available ports as the master. This command is disabled by default.
Track L4 Ports	Enables or disables tracking Layer 4 port states for priority adjustment. This is applied when a virtual server is configured as a VRRP virtual router. When enabled for virtual server routers, the priority for this virtual router will be increased for each physical switch port which has active Layer 4 processing on this switch. This helps elect the main Layer 4 switch as the master.
Track Real Servers	Enables or disables tracking real server states for priority adjustment. This is applied when a virtual server is configured as a VRRP virtual router. When enabled for virtual server routers, the priority for this virtual router will be increased for each healthy real server. This helps elect the switch with the largest server pool as the master, increasing Layer 4 efficiency.
Track HSRP Advertisements	Enables Hot Standby Router Protocol (HSRP) for this virtual router group. HSRP is used with some types of routers for establishing router failover. In networks where HSRP is used, enable this switch option to increase the priority of this virtual router for each Layer 4 client-only port that receives HSRP advertisements. This helps elect the switch closest to the master HSRP router as the master, optimizing routing efficiency.
Track HSRP Advertisements by VLAN	Hot Standby Router on VLAN (HSRV) is used to work in VLAN-tagged environments. Enable this switch option to increment only that VRRP instance that is on the same VLAN as the tagged hsrp master flagged packet.

Configuring Virtual Routing: VIR Group



Click on **Add Virtual Routers** button to add a virtual router to a VIR Group.

Field	Description
Virtual Router Group	The index of the virtual router group.
Name	Defines virtual router group name.
State	Enables or disables the virtual router group.
Virtual Routers	Adds a virtual router to the group.
Priority	Defines the election priority bias for this virtual router group. During the master router election process, the routing device with the highest virtual router priority number wins. If there is a tie, the device with the highest IP interface address wins. If this virtual router's IP address (`addr`) is the same as the one used by the IP interface, the priority for this virtual router will automatically be set to 255 (highest). When priority tracking is used, this base priority value can be modified according to a number of performance and operational criteria.
Track Interfaces	When enabled, the priority will be increased for each IP interface active on this virtual router group. An IP interface is considered active when there is at least one active port on the same VLAN. This helps elect the virtual routers with the most available routes as the master.
Track VLAN Ports	When enabled, the priority will be increased for each active port on the VLAN on this virtual router group. A port is considered "active" if it has a link and is forwarding traffic. This helps elect the virtual routers with the most available ports as the master.
Track Layer 4 Ports	When enabled for virtual server routers, the priority will be increased for each physical switch port which has active Layer 4 processing on this virtual router group. This helps elect the main Layer 4 switch as the master.
Track Real Servers	When enabled for virtual server routers, the priority will be increased for each healthy real server behind the virtual server IP address of the same IP address as the virtual router on this virtual router group. This helps elect the switch with the largest server pool as the master, increasing Layer 4 efficiency.
Track HSRP Advertisements	Hot Standby Router Protocol (HSRP) is used with some types of routers for establishing router failover. In networks where HSRP is used, enable this switch option to increase the priority of this virtual router group for each Layer 4 client-only port that receives HSRP advertisements. Enabling HSRP helps elect the switch closest to the master HSRP router as the master, optimizing routing efficiency.

Field	Description
Track HSRP Advertisements by VLAN	Hot Standby Router on VLAN (HSRV) is used to work in VLAN-tagged environments. Enable this switch option to increment only that vrrp instance on the virtual router group that is on the same VLAN as the tagged hsrp master flagged packet. This command is disabled by default.Hot Standby Router on VLAN (HSRV) is used to work in VLAN-tagged environments. Enable this switch option to increment only that vrrp instance on the virtual router group that is on the same VLAN as the tagged hsrp master flagged packet.
Track Virtual Router [1]	Allows you to track the virtual router for this virtual router group. Tracking is Alteon's proprietary extension to VRRP, used for modifying the standard priority when electing the master router from a pool of virtual routers.

Note: This feature is applicable only on Alteon Application Switches and on Alteon OS 21.0 and higher.

1. This is applicable only to Alteon OS and higher.

Configuring Virtual Routing: Synchronizing to a Peer Switch

Use this table to determine which properties of your primary switch you want to synchronize with the VRRP peer switch. All of the settings in the following table can be synchronized to a peer switch by using the Synchronize button.



You can click on **Synchronize** button to synchronize the virtual routing settings to a peer switch.

Note: Before synchronizing, make sure that you have first configured a VRRP peer switch.

Field	Description
Synch Filter	Enables or disables the configuration filter synchronization.
Synch Port	Enables or disables synchronization of port configuration.
Synch VRRP Priorities	Enables or disables synchronization of VRRP priorities.
Synch Proxy IP Address	Enables or disables synchronization of proxy IP addresses.
Sync Bandwidth Management	Enables or disables synchronization of bandwidth management.
Sync Stateful Failover [1]	Enables or disables the synchronization of stateful failover.
Stateful Failover Update Period [1]	Sets the period of the stateful failover update.
Sync Peer Proxy IP	Enables or disables the synchronization of peer proxy IP address.

1. This is not available on ALO switch.

Configuring Virtual Routing: Peers

Use this table to set up another switch as a VRRP-capable peer switch. For example, if you have two switches you want to use in a Virtual Router Redundancy Protocol (VRRP) configuration, configure the two switches as peers to each other.

Field	Description
Peer	The number of the peer switch.
IP Address	The IP address of the peer switch.
Synchronization	Enables or disables synchronization to the peer switch.

Configuring Bandwidth Management

Bandwidth Management (BWM) enables Web site managers to allocate a portion of the available bandwidth for specific users or applications. It allows companies to guarantee that critical business traffic, such as e-commerce transactions, receive higher priority versus non-critical traffic. Traffic classification can be based on user or application information. BWM policies can be configured to set lower and upper bounds on the bandwidth allocation.

Bandwidth management must be enabled before all the tabs will appear. For more information, see “Enabling Special Software Features on the Switch” on page 18.

The following Bandwidth Management topics are covered in this section:

- “Configuring General Bandwidth Management” on page 217
- “Configuring BWM Policies on Alteon 180 or AD series” on page 218
- “Configuring BWM Policies on Alteon Application Switches” on page 220
- “Configuring BWM Contracts” on page 222
- “Configuring BWM Contracts: Time Policies” on page 224
- “Configuring BWM Contract Group” on page 225

Configuring General Bandwidth Management

This tab is used to configure general Bandwidth Management features on the switch.



You can click on the **Send BWM History** button to enable sending of BWM History to an SMTP server. Then click the **Apply** button to ensure this change takes effect.

Note: The Alteon AD3 and Alteon 180e Web switches do not support Bandwidth Management.

Note: You need to buy the software key to enable BWM on your switch.

Field	Description
Bandwidth Management	Sets the current state of BWM: on or off.
Enforce BWM Policies	Enables or disables the enforcement of bandwidth management policies. When disabled, no bandwidth limits will be applied on queues. By default, this option is enabled.
SMTP Host	The address of the SMTP mail server. This can be used to e-mail Bandwidth Management history.
SMTP User Name	The current SMTP user name (E-mail address) to whom the history statistics will be mailed. The default is set to none (blank).
EMAIL Frequency [1]	Sets the frequency of Bandwidth Management email in minutes. The default is set to 0.
Entries in the IP User Table [1]	Sets the number of entries in the Bandwidth Management IP user table.

1. This is applicable only to Alteon OS and higher.

Configuring BWM Policies on Alteon 180 or AD series

Bandwidth policies are bandwidth limitations defined for any set of frames, specifying the guaranteed bandwidth rates. A bandwidth policy is often based on a rate structure whereby a Web host or co-location provider could charge a customer for bandwidth utilization. There are three rates that are configured: a Committed Information Rate (CIR)/Reserved Limit, a Soft Limit, and a Hard Limit, as described below.

For traffic shaping contracts, a queue depth is also associated with a policy. A queue depth is the size of the queue that holds the data. It can be adjusted to accommodate delay-sensitive traffic (such as audio) versus drop-sensitive traffic (such as FTP).

Packet Coloring (TOS bits) for Burst Limit

Whenever the soft limit is exceeded, optional packet coloring can be done to allow downstream routers to use diff-serv mechanisms (that is, writing the Type-Of-Service (TOS) byte of the IP header) to delay or discard these out-of-profile frames. Frames that are not out-of -profile are marked with a different, higher priority value. This feature can be enabled or disabled on a per-contract basis using the TOS Overwrite feature in the Configuring BWM Contracts tab.

The actual values used by the switch for overwriting TOS values (depending on whether traffic is over or under the soft TOS limit) are set in the bandwidth policy tab with the Under Soft Limit TOS Value and Over Soft Limit TOS Value options. The values allowed are 0-255. Typically, the values specified should match the appropriate diff-serv specification but could be different, depending on the customer environment.

Field	Description
Policy	The index number of the BWM traffic policy.
Under Soft Limit TOS Value	This TOS value is used to overwrite the TOS values of IP packets if the traffic for a contract is under the soft limit. These values only have significance to a contract if TOS overwrite is enabled in the “Configuring BWM Contracts” on page 222. The profile state of IP Type of Service (TOS) in the traffic policy.
Over Soft Limit TOS Value	This TOS value is used to overwrite the TOS values of IP packets if the traffic for a contract is over the soft limit. These values only have significance to a contract if TOS overwrite is enabled in “Configuring BWM Contracts” on page 222.

Field	Description
Hard (Maximum) Limit	Sets the hard bandwidth limit for this policy. This is the highest amount of bandwidth available to this policy. The hard speed limit can be configured in unites of kilobytes per second (k) or Megabytes per second (M) as follows: • 250k to 5,000k in 250k increments • 1M to 20M in 1M increments • 20M to 50M in 5M increments • 50M to 150M in 10M increments • 150M to 500M in 25M increments • 500M to 1000M in 50M increments. If K or M units are not entered, M is assumed.
Soft Limit	Sets the soft bandwidth limit for this policy. This is the lowest amount of bandwidth available to this policy. The soft speed limit can be configured in unites of kilobytes per second (k) or Megabytes per second (M) as follows: • 250k to 5,000K in 250k increments • 1M to 20M in 1M increments • 20M to 50M in 5M increments • 50M to 150M in 10M increments • 150M to 500M in 25M increments • 500M to 1000M in 50M increments. If k or M units are not entered, M is assumed.
Reserve (Minimum) Limit	Sets the reserve limit for this policy. This is the amount of bandwidth always available to this policy. The reserve speed limit can be configured in unites of kilobytes per second (k) or Megabytes per second (M) as follows: • 250k to 5,000K in 250k increments • 1M to 20M in 1M increments • 20M to 50M in 5M increments • 50M to 150M in 10M increments • 150M to 500M in 25M increments • 500M to 1000M in 50M increments. If k or M units are not entered, M is assumed.
Buffer Limit	The buffer limit for the traffic policy.

Configuring BWM Policies on Alteon Application Switches

Bandwidth policies are bandwidth limitations defined for any set of frames, specifying the guaranteed bandwidth rates. A bandwidth policy is often based on a rate structure whereby a Web host or co-location provider could charge a customer for bandwidth utilization. There are three rates that are configured: a Committed Information Rate (CIR)/Reserved Limit, a Soft Limit, and a Hard Limit, as described below.

For traffic shaping contracts, a queue depth is also associated with a policy. A queue depth is the size of the queue that holds the data. It can be adjusted to accommodate delay-sensitive traffic (such as audio) versus drop-sensitive traffic (such as FTP).

Packet Coloring (TOS bits) for Burst Limit

Whenever the soft limit is exceeded, optional packet coloring can be done to allow downstream routers to use diff-serv mechanisms (that is, writing the Type-Of-Service (TOS) byte of the IP header) to delay or discard these out-of-profile frames. Frames that are not out-of -profile are marked with a different, higher priority value. This feature can be enabled or disabled on a per-contract basis using the TOS Overwrite feature in the BWM Contracts tab.

The actual values used by the switch for overwriting TOS values (depending on whether traffic is over or under the soft TOS limit) are set in the bandwidth policy tab with the Under Soft Limit TOS Value and Over Soft Limit TOS Value options. The values allowed are 0-255. Typically, the values specified should match the appropriate diff-serv specification but could be different, depending on the customer environment.

Field	Description
Policy	The index number of BWM traffic policies.
Under Soft Limit TOS Value	This TOS value is used to overwrite the TOS values of IP packets if the traffic for a contract is under the soft limit. These values only have significance to a contract if TOS overwrite is enabled in the Bandwidth Management Contract Menu.
Over Soft Limit TOS Value	This TOS value is used to overwrite the TOS values of IP packets if the traffic for a contract is over the soft limit. These values only have significance to a contract if TOS overwrite is enabled in the Bandwidth Management Contract Menu.

Field	Description
Hard (Maximum) Limit	Sets the hard bandwidth limit for this policy. This is the highest amount of bandwidth available to this policy. The hard speed limit can be configured in unites of kilobytes per second (k) or Megabytes per second (M) as follows: • 64k to 1,000k in 1k increments **Note:** This applies to releases below Alteon OS 21.0. In Alteon OS 21.0. and above, the hard speed limit is 0k to 1,000k. • 1M to 1000M in 1M increments. If k or M units are not entered, M is assumed.
Soft Limit	Sets the soft bandwidth limit for this policy. This is the lowest amount of bandwidth available to this policy. The soft speed limit can be configured in unites of kilobytes per second (k) or Megabytes per second (M) as follows: • 64k to 1,000k in 1k increments **Note:** This applies to releases below Alteon OS 21.0. In Alteon OS 21.0. and above, the hard speed limit is 0k to 1,000k. • 1M to 1000M in 1M increments. If k or M units are not entered, M is assumed.
Reserve (Minimum) Limit	The reservation speed limit for the traffic policy: 64k to 1,000k in 1k increments; 1M to 1000M in 1M increments. If K or M units are not entered, M is assumed. **Note:** This applies to releases below Alteon OS 21.0. In Alteon OS 21.0. and above, the hard speed limit is 0k to 1,000k.
Buffer Limit	The buffer limit for the traffic policy.
User Limit [1]	Sets the bandwidth limit for each IP address in the contract traffic.

This is applicable only on Alteon OS 22.0 and higher.

Configuring BWM Contracts

To manage bandwidth on an Alteon Application Switch, you must create one or more bandwidth management contracts. The switch uses these contracts to limit individual traffic flows.



This button allows you to configure Time Policies.

Note: This feature is available only on Alteon OS and higher.

Field	Description
Contract	The contract number of the Bandwidth Management (BWM) traffic contract. This value can be set through the Insert button.
Name	The traffic contract name.
State	Enables or disables the state of the traffic contract.
Policy	The policy number of the traffic contract. To select a Bandwidth policy, use **Browse...** button to select a policy that you configured in the BWM Policy tab.
Precedence	Sets the precedence value of the traffic contract. If a frame qualifies for different classifications, it is important to be able to specify the classification with which it should be associated. If a contract does not have an assigned precedence value, then the ordering is as follows: 1. Layer 7 applications (for example, URL, HTTP, headers, cookies, and so forth) 2. Layer 4 services on the virtual server 3. Filter 4. VLAN 5. Source Port/Default Assignment
TOS Overwrite	Enables or disables overwriting the IP Type of Service (TOS) for this contract.
Keep Statistics on TFTP Server	Enables or disables saving contract statistics on the Trivial File Transfer Protocol (TFTP) server of the traffic contract.
Traffic Shaping [1]	Enables or disables traffic shaping.
TCP Window Size [2]	Enables or disables overwriting TCP Window for this Contract. By overwriting the default window size, the user can modify the TCP window size to a lower value so that when the packet arrives carrying the bytes within that window size, the receiver of that packet does not have to wait for acknowledgement. This may help reduce the traffic congestion. Do not set the value to lower than 1500 bytes. For details, refer to *Alteon OS Application Guide*.

Field	Description
User Rate Limiting [2]	Enables or disables user (IP address) limiting for this contract. If enabled, each IP address is limited to the user limit configured in the Policies tab.
IP Type [2]	Defines the IP type for this contract, whether the user (IP address) limiting is enforced by the source IP address (SIP) or the destination IP address (DIP).
Monitor-Only Mode [2]	Enables or disables monitor-only mode for this Contract. This field is used for design and auditing purposes only. The statistics are generated but no shaping or limiting will apply to this contract.
Contract Group [2]	Displays Contract Group configuration for this contract.

1. This field is applicable only on Alteon Application Switches.
2. This is applicable only on Alteon OS 22.0.1.0 and higher.

Configuring BWM Contracts: Time Policies

To set BWM Contracts on an Alteon Application Switch to work during certain times, you must create one or more time policies.

Note: This feature is available only on Alteon OS and higher.

Field	Description
Contract	The contract number of the Bandwidth Management (BWM) traffic contract. This value can be set through the Insert button.
Time Policy	Defines the policy number for the time policy.
Day	Defines the day(s) of the week.
Starting Time	Defines the start time for the policy.
Ending Time	Defines the end time for the policy.
Policy	Defines the policy number for the contract.
State	Shows the current state of the time policy.

Configuring BWM Contract Group

In earlier releases of Alteon OS, a single level bandwidth management contract was used to manage bandwidth on an Alteon Application Switch. In Alteon OS 22.0, bandwidth contract groups can be configured to aggregate contract resources and share unused bandwidth within the contract group. For detailed information on this feature, refer to the *Alteon OS 22.0 Application Guide.*



The **Add Contract to Group** button allows you to add contracts to a contract group.

Field	Description
Group	Displays the contract group number.
Name	Displays the contract group name.
Contracts	Displays the contract numbers in the group.

Configuring SNMP version 3

SNMP version 3 (SNMPv3) is an extensible SNMP Framework that supplements the SNMPv2 Framework by supporting the following:

- a new SNMP message format
- security for messages
- access control
- remote configuration of SNMP parameters

For more details on the SNMPv3 architecture please refer to RFC2271 to RFC2276.

Note: You must be logged in through SNMPv3 to configure SNMPv3 options.

The following topics are discussed in this section:

- "Configuring SNMPv3: User-based Security Model Table" on page 227
- "Configuring SNMPv3: View-based Access Control Model Table: Group Membership" on page 228
- "Configuring SNMPv3: View-based Access Control Model Table: Group Access Right" on page 229
- "Configuring SNMPv3: View-based Access Control Model Table: MIB View" on page 230
- "Configuring SNMPv3: Community Table" on page 231
- "Configuring SNMPv3: Target Table" on page 232
- "Configuring SNMPv3: Target Params Table" on page 233
- "Configuring SNMPv3: Notify Table" on page 234

Configuring SNMPv3: User-based Security Model Table

You must be logged in through SNMP version 3 (SNMPv3) to view the SNMPv3 configuration tab.

This tab allows you to create a user security model (USM) entry for an authorized user. You can also configure this entry through SNMP.

You can make use of a defined set of user identities using this Security Model. An SNMP engine must have the knowledge of applicable attributes of a user.

This table helps you create a user security model entry for an authorized user. You need to provide a security name to create the USM entry.

Note: This feature is available only on Alteon OS and higher.

Field	Description
Engine ID	The ID of the SNMP engine.
Name	This field allows you to configure a string that represents the name of the user. This is the login name that you need in order to access the switch.
Security Name	This field represents the security name.
Authentication Protocol	This field allows you to configure the authentication protocol between HMAC-MD5-96 or HMAC-SHA-96.
Privacy Protocol	This command allows you to configure the type of privacy protocol on your switch. The privacy protocol protects messages from disclosure. The options are des (CBC-DES Symmetric Encryption Protocol) or none. If you specify des as the privacy protocol, then make sure that you have selected one of the authentication protocols (HMAC-MD5-96 or HMAC-SHA-96).

Configuring SNMPv3: View-based Access Control Model Table: Group Membership

The view-based Access Control Model defines a set of services that an application can use for checking access rights of the user. Access control is needed when the user has to process SNMP retrieval or modification request from an SNMP entity.

Field	Description
Security Model	Allows you to select the security model to be used. The options are: USM, SNMPv1, and SNMPv2.
Security Name	Displays the security name for the selected security model.
Group Name	Defines the name of the group.

Configuring SNMPv3: View-based Access Control Model Table: Group Access Right

Field	Description
Group Names	Defines the group name for the group.
Context Prefix	Displays the context prefix used for the group.
Security Model	Displays the security model used for the group.
Security Level	Displays the security level of the group.
Context Match	Defines the context match for the group. Choices are prefix or exact.
Read View Name	Defines the read view name for the group.
Write View Name	Defines the write view name for the group.
Notify View Name	Defines the notify view name for the group.

Configuring SNMPv3: View-based Access Control Model Table: MIB View

Field	Description
View Name	Displays the view name.
Subtree	Displays the subtree.
Mask	Defines the mask to be used.
Type	Defines the type. Choices are included and excluded.

Configuring SNMPv3: Community Table

The community table contains objects for mapping community strings and version-independent SNMP message parameters. This column is used for configuring the community table entry. The configured entry is stored in the community table list in the SNMP engine. This table is used to configure community strings in the Local Configuration Datastore (LCD) of SNMP engine.

Field	Description
Index	Allows you to configure the unique index value of a row in this table consisting of 32 characters maximum.
Name	This field allows you to configure a string up to 32 characters long that represents the name of the user. This is the login name that you need in order to access the switch.
Security Name	Defines a readable 32 character long string that represents the corresponding value of an SNMP community name in a security model.

Configuring SNMPv3: Target Table

This feature allows you to configure destination information, consisting of a transport domain and a transport address. This is also termed as transport endpoint. The SNMP MIB provides a mechanism for performing source address validation on incoming requests, and for selecting community strings based on target addresses for outgoing notifications.

This column is used to configure the target transport entry. The configured entry is stored in the target address table list in the SNMP engine. This table of transport addresses is used in the generation of SNMP messages

Field	Description
Address Name	Allows you to configure the locally arbitrary, but unique identifier, target address name associated with this entry.
Transport Type Address	Allows you to configure a transport address IP that can be used in the generation of SNMP traps.
Transport Address	Allows you to configure a transport address port that can be used in the generation of SNMP traps.
Tag List	Allows you to configure a list of tags that are used to select target addresses for a particular operation.
Parameters	Allows you to configure the parameters to be associated with this entry.

Configuring SNMPv3: Target Params Table

This feature allows you to configure SNMP parameters, consisting of message processing model, security model, security level, and security name information. There may be multiple transport endpoints associated with a particular set of SNMP parameters, or a particular transport endpoint may be associated with several sets of SNMP parameters.

This table allows you to configure the target parameters entry and store it in the target parameters table in the SNMP engine. This table contains parameters that are used to generate a message. The parameters include the message processing model (for example: SNMPv3, SNMPv2c, SNMPv1), the security model (for example: USM), the security name, and the security level (noAuthnoPriv, authNoPriv, or authPriv).

Field	Description
Name	Allows you to configure the locally arbitrary, but unique identifier that is associated with this entry.
Message Processing Model	Allows you to configure the message processing model that is used to generate SNMP messages.
Security Model	Allows you to select the security model to be used when generating the SNMP messages. The options are: USM, SNMPv1, and SNMPv2.
Security Name	Defines the name that identifies the user in the USM table (page 227) on whose behalf the SNMP messages are generated using this entry.
Security Level	Allows you to select the level of security to be used when generating the SNMP messages using this entry. The level noAuthNoPriv means that the SNMP message will be sent without authentication and without using a privacy protocol. The level authNoPriv means that the SNMP message will be sent with authentication but without using a privacy protocol. The authPriv means that the SNMP message will be sent both with authentication and using a privacy protocol.

Configuring SNMPv3: Notify Table

A notification application typically monitors a system for particular events or conditions, and generates Notification-Class messages based on these events or conditions.

SNMPv3 uses Notification Originator to send out traps. A notification typically monitors a system for particular events or conditions, and generates Notification-Class messages based on these events or conditions.

Field	Description
Name	Defines a locally arbitrary but unique identifier associated with this SNMP notify entry.
Tag	Allows you to configure a tag of 255 characters maximum that contains a tag value which is used to select entries in the Target Address Table. Any entry in the snmpTargetAddrTable, that matches the value of this tag, is selected.
Type	The type is set to trap.

Configuring Ports

You can configure physical properties and server load balancing properties on a per-port basis. Click on the desired port, and drill down through the **Configure** folder to the **Port** node.

The following topics are covered in this section:

- "Configuring General Properties for Ports" on page 236
- "Configuring Port Properties" on page 237
- "Configuring Spanning Tree Protocol on Ports" on page 239
- "Configuring Filtering on Ports" on page 240

Configuring General Properties for Ports

Note: Only the Name and Link Trap field can be configured in this window.

Field	Description
Name	Defines the name of the port.
Mode	The mode of the port: full-duplex, half-duplex, full-or-half-duplex, or other.
Flow Control	The flow control of the port: transmit, receive, both, none, or other.
Link	The status of the link: up, down, disabled, or inoperative.
Speed	The current speed of the port: 10Mbs, 100Mbs, 1,000Mbs, or other.
Description	Displays a description of the Network Interface Card (NIC).
Type	The type of interface.
MTU (Largest Packet)	The largest number of bytes in a packet. This is the Maximum Transmission Unit of the port.
MAC Address	The MAC address of the switch.
Operational Status	The status: up, down, or testing.
Last Change	This field indicates the last change to the current operational state, in relation to the timestamp shown in the System Up Since field in the Configure>Switch>General tab. For example, if the switch system has been up since `2002/11/01-17:51:56` and the Last Change value is `3 days 0h:0m:4s`, then the current operational state was last changed on `2002/11/04-17:52:00`. **Note:** If the current state is configured before the network management system, Last Change will be 0 (zero).
Link Trap	Enables or disables linkUp/linkDown traps.
Physical Connection Type [1]	Displays the type of physical connection the port supports, for example: Gigabit Ethernet Copper (geCopper) or Gigabit Ethernet SFP (Small Form-factor Pluggable).
Preferred Connection Type [1]	Sets up the preferred connection type on the port. The options are: Gigabit Ethernet Copper and Gigabit Ethernet SFP (Small Form-factor Pluggable). This is applicable only on dual port numbers 3, 4, 5, and 6 on Alteon 3000 series.
Backup Connection Type [1]	Sets up the preferred connection type on the backup port. This is applicable only on dual ports. The options are: Gigabit Ethernet Copper and Gigabit Ethernet SFP (Small Form-factor Pluggable).

1. This is applicable only on Alteon 3000 series.

Configuring Port Properties

Field	Description
State	Enables or disables the port.
VLAN	Sets the VLAN tagging of the port: *tagged* or *untagged*. You cannot add a port to more than one VLAN unless the port is *tagged*.
Default VLAN	Sets the default VLAN ID for the port. **Note:** To select another VLAN ID for this port, you can enter the VLAN number into the field. To choose an existing VLAN, select the **Browse...** button and select any of the VLANs that appear in the list. Then Select the **Modify** button. The Default VLAN field will now display the new selection.
Gig Auto Negotiate	Sets the autonegotiation for Gigabit Ethernet connection: on or off.
Gig Flow Control	Sets the port flow control for Gigabit Ethernet connection: other, transmit, receive, both, or none.
Auto Negotiate	Sets the autonegotiation for the Fast Ethernet connection: on or off.
Speed	The port speed for Fast Ethernet connection: 10Mbs, 100Mbs, or 1000Mbs.
Mode	The port mode for Fast Ethernet connection: other, full-duplex, half-duplex, or full-or half-duplex.
Flow Control	Sets the port flow control for Fast Ethernet connection: transmit, receive, both, or none.
RMON	Sets the remote monitoring: on or off.
Discard Non-IP	Enables or disables discarding all non-IP traffic on the switch port.
Preferred Link [1]	Displays the preferred link type based on the characteristics of the port on the switch.
Backup Link [1]	Displays the backup link based on the port characteristics of the switch. Only available on models with dual-media ports.
BWM Contract	Sets the number of the bandwidth management contract. Only one contract may be assigned to the selected port. **Note:** To select another BWM contract for this port, select the **Browse...** button. Select any one of the BWM contracts that appear in the list, then Select the Modify button. The BWM Contract will now display the new selection.

Field	Description
Egress BWM Limit [2]	Sets the egress bandwidth limit for the port to avoid overloading the receiving router or switch. Using this field, you can configure the egress bandwidth limit of the port to match with the bandwidth link of the receiving router or the switch. This means that the port's speed will be taken as the egress bandwidth. For example, the egress bandwidth for an FE port will be 100m. The default is 0. **Note:** You need Bandwidth Management license to use this command.
Non-IP BWM Contract [2]	Sets the Bandwidth Management contract for non-IP traffic for this port.

1. This field is applicable only on Alteon 180 or AD series and on ALO.
2. This is applicable only to Alteon OS 22.0 and higher.

Note: You need to buy the software key to enable BWM on your switch.

Configuring Spanning Tree Protocol on Ports

This tab is used to configure spanning tree protocol priority and path costs for the selected port.

See Also:

- “Configuring Spanning Tree Group Ports on the Bridge” on page 61
- “Configuring Spanning Tree Protocol on Individual Ports” on page 62

Field	Description
Priority	The port priority helps determine which bridge port becomes the designated port. In a network topology that has multiple bridge ports connected to a single segment, the port with the lowest port priority becomes the designated port for the segment.
State	The port’s current state: disabled, blocking, listening, learning, forwarding, or broken.
Path Cost	Sets the cost of the port path: 1 to 65,535. The faster the port, the lower the cost. The default is 10 for 100Mbps ports, and 1 for Gigabit ports. A value of 0 indicates that the default cost will be computed for an autonegotiated link speed.
Root	The unique identifier of the bridge that is recorded as the root bridge in the configuration bridge protocol data units (BPDU).
Root Cost	The cost of the path to the root as seen from this bridge.
Bridge	The bridge identifier. The port interprets this bridge as the root bridge for the port’s segment.
Bridge Port	The port identifier. This port is the designated bridge for the port’s segment.
Learn-Forward Transitions	The number of times the port has transitioned from the learning state to the forwarding state.

Configuring Filtering on Ports

Field	Description
Filtering	Enables or disables filtering on the selected port.
Filters Applied	The numbers of the filters that have been applied to the selected port. You can double-click the filter number(s) shown here to view or modify detailed information about Filter Membership.

Configuring Filter Membership on Ports



This window is accessed by selecting the **Add filter to Port...** button in the Configuring Filtering on Ports tab, or by double-clicking on the filter number(s) that appear in the Filters Applied field.

If you have many filters configured and wish to view a subset of the items in this table, see the procedure in *Using Alteon EMS 3.1 - Help*.

Monitoring the Switch

The following topics are covered in this section:

- Monitoring Summary
- Monitoring the switch
- Monitoring Bridge
- Monitoring Security
- Monitoring IP
- Monitoring OSPF
- Monitoring BGP
- Monitoring Layer 4
- Monitoring Layer 7
- Monitoring VRRP
- Monitoring Bandwidth Management
- Monitoring SNMPv3
- Monitoring Ports

Monitoring Summary

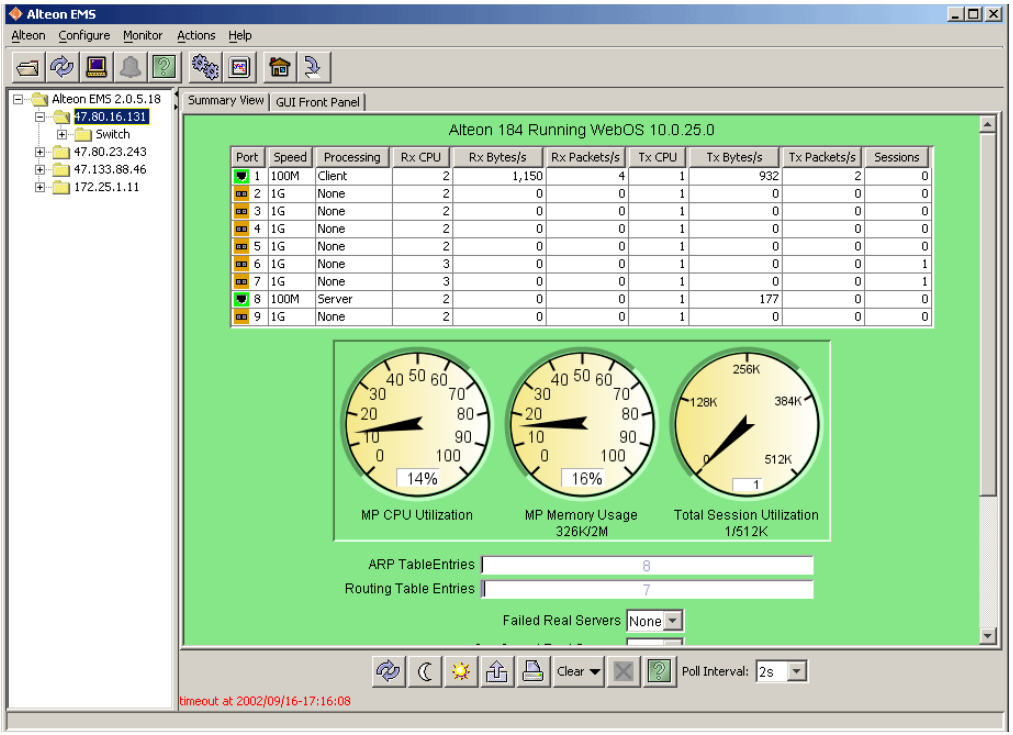
The following topics are covered in this section:

- Switch Summary View
- GUI Front Panel View

Switch Summary View

When you open the Monitor menu, a view of the selected switch appears. The Summary View Help provides a detailed description of each item in this view.

Figure 1 The following is a display of the Summary View of an Alteon 184.





You can select the **Pause** button to stop the switch from polling the statistics.



You can select the **Resume** button to let the switch resume polling the statistics.

Field	Description
Port	Displays the physical port on the switch. Green indicates the port is connected. Orange indicates the port is not in use. To view the legend, go to the **Help > Legend** menu.
Speed	Displays the port speed. Options are 10M for 10 Mbps (Ethernet), 100M for 100 Mbps (Fast Ethernet), and IG for 1000 Mbps (Gigabit Ethernet).

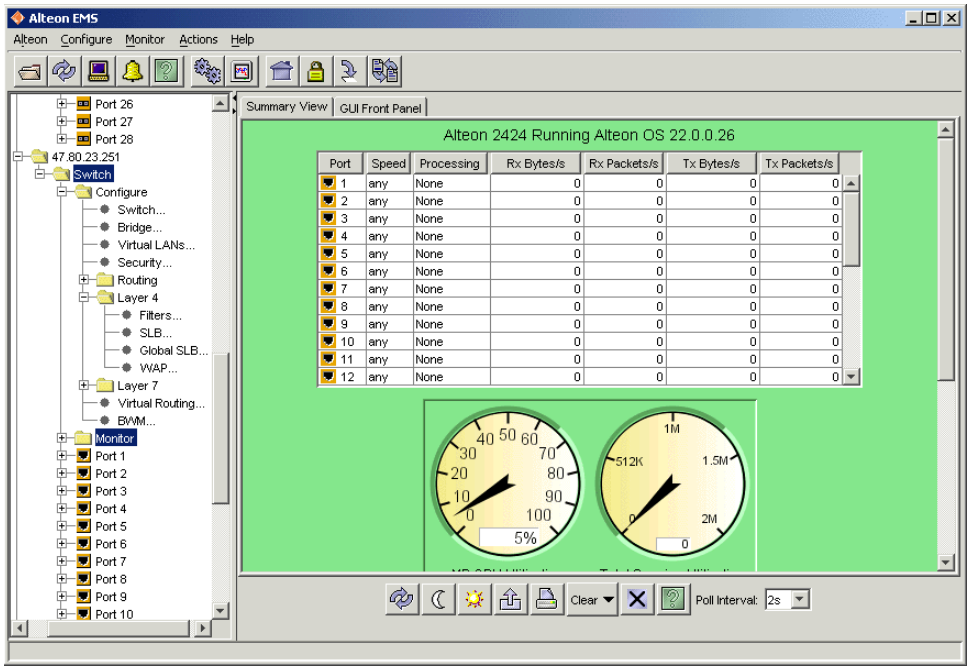
Field	Description
Processing	Displays the type of load balancing state for each port: client, server, client-server, or none. To configure, go to Configure> Layer4>SLB>Ports.
Rx CPU	Displays the number of bytes being received by the CPU.
Rx Bytes/s	The number of bytes per second that are being received by the port.
Rx Packets/s	The number of packets per second that are being received by the port.
Tx CPU	Displays the number of bytes being transmitted by the CPU.
Tx Bytes/s	The number of bytes per second that are being transmitted by the port.
Tx Packets/s	The number of packets per second that are being transmitted by the port.
Sessions	Displays the number of sessions being processed on the port.
MP CPU Utilization	This dial displays the percentage of management processor (MP) CPU time that is currently in use.
MP Memory Usage	This dial displays the percentage of management processor (MP) memory being used by the switch. This dial does not display on Alteon Application Switches.
Total Session Utilization	This dial displays the total number of current sessions that are being utilized on the switch. The value is shown numerically inside the gauge.
ARP Table Entries	This bar graph displays the number of Address Resolution Protocol table entries on the switch. The value is shown numerically inside the bar. The percentage of total session utilization is represented by a gray bar that fills to the right.
Routing Table Entries	This bar graph displays the number of Routing Table Entries on the switch. The value is shown numerically inside the bar. The percentage of total session utilization is represented by a gray bar that fills to the right.
Failed Real Servers	This drop-down combo box displays any failed real servers. Click in the box to display all failed real servers. If all real servers are functioning properly, the field will display as None. To view a graphical representation of a server load balancing (SLB) configuration, go to **Monitor>Layer4>SLB Summary**.
Overflowed Real Servers	This drop-down combo box displays any overflowed real servers. Click in the box to display all failed real servers. If all real servers are functioning properly, the field will display as None. To view a graphical representation of a server load balancing (SLB) configuration, go to **Monitor>Layer4>SLB Summary**.
Disabled Real Servers	This drop-down combo box displays any real servers that have been disabled by the user. Click in the box to display all disabled real servers. If all real servers are functioning properly, the field will display as None. To view a graphical representation of a server load balancing (SLB) configuration, go to **Monitor>Layer4>SLB Summary**.

Field	Description
Affected Groups	This drop-down combo box displays any real server groups that are affected by any of the server conditions described above. **Note:** To configure real server groups for server load balancing, go to Configuring Layer 4 SLB: Real Server Groups. To view a graphical representation of a server load balancing (SLB) configuration, go to SLB Summary View.
Syslog Messages	This window displays a filtered view of any syslog messages that have been generated by the switch. In order to receive syslog messages in Alteon EMS, set your workstation as the syslog target.

Switch Summary View

When you open the Monitor menu, a view of the selected switch appears. The Summary View Help provides a detailed description of each item in this view.

Figure 2 The following is a display of the Summary View of an Alteon Application Switch 2000 Series.



You can select the **Pause** button to stop the switch from polling the statistics.

You can select the **Resume** button to let the switch resume polling the statistics.

Field	Description
Port	Displays the physical port on the switch. Green indicates the port is connected. Orange indicates the port is not in use. To view the legend, go to the **Help > Legend** menu.
Speed	Displays the port speed. Options are 10M for 10 Mbps (Ethernet), 100M for 100 Mbps (Fast Ethernet), and IG for 1000 Mbps (Gigabit Ethernet).

Field	Description
Processing	Displays the type of load balancing state for each port: client, server, client-server, or none. To configure, go to Configure> Layer4>SLB>Ports.
Rx Bytes/s	The number of bytes per second that are being received by the port.
Rx Packets/s	The number of packets per second that are being received by the port.
Tx Bytes/s	The number of bytes per second that are being transmitted by the port.
Tx Packets/s	The number of packets per second that are being transmitted by the port.
ARP Table Entries	This bar graph displays the number of Address Resolution Protocol table entries on the switch. The value is shown numerically inside the bar. The percentage of total session utilization is represented by a gray bar that fills to the right.
Routing Table Entries	This bar graph displays the number of Routing Table Entries on the switch. The value is shown numerically inside the bar. The percentage of total session utilization is represented by a gray bar that fills to the right.
Failed Real Servers	This drop-down combo box displays any failed real servers. Click in the box to display all failed real servers. If all real servers are functioning properly, the field will display as None. To view a graphical representation of a server load balancing (SLB) configuration, go to **Monitor>Layer4>SLB Summary**.
Overflowed Real Servers	This drop-down combo box displays any overflowed real servers. Click in the box to display all failed real servers. If all real servers are functioning properly, the field will display as None. To view a graphical representation of a server load balancing (SLB) configuration, go to **Monitor>Layer4>SLB Summary**.
Disabled Real Servers	This drop-down combo box displays any real servers that have been disabled by the user. Click in the box to display all disabled real servers. If all real servers are functioning properly, the field will display as None. To view a graphical representation of a server load balancing (SLB) configuration, go to **Monitor>Layer4>SLB Summary**.
Affected Groups	This drop-down combo box displays any real server groups that are affected by any of the server conditions described above. **Note:** To configure real server groups for server load balancing, go to Configuring Layer 4 SLB: Real Server Groups. To view a graphical representation of a server load balancing (SLB) configuration, go to SLB Summary View.
Syslog Messages	This window displays a filtered view of any syslog messages that have been generated by the switch. In order to receive syslog messages in Alteon EMS, set your workstation as the syslog target.

GUI Front Panel View

The GUI Front Panel tab allows you to view a physical representation of the selected switch.

Features

- You can click on any port to open the General port configuration tab for the selected port.
- You can Ctrl-click to select specific ports, or drag across a group of ports to open the port configuration tabs for the selected ports.

Monitoring the switch

The monitor tabs allow you to monitor switch functions. Use this menu to monitor the switch.

The following switch monitoring topics are covered in this section:

The following switch monitoring topics are covered in this section:

- Monitoring Simple Network Management Protocol (SNMP)
- Monitoring Web OS Statistics on Alteon 180 or AD series
- Monitoring Alteon OS Statistics on ALO and on Alteon Application Switches
- Monitoring Switch MP CPU Stats on ALO and on Alteon 180 or AD series
- Monitoring Switch MP CPU Stats on Alteon Application Switches
- Monitoring SP CPU Statistics on Alteon Application Switches
- Monitoring SP Maintenance on Alteon Application Switches
- Monitoring SP Maintenance Received on Alteon Application Switches
- Monitoring SP Maintenance Send on Alteon Application Switches
- Monitoring the Management Port on Alteon Application Switches
- Monitoring SONMP
- Monitoring Aggregated Ports
- Monitoring Link Aggregation Information
- Monitoring Link Aggregation Control Protocol Ports
- Monitoring NTP
- Monitoring Spanning Tree Group Information

Monitoring Simple Network Management Protocol (SNMP)

Field	Description
Packets In	The number of messages delivered to the SNMP switch from the transport service.
Packets Out	The number of SNMP Messages passed from the SNMP switch to the transport service.
MIB Variables Retrieved	The number of MIB objects successfully retrieved by the SNMP switch after valid SNMP get-request and get-next Protocol Data Units (PDU).
MIB Variables Modified	The number of MIB objects that were successfully altered by the SNMP stack after valid SNMP set-request PDUs.
GET Requests In	The number of SNMP get-request PDUs that were accepted and processed by the SNMP stack.
GET NEXT Requests In	The number of SNMP get-next PDUs that were accepted and processed by the SNMP stack.
SET Requests In	The number of SNMP set-request PDUs that were accepted and processed by the SNMP stack.
GET Responses Out	The total number of SNMP get-response PDUs that were generated by the SNMP entity.
Traps Out	The number of SNMP Trap PDUs that were generated by the SNMP entity.
Too Big Errors In	The number of SNMP PDUs that were delivered to the SNMP entity when Too Big Errors In occurred.
Too Big Errors Out	The number of SNMP PDUs that were generated by the SNMP entity when Too Big Errors Out occurred.
No Such Name Errors In	The number of SNMP PDUs that were delivered to the SNMP entity when the No Such Names In error occurred.
No Such Names Out	The number of SNMP PDUs that were generated by the SNMP entity when No Such Names Out error occurred.
Bad Value Errors In	The number of SNMP PDUs that were delivered to the SNMP entity when Bad Value Errors occurred.
Bad Value Errors Out	The number of SNMP PDUs that were generated by the SNMP entity when Bad Value Errors Out occurred.
Generic Errors In	The number of SNMP PDUs that were delivered to the SNMP entity when Generic Errors In occurred.
Generic Errors Out	The number of SNMP PDUs that were generated by the SNMP when Generic Errors Out occurred.

Field	Description
Packets Using Unsupported SNMP Version	The number of SNMP messages that were received for an unsupported SNMP version.
Packets with Unknown Community String	The number of SNMP messages received that used an unknown SNMP community name.
Packets with Wrong Community String	The number of SNMP messages that represented an SNMP operation that was not allowed by the SNMP community named in the message.
ASN1 Decode Errors	The number of Abstract Syntax Notation One (ASN.1) or BER errors that occurred while the SNMP was decoding received SNMP messages. **Note:** OSI's method of specifying abstract objects is called ASN.1 (Abstract Syntax Notation One, defined in X.208), and one set of rules for representing such objects as strings of ones and zeros is called the BER (Basic Encoding Rules, defined in X.209). ASN.1 is a flexible notation that allows one to define a variety of data types, from simple types such as integers and bit strings to structured types such as sets and sequences. BER describes how to represent or encode values of each ASN.1 type as a string of eight-bit octets.
Read Only Errors In	The number of valid SNMP PDUs that were delivered to the SNMP entity when the Read Only Errors In occurred. **Note:** This is a protocol error that generates an SNMP PDU that contains readOnly in the error status field. This method detects incorrect implementations of the SNMP.

Clear Buttons



This button clears the statistics on the switch and resets them to zero only on Alteon OS.



This button clears the statistics only on the EMS display (and not on the switch) and resets the base values to zero.

Monitoring Web OS Statistics on Alteon 180 or AD series

Field	Description
Memory Allocations	The outstanding bytes of memory that have been allocated.
Memory Frees	The total number of bytes of memory frees.
Failed Allocations	The total number of failed memory allocations.
Bytes Allocated	The total number bytes of memory allocations.
Most Bytes Allocated	The number of allocated bytes with the high water mark.
Bytes in Memory Pool	The number of bytes in the memory pool.
Largest Block Allocated	The number of bytes of the largest allocated memory block.
Packets Allocated	Total number of packet allocations from the packet buffer pool by the TCP/IP protocol stack.
Packets Freed	Total number of times the packet buffers are freed (released) to the packet buffer pool by the TCP/IP protocol stack.
Failed Packet Allocations	The total number of failed allocated packets.
Small Packet Allocations	The current number of allocated small size packets. A small packet contains 128 bytes or less.
Medium Packet Allocations	Total number of packet allocations with size less than 256 bytes from the packet buffer pool by the TCP/IP protocol stack.
Jumbo Packet Allocations	The current number of allocated jumbo size packets. A jumbo packet contains between 1537 and 9,216 bytes.

Monitoring Alteon OS Statistics on ALO and on Alteon Application Switches

Field	Description
Packets Allocated	The total number of allocated packets.
Packets Freed	The total number of freed allocated packets.
Failed Packet Allocations	The total number of failed allocated packets.
Small Packet Allocations	The number of allocated small size packets. A small packet contains 128 bytes or less.
Medium Packet Allocations	The current number of allocated medium size packets. A medium packet contains between 129 and 1,536 bytes.
Jumbo Packet Allocations	The current number of allocated jumbo size packets. A jumbo packet contains between 1537 and 9,216 bytes.
Small Packet Allocations High Water Mark	The maximum number of allocated small size packets. A small packet contains 128 bytes or less.
Medium Packet Allocations High Water Mark	The maximum number of allocated medium size packets. A medium packet contains between 129 and 1,536 bytes.
Jumbo Packet Allocations High Water Mark	The maximum number of allocated jumbo size packets. A jumbo packet contains between 1,536 and 9,216 bytes.
Discarded due to Packet Buffer Pool Low	The total number of packets that were chosen to be discarded because the number of buffers available in the packet buffer pool is low.

Monitoring Switch MP CPU Stats on ALO and on Alteon 180 or AD series

Field	Description
MP CPU A Utilization (1 Second Avg)	The percentage of CPU A's utilization as measured over the last one second interval.
MP CPU B Utilization (1 Second Avg)	The percentage of CPU B's utilization as measured over the last one second interval.
MP CPU A Utilization (4 Second Avg)	The percentage of CPU A's utilization as measured over the last four second interval.
MP CPU B Utilization (4 Second Avg)	The percentage of CPU B's utilization as measured over the last four second interval.
MP CPU A Utilization (64 Second Avg)	The percentage of CPU A's utilization as measured over the last 64 second interval.
MP CPU B Utilization (64 Second Avg)	The percentage of CPU B's utilization as measured over the last 64 second interval.

Monitoring Switch MP CPU Stats on Alteon Application Switches

Field	Description
MP CPU Utilization (1 Second Avg)	The percentage of CPU utilization as measured over the last one second interval.
MP CPU Utilization (4 Second Avg)	The percentage of CPU utilization as measured over the last four second interval.
MP CPU Utilization (64 Second Avg)	The percentage of CPU utilization as measured over the last 64 second interval.

Monitoring MP Memory Statistics

Field	Description
Total	Total amount of MP memory.
Used	Amount of used MP memory.
Free	Amount of free MP memory.
Lowest Free	The lowest free amount of MP memory.

Monitoring SP CPU Statistics on Alteon Application Switches

Field	Description
SP	The SP Index number.
Utilization (1 second Avg.)	The utilization of this SP over 1 second. It shows the percentage.
Utilization (4second Avg.)	The utilization of this SP over 4 seconds. It shows the percentage.
Utilization (64 second Avg.)	The utilization of this SP over 64 seconds. It shows the percentage.

Monitoring SP Maintenance on Alteon Application Switches

Field	Description
SP	The SP index.
Attempts to add to full FDB	The number of times the attempts were made to add entries to an already full FDB.
MAC address resolution failure	The number of times SP is unable to send to MP (due to no letter buffer) that a MAC address needs to be resolved on the SP.
MAC address learn failure	The number of times SP is unable to send to MP (due to no letter buffer) that a new MAC address is learned by the SP.
MAC address aging failure	The number of times SP is unable to send to MP (due to no letter buffer) that an FDB entry on the SP is not touched since the last age.
MAC address not found	The number of times SP does not find the corresponding FDB entry on the SP when requested by MP to delete the entry.

Monitoring SP Maintenance Received on Alteon Application Switches

Note: This feature is available only on Alteon OS 20.x and higher.

Field	Description
SP	The SP index.
Receive Letter Errors from MP	The number of receive letter errors from MP.
Receive Letter Errors from SP1	The number of receive letter errors from SP1. If the current table index is the same as the SP number then a value of 0 is returned.
Receive Letter Errors from SP2	The number of receive letter errors from SP2. If the current table index is the same as the SP number then a value of 0 is returned.
Receive Letter Errors from SP3	The number of receive letter errors from SP3. If the current table index is the same as the SP number then a value of 0 is returned.
Receive Letter Errors from SP4	The number of receive letter errors from SP4. If the current table index is the same as the SP number then a value of 0 is returned.
Receive Letter Success from MP	The number of receive letter success from MP.
Receive Letter Success from SP1	The number of receive letter success from SP1. If the current table index is the same as the SP number then a value of 0 is returned.
Receive Letter Success from SP2	The number of receive letter success from SP2. If the current table index is the same as the SP number then a value of 0 is returned.
Receive Letter Success from SP3	The number of receive letter success from SP3. If the current table index is the same as the SP number then a value of 0 is returned.
Receive Letter Success from SP4	The number of receive letter success from SP4. If the current table index is the same as the SP number then a value of 0 is returned.

Note: Alteon Application switches 2208 and 2216 do not support SP3 and SP4.

Monitoring SP Maintenance Send on Alteon Application Switches

Note: This feature is available only on Alteon OS 20.x and higher.

Field	Description
SP	The SP index.
Send Letter Failures to MP	The number of send letter failures to MP.
Send Letter Failures to SP1	The number of send letter failures to SP1. If the current table index is the same as the SP number then a value of 0 is returned.
Send Letter Failures to SP2	The number of send letter failures to SP2. If the current table index is the same as the SP number then a value of 0 is returned.
Send Letter Failures to SP3	The number of send letter failures to SP3. If the current table index is the same as the SP number then a value of 0 is returned.
Send Letter Failures to SP4	The number of send letter failures to SP4. If the current table index is the same as the SP number then a value of 0 is returned.
Send Letter Success to MP	The number of send letter success to MP.
Send Letter Success to SP1	The number of send letter success to SP1. If the current table index is the same as the SP number then a value of 0 is returned.
Send Letter Success to SP2	The number of send letter success to SP2. If the current table index is the same as the SP number then a value of 0 is returned.
Send Letter Success to SP3	The number of send letter success to SP3. If the current table index is the same as the SP number then a value of 0 is returned.
Send Letter Success to SP4	The number of send letter success to SP4. If the current table index is the same as the SP number then a value of 0 is returned.
Rate Limiting ARP Drops [1]	The number of ARP packets that were dropped due to rate limiting.
Rate Limiting ICMP Drops [1]	The number of ICMP packets that were dropped due to rate limiting.
Rate Limiting TCP Drops [1]	The number of TCP packets that were dropped due to rate limiting.
Rate Limiting UDP Drops [1]	The number of UDP packets that were dropped due to rate limiting.

1. This is applicable only to Alteon OS 22.0 and higher.

Note: Alteon Application switches 2208 and 2216 do not support SP3 and SP4.

Monitoring the Management Port on Alteon Application Switches

Field	Description
Received Packets	Total number of packet allocations from the packet buffer pool by the TCP/IP protocol stack.
Received Errors	The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.
Received Dropped	The number of inbound packets that were dropped.
Received Overruns	The number of data overruns over this link.
Received Frames	The number of frames received on this link.
Bytes Received [1]	The number of bytes received on this link.
Transmitted Packets	Total number of packet allocations from the packet buffer pool by the TCP/IP protocol stack.
Transmitted Errors	The number of outbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.
Transmitted Dropped	The number of transmitted packets that were dropped.
Transmitted Overruns	The number of transmitted data overruns over this link.
Transmitted Carrier	The number of transmitted carriers over this link.
Transmitted Collisions	The total number of collisions on the Management port. Collisions occur when two or more stations are transmitting signals at the same time.
Transmitted Queue Length	The queue length in bytes.
Received Multicast Packets [1]	The number of multicast packets received on this link.
Bytes Transmitted [1]	The total number of outgoing bytes successfully transferred by the interface.

1. This is applicable only on Alteon Application Switches and on ALO 1.0 and higher.

Monitoring SONMP

You have to enable SONMP for this tab to appear. On Configure -> Switch -> SONMP -> Topology Status, set the option to On.

Field	Description
Slot	Specifies the slot on which the topology message was received.
Port	Specifies the port on which the topology message was received.
IP Address	This is the IP address of the sender of the topology message.
Segment	The “segment identifier” of the segment from which the remote agent send the topology message. Different devices may use different methods for representing the segment identifier.
MAC Address	The MAC address of the sender of the topology message.
Chasis Type	The chassis type of the device that sent the topology message.
Backplane Type	The backplane type of the device that sent the topology message.
Local Segment	Indicates if the sender of the topology message is on the same Ethernet segment (i.e. not across a bridge) as the reporting agent.
State of Sender	The current state of the sender of the topology message. the values are: topChanged—topology information has recently changed heartbeat—topology information unchanged. new—sending agent is in new state.

Note: This feature is applicable only on Alteon Application Switches and on ALO 1.0 and higher.

Monitoring Aggregated Ports

Note: This feature is available only on Alteon OS 22.0 and higher.

Field	Description
Selected Aggregator	The number of the aggregator.
Port	The number of the port.

Monitoring Link Aggregation Information

Note: This feature is available only on Alteon OS 22.0 and higher.

Field	Description
Port	The number of the port.
Valid Received LACPDUs	The number of the valid LACPDUs that the switch received on this port.
Valid Received Marker PDUs	The number of valid Marker PDUs that the switch received on this port.
Valid Received Marker Response PDUs	The number of valid Marker Responses that the switch received on this port.
Received Unknown	The number of unknown version or TLV type that the switch received on this port.
Received Illegal	The number of illegal LACP subtype received on this port.
Transmitted LACPDUs	The number of LACPDUs transmitted out of this port.
Transmitted Marker PDUs	The number of Marker PDUs transmitted out of this port.
Transmitted Marker Response PDUs	The number of Marker Responses transmitted out of this port.

Monitoring Link Aggregation Control Protocol Ports

Note: This feature is available only on Alteon OS 22.0 and higher.

Field	Description
Port	The number of the port.
State	This field indicates the aggregation state of the port. The `selected` value indicates the port is aggregated. The `standby` value indicates the port is in LACP standby state. The `unselected` value indicates the port is not aggregated or LACP is not configured.
ntt [1]	The ntt (Need-To-Transmit) field displays the port's state about the need to transmit LACPDU. This state is represented by `true` or `false` values. `True` value of this field indicates that there is a change in the information on the switch. `False` indicates that there is no new information so there is no need to transmit LACPDU.
Ready_N [1]	This flag displays the value for `Ready_N`. The `true` value indicates that the port is ready to be attached to an aggregator. Each port has its own Ready_N value.
Moved [1]	This field indicates the physical connectivity changes that occur for an LACP port. `True` value of this field indicates that the partner port is no longer connected to this port and has been moved to a different port. `False` value indicates that the partner port is still connected to this port.

1. These tabs are read-only objects and are used only for LACP debugging purposes.

Monitoring NTP

Note: This feature is available only on Alteon OS 22.0 and higher.

Field	Description
NTP Requests Sent to Primary NTP Server	The total number of NTP requests the switch sent to the primary NTP server to synchronize time.
NTP Responses received from Primary NTP Server	The total number of NTP responses received from the primary NTP server.
Update Clock Using NTP Primary NTP Server Response	The total number of times the switch updated its time based on the NTP responses received from the primary NTP server.
NTP Requests sent to Secondary NTP Server	The total number of NTP requests the switch sent to the secondary NTP server to synchronize time.
NTP Responses received from Secondary NTP Server	The total number of NTP responses received from the secondary NTP server.
Update clock using Secondary NTP Server Response	The total number of times the switch updated its time based on the NTP responses received from the secondary NTP server.
Last Update using NTP Response From Server	Last update of time on the switch based on either primary or secondary NTP response received.
Last Time Update by NTP Server	The time stamp showing the time when the switch was last updated.

Monitoring Spanning Tree Group Information

Note: This feature is available only on Alteon OS 22.0 and higher.

Field	Description
STG	Displays the STG number.
Port	Displays the port number.
Receive Cfg	Displays the number of configuration BPDUs received.
Receive TCN	Displays the number of TCN (Topology Change Notification) messages received.
Transmit Cfg	Displays the number of configuration BPDUs transmitted.
Transmit TCN	Displays the number of TCN (Topology Change Notification) messages transmitted.

Monitoring Bridge

The following topics are covered in this section:

- Monitoring Bridge: Forwarding Database on ALO and on Alteon 180 or AD series
- Monitoring Bridge: Forwarding Database on Alteon Application Switches
- Monitoring Bridge: Forwarding Statistics on Alteon Application Switches
- Monitoring Bridge: Base Ports
- Monitoring Bridge: Base Ports on Alteon Application Switches
- Monitoring Bridge: TP Ports

Monitoring Bridge: Forwarding Database on ALO and on Alteon 180 or AD series

Field	Description
Status	The status of the bridge: learned, self, or other.
MAC Address	The MAC address of the bridge.
Port	The physical port on which the MAC address is located

Monitoring Bridge: Forwarding Database on Alteon Application Switches

The forwarding database (FDB) contains information that maps the media access control (MAC) address of each known device to the switch port where the device address was learned.



If you are monitoring Forwarding Database on Alteon Application Switchesyou can select the **Clear** button to delete the Forwarding Database from the switch memory.

Field	Description
MAC Address	The MAC address of the FDB entry.
VLAN	The VLAN number of the FDB entry.
Port	The physical port on which the MAC address is located
State	The status of the bridge: forwarding or unknown. An address that is in the forwarding state means that it has been learned by the switch. If the state for the port is listed as unknown, the MAC address has not yet been learned by the switch, but has only been seen as a destination address.
SP	Displays the index number that identifies the Switch Processor (SP).
Learned Port	The port number that has been learned by the switch.
Trunk [1]	Displays all FDB entries on a single trunk. When trunk groups are configured, you can view the state of each port in the various trunk groups.

1. This field is applicable only on Alteon Application Switches and on ALO 1.0 and higher.

Monitoring Bridge: Forwarding Statistics on Alteon Application Switches

Field	Description
Created Entries	Number of entries created in the Forwarding Database.
Deleted Entries	Number of entries deleted from the Forwarding Database.
Current Entries	Current number of entries in the Forwarding Database.
Highest Number of Entries	Highest number of entries recorded at any given time in the Forwarding Database.
Lookups	Number of entry lookups in the Forwarding Database.
Failed Lookups	Number of unsuccessful searches made in the Forwarding Database.
Total Searches	Number of searches in the Forwarding Database.
Failed Searches	Number of search failures in the Forwarding Database.
Found/Created	Number of entries found or created in the Forwarding Database.
Overflow	Number of entries overflowing the Forwarding Database.

Monitoring Bridge: Base Ports

Field	Description
Port	The physical port.
Port Interface	The interface number to the physical port.
Circuit	The circuit number of the physical port.
Exceeded Delay Discarded Frames	The number of frames that were discarded because of excessive transit delay through the bridge. Discards Due to Transit Delay is incremented by transparent and source route bridges.
Exceeded Size Discarded Frames	The number of excessively large frames that were discarded. Discards Due to Excessive Size is incremented by transparent and source route bridges.

Note: This description of Base Ports is applicable on ALO, on Alteon 180 or AD series, and on Alteon Application Switches that are running Alteon OS below 21.0.

Monitoring Bridge: Base Ports on Alteon Application Switches

Field	Description
STP	Displays the index for Spanning Tree Protocol groups.
Port	Displays port number for Spanning Tree Protocol groups and priority.
State	Displays the current state of the port. The state field can be either BLOCKING, LISTENING, LEARNING, FORWARDING, or DISABLED.
Designated Root	The unique Bridge Identifier of the Bridge recorded as the Root in the Configuration BPDUs transmitted by the Designated Bridge for the segment to which the port is attached.
Designated Cost	The path cost of the Designated Port of the segment connected to this port. This value is compared to the Root Path Cost field in received bridge PDUs.
Designated Bridge	The designated bridge resides closest to the root bridge and is responsible for forwarding packets from the LAN towards the root bridge. This bridge is displayed as character string starting with the bridge priority (1-65535) followed by a hyphen and six byte MAC address of that switch.
Designated Port	The designated port identifies a physical port. This is a number that is the numerical sum of bridge priority and the actual physical port number. For example, a physical port number four with bridge priority 32768 will be displayed as 32678+4=32772.
Forward Transitions	The number of times this port has transitioned from the Learning state to the Forwarding state.
Path Cost	The port path cost parameter is used to help determine the designated port for a segment. Generally speaking, the faster the port, the lower the path cost. A setting of 0 indicates that the cost will be set to the appropriate default after the link speed has been auto negotiated.

Note: This description of Base Ports is applicable only on Alteon Application Switches that are running Alteon OS 21.0 and higher.

Monitoring Bridge: TP Ports

Note: This menu applies to the Spanning Tree Group selected in the **STP Group:** drop-down menu at the bottom right of this window. There are 16 possible Spanning Tree Groups that can be configured using this window.

Field	Description
Port	The port number of the switch.
Maximum size of INFO	The maximum size of the INFO (excluding MAC header) field that the port will receive or transmit.
Frames In	The number of frames that have been received and processed on this port.
Frames Out	The number of frames that have been transmitted on this port.
Discarded Frames In	The number of valid frames received which were discarded by the Forwarding Process of the switch.

Note: This description of TP Ports is applicable on ALO, on Alteon 180 or AD series, and on Alteon Application Switches that are running Alteon OS 20.x and lower.

Monitoring Security

The following topics are covered in this section:

- Monitoring Security: Port Denial of Service
- Monitoring Security: Pattern Match Group
- Monitoring Security: UDB Blast
- Monitoring Security: IP ACL

Note: This feature is available only on Alteon Application Switches that are running Alteon OS 21.0 and higher.

Note: You need to obtain a key/license from Nortel Networks to activate the Security features on your switch.

Monitoring Security: Port Denial of Service

Field	Description
Port	Displays the number of times the packets were dropped for each of the following types of DOS attacks, on the selected port only.
Smurf	The ICMP ping request to a broadcast destination IP(x.x.x.255).
Land Attack	Packets with source IP equal destination IP.
Fraggle	The UDP packet to a broadcast destination IP(x.x.x.255).
Null Scan	TCP sequence number is zero and all control bits are zeros.
XMAS Scan	TCP sequence number is zero and the FIN, URG and PSH bits are set.
Port Zero	TCP/UDP Packets with either source/destination port is zero.
SYN/FIN Set	SYN and FIN bits are set in the packet.
Blat	TCP packets with SIP!=DIP and SPORT=DPORT.

Monitoring Security: Pattern Match Group

When a virus or other attack contains multiple patterns or strings, it is useful to combine them into one group and give the group a name that is easy to remember. When a pattern group is applied to a deny filter, the switch will match any of the strings or patterns within that group before denying and dropping the packet. Up to five patterns can be combined into a single pattern group. Configure the binary or ascii pattern strings, group them into a pattern group, name the pattern group, and then apply the group to a filter.

The filtering commands in Alteon OS Security Pack allow the administrator to define groups of patterns and place them into groups. By applying the patterns and groups to a deny filter, the packet content can be detected and thus denied access to the network.

Field	Description
Pattern Group	The index of the pattern match group.
Name	Specifies a descriptive name for this pattern group.
Hits	Displays the number of times each configured pattern group has been matched and a subsequent filtering action performed.

Monitoring Security: UDB Blast

Malicious attacks over UDP protocol ports are becoming a common way to bring down real servers. Alteon OS can be configured to restrict the amount of traffic allowed on any UDP port, thus ensuring that backend servers are not flooded with data and disabled.

You can specify a series of UDP port ranges and the allowed packet limit for that range. When the maximum number of packets/second is reached, UDP traffic is shut down on those ports.

Alteon OS supports up to 5000 UDP port numbers, using any integer from 1 to 65535. The maximum port range is 5000. If the first port number is 300, the last number that can be used is 5300.

While you can configure multiple port ranges, the sum of ranges cannot exceed the maximum of 5000 ports.

Field	Description
Index	The index of the UDP blast attacks.
Port	UDP ports that experienced UDP blast attacks.
Blocked Packets	Displays all the accumulated blocked packets for each port.
Packet Rate per Second	Displays the current packet rate per second.

Monitoring Security: IP ACL

Alteon OS can be configured with IP access control lists (ACLs) composed of ranges of client IP addresses that are to be denied access to the switch. When traffic ingresses the switch, the client source IP address is checked against this pool of addresses. If a match is found, then the client traffic is blocked.

Field	Description
IP ACL Group	Displays the IP ACL group number.
Address	Displays the ranges of client IP addresses that are to be denied access to the switch.
Blocked Packets	Displays the accumulated blocked packets for each IP address and mask pair.

Monitoring IP

The following topics are covered in this area:

- Monitoring IP: Routes
- Monitoring IP: Routes on ALO and on Alteon 180 or AD series
- Monitoring IP: Routes on Alteon Application Switches
- Monitoring IP: Routes - Standard
- Monitoring IP: Route Statistics
- Monitoring IP: Address Resolution Protocol (ARP)
- Monitoring IP: ARP Statistics
- Monitoring IP: Interfaces
- Monitoring IP: Interface Statistics
- Monitoring IP: IP Addresses
- Monitoring IP: TCP
- Monitoring IP: TCP Connection
- Monitoring IP: UDP
- Monitoring IP: UDP Local
- Monitoring IP: Switch IP Properties on Alteon 180 or AD series
- Monitoring IP: Switch IP Properties on Alteon Application Switches
- Monitoring IP: ICMP In
- Monitoring IP: ICMP Out
- Monitoring IP: Routing Information Protocol (RIP)
- Monitoring IP: Gateways

Monitoring IP: Routes

Field	Description
Destination IP Address	The destination IP address of this route. Note: Multiple routes to a single destination can appear in the table if the Destination IP Address has been defined by the Network Management Protocol.
Interface	The number of the Interface.
Next Hop IP Address	The IP address of the next hop of this route. Note: If a route bound to an interface is through a broadcast media, Next Hop Address is the agent's IP address on that interface.
Type	The type of route: direct, indirect, invalid, or other. Note: The type invalid disassociates both the destination and the route entry that are identified with this entry. Management stations must be prepared to receive information from agents that correspond to entries that are not currently in use.
Route Learned Via	The routing mechanism through which this route was learned. Note: Including values for gateway routing protocols does not indicate that hosts will also support those protocols.
Time Since Last Update	The number of seconds since this route was last updated.
IP Subnet Mask	The mask that must be logically ended with the destination address before it is compared to the destination address of the router. If the value of the destination address is 0.0.0.0 (default value), the mask value is also 0.0.0.0. If the system does not support arbitrary subnet masks, an agent constructs the router mask based on the class of the network of the destination address: 255.0.0.0 for class A 255.255.0.0 for class B 255.255.255.0 for class C

Note: This feature is applicable only on Alteon 180 or AD series running Web OS 8.3 and lower.

Monitoring IP: Routes on ALO and on Alteon 180 or AD series

Field	Description
Route	The index number of the routing table.
Destination IP Address	The destination IP address of this route.
Destination IP Mask	The IP mask of this route.
Next-Hop Router	The gateway of this route.
Tag Type	The tag type: ICMP, static, SNMP, addr, RIP, broadcast, martian, or multicast.
Route Type	The type of route: indirect, direct, local, broadcast, martian, multicast, or other.
Interface	The IP interface of this route that is used as the source IP for routing.

Note: This feature is applicable on ALO and on Alteon 180 or AD series running Web OS 9.0 and 10.0.

Monitoring IP: Routes on Alteon Application Switches



You can use the **Clear IP Table** button to clear the entire IP list from the switch memory.

Field	Description
Route	The index number of the routing table.
Destination IP Address	The destination IP address of this route.
Destination IP Mask	The IP mask of this route.
Next-Hop Router 1	The gateway of this route.
Tag Type	The tag type: ICMP, static, SNMP, addr, RIP, broadcast, martian, or multicast.
Route Type	The type of route: indirect, direct, local, broadcast, martian, multicast, or other.
Interface	The IP interface of this route that is used as the source IP for routing.
Next-Hop Router 2 [1]	The gateway of this route.
Next-Hop Router 3 [1]	The gateway of this route.

1. This is applicable on only Alteon OS 22.0 and higher.

Monitoring IP: Routes - Standard

Field	Description
Destination IP address	The destination IP address of this route. Note: Multiple routes to a single destination can appear in the table if the Destination IP Address has been defined by the Network Management Protocol.
Interface	The number of the Interface.
Next Hop IP Address	The IP address of the next hop of this route. Note: If a route bound to an interface is through a broadcast media, Next Hop Address is the agent's IP address on that interface.
Type	The type of route: direct, indirect, invalid, or other. Note: The type invalid disassociates both the destination and the route entry that are identified with this entry. Management stations must be prepared to receive information from agents that correspond to entries that are not currently in use.
Route Learned via	The routing mechanism through which this route was learned. Note: Including values for gateway routing protocols does not indicate that hosts will also support those protocols.
Time Since Last Update	The number of seconds since this route was last updated.
IP Subnet Mask	The mask that must be logically Ended with the destination address before it is compared to the destination address of the router. If the value of the destination address is 0.0.0.0 (default value), the mask value is also 0.0.0.0. If the system does not support arbitrary subnet masks, an agent constructs the router mask based on the class of the network of the destination address: 255.0.0.0 for class A 255.255.0.0 for class B 255.255.255.0 for class C

Monitoring IP: Route Statistics

Field	Description
IP Routes	The current number of IP routes.
Most IP Routes	The highest number of IP routes.
Maximum IP Routes	The maximum number of IP routes.

Monitoring IP: Address Resolution Protocol (ARP)



If you are monitoring ARP on Alteon Application Switches, you can use the **Clear ARP Table** button to clear the entire ARP list from switch memory.

Field	Description
Destination IP Address	The destination IP address of the address resolution.
MAC Address	The MAC address for the Address Resolution Protocol (ARP) entry.
VLAN ID	The VLAN identifier for the ARP.
Source Port	The port number.
Reference SP	The SP that is associated with this ARP.
Flag	The flag status of this ARP: *clear*, *unresolved* (U), *permanent* (P), *indirect* (R), or *layer4* (p 4) (in 20.1.1.0 and higher). These flags mean the following: **U**: Unresolved or unknown ARP entry. The MAC address of the client has not yet been learned. **P**: Permanent entry created for switch IP interface. This entry never ages out. **P 4**: Permanent entry created for Layer 4 proxy IP address or virtual server IP address. **R**: Indirect ARP cache entry. This entry is used for faster forwarding the next time the packet comes for the same destination.

Monitoring IP: ARP Statistics

Field	Description
ARP Entries	The current number of ARP entries.
Most ARP Entries	The highest number of ARP entries.
Maximum ARP Entries	The maximum number of ARP entries.

Monitoring IP: Interfaces

Field	Description
Interface	Displays two types of interfaces: • an IP interface from 1 to 256; for example *IP 10*. • a physical (port) number depending on the switch; for example *Port 2.*
Description	A text string containing information about the interface. • A logical interface is described as *net0*, *net1*, etc. • A Fast Ethernet physical (port) interface is described as *utp ethernet (10/100)* • A Gigabit Ethernet physical (port) interface is described as *fiber ethernet (1000)*
Type	The type of interface. A virtual interface (`propVirtual`) or a physical interface that is assigned to a switch port (e.g. `ethernetCsmacd`).
MTU (Largest Packet)	The size of the largest datagram which can be sent or received on the interface, specified in octets
Speed	The speed of the physical interface. 10 Mbps, 100 Mbps, 1000Mbps, or other.
MAC Address	The MAC address of the physical interface.
Admin State	The administrative state of the Interface: up or down.
Operational Status	The status of the Interface: up or down.
Last Change	Lists the date of the last change to the interface.
MIB Specification	A reference to MIB definitions that are specific to the media that realizes the interface. Example: if the interface is realized by Ethernet, then MIB Specific refers to a document that defines Ethernet objects.

Monitoring IP: Interface Statistics

Note: If you are monitoring IP interface statistics on Alteon Application Switches you can right-click and select Clear Interface Statistics to clear the selected interface statistics. IP interfaces are labelled as IP1, IP2, etc. Physical port interfaces are labelled Port 1, Port 2, and so on.

Field	Description
Interface	The number of the interface. The interface number is either one of the 256 IP interfaces or one of the physical ports.
Bytes In	The number of bytes received on the interface, including framing characters.
Bytes Out	The number of bytes transmitted out of the interface, including framing characters.
Unicast Packets In	The number of packets, delivered by this sublayer to a higher layer that were not addressed to a multicast or a broadcast address at this sublayer.
Unicast Packets Out	The number of packets that higher-level protocols requested to transmit that were not addressed to a multicast or broadcast address at this sublayer. The count includes the packets that were discarded or not delivered.
Multicasts In	The number of packets, delivered by this sublayer to a higher layer that were addressed to a multicast address at this sublayer. For a MAC layer protocol, this includes Group and Functional addresses.
Multicasts Out	The number of packets that higher-level protocols requested to transmit that were addressed to a multicast address at this sublayer. The count includes the packets that were discarded or not sent.For a MAC layer protocol, this includes Group and Functional addresses.
Broadcast In	The number of packets, delivered by this sublayer to a higher layer, that were addressed to a broadcast address at this sublayer.
Broadcast Out	The number of packets that higher-level protocols requested to transmit, that were addressed to a broadcast address at this sublayer. The count includes the packets that were discarded or not delivered.
Discarded Packets	The number of inbound packets that were discarded, although no errors had been detected to prevent their delivery to a higher-layer protocol. This can occur to free up buffer space.
Outbound Discards	The number of outbound packets that were discarded, although no errors had been detected that would prevent their transmission. This can occur to free up buffer space.

Field	Description
Error Packets	For packet-oriented interfaces, the number of inbound packets with errors that prevented their delivery to a higher-layer protocol.For character-oriented or fixed-length interfaces, the number of inbound transmission units with errors that prevented their delivery to a higher-layer protocol.
Not Sent Due to Error	For packet-oriented interfaces, the number of outbound packets that could not be transmitted because of errors. For character-oriented or fixed-length interfaces, the number of outbound transmission units that could not be transmitted because of errors.
Unknown Protocol Packets	For packet-oriented interfaces, the number of packets received via the interface that were discarded because of an unknown or unsupported protocol. For character-oriented or fixed-length interfaces that support protocol multiplexing, the number of transmission units received via the interface that were discarded because of an unknown or unsupported protocol. **Note:** If the interface does not support protocol multiplexing, Unknown Protocol Packets will be 0 (zero).
Outbound Packet Queue Length	The number of packets in the output queue.

Monitoring IP: IP Addresses



If you are monitoring IP addresses on Alteon Application Switches, you can select the **Clear IP Statistics** button to clear all IP Statistics on the switch.

Field	Description
IP Address	The IP address.
Interface	The index number of the interface.
IP Subnet Mask	The subnet mask of the IP address. The subnet mask is an IP address with all the network bits set to 1 and all the hosts bits set to 0.
Broadcast LSB	The broadcast address of the interface.
Maximum Reassembly Size	The size of the largest IP datagram that can be re-assembled from fragmented IP datagrams.

Monitoring IP: TCP

Field	Description
Current TCP Connections [1]	The total number of outstanding TCP sessions that are currently opened.
TCP SYN Received w/o ACK [2]	The total number of new half open sessions that have not been acknowledged.
Active Opens	The number of TCP connections that were a direct transition to the SYN-SENT state from the CLOSED state.
Passive Opens	The number of TCP connections that were a direct transition to the SYN-RCVD state from the LISTEN state.
Failed Attempts	The number of TCP connections that were a direct transition to the CLOSED state from the SYN-SENT state or the SYN-RCVD state, and a direct transition to the LISTEN state from the SYN-RCVD state.
Resets In	The number of /TCP connections that made a direct transition to the CLOSED state from either the ESTABLISHED state or the CLOSE-WAIT state
Established	The number TCP connections that were a direct transition to the CLOSED state from the ESTABLISHED state or the CLOSE-WAIT state.
Segments In	The total number of segments received, including those received in error. This count includes segments received on currently established connections
Segments Out	The total number of transmitted segments, including those on current connections, but excluding those that contain only retransmitted bytes.
Retransmitted Segments	The total number of retransmitted segments: the number of TCP segments transmitted that contain one or more previously transmitted bytes.
Segments Received with Errors	The total number of received segments, including errors. This count includes segments received on currently established connections.
Resets Out	The number of transmitted TCP segments that contain the RST flag.
OutBound TCBs [3]	The total number of transmitted TCBs.
InBound TCBs [3]	The total number of received TCBs.
Listening TCBs [3]	TCP control blocks in the listening state.

1. This is applicable only on Alteon 180 or AD series and on ALO switches.
2. This is applicable only on Alteon 180 or AD series.
3. This is applicable only on Web OS 10.1 and higher.

Monitoring IP: TCP Connection

Field	Description
Connection State	Displays the TCP connection state.
Local IP Address	Displays the local IP address.
Local TCP Port	Displays the number of the local port.
Remote IP Address	Displays the remote IP address.
Remote TCP Port	Displays the number of the remote port.

Monitoring IP: UDP

Field	Description
Datagrams In	The total number of UDP datagrams delivered to UDP users.
No Application at Port	The total number of received UDP datagrams when no application was at the destination port.
Dropped Datagrams	The number of received UDP datagrams that could not be delivered for reasons other than the absence of an application at the destination port.
Datagrams Out	The total number of delivered UDP datagrams.

Monitoring IP: UDP Local

Field	Description
Local IP Address	The local IP address for the UDP listener. When the UDP listener accepts datagrams for any IP interface associated with the node, the address is 0.0.0.0.
Local UDP Port	The local port number for the UDP listener.

Monitoring IP: Switch IP Properties on Alteon 180 or AD series

Field	Description
Good Packets In	The number of input datagrams received from interfaces, including those received in error.
Header Error Packets In	The number of input datagrams that were discarded because of errors in the IP headers. Errors: bad checksums, version number mismatch, other format errors, time-to-live exceeded, errors discovered in processing their IP options, and so on.
Address Errors In	The number of input datagrams that were discarded because the IP address in the IP header's destination field was not a valid address at this switch. Invalid addresses: 0.0.0.0, addresses of unsupported Classes such as Class E, and so forth.For entities that are not IP Gateways that do not forward datagrams, the count includes datagrams that were discarded because the destination address was not a local address.
Packets Routed	The number of input datagrams for which this entity was not their final IP destination. An attempt was made to find a route to forward them to that final destination.In entities that do not act as IP Gateways, the count only includes packets that were Source-Routed via this entity, and that the Source-Route option processing was successful.
Packets In with Unknown Protocol	The number of locally-addressed datagrams that were received successfully, but were discarded because of an unknown or an unsupported protocol.
Inbound Dropped Packets	The number of input IP datagrams that were discarded, although no errors were identified. This can occur because of insufficient buffer space. **Note:** This counter does not include any datagrams that were discarded while waiting for re-assembly.
Packets Consumed	The total number of input datagrams successfully delivered to IP user-protocols, including ICMP.
Packets Out	The total number of IP datagrams that local IP user-protocols, including ICMP, supplied to IP in requests for transmission. **Note:** This counter does not include any datagrams that were counted in Packets Routed.
Outbound Dropped Packets	The number of output IP datagrams that were discarded, although no problems were noted. This can occur because of insufficient buffer space. **Note:** This counter includes datagrams that were counted in Packets Routed if the packets met this discard criterion.

Field	Description
Non-Routable Dropped Packets	The number of IP datagrams discarded because no route was available for transmitting them to their destinations. **Note:** This counter includes any packets counted in Packets Routed that meet this no-route criterion. Also included, are any datagrams that a host cannot route because all of the default gateways are down.
Successful Packet Fragmentation	The number of IP datagrams that have been successfully fragmented.
Failed Packet Fragmentation	The number of IP datagrams that have been discarded because they could not be fragmented, such as when the Don't Fragment flag has been set.
Fragments Created	The number of IP datagrams that have been fragmented.
IP Fragments Reassembled	The number of received IP fragments that needed to be reassembled.
Packet Reassembly Successes	The number of IP datagrams successfully reassembled.
Packet Reassembly Failures	The number of failures detected by the IP re-assembly algorithm. Possible failures include timed out, errors, and so on. **Note:** This is not necessarily a count of discarded IP fragments. Some algorithms, notably the algorithm in RFC 815, can lose track of the number of fragments by combining them as they are received.
Routing Discards	The number of dropped packets.

Monitoring IP: Switch IP Properties on Alteon Application Switches



Select the **Clear IP Statistics** button to clear all IP Statistics on the switch

Field	Description
Good Packets In	The number of input datagrams received from interfaces, including those received in error.
Header Error Packets In	The number of input datagrams that were discarded because of errors in the IP headers. Errors: bad checksums, version number mismatch, other format errors, time-to-live exceeded, errors discovered in processing their IP options, and so on.
Address Errors In	The number of input datagrams that were discarded because the IP address in the IP header's destination field was not a valid address at this switch. Invalid addresses: 0.0.0.0, addresses of unsupported Classes such as Class E, and so forth. For entities that are not IP Gateways that do not forward datagrams, the count includes datagrams that were discarded because the destination address was not a local address.
Packets Routed	The number of input datagrams for which this entity was not their final IP destination. An attempt was made to find a route to forward them to that final destination.In entities that do not act as IP Gateways, the count only includes packets that were Source-Routed via this entity, and that the Source-Route option processing was successful.
Packets In with Unknown Protocol	The number of locally-addressed datagrams that were received successfully, but were discarded because of an unknown or an unsupported protocol.
Inbound Dropped Packets	The number of input IP datagrams that were discarded, although no errors were identified. This can occur because of insufficient buffer space. **Note:** This counter does not include any datagrams that were discarded while waiting for re-assembly.
Packets Consumed	The total number of input datagrams successfully delivered to IP user-protocols, including ICMP.
Packets Out	The total number of IP datagrams that local IP user-protocols, including ICMP, supplied to IP in requests for transmission. **Note:** This counter does not include any datagrams that were counted in Packets Routed.

Field	Description
Outbound Dropped Packets	The number of output IP datagrams that were discarded, although no problems were noted. This can occur because of insufficient buffer space. **Note:** This counter includes datagrams that were counted in Packets Routed if the packets met this discard criterion.
Non-Routable Dropped Packets	The number of IP datagrams discarded because no route was available for transmitting them to their destinations. **Note:** This counter includes any packets counted in Packets Routed that meet this no-route criterion. Also included, are any datagrams that a host cannot route because all of the default gateways are down.
Successful Packet Fragmentation	The number of IP datagrams that have been successfully fragmented.
Failed Packet Fragmentation	The number of IP datagrams that have been discarded because they could not be fragmented, such as when the Don't Fragment flag has been set.
Fragments Created	The number of IP datagrams that have been fragmented.
IP Fragments Reassembled	The number of received IP fragments that needed to be reassembled.
Packet Reassembly Successes	The number of IP datagrams successfully reassembled.
Packet Reassembly Failures	The number of failures detected by the IP re-assembly algorithm. Possible failures include timed out, errors, and so on. **Note:** This is not necessarily a count of discarded IP fragments. Some algorithms, notably the algorithm in RFC 815, can lose track of the number of fragments by combining them as they are received.
Routing Discards	The number of dropped packets.

Monitoring IP: ICMP In

Field	Description
Source Quench Packets In	The number of received Internet Control Message Protocol (ICMP) Source Quench messages.
Redirect Packets In	The number of received ICMP Redirect messages.
Echo (Ping) Request Packets In	The number of received ICMP Echo (request) messages.
Echo (Ping) Reply Packets In	The number of received ICMP Echo Reply messages.
Timestamp Request Packets In	The number of received ICMP Timestamp (request) messages.
Timestamp Reply Packets In	The number of received ICMP Timestamp Reply messages.
Address Mask Request Packets In	The number of received ICMP Address Mask Request messages.
Address Mask Reply Packets In	The number of received ICMP Address Mask Reply messages.
Parameter Problem Packets In	The number of received ICMP Parameter Problem messages.
Destination Unreachable Packets In	The number of received ICMP Destination Unreachable messages.
Time Exceeded Packets In	The number of received ICMP Time Exceeded messages.
Packets In	The number of received ICMP messages.
Error Packets In	The number of received ICMP Time error messages.

Monitoring IP: ICMP Out

Field	Description
Source Quench Packets Out	The number of Internet Control Message Protocol (ICMP) Source Quench messages sent.
Redirect Packets Out	The number of ICMP Redirect messages sent. **Note:** For a host, this object will always be 0 (zero) since hosts do not send redirects.
Echo (Ping) Request Packets Out	The number of transmitted ICMP Echo request messages.
Echo Reply (Ping) Packets Out	The number of transmitted ICMP Echo Reply messages.
Timestamp Request Packets Out	The number of transmitted ICMP Timestamp request messages.
Timestamp Reply Packets Out	The number of transmitted ICMP Timestamp Reply messages.
Address Mask Request Packets Out	The number of transmitted ICMP Address Mask Request messages.
Address Mask Reply Packets Out	The number of transmitted ICMP Address Mask Reply messages.
Parameter Problem Packets Out	The number of transmitted ICMP Parameter Problem messages.
Destination Unreachable Packets Out	The number of transmitted ICMP Destination Unreachable messages.
Time Exceeded Packets Out	The number of transmitted ICMP Time Exceeded messages.
Packets Out	The total number of delivered ICMP packets.
Error Packets Out	The number of ICMP packets delivered with error messages.

Monitoring IP: Routing Information Protocol (RIP)

Field	Description
Good RIP Packets In	The number of good RIP packets that were received.
RIP Packets Out	The number of transmitted RIP packets that were transmitted.
Bad RIP Packets In	The number of received error RIP packets.
RIP routes aged out	The number of rip routes that have aged out.

Monitoring IP: Gateways

Field	Description
Gateway	The index of the gateway.
Address	Displays the IP address of the gateway.
VLAN	Displays the VLAN number of the gateway.
Status	Displays the status of the gateway.

Note: This feature is applicable only on Alteon Application Switches and on ALO 1.0 and higher.

Monitoring OSPF

The following topics are covered in this area:

- Monitoring OSPF: Administrative Status
- Monitoring OSPF: Area
- Monitoring OSPF: Area Nbr on Alteon 180 or AD series
- Monitoring OSPF: Area Nbr on Alteon Application Switches
- Monitoring OSPF: Area Interface
- Monitoring OSPF: Interface Transmissions
- Monitoring OSPF: Interface Nbr
- Monitoring OSPF: Interfaces
- Monitoring OSPF: Stats on Alteon 180 or AD series
- Monitoring OSPF: Stats on Alteon Application Switches
- Monitoring OSPF: Stats 2
- Monitoring OSPF: Area Information
- Monitoring OSPF: Interface Information
- Monitoring OSPF: Link-State DB
- Monitoring OSPF: External Link-State DB
- Monitoring OSPF: Area Receive Error Statistics on Alteon Application Switches
- Monitoring OSPF: Area Interface Receive Error Statistics on Alteon Application Switches
- Monitoring OSPF: Neighbor Interface

Monitoring OSPF: Administrative Status

This window simply displays whether or not OSPF is enabled on the Web Switch. You can configure the OSPF administrative status of the switch via the **Configure > Routing > OSPF** menu.

Monitoring OSPF: Area

Field	Description
Index	The index of the OSPF Area for which these statistics apply.
Packets In	The total number of OSPF packets received for this OSPF interface.
Packets Out	The total number of OSPF packets transmitted for this OSPF interface.
Hello In	The total number of Hello packets received for this OSPF interface.
Hello Out	The total number of Hello packets transmitted for this OSPF interface.
Database Description In	The total number of Database Description packets received for this OSPF interface.
Database Description Out	The total number of Database Description packets transmitted for this OSPF interface.
Link State In	The total number of Link State Request packets received for this OSPF interface.
Link State Out	The total number of Link State Request packets transmitted for this OSPF interface.
Link State Ack In	The total number of Link State Acknowledgement packets received for this OSPF interface.
Link State Ack Out	The total number of Link State Acknowledgement packets transmitted for this OSPF interface.
Link State Update In	The total number of Link State Update packets received for this OSPF interface.
Link State Update Out	The total number of Link State Update packets transmitted for this OSPF interface.

Monitoring OSPF: Area Nbr on Alteon 180 or AD series

Field	Description
Index	The index of the OSPF Area for which these statistics apply.
Hello In	The total number of Hello packets received from neighbors in this OSPF interface.
Start State	The total number of neighbors in this state (i.e. an indication that Hello packets should now be sent to the neighbor at intervals of HelloInterval seconds) in this OSPF interface.
Adjoint Okay	The total number of decisions to be made (again) as to whether an adjacency should be established or maintained with the neighbor for this OSPF interface.
Negotiated Done	The total number of neighbors in this state wherein the Master/slave relationship has been negotiated, and sequence numbers have been exchanged, for this OSPF interface.
Exchange Done	The total number of neighbors in this state (i.e. in an adjacency's final state) having transmitted a full sequence of Database Description packets, for this OSPF interface.
Bad Link State Request	The total number of Link State Requests which have been received for a link state advertisement not contained in the database for this interface.
Bad Sequences	The total number of Database Description packets that have been received that either: a) have an unexpected DD sequence number b) unexpectedly have had the init bit set c) Have an options field that differs from the last Options field that was received in a Database Description packet. Any of these conditions indicate that some error has occurred during adjacency establishment for this interface.
Loading Done	The total number of link state updates received for all out-of-date portions of the database for this OSPF interface.
Hello 1 way	The total number of Hello packets received from neighbors, in which this router is not mentioned for this OSPF interface.
Reset Adjacency	The sum total number of times the Neighbor adjacency has been reset on this interface.
Down	The total number of Neighboring routers down (i.e. in the initial state of a neighbor conversation.) for this interface.

Monitoring OSPF: Area Nbr on Alteon Application Switches

Field	Description
Index	The index of the OSPF Area for which these statistics apply.
Hello In	The total number of Hello packets received from neighbors in this OSPF interface.
Start State	The total number of neighbors in this state (i.e. an indication that Hello packets should now be sent to the neighbor at intervals of HelloInterval seconds.) in this OSPF interface.
Adjoint Okay	The total number of decisions to be made (again) as to whether an adjacency should be established or maintained with the neighbor for this OSPF interface.
Negotiated Done	The total number of neighbors in this state wherein the Master/slave relationship has been negotiated, and sequence numbers have been exchanged, for this OSPF interface.
Exchange Done	The total number of neighbors in this state (i.e. in an adjacency's final state) having transmitted a full sequence of Database Description packets, for this OSPF interface.
Bad Link State Request	The total number of Link State Requests which have been received for a link state advertisement not contained in the database for this interface.
Bad Sequences	The total number of Database Description packets that have been received that either: • have an unexpected DD sequence number • unexpectedly have had the init bit set • have an options field that differs from the last Options field that was received in a Database Description packet. Any of these conditions indicate that some error has occurred during adjacency establishment for this interface.
Loading Done	The total number of link state updates received for all out-of-date portions of the database for this OSPF interface.
Hello 1 way	The total number of Hello packets received from neighbors, in which this router is not mentioned for this OSPF interface.
Reset Adjacency	The sum total number of times the Neighbor adjacency has been reset on this interface.
Down	The total number of Neighboring routers down (i.e. in the initial state of a neighbor conversation.) for this interface.
Hello packets received	The total number of Hello packets received from neighbors, in which this router is mentioned in this OSPF area.

Monitoring OSPF: Area Interface

Field	Description
Index	The index of the OSPF Area for which these statistics apply.
Hello Sent	The total number of Hello packets sent by this interface.
Down	The total number of times the interface was down.
Not Connected	The total number of times the interface was no longer connected to the attached network.
Connected	The total number of times the interface connected back to the attached network.
Wait Timer Fired	The total number of times the Wait Timer has been fired, (indicating the end of the waiting period that is required before electing a (Backup) Designated Router) for this OSPF interface.
Backup Routers	The total number of Backup Designated Routers on the attached network for this OSPF interface.
Bidirectional Changes	The total number of changes in the set of bidirectional neighbors associated with the interface for this OSPF interface.

Monitoring OSPF: Interface Transmissions

Field	Description
Index	The index of the OSPF Area for which these statistics apply.
Packets In	The total number of OSPF packets received for this OSPF interface.
Packets Out	The total number of OSPF packets transmitted for this OSPF interface.
Hello In	The total number of Hello packets received for this OSPF interface.
Hello Out	The total number of Hello packets transmitted for this OSPF interface.
Database Description In	The total number of Database Description packets received for this OSPF interface.
Database Description Out	The total number of Database Description packets transmitted for this OSPF interface.
Link State Request In	The total number of Link State Request packets received for this OSPF interface.
Link State Request Out	The total number of Link State Request packets transmitted for this OSPF interface.
Link State Acks In	The total number of Link State Acknowledgement packets received for this OSPF interface.
Link State Acks Out	The total number of Link State Acknowledgement packets transmitted for this OSPF interface.
Link State Updates In	The total number of Link State Update packets received for this OSPF interface.
Link State Updates Out	The total number of Link State Update packets transmitted for this OSPF interface.

Monitoring OSPF: Interface Nbr

Field	Description
Index	The index of the OSPF Area for which these statistics apply.
Hello In	The total number of Hello packets received from neighbors in this OSPF interface.
State	The total number of neighbors in this state (i.e. an indication that Hello packets should now be sent to the neighbor at intervals of HelloInterval seconds) in this OSPF interface.
Adjoint Okay	The total number of decisions to be made (again) as to whether an adjacency should be established or maintained with the neighbor for this OSPF interface.
Negotiated Done	The total number of neighbors in this state in which the Master/slave relationship has been negotiated, and sequence numbers have been exchanged, for this OSPF interface.
Exchange Done	The total number of neighbors in this state (i.e. in an adjacency's final state) having transmitted a full sequence of Database Description packets, for this OSPF interface.
Bad Link State Request	The total number of Link State Requests which have been received for a link state advertisement not contained in the database for this interface.
Bad Sequences	The total number of Database Description packets which have been received that either • has an unexpected DD sequence number • unexpectedly has the init bit set • has an options field differing from the last Options field received in a Database Description packet. Any of these conditions indicate that some error has occurred while establishing adjacency for this interface.
Loading Done	The total number of link state updates received for all out-of-date portions of the database for this OSPF interface.
Hello 1 way	The total number of Hello packets received from neighbors, in which this router is not mentioned for this OSPF interface.
Reset Adjacency	The sum total number of times the Neighbor adjacency has been reset on this interface.
Down	The total number of Neighboring routers down (i.e. in the initial state of a Neighbor conversation) for this interface.

Monitoring OSPF: Interfaces

Field	Description
Index	The index of the OSPF Area for which these statistics apply.
Hello Sent	The total number of Hello packets sent by this interface.
Down	The total number of times the interface was down.
Not Connected	The total number of times the interface was no longer connected to the attached network.
Connected	The total number of times the interface connected back to the attached network.
Wait Timer Fired	The total number of times the Wait Timer has been fired, (indicating the end of the waiting period that is required before electing a (Backup) Designated Router) for this OSPF interface.
Backup Routers	The total number of Backup Designated Routers on the attached network for this OSPF interface.
Bidirectional Changes	The total number of changes in the set of bidirectional neighbors associated with the interface for this OSPF interface.

Monitoring OSPF: Stats on Alteon 180 or AD series

Field	Description
Packets In	The sum total of all OSPF packets received on all OSPF areas and interfaces.
Packets Out	The sum total of all OSPF packets transmitted on all OSPF areas and interfaces.
Hello In	The sum total of all Hello packets received on all OSPF areas and interfaces.
Hello Out	The sum total of all Hello packets transmitted on all OSPF areas and interfaces.
Database Description In	The sum total of all Database Description packets received on all OSPF areas and interfaces.
Database Description Out	The sum total of all Database Description packets transmitted on all OSPF areas and interfaces.
Link State Request In	The sum total of all Link State Request packets received on all OSPF areas and interfaces.
Link State Request Out	The sum total of all Link State Request packets transmitted on all OSPF areas and interfaces.
Link State Acks In	The sum total of all Link State Acknowledgement packets received on all OSPF areas and interfaces.
Link State Acks Out	The sum total of all Link State Acknowledgement packets transmitted on all OSPF areas and interfaces.
Link State Updates In	The sum total of all Link State Update packets received on all OSPF areas and interfaces.
Link State Updates Out	The sum total of all Link State Update packets transmitted on all OSPF areas and interfaces.
Neighbor Hello In	The sum total of all Hello packets received from neighbors on all OSPF areas and interfaces.
Neighbor State	The sum total number of neighbors in this state (i.e. an indication that Hello packets should now be sent to the neighbor at intervals of HelloInterval seconds), across all OSPF areas and interfaces.
Neighbor Adjoint Ok	The sum total number of decisions to be made (again) as to whether an adjacency should be established/maintained with the Neighbor across all OSPF areas and interfaces.
Neighbor Negotiation Done	The sum total number of neighbors in this state wherein the Master/ slave relationship has been negotiated, and sequence numbers have been exchanged, across all OSPF areas and interfaces.

Field	Description
Neighbor Exchange Done	The sum total number of neighbors in this state (i.e. in an adjacency's final state) having transmitted a full sequence of Database Description packets, across all OSPF areas and interfaces.
Neighbor Bad Link State Request	The sum total number of Link State Requests that have been received for a link state advertisement that is not contained in the database across all interfaces and OSPF areas.
Neighbor Bad Sequence	The sum total number of Database Description packets which have been received that either • has an unexpected DD sequence number • unexpectedly has the init bit set • has an options field differing from the last Options field received in a Database Description packet. Any of these conditions indicate that some error has occurred during adjacency establishment for all OSPF areas and interfaces.
Neighbor Loading Done	The sum total number of link state updates received for all out-of-date portions of the database across all OSPF areas and interfaces.
Neighbor Hello 1 way	The sum total number of Hello packets received from neighbors, in which this router is not mentioned across all OSPF interfaces and areas.
Neighbor Reset Adjacency	The sum total number of times the Neighbor adjacency has been reset across all OPSF areas and interfaces.
Neighbor Down	The total number of Neighboring routers down (i.e. in the initial state of a neighbor conversation) across all OSPF areas and interfaces.
Interface Hello In	The sum total number of Hello packets sent on all interfaces and areas.
Interface Down	The sum total number of interfaces down in all OSPF areas.
Interface Not Connected	The sum total of interfaces no longer connected to the attached network across all OSPF areas and interfaces.
Interface Connected	The sum total number of interfaces, connected to the attached network in all OSPF areas.
Interface Wait Timer Fired	The sum total number of times the Wait Timer has been fired, (indicating the end of the waiting period that is required before electing a (Backup) Designated Router) across all OSPF areas and interfaces.
Interface Backup Routers	The sum total number of Backup Designated Routers on the attached network for all OSPF areas and interfaces.
Interface Bidirectional Changes	The sum total number of changes in the set of bidirectional neighbors associated with any interface across all OSPF areas.
Hello Timer Fired	The sum total number of times the Hello timer has been fired (which triggers the send of a Hello packet) across all OPSF areas and interfaces.

Field	Description
Retransmit Timer Fired	The sum total number of times the Retransmit timer has been fired across all OPSF areas and interfaces.
Link State Lock Timer Fired	The sum total number of times the Lsa Lock timer has been fired across all OSPF areas and interfaces.
Link State Ack Timer Fired	The sum total number of times the LSA Ack timer has been fired across all OSPF areas and interfaces.
Dbage Fired	The total number of times the Dbage has been fired.
Summary Timer Fired	The total number of times the Summary timer has been fired.
ASE Export Timer Fired	The total number of times the (Autonomous System External route) ASE Export timer has been fired.

Monitoring OSPF: Stats on Alteon Application Switches

Field	Description
Packets In	The sum total of all OSPF packets received on all OSPF areas and interfaces.
Packets Out	The sum total of all OSPF packets transmitted on all OSPF areas and interfaces.
Hello In	The sum total of all Hello packets received on all OSPF areas and interfaces.
Hello Out	The sum total of all Hello packets transmitted on all OSPF areas and interfaces.
Database Description In	The sum total of all Database Description packets received on all OSPF areas and interfaces.
Database Description Out	The sum total of all Database Description packets transmitted on all OSPF areas and interfaces.
Link State Request In	The sum total of all Link State Request packets received on all OSPF areas and interfaces.
Link State Request Out	The sum total of all Link State Request packets transmitted on all OSPF areas and interfaces.
Link State Acks In	The sum total of all Link State Acknowledgement packets received on all OSPF areas and interfaces.
Link State Acks Out	The sum total of all Link State Acknowledgement packets transmitted on all OSPF areas and interfaces.
Link State Updates In	The sum total of all Link State Update packets received on all OSPF areas and interfaces.
Link State Updates Out	The sum total of all Link State Update packets transmitted on all OSPF areas and interfaces.
Neighbor Hello In	The sum total of all Hello packets received from neighbors on all OSPF areas and interfaces.
Neighbor State	The sum total number of neighbors in this state (i.e. an indication that Hello packets should now be sent to the neighbor at intervals of HelloInterval seconds), across all OSPF areas and interfaces.
Neighbor Adjoint Ok	The sum total number of decisions to be made (again) as to whether an adjacency should be established/maintained with the Neighbor across all OSPF areas and interfaces.
Neighbor Negotiation Done	The sum total number of neighbors in this state wherein the Master/ slave relationship has been negotiated, and sequence numbers have been exchanged, across all OSPF areas and interfaces.

Field	Description
Neighbor Exchange Done	The sum total number of neighbors in this state (i.e. in an adjacency's final state) having transmitted a full sequence of Database Description packets, across all OSPF areas and interfaces.
Neighbor Bad Link State Request	The sum total number of Link State Requests that have been received for a link state advertisement that is not contained in the database across all interfaces and OSPF areas.
Neighbor Bad Sequence	The sum total number of Database Description packets which have been received that either • has an unexpected DD sequence number • unexpectedly has the init bit set • has an options field differing from the last Options field received in a Database Description packet. Any of these conditions indicate that some error has occurred during adjacency establishment for all OSPF areas and interfaces.
Neighbor Loading Done	The sum total number of link state updates received for all out-of-date portions of the database across all OSPF areas and interfaces.
Neighbor Hello 1 way	The sum total number of Hello packets received from neighbors, in which this router is not mentioned across all OSPF interfaces and areas.
Neighbor Reset Adjacency	The sum total number of times the Neighbor adjacency has been reset across all OPSF areas and interfaces.
Neighbor Down	The total number of Neighboring routers down (i.e. in the initial state of a neighbor conversation) across all OSPF areas and interfaces.
Neighbor Sum Hello Packets Received	The sum total number of Hello packets received from neighbors, in which this router is mentioned across all OSPF interfaces and areas.
Interface Hello In	The sum total number of Hello packets sent on all interfaces and areas.
Interface Down	The sum total number of interfaces down in all OSPF areas.
Interface Not Connected	The sum total of interfaces no longer connected to the attached network across all OSPF areas and interfaces.
Interface Connected	The sum total number of interfaces, connected to the attached network in all OSPF areas.
Interface Wait Timer Fired	The sum total number of times the Wait Timer has been fired, (indicating the end of the waiting period that is required before electing a (Backup) Designated Router) across all OSPF areas and interfaces.
Interface Backup Routers	The sum total number of Backup Designated Routers on the attached network for all OSPF areas and interfaces.
Interface Bidirectional Changes	The sum total number of changes in the set of bidirectional neighbors associated with any interface across all OSPF areas.

Field	Description
Hello Timer Fired	The sum total number of times the Hello timer has been fired (which triggers the send of a Hello packet) across all OPSF areas and interfaces.
Retransmit Timer Fired	The sum total number of times the Retransmit timer has been fired across all OPSF areas and interfaces.
Link State Lock Timer Fired	The sum total number of times the LSA Lock timer has been fired across all OSPF areas and interfaces.
Link State Ack Timer Fired	The sum total number of times the LSA Ack timer has been fired across all ospf areas and interfaces.
Dbage Fired	The total number of times the Dbage has been fired.
Summary Timer Fired	The total number of times the Summary timer has been fired.
ASE Export Timer Fired	The total number of times the (Autonomous System External route) ASE Export timer has been fired.

Monitoring OSPF: Stats 2

Field	Description
Start Time	The time when OSPF has been started.
Up Time	The time since OSPF has been started.
Supported Types	The Link State Types that are supported.
Interfaces for Router	The number of interfaces for this router.
Virtual Links for Router	The number of virtual links for this router.
Total Neighbors	The total number of OSPF neighbors.
Neighbors in Initial State	The number of neighbors in the initial state of exchange.
Neighbors in Exchange State	The number of neighbors in the exchange state.
Neighbors in Full State	The number of neighbors in the initial state of exchange.
Areas	The total number of areas.
Transit Areas	The total number of transit areas.
NSSA Areas	The total number of NSSA areas.

Monitoring OSPF: Area Information

Field	Description
Index	The OSPF area number for which the OSPF info table is related.
Area IP address	The IP address associated with the OSPF area.
Interfaces	The total number of interfaces for this OSPF area.
Interfaces Up	The total number of interfaces that are UP in this area.
Link State Database Entries	The number of Link State Database entries for this OSPF area.

Monitoring OSPF: Interface Information

Field	Description
Index	The OSPF interface number for which the OSPF info table is related.
Interface IP address	The IP interface of the OSPF area.
Designated Router	The OSPF Designated Router ID (IP Address) for this OSPF interface.
Backup Designated Router	The OSPF Backup Designated Router ID (IP Address) for this OSPF interface.
Wait Interval	The OSPF Wait interval for this OSPF interface.
Total Neighbors	The Total number of neighbors for this OSPF interface.

Monitoring OSPF: Link-State DB

Field	Description
Area of Link-state Advertisement	The 32 bit identifier of the Area from which the Link-state Advertisement was received.
Type	The type of the link state advertisement. Each link state type has a separate advertisement format.
Link-state ID	The Link State ID is an LS Type Specific field containing either a Router ID or an IP Address; it identifies the piece of the routing domain that is being described by the advertisement.
Originating Router	The 32 bit number that uniquely identifies the originating router in the Autonomous System.
Sequence	The sequence number field is a signed 32-bit integer. It is used to detect old and duplicate link state advertisements. The space of sequence numbers is linearly ordered. The larger the sequence number the more recent the advertisement.
Age	This field is the age of the link state advertisement in seconds.
Checksum	This field is the checksum of the complete contents of the advertisement, excepting the age field. The age field is excepted so that an advertisement's age can be incremented without updating the checksum. The checksum used is the same that is used for ISO connectionless datagrams; it is commonly referred to as the Fletcher checksum.
Advertisement	The entire Link State Advertisement, including its header.

Monitoring OSPF: External Link-State DB

Field	Description
Type	The type of the link state advertisement. Each link state type has a separate advertisement format.
ID	The Link State ID is an LS Type Specific field containing either a Router ID or an IP Address; it identifies the piece of the routing domain that is being described by the advertisement.
Router	The 32 bit number that uniquely identifies the originating router in the Autonomous System.
Sequence	The sequence number field is a signed 32-bit integer. It is used to detect old and duplicate link state advertisements. The space of sequence numbers is linearly ordered. The larger the sequence number, the more recent the advertisement.
Age	This field is the age of the link state advertisement in seconds.
Checksum	This field is the checksum of the complete contents of the advertisement, excepting the age field. The age field is excepted so that an advertisement's age can be incremented without updating the checksum. The checksum used is the same that is used for ISO connectionless datagrams; it is commonly referred to as the Fletcher checksum.
Advertisement	The entire Link State Advertisement, including its header.

Monitoring OSPF: Area Receive Error Statistics on Alteon Application Switches

Field	Description
Index	The index of the OSPF Area for which these statistics apply.
Wrong Password	The total number of packets received with a wrong password in this area.
Wrong NetMask	The total number of packets received with a wrong netmask in this area.
Wrong Hello Interval	The total number of packets received with a different hello interval in this area.
Dead Interval	The total number of packets received with a different dead interval in this area.
Options	The total number of packets received with a different options in this area.
Unknown Neighbor	The total number of packets received from an unknown neighbor in this area.

Monitoring OSPF: Area Interface Receive Error Statistics on Alteon Application Switches

Field	Description
Index	The index of the OSPF Intf for which these statistics apply.
Wrong Password	The total number of packets received with a wrong password in this area.
Wrong NetMask	The total number of packets received with a wrong netmask in this area.
Wrong Hello Interval	The total number of packets received with a different hello interval in this area.
Dead Interval	The total number of packets received with a different dead interval in this area.
Options	The total number of packets received with a different options in this area.
Unknown Neighbor	The total number of packets received from an unknown neighbor in this area.

Monitoring OSPF: Neighbor Interface

Field	Description
Interface	Displays the OSPF interface number.
Neighbor	Displays the OSPF neighbor identifier.
Priority	Displays the OSPF neighbor's priority.
State	Displays the state of the OSPF neighbor.
Designated Router	IP address of the designated router.
Backup Router	IP address of the backup router.
IP Address	IP address of the interface.

Note: This feature is applicable only on Alteon Application Switches and on ALO 1.0 and higher.

Monitoring BGP

The following topics are covered in this area:

- Monitoring BGP: Administration on Alteon Application Switches
- Monitoring BGP: Peers Summary on Alteon Application Switches

Monitoring BGP: Administration on Alteon Application Switches

This window simply displays whether or not Border Gateway Protocol (BGP) is turned on or off at the Web Switch. You can configure the BGP administrative status of the switch via the **Configure > Routing > BGP > Administration** menu.

Monitoring BGP: Peers Summary on Alteon Application Switches

Field	Description
Peer	The BGP Identifier of this entry's BGP peer.
State	The BGP peer connection state.
Version	The negotiated version of BGP running between the two peers.
Local Address	The local IP address of this entry's BGP connection.
Local Port	The local port for the TCP connection between the BGP peers.
Remote Address	The remote IP address of this entry's BGP peer.
Remote Port	The remote port for the TCP connection between the BGP peers. Note that the objects *bgpPeerLocalAddr*, *bgpPeerLocalPort*, *bgpPeerRemoteAddr* and *bgpPeerRemotePort* provide the appropriate reference to the standard MIB TCP connection table.
Remote Autonomous System	The remote autonomous system number.
Received Updates	The number of BGP UPDATE messages received on this connection. This object should be initialized to zero (0) when the connection is established.
Sent Updates	The number of BGP UPDATE messages transmitted on this connection. This object should be initialized to zero (0) when the connection is established.
Received Messages	The total number of messages received from the remote peer on this connection. This object should be initialized to zero when the connection is established.
Sent Messages	The total number of messages transmitted to the remote peer on this connection. This object should be initialized to zero when the connection is established.
Last Error	The last error code and subcode seen by this peer on this connection. If no error has occurred, this field is zero. Otherwise, the first byte of this two byte OCTET STRING contains the error code, and the second byte contains the subcode.
FSM Established	The total number of times the BGP FSM transitioned into the established state.
Established Time	This timer indicates how long (in seconds) this peer has been in the Established state or how long since this peer was last in the Established state. It is set to zero when a new peer is configured or the router is booted.
Hold Time	Time interval in seconds for the Hold Timer established with the peer.

Field	Description
Keep Alive	Time interval in seconds for the KeepAlive timer established with the peer.
Time Since Last Update	Elapsed time in seconds since the last BGP UPDATE message was received from the peer. Each time *bgpPeerInUpdates* is incremented, the value of this object is set to zero (0).

Monitoring Layer 4

The following switch monitoring topics are covered in this section:

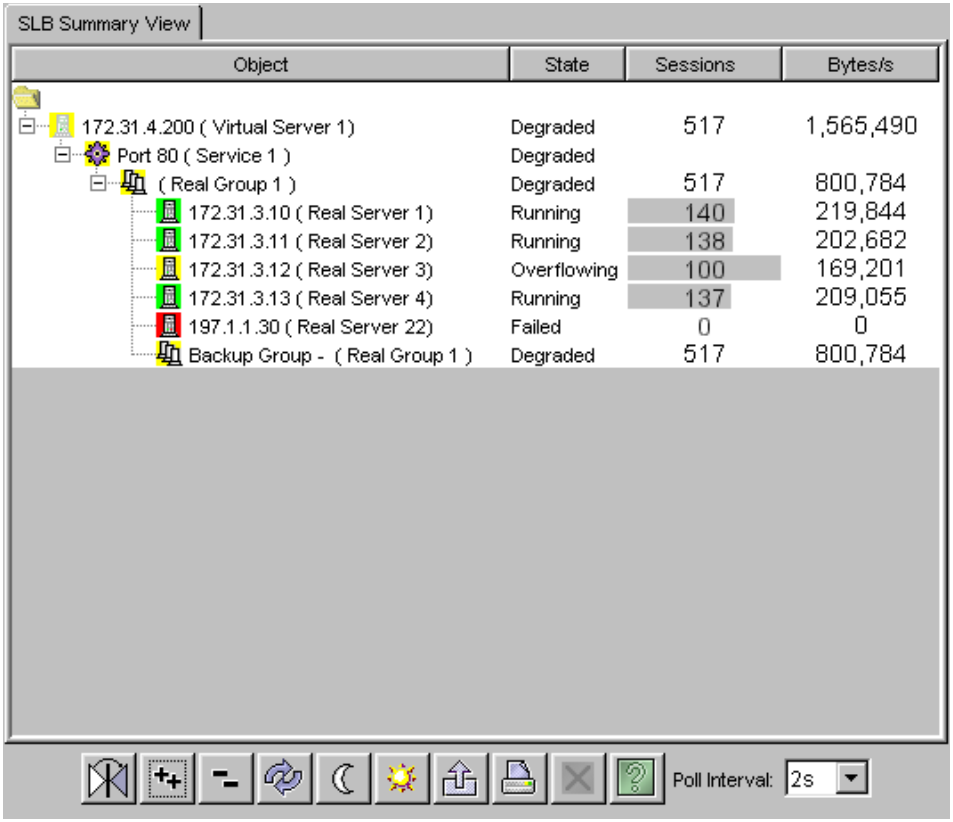
- SLB Summary View
- Monitoring Layer 4 Filters: Statistics
- Monitoring Layer 4 Filters: Rate Limit
- Monitoring Layer 4 Filters: SP Filters on Alteon Application Switches
- Monitoring Layer 4 SLB: Real Servers
- Monitoring Layer 4 SLB: Real Servers by SP
- Monitoring Layer 4 SLB: Groups
- Monitoring Layer 4 SLB: Virtual Servers
- Monitoring Layer 4 SLB: Real Servers State
- Monitoring Layer 4 SLB: FTP on Alteon 180 or AD series
- Monitoring Layer 4 SLB: FTP on Alteon Application Switches
- Monitoring Layer 4 SLB: DNS on Alteon 180/AD series
- Monitoring Layer 4 SLB: DNS on Alteon Application Switches
- Monitoring Layer 4 SLB: Stats on Alteon 180 or AD series
- Monitoring Layer 4 SLB: Stats on Alteon Application Switches
- Monitoring Layer 4 SLB: SP Maintenance on Alteon Application Switches
- Monitoring Layer 4 SLB: SSL Statistics on Alteon Application Switches
- Monitoring Layer 4 SLB: Virtual Server Service Status on Alteon Application Switches
- Monitoring Layer 4 SLB: Virtual Server Service Statistics
- Monitoring Layer 4 SLB: The Auxiliary Session Statistics on Alteon Application Switches
- Monitoring Layer 4 SLB: The Auxiliary Session SP Statistics on Alteon Application Switches
- Monitoring Layer 4 SLB: Sessions
- Monitoring Layer 4 SLB: Formatted Sessions
- Monitoring Layer 4 SLB: Session Filter Criteria
- Monitoring Layer 4: Global SLB: General
- Monitoring Layer 4: Global SLB: Remote Real Servers on Alteon Application Switches

- Monitoring Layer 4: Global SLB: Real Server Groups on Alteon Application Switches
- Monitoring Layer 4: Global SLB: Virtual Servers on Alteon Application Switches
- Monitoring Layer 4: Global SLB: Remote Sites on Alteon Application Switches
- Monitoring Layer 4: Global SLB: Remote Real Servers Information on Alteon Application Switches
- Monitoring Layer 4: Global SLB: Virtual Server Information on Alteon Application Switches
- Monitoring Layer 4: Global SLB: Remote Site Information on Alteon Application Switches
- Monitoring Layer 4: Global SLB: Networks on Alteon Application Switches
- Monitoring Layer 4: Global SLB: Rules on Alteon Application Switches
- Monitoring Layer 4: Global SLB: Geographical Regions on Alteon Application Switches
- Monitoring Layer 4: RTSP on Alteon 180 or AD series
- Monitoring Layer 4: RTSP on Alteon Application Switches
- Monitoring Layer 4 WAP: Add Sessions on Alteon 180 or AD series
- Monitoring Layer 4 WAP: Add Sessions on Alteon Application Switches
- Monitoring Layer 4: WAP: Delete Sessions on Alteon 180 or AD series
- Monitoring Layer 4: WAP: Delete Sessions on Alteon Application Switches
- Monitoring Layer 4: WAP: RADIUS Accounting on Alteon 180 or AD series
- Monitoring Layer 4: WAP: RADIUS Accounting on Alteon Application Switches
- Monitoring Layer 4: Remote URL Buffers
- Monitoring Layer 4: Remote URL Errors
- Monitoring Layer 4: Remote URL Maintenance
- Monitor: Layer 4: Remote URL Miscellaneous
- Monitor: Layer 4: Remote URL Sessions
- Monitoring Layer 4: Remote URL Tables
-

SLB Summary View

This window provides a summary view of the real servers, virtual servers, and real server groups that have been configured on the switch for server load balancing.

You can expand the tree to view the state of each service and server at a glance. The state of each node is indicated by color: green (good), yellow (degraded), and red (failed). For a description and meaning of these colors, see the field `State` in the following table.





The **Invert** button lets you reverse the hierarchy of the view so that you can view the SLB summary in terms of the configured real servers, or in terms of the configured virtual servers.



The **Expand All** button expands the entire tree to show the real servers, services, and groups.



The **Collapse All** button collapses the entire tree to show only the root nodes. You can use the Invert button to toggle between the Virtual Server nodes and the Real Server nodes.



The **Pause** button allows you to stop the switch from polling the statistics.



The **Resume** button allows the switch to resume polling the statistics.

Field	Description
Object	The SLB object; a virtual server, a real server, the Service port (and index number), the Real Group, the Backup Group.
State	The state of the object: Running, Failed, Blocked, Degraded, and Overflowing. These states are represented by different colors. See Different States of the Object to understand the meaning of each state of the object.
Current Sessions	The number of current sessions that are being processed on the object.
Bytes/s	The number of bytes per second being processed on the object.

Different States of the Object

Field	Description
Real servers	**Running** (Green): This means that the real server is up and running. **Failed** (Red): This means that the real server is down. **Blocked** (Blue): This means that some of the services on this real server are down. **Degraded** (Yellow): This means that the real server group or a virtual server is up but it is overflowing and cannot receive any more traffic. **Overflowing** (Yellow): This means that the real server is up but it has exceeded the limit of the maximum connections. If it has a back up server, the excess trafific will be diverted to that server.
Real Server Groups	**Running** (Green): This means that all the servers are running. **Degraded** (Yellow): This means that one or more than one of the real servers in the group are not working. **Failed** (Red): This means that none of the real servers in the group are working.
Virtual Services	These objects behave the same way as the real server groups do.
Virtual Servers	**Unknown** (Faded Grey): This means that no information about this virtual server is available as yet. **Degraded** (Yellow): This means that some of the services are down. **Failed** (red): This means that none of the Virtual Servers are up

Monitoring Layer 4 Filters: Statistics

Field	Description
Filter	The index number of the filters. In some versions of Web OS, this field may appear as Index, but the meaning is the same.
Name	The name of the filter.
Filter Matches	The number of received packets that matched the filter rule.

Monitoring Layer 4 Filters: Rate Limit

Alteon OS allows you to detect and block certain kinds of protocol-based attacks. These attacks can flood servers with enough traffic to severely affect their performance or bring them down altogether. Protocol-based rate limiting is implemented via filters. Alteon OS currently supports rate limiting on TCP, UDP and ICMP protocols. Each filter is configured with one of the above protocols, and then rate limiting is enabled or disabled in the Filtering Advanced menu.

This tab is used to monitor the rate limiting feature. Each field is displayed in absolute values.

Field	Description
TCP Client Hold Downs	The total number of TCP client hold downs that occurred since the last stats clear. The switch monitors the number of new TCP connections. When the number of new connections or packets exceeds the configured limit, any new TCP connection requests from the client are blocked. When blocking occurs, the client is said to be held down. The client is held down for a specified number of minutes, after which new TCP connection requests from the client are allowed once again to pass through.
TCP Rate Limiting Per-Client State	The current number of TCP client hold down, as recorded in the session table.
UDP Client Hold Downs [1]	The total number of UDP client hold downs that occurred since the last stats clear. The switch monitors the number of new UDP packets received. When the number of packets exceeds the configured limit, any new UDP packets from the client are blocked. When blocking occurs, the client is said to be held down. The client is held down for a specified number of minutes, after which new packets from the client are allowed once again to pass through.
UDP Rate Limiting Per-Client State [1]	UDP Rate limiting per client state. The switch counts all received packets from a client and compares against the configured maximum threshold. When the maximum configured threshold has been reached before the time window expires, the switch will drop until the configured hold-down period expires.

Field	Description
ICMP Client Hold Downs [1]	The total number of ICMP client hold downs that occurred since the last stats clear. The switch monitors the number of new ICMP packets received. When the number of new packets exceeds the configured limit, any new ICMP packets from the client are blocked. When blocking occurs, the client is said to be held down. The client is held down for a specified number of minutes, after which new packets from the client are allowed once again to pass through.
ICMP Rate Limiting Per-Client State [1]	ICMP Rate limiting per client state. The switch counts all received packets from a client and compares against the configured maximum threshold. When the maximum configured threshold has been reached before the time window expires, the switch will drop until the configured hold-down period expires.

1. This is applicable only on Alteon Application Switches, and on ALO 1.0 and higher.

Monitoring Layer 4 Filters: SP Filters on Alteon Application Switches

This tab allows you to monitor filter firings on a per-Switch Processor (SP) basis.

Filtering the view

If you wish to create a filtered view of the SPs and filters in this screen, use the drop-down combo boxes on the bottom right. The drop-down combo boxes allow you to filter data in the first and second table columns, respectively.

The default view for this screen is filtered based on the first entry that appears in each of the drop-down combo boxes. To view all data (unfiltered), select **any** in the first combo box, and **any** in the second combo box.

Field	Description
SP	The index number of the switch processor (SP), 1-4.
Filter	The filter number.
Firings	The number of instances that the received packet matches the filter rule on this switch processor.

Monitoring Layer 4 SLB: Real Servers



Clear button allows you to delete the session table.

Field	Description
Real Server	The index number that identifies the real server.
Real Server Name	The name of the real server.
Current Sessions	The number of sessions currently handled by the real server.
Total Sessions	The total number of sessions handled by the real server.
Highest Sessions	The highest number of sessions handled by the real server.
Failures	The total number of times the real server was claimed down.
Bytes	The total bytes received and transmitted through the real server.

Monitoring Layer 4 SLB: Real Servers by SP

This tab allows you to monitor real servers' concurrent sessions according to the switch processor (SP) to which the real server is assigned. This information is useful for understanding how traffic is balancing amongst the real servers.

Filtering the view

If you wish to create a filtered view of the SPs and real servers in this screen, use the drop-down combo boxes on the bottom right. The drop-down combo boxes allow you to filter data in the first and second table columns, respectively.

The default view for this screen is filtered based on the first entry that appears in each of the drop-down combo boxes. To view all data (unfiltered), select **any** in the first combo box, and **any** in the second combo box.

Right-Clicking for Operational Commands on Real Server Ports

You can right-click to operationally clear port sessions in the Real Server Ports window. The setting will remain in effect until the next reset of the switch. To configure the setting, right-click on the a real server index field, and select the desired command.



Clear button allows you to delete the session table.

Field	Description
SP	The index number that identifies the switch processor (SP). On the Alteon 180 or AD series platform, the SP number is the same as the physical port number.
Real Server	The index number that identifies the real server.
Current Sessions	The current number of sessions handled by the real server.
Total Sessions	The total number of sessions handled by the real server.
Bytes	The total bytes received and transmitted through a specific port of the real server.

Monitoring Layer 4 SLB: Groups

Field	Description
Group	The group number of the real server group. In some versions of Web OS, this field may appear as Index, but the meaning is the same.
Name	The name of the real server group.
Current Sessions	The number of sessions currently handled by the real server group.
Total Sessions	The total number of sessions handled by the real server group.
Highest Sessions	The highest number of sessions that were handled by the real server group.
Bytes	The total bytes received and transmitted through the real server group.

Monitoring Layer 4 SLB: Virtual Servers

Field	Description
VServer	The index number of the virtual server.
Current Sessions	The number of sessions that are currently handled by the virtual server.
Total Sessions	The total number of sessions that were handled by the virtual server.
Highest Sessions	The highest number of sessions that were handled by the virtual server.
Bytes	The total bytes that were received and transmitted through the virtual server.
HTTP Header Hits	The number of HTTP header hits.
HTTP Header Misses	The number of HTTP header misses.
HTTP Header Sessions	The number of HTTP header sessions.
Cookie Rewrites	The number of cookie rewrites.
Cookie Inserts	The number of cookie inserts.
Bytes	The total bytes received and transmitted through the virtual server.

Monitoring Layer 4 SLB: Real Servers State

Field	Description
Real Server	The index number of the real server.
Real Server Name	The name of the real server.
IP Address	The IP address of the real server.
Server State	The state of the real server: running, failed, or disabled.
Overflow State	The overflow state of the real server: overflow or no-overflow.
Switch Port	The switch port through which the real server is connected.
Health Check Layer	The OSI layer where the health of the real server is checked: layer3, or layer4.
MAC Address	The MAC address of the real server.
VLAN	The VLAN number assigned to the real server. This field is displayed on Alteon Application Switches running Alteon OS 21.0 and higher.

Monitoring Layer 4 SLB: FTP on Alteon 180 or AD series

Field	Description
FTP Control Sessions for SLB	The number of times the switch receives both active and passive FTP connections.
FTP Control Sessions for NAT	The number of times the switch receives the 'port' command from the client.

Monitoring Layer 4 SLB: FTP on Alteon Application Switches

Field	Description
FTP Control Sessions for SLB	The number of times the switch receives both active and passive FTP connections.
FTP Control Sessions for NAT	The number of times the switch receives the 'port' command from the client.
Create New Index Due to Port	The number of times the switch creates a new index due to 'port' command from the client.
Difference between ACK and SEQ for Packet Adjustment	The difference in the numbers of ACK and SEQ that the switch needs for packet adjustment.
Create New Index Due to PASV	The number of times the switch creates a new index in response to the 'pasv' command from the client.
Difference between ACK and SEQ	The difference in the numbers of ACK and SEQ that the switch needs for FTP SLB parsing.
Unable to Switch Between Active and Passive	The number of times the switch is not able to switch modes from active to passive and vice versa.

Monitoring Layer 4 SLB: DNS on Alteon 180/AD series

Field	Description
Good DNS Requests	The total number of well-formed DNS requests.
Bad DNS Requests	The total number of ill-formed DNS requests.
TCP Queries	Total number of TCP DNS queries.
UDP Queries	The total number of UDP DNS queries.
Invalid Queries	The total number of invalid DNS queries.
Multiple Queries	The total number of multiple DNS queries.
Parse Errors	The total number of domain name parse errors.
Failed Matches	The total number of failed real server name matches.
Internal Errors	The total number of DNS parsing internal errors.

Monitoring Layer 4 SLB: DNS on Alteon Application Switches

Field	Description
Good DNS Requests	The total number of well-formed DNS requests.
Bad DNS Requests	The total number of ill-formed DNS requests.
DNS Responses Sent	The total number of DNS responses that have been sent.
TCP Queries	Total number of TCP DNS queries.
UDP Queries	The total number of UDP DNS queries.
Invalid Queries	The total number of invalid DNS queries.
Multiple Queries	The total number of multiple DNS queries.
Parse Errors	The total number of domain name parse errors.
Failed Matches	The total number of failed real server name matches.
Internal Errors	The total number of DNS parsing internal errors.

Monitoring Layer 4 SLB: Stats on Alteon 180 or AD series

Field	Description
Backup Servers Become Active Primary Server Failed	The total number of backup servers that were activated when the primary servers failed.
Backup Servers Become Active Primary Server Overflowed	The total number of times the backup servers became active when the primary servers overflowed.
Incorrect Virtual Servers Specified	The total number of incorrectly specified virtual servers for server load balancing.
Incorrect Virtual Ports Specified	The total number of incorrectly specified virtual ports for server load balancing.
Incorrect Virtual Servers Specified	The total number of incorrectly specified virtual servers for server load balancing.
Incorrect Virtual Ports Specified	The total number of incorrectly specified virtual ports for server load balancing.
No Available Real Servers	No real servers are specified for server load balancing.

Monitoring Layer 4 SLB: Stats on Alteon Application Switches

Field	Description
Backup Servers Become Active Primary Server Failed	The total number of backup servers that were activated when the primary servers failed.
Backup Servers Become Active Primary Server Overflowed	The total number of times the backup servers became active when the primary servers overflowed.
Incorrect Virtual Servers Specified	The total number of incorrectly specified virtual servers for server load balancing.
Incorrect Virtual Ports Specified	The total number of incorrectly specified virtual ports for server load balancing.
No Available Real Servers	No real servers are specified for server load balancing.
Maximum Sessions	The maximum number of simultaneous sessions supported.
Current Sessions (1 Second Avg.)	The number of session bindings currently in use.
Current Sessions (4 Second Avg.)	The 4 second average of the current number of bindings on the port.
Current Sessions (64 Second Avg.)	The 64 second average of the current number of bindings on the port.
Closed Session due to Server Failed	The count of the number of sessions closed because the server failed.
Bindings Failures	The total number of Binding failures on the port. A Binding Failure occurs when a port runs out of binding table entries.
Non TCP/IP Frames Dropped	The total number of non-TCP/IP frames dropped on the port.
TCP Fragments Dropped	Indicates the number of TCP fragments that were dropped on the port.
UDP Datagrams Dropped	Indicates the number of UDP datagrams that were dropped on the port.
Frames Denied	The total number of frames that are denied on the port by the filter.

Field	Description
Attack Frames	The total number of attacks in which frames contain the same source and destination IP addresses.
Fragment Sessions	The total number of fragment sessions processed.
IP Fragment Sessions	The number of sessions in the IP fragment binding table.
Fragments Discarded	The total number of fragments discarded on the SP because there is no entry in the IP fragment binding table.
IP Fragment Table Full	The total number times IP fragment binding table became full on the SP.

Monitoring Layer 4 SLB: SP Maintenance on Alteon Application Switches

This tab is used to monitor any switch processor (SP) information related to server load balancing.



You may choose to clear any non-operational SLB statistics (resetting them to zero) by clicking on the **Clear SLB Non-Operational Statistics Per SP** button. This command is also available from the right-click pop-up menu. This command does not reset the switch and does not affect the following counters:

- Counters required for Layer 4 and Layer 7 operation (such as current real server sessions).
- All related SNMP counters.

Field	Description
SP	The switch processor (SP) number for which the statistics apply.
	The SP numbers correspond to the physical ports as follows: **Alteon 2224** • SP1: Ports 1-12 and 25 • SP2: Ports 13-24 • SP3: Port 26 • SP4: not used **Alteon 2424** • SP1: Ports 1-12 and 25 • SP2: Ports 13-24 and 27 • SP3: Port 26 • SP4: Port 28 **Alteon 2208** • SP1: Ports 1-8 • SP2: Ports 9 and 10 • SP3: Not used • SP4: Not used **Alteon 2216** • SP1: Ports 1-8 and 17 • SP2: Ports 9-16 and 18 • SP3: Not used • SP4: Not used **Alteon 3408** • SP1: Ports 1, 5, and 9 • SP2: Ports 2, 6, and 10 • SP3: Ports 3, 7, and 11 • SP4: Ports 4, 8, and 12
Maximum per Session Table	The maximum number of entries per SP in the session table.
Current Sessions (1 Second Avg.)	The current number of sessions on the SP.
Current Sessions (4 Second Avg.)	The 4 second average current number of sessions on the SP.
Current Sessions (64 Second Avg.)	The 64 second average current number of sessions on the SP.

Field	Description
Binding Failures	The total number of binding failures on the SP. A binding failure occurs when a SP runs out of session table entries.
Non-TCP/IP Drops	The total number of non-TCP/IP frames dropped on the SP.
UDP Datagram Drops	The total number of UDP datagrams dropped on the SP.
Incorrect VIP Drops	The total number of frames with incorrect VIPs that are dropped on the SP.
Incorrect Virtual Port Drops	The total number of frames with incorrect Virtual Port that are dropped on the SP.
Real Server Unavailable Drops	The total number of frames that are dropped on the SP because no real server is available.
Filter Denied Frames	The total number of frames that are denied on the SP by the filter.
Sessions Closed/Server Failed	The count of the number of sessions closed because the server failed.
Attacks	The total number of attacks that frames contain the same source and destination IP addresses.
Fragment Sessions Processed	The total number of fragment sessions processed on the SP.
IP Fragment Sessions	The number of sessions in the IP fragment binding table on the SP.
IP Fragments Discarded	The total number of fragments discarded on the SP because there is no entry in the IP fragment binding table.
IP Fragment Table Full	The total number of times IP fragment binding table is full on the SP.

Monitoring Layer 4 SLB: SSL Statistics on Alteon Application Switches

Field	Description
Session ID Allocation Fails	The number of times allocation of a session table entry failed when attempting to store a *SessionId* in the table.
SSL Connections	The current number of different TCP sessions using SSL service.
Total Sessions	The total number of different TCP sessions using SSL service.
Highest Sessions	The high water mark of current sessions of different TCP sessions using SSL service.
Current Unique Sessions	The current number of unique SSL sessions seen on the switch.
Total Unique Sessions	The total number of unique SSL sessions seen on the switch.
Highest Unique Sessions	The high water mark of unique SSL sessions seen on the switch.
Current Persistent Port Sessions	The current number of *SessionIds* maintained on SP 4, to allow for persistence across different client ports.
Total Persistent Port Sessions	The total number of SessionIds maintained on SP 4, to allow for persistence across different client ports.
Highest Persistent Port Sessions	The high water mask of SessionIds maintained on SP 4, to allow for persistence across different client ports.

Note: The Alteon Application switches 2208 and 2216 do not support SP3 and SP4.

Monitoring Layer 4 SLB: Virtual Server Service Status on Alteon Application Switches

Note: This tab is available on switches running Alteon OS 20.1.1.0 and higher.

Field	Description
Virtual Server	Displays the virtual server number that identifies the virtual server.
Services	Displays the services running on the virtual server.
Real Server	Displays the real server number.
Virtual Port	Displays the number of the Virtual Port.
Real Port	Displays the real server TCP or UDP port assigned to this service. By default, this is the same as the virtual port (service virtual port).
State	Displays the state of the service on the virtual server.
Health Check Response Time [1]	Health check response time for the virtual server for this virtual service.
Real Server Weight [1]	Displays the real server weight.

1. This is applicable only on Alteon Application Switches and on ALO 1.0 and higher.

Monitoring Layer 4 SLB: Virtual Server Service Statistics

Note: You need to enable this field by going to: Configure -> Switch ->Layer 4 -> SLB ->General -> Virtual Server Service Statistics (Configuring General Server Load Balancing) for this tab to appear.

Field	Description
Virtual Server	The virtual server index.
Virtual Service	The virtual service number that identifies the service.
Real Server	The real server index.
Current Sessions	The number of sessions that are currently handled by the virtual service.
Total Sessions	The total number of sessions that are handled by the virtual service.
Highest Sessions	The highest sessions that have been handled by the virtual service.
Total Octets	Total octets received and transmitted out of the virtual service.

Note: This is applicable on Alteon Application Switches and Alteon OS 20.0 through 21.x.

Monitoring Layer 4 SLB: The Auxiliary Session Statistics on Alteon Application Switches

Note: This tab is available on switches running Alteon OS 20.x and higher.

Field	Description
Session Table	Displays the session table number.
Current Connections	Displays the number of current sessions for the session table.
Maximum Connections	Displays the maximum number of simultaneous sessions supported for the session table.
Allocation Failures	Displays the number of sessions that were not allocated to the session table.

Monitoring Layer 4 SLB: The Auxiliary Session SP Statistics on Alteon Application Switches

Note: This tab is available on switches running Alteon OS 20.x and higher.

Field	Description
SP	Displays the index number that identifies the Switch Processor (SP).
Session	Displays the session table number.
Current Connections	Displays the number of current sessions for the session table.
Maximum Connections	Displays the maximum number of simultaneous sessions supported for the session table.
Allocation Failures	Displays the number of sessions that did not get allocated to the session table.

Monitoring Layer 4 SLB: Sessions

Note: This feature is available on Alteon OS 22.0.1.0 and higher.

Field	Description
SP	This field indicates the Switch Port number that created the session.
Port	The ingress port.
Source IP	The client's source IP address.
Destination IP	The destination IP address.
Virtual IP	The virtual server IP address.
Real IP	Displays all session entries with real server IP address. For load balancing, this field contains the IP address of the real server that the switch selects to forward client packet to. If the switch does not find live server, this field is the same as destination IP address. For example: 3,01: 1.1.1.1 1040, 2.2.2.1 http -> 3.3.3.1 http age 10 3,01: 1.1.1.1 6970, 2.2.2.1 rtsp -> 2.2.2.1 21220 age 10 P For filtering, this field also shows the real server IP address. No address is shown if the filter action is Allow, Deny or NAT. It will show ALLOW, DENY or NAT instead. For example: 3,01: 1.1.1.1 1040, 2.2.2.1 http -> 3.3.3.1 http age 10 f:11 2,07: 1.1.1.1 1706, 2.2.2.1 http-> 192.168.4.10 linklb age 8 f:10 E
Proxy IP	The proxy IP address.
Server IP	The destination IP address.
Sequence	The packet sequence.
Source Port	The source (client) port.
Destination Port	The destination port.
PIP/DAM Port	This field identifies the TCP/UDP source port substituted by the switch.The switch does this substitution when Direct Access Mode is enabled or proxy is enabled.
Filter	This field indicates the session created by the filtering code as a result of the IP header keys matching the filtering criteria.
Protocol	Displays the protocol number.
L4 Protocol	Displays the Layer 4 protocol number.
Real Protocol	Displays the real server protocol number.

Field	Description
Age	This field indicates the session created by filtering code as a result of the IP header keys matching the filtering criteria. For example, age = 10. This means that the session will age out in 10 minutes.
Is Slowage?	This field displays slowage configuration.
E	Indicates the session is in use and will be aged out if no traffic is received within session timeout value.
L	Indicates the session is a link load balance session.
N	Indicates the session only translates the destination MAC when forwarding client traffic to the real server.
P	Indicates the session is a persistent session and will not age out.
S	Indicates the session is a persistent session and the application is either SSL session ID, or cookie persistent bind.
T	Indicates the session is TCP rate limiting for every client entry.
Ru	Indicates the session is UDP rate limiting for every client entry.
Ri	Indicates the session is ICMP rate limiting for every client entry.
Vr	Indicates the session is a SIP REGISTER session.
Vs	Indicates the session is a SIP SUBSCRIBE session.
Vi	Indicates the session is a SIP INVITE session.
Vm	Indicates the session is a SIP MESSAGE session.
U	Indicates the session is Layer 7 delayed binding and the switch is trying to open TCP connection to the real server.
W	Indicates the session only translates the destination MAC when forwarding Layer 7 WCR traffic to the real server.
Deny?	Indicates the session created by `Deny` filter.
NAT?	Indicates the session created by `NAT` filter.
WCR?	Indicates the session created by `WCR` filter.
FTP?	Indicates the session created by `FTP` filter.
Allow?	Indicates the session created by `Allow` filter.

Monitoring Layer 4 SLB: Formatted Sessions

Note: This feature is available only on Alteon OS 22.0 and higher.

Field	Description
Info	Displays all session entries. Information similar to the following may appear in a formatted session table: 3, 01: 1.1.1.1 4586, 2.2.2.1 http -> 1.1.1.2 3567 3.3.3.1 http age 6 f:10 EUSPT c (1) (2) (3) (4) (5) (6) (7a) (7) (8) (9) (10) (11) (12) (13) **Note:** The fields 1 to 13 associated with a session as identified in the above example, are described in Session Dump Information in Alteon OS.

Session Dump Information in Alteon OS

Field	Description
(1) SP number	This field indicates the Switch Port number that created the session.
(2) Ingress port	This field shows the physical port through which the client traffic enters the switch.
(3) Source IP address	This field contains the source IP address from the client's IP packet.
(4) Source port	This field identifies the source port from the client's TCP/UDP packet.
(5) Destination IP address	This field identifies the destination IP address from the client's TCP/UDP packet.
(6) Destination port	This field identifies the destination port from client's TCP/UDP packet.
(7a) Proxy IP address	This field contains the Proxy IP address substituted by the switch. This field contains the real server IP address of the corresponding server that the switch selects to forward the client packet to, for load balancing. If the switch does not find a live server, this field contains the sameinformation as the destination IP address mentioned in field (5). This field also shows the real server IP address for filtering. No address is shown if the filter action is Allow, Deny or NAT. It will show "ALLOW", "DENY" or "NAT" instead.

Field	Description
(7) Proxy Port	This field identifies the TCP/UDP source port substituted by the switch.
(8) Real Server IP Address	For load balancing, this field contains the IP address of the real server that the switch selects to forward client packet to. If the switch does not find live server, this field is the same as destination IP address (as in row 5). For example: 3,01: 1.1.1.1 1040, 2.2.2.1 http -> 3.3.3.1 http age 10 3,01: 1.1.1.1 6970, 2.2.2.1 rtsp -> 2.2.2.1 21220 age 10 P For filtering, this field also shows the real server IP address. No address is shown if the filter action is Allow, Deny or NAT. It will show ALLOW, DENY or NAT instead. For example: 3,01: 1.1.1.1 1040, 2.2.2.1 http -> 3.3.3.1 http age 10 f:11 2,07: 1.1.1.1 1706, 2.2.2.1 http-> 192.168.4.10 linklb age 8 f:10 E
(9) Server port	This field is the same as the destination port (field 6) for load balancing except for the RTSP UDP session. For RTSP UDP session, this server port is obtained from the client-server negotiation. This field is the filtering application port for filtering. It is for internal use only. This field can be `urlwcr`, `wcr`, `idslb`, `linkslb` or `nonat`.
(10) Age	This is the session timeout value. If no packet is received within the value specified, the session is freed.
(11) Filter number	This field indicates the session created by filtering code as a result of the IP header keys matching the filtering criteria.

Field	Description
(12) Flag	“E”: Indicates the session is in use and will be aged out if no traffic is received within session timeout value. “L”: Indicates the session is a link load balance session. “N”: Indicates the session only translates the destination MAC when forwarding client traffic to the real server. “P”: Indicates the session is a persistent session and is not to be aged out. Fields (6), (7) and (8) cannot have persistent session. “S”: Indicates the session is a persistent session and the application is SSL session ID, or Cookie `Pbind`. “T”: Indicates the session is TCP rate limiting for every client entry. “Ru”: Indicates the session is UDP rate limiting for every client entry. “Ri”: Indicates the session is ICMP rate limiting for every client entry. “Vr”: Indicates the session is a SIP REGISTER session. “Vs”: Indicates the session is a SIP SUBSCRIBE session. “Vi”: Indicates the session is a SIP INVITE session. “Vm”: Indicates the session is a SIP MESSAGE session. “U”: Indicates the session is Layer 7 delayed binding and the switch is trying to open TCP connection to the real server. “W”: Indicates the session only translates the destination MAC when forwarding layer 7 WCR traffic to the real server.
(13) Persistent session user count	This counter indicates the number of client sessions created to associate with this persistent session.

Monitoring Layer 4 SLB: Session Filter Criteria

Note: This feature is available only on Alteon OS 22.0 and higher.

Field	Description
Type	The type criteria to be used for the session filter. Choices are **all**, **cip**, **cport**, **dip**, **dport**, **pip**, **pport**, **filter**, **flag**, **port**, **real**. Default is **all**.
IP Address	The IP Address to use for the session filter criteria.
Filter ID	The filter ID number to use for the session filter criteria
Port	The port number for the session filter criteria.
Flag	The flag to use for the session filter criteria. Choices are **eFlag**, **lFlag**, **nFlag**, **pFlag**, **sFlag**, **tFlag**, **uFlag**, **wFlag**, **ruFlag**, **riFlag**, **viFlag**, **vrFlag**, **vsFlag**, **vmFlag**, **none**. Default is **none**.

Monitoring Layer 4 SLB: SIP

Note: This feature is available only on Alteon OS 22.0 and higher.

Field	Description
Client Parse Errors	The total number of errors encountered during client processing when parsing an incoming SIP packet.
Server Parse Errors	The total number of errors encountered during server processing when parsing an incoming SIP packet.
Unknown method Requests	Total number of packets received with methods not known to the SIP parser on the switch.
Incomplete Messages	Total number of packets received which do not have the complete SIP message in a single packet.

Monitoring Layer 4: Global SLB: General

Field	Description
Good Remote Site Updates	The number of good remote site updates received.
Bad Remote Site Updates	The number of bad remote site updates received.
Remote Site Updates Sent	The number of remote site updates sent.
DSSPv2 Good Remote Site Updates Received	The number of Distributed Site State Protocl version 2 (DSSPv2) good remote site updates received.
DSSPv2 Remote Site Updates Sent	The number of DSSPv2 remote site updates sent
DNS Queries Received	The number of DNS queries received.
Bad DNS Queries Received	The number of bad DNS queries received.
DNS Responses Sent	The number of DNS responses sent.
HTTP Request Received	The number of HTTP requests received.
Bad HTTP Requests Received	The number of bad HTTP requests received.
HTTP Responses Sent	The number of HTTP responses sent.
No Server Selected	The number of requests received with no server selected.
No Matching Domain	The number of requests received with no matching domain.

Monitoring Layer 4: Global SLB: Remote Real Servers on Alteon Application Switches

Field	Description
Remote Real Server	The index number of the remote real server.
Real Server Name	The name of the real server.
DNS Handoffs	The number of DNS handoffs.
HTTP Redirects	The number of HTTP redirects.

Monitoring Layer 4: Global SLB: Real Server Groups on Alteon Application Switches

Note: This feature is only available on Alteon OS 21.x and lower.

Field	Description
Real Server Group	The group number that identifies the real server group.
Name	The name of the real server group.
DNS Handoffs	The total number of DNS hand-offs sent to the remote real servers in the group.
HTTP Redirects	The total number of HTTP redirects sent to the remote real servers in the group.

Monitoring Layer 4: Global SLB: Virtual Servers on Alteon Application Switches

This tab allows you to monitor virtual servers in a Global Server Load Balancing configuration.

Filtering the view

If you wish to create a filtered view of the virtual servers in this screen use the drop-down combo boxes on the bottom right. The drop-down combo boxes allow you to filter data in the first, second, and third table columns, respectively.

The default view for this screen is filtered based on the first entry that appears in each of the drop-down combo boxes. To view all data (unfiltered), select **any** in the first combo box, and **any** in the second combo box.

Field	Description
Virtual Server	The virtual server number that identifies the virtual server.
Virtual Service	The virtual server service number that identifies the virtual service.
Real Server	The real server number that identifies a remote site.
Port	The virtual server service port.
IP Address	The IP address of the server.
Response Time	The average time (current weight) that each service takes to respond to information exchanges with its peers The time is specified in ticks of 65 milliseconds.
Sessions Available	The current number of sessions available for serving client requests. This number will change as client traffic loads change, or as real servers under the virtual server or remote sites go in or out of service.
Domain Name [1]	The domain name of the virtual server.
Remote Site [1]	The remote site index number.
DNS Redirects [1]	The number of DNS redirects.

1. This is applicable only to Alteon OS 22.0.1.0 and higher.

NORTEL NETWORKS
216515-B, September 2004

Monitoring Layer 4: Global SLB: Remote Sites on Alteon Application Switches

Note: This feature is available only on Alteon OS 22.0.1.0 and higher.

Field	Description
Remote Site	The index number of the remote site.
Updates Sent	The number of updates sent.
Good Updates Received	The number of good updates received.
DSSPv2 Updates Sent	The number of DSSPv2 updates sent.
DSSPv2 Good Updates Received	The number of good DSSPv2 updates received.
Bad Updates Received	The number of bad updates received.

Monitoring Layer 4: Global SLB: Remote Real Servers Information on Alteon Application Switches

Note: This feature is available only on Alteon OS 22.0.1.0 and higher.

Field	Description
Remote Real Server	The index number of the remote real server.
IP Address	The IP address of the remote real server.
Name	The name of the remote real server.
State	The state of the remote real server.

Monitoring Layer 4: Global SLB: Virtual Server Information on Alteon Application Switches

Note: This feature is available only on Alteon OS 22.0.1.0 and higher.

Field	Description
Virtual Server	The virtual server index number.
Virtual Service	The virual service index number that identifies the virtual service
Real Server	The real server index.
Domain Name	The domain name assigned to this server.
Service Port	Identifies the port assigned to this server.
IP Address	The IP address assigned to this server.
Health Check Response Time	The health check response time for the virtual server.
Available Sessions	The number of sessions available.
Current Sessions	The number of sessions currently being handled by the virtual server.
Maximum Sessions Supported	The maximum number of sessions supported.
Sessions Utilization	Displays the session utilization of the virtual server.
CPU Utilization	Displays the utilization of the CPU by this virtual server.
Remote Site	The index number of the remote site.
Weight	Displays the server weight.
Availability	Displays the server availability.
Region	The geographic region of the remote site.

Monitoring Layer 4: Global SLB: Remote Site Information on Alteon Application Switches

Note: This feature is available only on Alteon OS 22.0.1.0 and higher.

Field	Description
Virtual Server	The virtual server index number.
Virtual Service	The virtual service index number that identifies the virtual service.
Real Server	The real server index.
Domain Name	The domain name assigned to this server.
Service Port	Identifies the port assigned to this server.
IP Address	The IP address assigned to this server.
Health Check Response Time	The health check response time for the server.
Available Sessions	The number of sessions available.
Current Sessions	The number of sessions currently being handled by the server.
Maximum Sessions Supported	The maximum number of sessions supported.
Sessions Utilization	Displays the session utilization of the server.
CPU Utilization	Displays the utilization of the CPU by this server.
Remote Site	The index number of the remote site.
Weight	Displays the server weight.
Availability	Displays the server availability.
Region	The geographic region of the remote site.

Monitoring Layer 4: Global SLB: Networks on Alteon Application Switches

Note: This feature is available only on Alteon OS 22.0.1.0 and higher.

Field	Description
Network	The index number of the network.
Hits	The number of hits on the network.

Monitoring Layer 4: Global SLB: Rules on Alteon Application Switches

Note: This feature is available only on Alteon OS 22.0.1.0 and higher.

Field	Description
Rule	The indext number of the rule.
Least Connections Used	Statistics for Least Connections Used.
Round Robin Used	Statistics for Round Robin Used.
Min Misses Used	Statistics for Min Misses Used.
Hash Used	Statistics for Hash Used.
Response Used	Statistics for Response Used.
Geographical Used	Statistics for Geographical Used.
Network Used	Statistics for Network Used.
Random Used	Statistics for Random Used.
Availability Used	Statistics for Availability Used.
Quality of Service Used	Statistics for Quality of Service Used.
Local Used	Statistics for Local Used.
Always Used	Statistics for Always Used.
All Metrics Used	Statistics for All Metrics Used.

Monitoring Layer 4: Global SLB: Geographical Regions on Alteon Application Switches

Note: This feature is available only on Alteon OS 22.0.1.0 and higher.

Field	Description
North America	Statistics originating from the geographical region North America.
South America	Statistics originating from the geographical region South America.
Europe	Statistics originating from the geographical region Europe.
Caribbean	Statistics originating from the geographical region Caribbean.
Pacific Rim	Statistics originating from the geographical region Pacific Rim.
Sub-Sahara	Statistics originating from the geographical region Sub-Sahara.
Japan	Statistics originating from the geographical region Japan.
Regions Selected	Statistics originating from the geographical region selected.

Monitoring Layer 4: RTSP on Alteon 180 or AD series

Field	Description
Active RTSP Control Connections	The number of active RTSP control connections.
Active UDP Streams	The number of active User Datagram Protocol (UDP) for data channels. The number depends upon the type of media player being used.
Switch Redirects	The number of switch redirects.
Connections Denied	The total number of times the connections got denied due to shortage of resources or the real server being down.
Failed Memory Allocations	The total number of times the buffer allocation failed.

Monitoring Layer 4: RTSP on Alteon Application Switches

Field	Description
Active RTSP Control Connections	The number of active RTSP control connections.
Active UDP Streams	The number of active User Datagram Protocol (UDP) for data channels. The number depends upon the type of media player being used.
Switch Redirects	The number of switch redirects.
Connections Denied	The total number of times the connections got denied due to shortage of resources or the real server being down.
Failed Memory Allocations	The total number of times the buffer allocation failed.
Buffer Allocations Used	The total number of buffer allocations used.

Monitoring Layer 4 WAP: Add Sessions on Alteon 180 or AD series

Field	Description
Add Session Requests	The number of WAP session add requests via TPCP.
Add Failed, Queue Full	The number of Add Session Requests that failed because the queue was full.
Add Failed, Switch Port Dead	The number of Add Session Requests that failed because the target port was dead.
Add Failed, Specific Entry in Use	The number of Add Session Requests that failed because the specified entry was in use.
Add Failed, All Entries in Use	The number of Add Session Requests that failed because all entries were in use.

Monitoring Layer 4 WAP: Add Sessions on Alteon Application Switches

Field	Description
Add Session Requests	The number of WAP session add requests via TPCP.
Add Failed, Switch Port Dead	The number of Add Session Requests that failed because the port was dead.

Monitoring Layer 4: WAP: Delete Sessions on Alteon 180 or AD series

Field	Description
Delete Session Requests	The number of WAP session delete requests via TPCP.
Delete Failed, Queue Full	The number of Delete Session Requests that failed because the queue was full.
Delete Failed, Switch Port Dead	The number of Delete Session Requests that failed because the port was dead.
Deleted Failed, Specific Entry in Use	The number of Delete Session Requests that failed because the specified entry was in use.
Delete Failed, All Entries in Use	The number of Delete Session Requests that failed because all entries were in use.
Delete Sent to Wrong Switch Port	The number of Delete Session Requests that failed because they were delivered to the wrong port.

Monitoring Layer 4: WAP: Delete Sessions on Alteon Application Switches

Field	Description
Delete Session Requests	The number of delete session requests for Wireless Application Protocol (WAP).
Delete Failed, Switch Port Dead	The number of Delete Session Requests that failed because the port was dead.
Delete Sent to Wrong Switch Port	The number of Delete Session Requests that failed because they were delivered to the wrong port.

Monitoring Layer 4: WAP: RADIUS Accounting on Alteon 180 or AD series

Field	Description
Requests	The number of RADIUS accounting requests.
Wrap Requests	The number of RADIUS accounting requests in an internally wrapped buffer.
Start Requests	The number of RADIUS accounting start requests.
Update Requests	The number of RADIUS accounting update requests.
Stop Requests	The number of RADIUS accounting stop requests.
Bad Requests	The number of RADIUS accounting requests in bad format.
Add Session Requests	The number of RADIUS accounting add session requests.
Delete Session Requests	The number of RADIUS accounting delete session requests.
Request Failed, Queue Full	The number of requests that failed because the DMA queue was full.
Request Failed, Switch Port Dead	The number of requests that failed because the switch port was dead.
Request Failed, DMA Failure	The number of requests that failed because of DMA write failures.
Request Failed, All Entries In Use	The number of requests that failed because all entries were in use.

Monitoring Layer 4: WAP: RADIUS Accounting on Alteon Application Switches

Field	Description
Requests	The number of RADIUS accounting requests.
Wrap Requests	The number of RADIUS accounting requests in an internally wrapped buffer.
Start Requests	The number of RADIUS accounting start requests.
Update Requests	The number of RADIUS accounting update requests.
Stop Requests	The number of RADIUS accounting stop requests.
Bad Requests	The number of RADIUS accounting requests in bad format.
Add Session Requests	The number of RADIUS accounting add session requests.
Delete Session Requests	The number of RADIUS accounting delete session requests.
Request Failed, Switch Port Dead	The number of requests that failed because the switch port was dead.
Request Failed, DMA Failure	The number of requests that failed because of DMA write failures.
Request FRAMED_IP Field	The number of requests that contained FRAMED_IP field.
Request Without FRAMED_IP Field	The number of requests that did not contain FRAMED_IP field.

Monitoring Layer 4: Remote URL Buffers

Note: This tab is for switches running Web OS 9.0.34 and lower.

Field	Description
Successful Sequence Buffer Allocations	The total number of successful RURL sequence buffer allocations.
Successful Sequence Buffer Frees	The total number of successful RURL sequence buffer Frees.
Failed Sequence Buffer Allocations	The total number of failed RURL sequence buffer allocations.
Failed Sequence Buffer Frees	The total number of failed RURL sequence buffer frees.
Successful Frame Buffer Allocations	The total number of successful RURL frame buffer allocations.
Failed Frame Buffer Allocations	The total number of failed RURL frame buffer allocations.
Failed Frame Buffer Frees	The total number of failed RURL frame buffer frees.
Frame Buffer Retransmissions	The total number of retransmissions of an existing RURL frame buffer.
Frame Buffer Changes	The total number of retransmissions of an existing RURL frame buffer that changed in length.

Monitoring Layer 4: Remote URL Errors

Note: This tab is for switches running Web OS 9.0.34 and lower.

Field	Description
Session Connect Errors	Displays the connect errors.
Packaging Errors	Displays the packaging errors.
Unpacking Errors	Displays the unpacking errors.
DMA Write Errors	Displays the DMA write errors.
No Available Buffers Errors	Displays errors because of unavailable buffers.
Buffer Wrap Errors	Displays buffer wrap errors.
Invalid Protocol Errors	Displays invalid protocol errors.

Monitoring Layer 4: Remote URL Maintenance

Note: This tab is for switches running Web OS 9.0.34 and lower.

Field	Description
Origin Server Hits	The total number of session setups to the end server.
HTTP Redirects	The total number of HTTP redirect responses to the client.
Server Requests	The total number of request packets sent from the switch to the iSD.
Server Acknowledgements	The total number of response packets sent from the iSD to the switch.
Session Connections	The total number of session connections to the iSD made by the switch.
Last Frames	The total number of last frame packets sent from the iSD to the switch.
Client Retransmissions	The total number of client retransmissions.
Client Resets due to Retransmissions	The total number of client resets due to excessive retransmissions.

Monitor: Layer 4: Remote URL Miscellaneous

Note: This tab is for switches running Web OS 9.0.34 and lower.

Field	Description
Client Wraps	The total number of client packets processed using frame wrap buffers.
Server Wraps	The total number of server packets processed using frame wrap buffers.
Buffer Wraps	The total number of packets processed using RURL wrap copy mechanism.
Free Ring Calls	The total number of RURL sequence buffer frees.
Client Resets	The total number of client resets by the switch.
Server Resets	The total number of server resets by the switch.
Frame Pass-Through L2	The total number of packets dropped to L2 processing because of the switch running out of resources.
Parsing Filter Misses	The total number of packets leaking from RURL parsing to URL parsing.
Exceeded Buffer Length	The total number client requests that exceeded the maximum buffer size of the switch.
Exceeded Frame Depth	The total number of client requests that exceeded the maximum buffer depth of the switch.
Zero Content Length	The total number of occurrences where the Content-Length of the HTTP request was zero.
Non-Typical Offsets	The total number of occurrences where the RURL header offsets were not typical.
FIN/RST Session Backups	The total number of occurrences where a FIN or RST packet was used to establish a new session in the switch.
PSH Session Setups	The total number of occurrences when a PSH packet established a new session in the switch.
Non-SYN Session Setup	The total number of occurrences when a non-SYN packet establishes a new session in the switch.

Monitor: Layer 4: Remote URL Sessions

Note: This tab is for switches running Web OS 9.0.34 and lower.

Field	Description
Layer 7 Bind Calls	The total number of requests to bind a session.
Layer 7 Session Reuse	The total number of remote URL (RURL) session setups encountered.
Session Setups	The total number of RURL session setups.
Miscellaneous Processing	The total number of sessions that fell through filter processing.
Client Packets In	The total number of client packets processed by the RURL filter.
Client Sans In	The total number of client SYN packets processed by the RURL filter.
ClientReTXSYNsSeen	The total number of client retransmitted SYN packets processed by the RURL filter.
ClientSYNACKsSent	The total number of switch-to-client SYN/ACK packets processed by the RURL filter.
Client ACKs In	Total number of switch-to-server SYN/ACK packets processed by the RURL filter.
Client Data In	The total number of client PSH packets processed by the RURL filter.
Client Data Retransmits	The total number of client data retransmit packets processed by the RURL filter.
Server SYNs Sent	The total number of SYN packets sent to the server by the switch.
Server Retransmitted SYNs	The total number of ACK packets sent to the server by the switch.
Server Retransmitted SYN Errors	The total number of ACK packets sent to the server by the switch.
Server SYN ACKs In	The total number of switch-to-server SYN/ACK packets processed by the RURL filter.
Server ACKs In	The total number of server-to-switch ACK packets processed by the RURL filters.
Server ACKs Sent	The total number of ACK packets sent to the server by the switch.
Connections Spliced	The total number of connections successfully spliced by the switch.

Monitoring Layer 4: Remote URL Tables

Note: This tab is for switches running Web OS 9.0.34 and lower.

Field	Description
IP Redirection Table Entries	The current number of IP redirection table entries.
PORT Redirection Table Entries	The current number of port redirection table entries.
IP/PORT Redirection Table Entries	The current number of IP/port redirection table entries.
Frame Buffer Entries	The current number of Remote URL (RURL) frame buffer entries.
Sequence Table Entries	The current number of RURL sequence table entries.
Highest IP Redirection Table Entries	The highest number of IP redirection table entries.
Highest PORT Redirection Table Entries	The highest number of port redirection table entries.
Highest IP/ PORT Redirection Table Entries	The highest number of IP/port redirection table entries.
Highest Sequence Table Entries	The highest RURL sequence table entries.
Highest Frame Buffer Entries	The highest RURL frame buffer entries.

Monitoring Layer 7

The following topics are covered in this section:

- Monitoring Layer 7: URL Parsing: WCR Redirect on Alteon Application Switches
- Monitoring Layer 7: URL Parsing: SLB Strings
- Monitoring Layer 7: URL Parsing: Maintenance on Alteon 180 or AD series
- Monitoring Layer 7: URL Parsing: Maintenance on Alteon Application Switches
- Monitoring Layer 7: URL Parsing: Parsing Information

Monitoring Layer 7: URL Parsing: WCR Redirect on Alteon 180 or AD series

Field	Description
Redirected Packets	The number of received packets with matching specified URL expressions that were redirected to a specified group of real servers.
Packets Sent to Origin Server	The number of received packets that were delivered to the original server. This occurs when there is a mis-match with the specified URL expressions, or detecting HTTP non-GETs, user cookies, and no-cache as user configuration.
Non-GET HTTP Packets	The number of received packets that contained non-GETs methods, such as POST, HEAD, PUT, and so forth.
Packets with 'Cookie'	The number of received packets that contained a Cookie: header
Packets with no-cache	The number of received packets that contained a no-cache header value.

Monitoring Layer 7: URL Parsing: WCR Redirect on Alteon Application Switches

Field	Description
Redirected Packets	The number of received packets with matching specified URL expressions that were redirected to a specified group of real servers.
Packets Sent to Origin Server	The number of received packets that were delivered to the original server. This occurs when there is a mis-match with the specified URL expressions, or detecting HTTP non-GETs, user cookies, and no-cache as user configuration.
Non-GET HTTP Packets	The number of received packets that contained non-GETs methods, such as POST, HEAD, PUT, and so forth.
Packets with 'Cookie'	The number of received packets that contained a Cookie: header
Packets with no-cache	The number of received packets that contained a no-cache header value.
HTTP Straight to Origin Server	The number of HTTP requests forwarded straight to the origin server.
RTSP Redirected to Cache Server	The number of RTSP requests redirected to the cache server.
RTSP Forwarded to Origin Server	The number of RTSP requests forwarded to the origin server.

Monitoring Layer 7: URL Parsing: SLB Strings

Field	Description
URL Path	The URL path table index.
String	The string associated with the URL path.
Hits	The total number of instances that are load-balanced due to matching of the particular URL path.

Monitoring Layer 7: URL Parsing: Maintenance on Alteon 180 or AD series

Field	Description
Clients Resetted/Client Side	The number of reset frames sent to the client by the switch during client connection termination.
Clients Resetted/Server Side	The number of reset frames sent to the server by the switch during server connection termination.
Connection Swapping	The total number of connection swapping between different real servers in supporting multiple HTTP/1.1 client requests.
Half Open Connections	The number of outstanding TCP connections have been half opened. This statistics is valid only when URL parsing has been turned on. It is incremented when the switch respond to TCP SYN packet and decremented upon receiving TCP SYN ACK packet from the requester.
Switch Retries	The total number of switch retries to connect to the real server.
Random Early Drops	The total number of SYN frames dropped when the buffer is low.
SP Memory Allocated	The amount of SP memory allocated.
SP Memory Allocated 1 - 8	The amount of SP memory allocated per bucket.
SEQ Buffers	The number of sequence buffers used.
Highest SEQ Buffers	The highest number of sequence buffers ever used.
URL Buffers in Use	The number of URL buffers in use.
Highest URL Buffers Used	The highest number of URL buffers ever used.
SP Buffers in Use	The number of SP buffers in use.
Highest SP Buffers Used	The highest number of SP buffers ever used.
SEQ Buffer Failed	The total number of failed sequence buffers.
URL Buffer Failed	The total number of failed URL buffers.

Field	Description
Maximum Sessions per Bucket	The maximum number of session per bucket.
Maximum Frames per Session	The maximum number of frames per session.
Maximum Bytes Transferred per Session	The maximum number of bytes transferred per session.
Lowest SP Memory Units Available 1 - 8	The lowest number SP memory units ever available per bucket.

Monitoring Layer 7: URL Parsing: Maintenance on Alteon Application Switches

Field	Description
Reset Frames Sent to Client	The number of reset frames sent to the client by the switch during client connection termination.
Reset Frames Sent to Server	The number of reset frames sent to the server by the switch during server connection termination.
Connection Swapping	The total number of connection swapping between different real servers in supporting multiple HTTP/1.1 client requests.
Half Opened TCP Connections	The number of outstanding TCP connections have been half opened. This statistics is valid only when URL parsing has been turned on. It is incremented when the switch respond to TCP SYN packet and decremented upon receiving TCP SYN ACK packet from the requester.
Switch Retries	The total number of switch retries to connect to the real server.
SYN Frames Dropped	The total number of SYN frames dropped when the buffer is low.
GET request Too Long	The total number of GET requests that exceeded 4500 bytes.
Invalid 3-way Handshakes Dropped Frames	The total number of dropped frames because of invalid 3-way handshakes.
Available SP Memory	The current available SP memory units.
Outstanding Used Sequence Buffers	The number of outstanding sequence buffers used.
Highest Used Sequence Buffers	The highest number of sequence buffers ever used.
Outstanding Used Data Buffers	The number of outstanding data buffers used.
Highest Used Data Buffers	The highest number of data buffers ever used.
Outstanding Used SP Buffers	The number of outstanding SP buffers used.
Highest Used SP Buffers	The number of SP buffers ever used.

Field	Description
Allocated Sequence Buffer Non Zero Length	The total number of sequence buffer allocations with non zero length.
Allocated Sequence Buffers	The total number of sequence buffer allocations.
Freed Sequence Buffers	The total number of sequence buffer freed.
Allocated Data Buffers	The total number of data buffers allocated to store client request.
Freed Data Buffers	The total number of data buffers freed.
Failed Allocated Sequence Buffer	The number of times sequence buffer allocation failed.
Failed Allocated URL Data Buffer	The number of times URL data buffer allocation failed.
Maximum Sessions allowed	The maximum number of items (sessions) allowed in the session table hash bucket chain.
Maximum Frames Buffered per Session	The maximum number of frames to be buffered per session.
Maximum Bytes Buffered per Session	The maximum number of bytes buffered per session.
Invalid Method Hits	The total number of invalid method hits.
Aged Delayed Binding Sessions	The total number of aged delayed binding sessions

Monitoring Layer 7: URL Parsing: Parsing Information

Field	Description
Cookie to Parse	16 or 20 characters entered in hexadecimal format.
Virtual IP Address from Parsed Cookie	Displays the virtual IP address from the parsed cookie.
Real IP Address from Parsed Cookie	Displays the real IP address from the parsed cookie.
Real Port Number from Parsed Cookie	Displays the real port number from the parsed cookie.

Monitoring VRRP

The following topics are covered in this section:

- Monitoring Virtual Routing: Statistics
- Monitoring Virtual Routing: State

Monitoring Virtual Routing: Statistics

Virtual Router Redundancy Protocol (VRRP) support on Alteon Web switches provides redundancy between routers in a LAN. This is accomplished by configuring the same virtual router IP address and ID number on each participating VRRP-capable routing device. One of the virtual routers is then elected as the master, based on a number of priority criteria, and assumes control of the shared virtual router IP address. If the master fails, one of the backup virtual routers will assume routing authority and take control of the virtual router IP address.

When virtual routers are configured, you can display the following protocol statistics for VRRP as shown in the table below.

Field	Description
VRRP Advertisements In	The number of good VRRP advertisements that were received.
VRRP Advertisements Out	The number of good VRRP advertisements that were transmitted.
Bad VRRP Advertisements	The number of bad VRRP advertisements that were received. Bad VRRP advertisements are the advertisements that are ignored.

Monitoring Virtual Routing: State

Virtual Router Redundancy Protocol (VRRP) support on Alteon Web switches provides redundancy between routers in a LAN. This is accomplished by configuring the same virtual router IP address and ID number on each participating VRRP-capable routing device. One of the virtual routers is then elected as the master, based on a number of priority criteria, and assumes control of the shared virtual router IP address. If the master fails, one of the backup virtual routers will assume routing authority and take control of the virtual router IP address.

Field	Description
Virtual Router	The index number of the VRRP virtual router.
State	The state of the VRRP virtual router: master or backup. • *master* identifies the elected master virtual router. • *backup* identifies that the virtual router is in backup mode.
VRRP Ownership	The ownership status of the VRRP virtual router: Owner or Renter. • *owner* identifies the preferred master virtual router. A virtual router is the owner when the IP address of the virtual router and its IP interface are the same. • *renter* identifies virtual routers which are not owned by this device.
VRRP Server State	The VRRP server state identifies virtual routers that support Layer 4 services. The server state identifies virtual routers that support Layer 4 services. These are known as virtual server routers: any virtual router whose IP address is the same as any configured virtual server IP address.
VRRP Proxy State	The VRRP proxy state identifies virtual proxy routers. The proxy state identifies virtual proxy routers, where the virtual router shares the same IP address as a proxy IP address. The use of virtual proxy routers enables redundant switches to share the same IP address, minimizing the number of unique IP addresses that must be configured.

Monitoring Bandwidth Management

The following topics are covered in this section:

- Monitoring BWM: Contracts
- Monitoring BWM: Contracts Per Port
- Monitoring BWM: Contract Rates on Alteon 180 or AD series
- Monitoring BWM: Contract Rate Per Port on Alteon 180 or AD series

Monitoring BWM: Contracts



If you are monitoring BWM contracts on Alteon Application Switches, you can select the **Clear BWM Statistics** button to clear all BWM Statistics on the switch.

Field	Description
Contract	The number of the bandwidth management contract.
Name	The name of the traffic contract queue, such as URL, service, URLcont, host, or default.
Bytes Out	The total number of bytes sent out from the traffic contract queue.
Bytes Dropped	The total number of bytes dropped from the traffic contract queue.
Buffers Used	The current amount of buffer space used to store the packets that is waiting to be transmitted.
Buffers Assigned	The total number of buffers assigned to the traffic contract queue.

Monitoring BWM: Contracts Per Port

This tab allows you to view the Bandwidth management contracts that have been assigned on a per-port basis.



If you are monitoring BWM contracts on Alteon Application Switches, you can select the **Clear BWM Statistics** button to clear all BWM Statistics on the switch.

Filtering the view

If you wish to create a filtered view of contracts in this screen use the drop-down combo boxes on the bottom right. The left combo box is used to filter the items in the first column index number. The right combo box selects the BWM contract number.

For example, to view statistics only for switch port 1, select **1** in the left combo box, and **any** in the right combo box.

The default view for this screen is filtered based on the first entry that appears in each of the drop-down combo boxes. To view all data (unfiltered), select **any** in the first combo box, and **any** in the second combo box.

Clearing statistics on Alteon Application Switches

If you are monitoring BWM contracts per port on Alteon Application Switches, you can select the Clear BWM Statistics button to clear all BWM Statistics on the switch.

Field	Description
Switch Port	The number of the monitored switch port.
Contract	The contract number.
Name	The name of the traffic contract queue, such as URL, service, URLcont, host, or default.
Bytes Out	The total number of bytes sent out from the traffic contract queue.
Bytes Dropped	The total number of dropped bytes from the traffic contract queue.
Buffers Used	The total number of buffers used by the traffic contract queue.
Buffers Assigned	The total number of buffers assigned to the traffic contract queue.

Monitoring BWM: Contract Rates on Alteon 180 or AD series

Field	Description
Contract	The contract queue number for which the statistics apply.
Name	The name of the traffic contract queue.
Rate Bytes Sent Out	The rate of bytes sent out from the traffic contract queue.
Bytes Sent Out	The of bytes sent out from the traffic contract queue.
Bytes Dropped	The total number of bytes dropped from the traffic contract queue.
Buffers Used	The total number of buffers used by the traffic contract queue.
Buffers Assigned	The total number of buffers assigned to the traffic contract queue.

Monitoring BWM: Contract Rate Per Port on Alteon 180 or AD series

Field	Description
Port	The Switch Port number for which the statistics apply.
Contract	The contract queue number for which the statistics apply.
Name	The name of the traffic contract queue.
Rate Bytes Sent Out	The rate of bytes sent out from the traffic contract queue.
Bytes Sent Out	The of bytes sent out from the traffic contract queue.
Bytes Dropped	The total number of bytes dropped from the traffic contract queue.
Buffers Used	The total number of buffers used by the traffic contract queue.
Buffers Assigned	The total number of buffers assigned to the traffic contract queue.

Monitoring SNMPv3

The following topics is covered in this section:

- Monitoring SNMPv3: Statistics

Monitoring SNMPv3: Statistics

You must be logged in through SNMP version 3 (SNMPv3) to view the SNMPv3 monitor tab.

Note: This feature is available only on Alteon OS 22.0 and higher.

Field	Description
Unknown Security Models	The total number of packets received by the SNMP engine which were dropped because they referenced a Security Model that was not known or supported by the SNMP engine.
Invalid Messages	The total number of packets received by the SNMP engine which were dropped because there were invalid or inconsistent components in the SNMP message.
Unknown PDU Handlers	The total number of packets received by the SNMP engine which were dropped because the PDU contained in the packet could not be passed to an application responsible for handling the pduType, for example, no SNMP application had registered for the proper combination of the contextEngineID and the pduType.
Unavailable Contexts	The total number of packets received by the SNMP engine which were dropped because the context contained in the message was unknown.
Unknown Contexts	The total number of packets received by the SNMP engine which were dropped because the context contained in the message was unavailable.
Unsupported Security Levels	The total number of packets received by the SNMP engine which were dropped because they requested a securityLevel that was unknown to the SNMP engine or otherwise unavailable.
Not In Time Windows	The total number of packets received by the SNMP engine which were dropped because they appeared outside of the authoritative SNMP engine's window.
Unknown User Names	The total number of packets received by the SNMP engine which were dropped because they referenced a user that was not known to the SNMP engine.
Unknown Engine IDs	The total number of packets received by the SNMP engine which were dropped because they referenced an snmpEngineID that was not known to the SNMP engine.
Wrong Digests	The total number of packets received by the SNMP engine which were dropped because they didn't contain the expected digest value.
Decryption Errors	The total number of packets received by the SNMP engine which were dropped because they could not be decrypted.

Monitoring Ports

The following topics are covered in this section:

- Monitoring Port: Interfaces
- Monitoring Port: Ethernet Errors
- Monitoring Port: Bridge
- Monitoring Port: Load Balancing on ALO and on Alteon 180 or AD series
- Monitoring Port: CPU Statistics on ALO and on Alteon 180 or AD series
- Monitoring Port: Statistics

Monitoring Port: Interfaces

Note: If you are monitoring port interfaces on Alteon Application Switches, you can right click and select Clear Port Statistics to clear the selected port statistics.

Field	Description
Bytes In	The number of bytes received on the interface, including framing characters.
Bytes Out	The number of bytes transmitted out of the interface, including framing characters.
Unicast Packets In	The number of packets, delivered by this sublayer to a higher layer that were not addressed to a multicast or a broadcast address at this sublayer.
Unicast Packets Out	The number of packets that higher-level protocols requested to transmit that were not addressed to a multicast or broadcast address at this sublayer. The count includes the packets that were discarded or not delivered.
Multicasts In	The number of packets, delivered by this sublayer to a higher layer that were addressed to a multicast address at this sublayer. For a MAC layer protocol, this includes Group and Functional addresses.
Multicasts Out	The number of packets that higher-level protocols requested to transmit that were addressed to a multicast address at this sublayer. The count includes the packets that were discarded or not sent.For a MAC layer protocol, this includes Group and Functional addresses.
Broadcast In	The number of packets, delivered by this sublayer to a higher layer, that were addressed to a broadcast address at this sublayer.
Broadcast Out	The number of packets that higher-level protocols requested to transmit, that were addressed to a broadcast address at this sublayer. The count includes the packets that were discarded or not delivered.
Discarded Packets	The number of inbound packets that were discarded, although no errors had been detected to prevent their delivery to a higher-layer protocol. This can occur to free up buffer space.
Outbound Discards	The number of outbound packets that were discarded, although no errors had been detected that would prevent their transmission. This can occur to free up buffer space.
Error Packets	For packet-oriented interfaces, the number of inbound packets with errors that prevented their delivery to a higher-layer protocol. For character-oriented or fixed-length interfaces, the number of inbound transmission units with errors that prevented their delivery to a higher-layer protocol.

Field	Description
Not Sent Due to Error	For packet-oriented interfaces, the number of outbound packets that could not be transmitted because of errors. For character-oriented or fixed-length interfaces, the number of outbound transmission units that could not be transmitted because of errors.
Unknown Protocol Packets	For packet-oriented interfaces, the number of packets received via the interface that were discarded because of an unknown or unsupported protocol. For character-oriented or fixed-length interfaces that support protocol multiplexing, the number of transmission units received via the interface that were discarded because of an unknown or unsupported protocol. **Note:** If the interface does not support protocol multiplexing, Unknown Protocol Packets will be 0 (zero).
Outbound Packet Queue Length	The number of packets in the output queue.

Monitoring Port: Ethernet Errors

Field	Description
Alignment Errors	The number of frames received on a particular interface that were not of integral length and did not pass the FCS check. The count is incremented when the Alignment Error status is returned by the MAC service to the LLC, or other MAC user.Frames with multiple errors are counted exclusively.
FCS Errors	The number of frames received on a particular interface that failed the FCS health check because of length. The count is incremented when the Frame Check Error status is returned by the MAC service to the LLC, or other MAC user. Frames with multiple errors are counted exclusively.
Internal MAC Transmission Errors	The number of frames transmitted on a particular interface that failed because of an internal MAC sublayer transmit error.This frame error is only counted if it was not recorded under Late Collisions, Excessive Collisions, or Carrier Sense Errors. **Note:** Internal Mac Transmit Errors may represent a number of transmission errors that were not otherwise recorded.
Internal MAC Receive Errors	The number of frames on a specific interface that could not be accepted because of an internal MAC sublayer error. This frame error is only counted if it was not recorded under Received Frames > Maximum Length, Alignment Errors, or FCS Errors. **Note:** Internal Mac Receive Errors may represent a number of receive errors that were not otherwise recorded.
Carrier Sense Errors	The number of times the carrier sense condition was lost or was never asserted while attempting to transmit a frame on a particular interface. The count, represented by an instance of this object, is incremented once per transmission attempt.
Received Frames > Maximum Length	A number of frames received on a specific interface that exceeded the allowed maximum frame size. The count is incremented when the Received Frames > Maximum Length status is returned by the MAC service to the LLC, or other MAC user.Received frames that have multiple errors are counted exclusively.
SQE Test Errors	The number of times the SQE TEST ERROR message was generated by the PLS sublayer for a particular interface.
Deferred Transmissions	A number of frames where the first transmission attempt, on a particular interface, is delayed because the medium is busy. **Note:** The count represented by an instance of this object does not include frames involved in collisions.

Field	Description
Single Collision Frames	The number successfully transmitted frames on a particular interface where transmission was inhibited by a single collision. **Note:** A frame that is counted by Single Collision Frames can also be counted by the occurrences of the Unicast Packets Out, Multicasts Out, or Broadcast Out, but not recorded by the event of Multiple Collision Frames.
Multiple Collision Frames	A count of successfully transmitted frames on a particular interface where transmission was inhibited by more than one collision. **Note:** A frame that is counted by Multiple Collision Frames can also be counted by Unicast Packets Out, Multicasts Out, or Broadcast Out, but not recorded by Single Collision Frames.
Late Collisions	The number of times that a collision is detected, on a particular interface, later than 512 bit-times into the transmission of a packet. A late collision, included in the count of Late Collisions, can be considered as a generic collision for other statistics. **Note:** bit-times vary per system. Example: On a 10Mbps system, 512 bit-times represents 51.2 microseconds.
Excessive Collisions	A number of frames on a particular interface in which transmission failed because of excessive collisions.

Monitoring Port: Bridge

Field	Description
Frames In	The number of frames that have been received by this port from its segment. **Note:** Packets In only counts frames that are for a protocol being processed by the local bridging function, including bridge management frames.
Frames Out	The number of frames that have been transmitted by this port to its segment. **Note:** Packets Out only counts frames that are for a protocol being processed by the local bridging function, including bridge management frames.
Discarded Frames In	The number of valid, received frames that were discarded by the Forwarding Process.
Exceeded Delay Discarded Frames	The number of frames that were discarded because of excessive transit delay through the bridge. Discards Due to Transit Delay is incremented by transparent and source route bridges.
Exceeded Size Discarded Frames	The number of excessively large frames that were discarded. Discards Due to Excessive Size is incremented by transparent and source route bridges.

Monitoring Port: Load Balancing on ALO and on Alteon 180 or AD series

Field	Description
Current Bindings (1 Second Avg)	The current number of binding sessions that average one second.
Current Bindings (4 Second Avg)	The current number of bindings that averaged four seconds.
Current Bindings (64 Second Avg)	The number of bindings that averaged 64 seconds.
Binding Failures	The total number of binding failures on the port. A Binding Failure occurs after a port has run out of binding table entries.
Non-TCP Drops	The total number of non-TCP/IP frames that were dropped from the port.
TCP Fragment Drops	The total number of TCP fragments that were dropped from the port.
UDP Datagrams Drops	The total number of UDP datagrams that were dropped from the port.
Incorrect VIP Drops	The total number of frames with incorrect virtual IP (VIP) addresses that were dropped from the port.
Incorrect Virtual Port Drops	The total number of frames with incorrect Virtual Port that were dropped from the port.
Real Server Unavailable Drops	The total number of frames that were dropped from the port because no real server was available.
Filtered Denied Drops	The total number of frames on the port that were denied by the filter.
Internal VMA Frames Dropped [1]	The total number of internal VMA frames that were dropped from the port.

1.This is applicable only on Web OS 10.1 and higher.

Monitoring Port: CPU Statistics on ALO and on Alteon 180 or AD series

Field	Description
Port CPU A Utilization (1 Second Avg)	In percentage, how much the MP CPU A was utilized more than one second. The percentage is based on total operation time.
Port CPU B Utilization (1 Second Avg)	In percentage, how much the MP CPU B was utilized more than one second. The percentage is based on total operational time.
Port CPU A Utilization (4 Second Avg)	In percentage, how much the MP CPU A was utilized more than four seconds. The percentage is based on total operation time.
Port CPU B Utilization (4 Second Avg)	In percentage, how much the MP CPU B was utilized more than four seconds. The percentage is based on total operation time.
Port CPU A Utilization (64 Second Avg)	In percentage, how much the MP CPU A was utilized more than 64 seconds. The percentage is based on total operation time.
Port CPU B Utilization (64 Second Avg)	In percentage, how much the MP CPU B was utilized more than 64 seconds. The percentage is based on total operation time.

Monitoring Port: Statistics

Note: This feature is available only on Web OS 10.1.1.0 and higher.

Field	Description
DMA Overflows	The number of frames that were placed on the software controlled DMA descriptor ring. The frame was not dropped.
Dropped Overflows	The number of frames that were dropped because there was no room on either the hardware or software DMA descriptor ring.
Read DMA Overruns	The number of times the Read DMA state machine encountered an overrun error, size of read operation exceeded size of FIFO.
Read DMA Underruns	The number of times the Read DMA state machine encountered an underrun error, size of read operation read more than what was available. It is a fatal error.
Write DMA Overruns	The number of times the Write DMA state machine encountered an overrun error, size of write operation tried to write more than what was available. Not fatal, Write DMA will be retried.
Write DMA Underruns	The number of times the unknown fatal errors occurred.
Flow Control Transmitted	The number of flow control frames transmitted.
Flow Control Received	The number of flow control frames received.
Port Lost/Gained Links	The number of times the port lost or gained link.
MAC Received Buffer Events	The number of times a MAC RX buffer attention event (a warning that RX buffer is almost full) occurred.
Adds to Full FDB	The number of times the attempts were made to add entries to an already full FDB.
Receive Buffer Events	The number of times an RX buffer attention event occurred and no cleanup occurred because frames were waiting to be DMA transferred.
MAC Address Resolution Failures	The number of times MAC address resolution failed because there were no DMA descriptors.
Receive Buffer Events Overflows	The number of times an RX buffer attention occurred and no cleanup occurred because frames were waiting to be DMA transferred on the software DMA descriptor ring.
MAC Address Learn Failures	The number of times MAC address learn failed because there were no DMA descriptors.

Field	Description
Received Buffer Events with Zero Dropped	The number of times an RX buffer attention event (a warning that RX buffer is almost full) resulted in zero frames being dropped.
Frame Deletion Failures	The number of times the frame failed to be deleted.
Received Buffer Events with One Dropped	The number of times an RX buffer attention event (a warning that RX buffer is almost full) resulted in one frame being dropped.
Frames Dropped Due to No Transcript Descriptors	The number of frames dropped because there were no TX MAC descriptors available.
Received Buffer Events with All Dropped	The number of times an RX buffer attention resulted in ALL frames in RX buffer being dropped. Usually occurs when port is in blocking mode for example, in STP.
CRC Error Drops	The number of times frames have been dropped due to CRC errors.
Received Collisions	The number of frames received that contained a collision.
Link de-asserted	The number of times the link was de-asserted during the reception of a packet.
Physical Errors	The number of frames received that the PHY (physical) detected packet error.
Nibble Errors	The number of frames received with an odd number of nibbles (four bits).
Aborted MACs	The number of frames received that were aborted by MAC.
Runt Frames	The number of runt frames (runt is a frame that is less than 64 bytes) received.
No Receive Buffer Errors	The number of frames that would not fit in the RX buffer.
Over 32K Errors	The number of frames received that were over 32K.
Over 16K Errors	The number of frames received that were over 16K.
Over 9K Errors	The number of frames received that were over 9K.

Index

Numbers

2000 and 3000 series
general configuration 21

A

Advanced Layer 4 Filters
configuring 125
Alteon OS Statistics
monitoring 255
ARP
monitoring 288
ARP Statistics
monitoring 289
AS paths 87
Auxiliary Session SP Statistics
monitoring on Alteon 2000 and 3000 series 361
Auxiliary session statistics
monitoring on Alteon 2000 and 3000 series 360

B

Bandwidth Management
configuring general 217
Base Ports
monitoring 274
Base Ports on Alteon 2000 and 3000 series
monitoring 275
BGP
enabling from Alteon EMS 112
BGP Administration
configuring on Alteon 2000 and 3000 series 112
monitoring on Alteon 2000 and 3000 series 330
BGP Aggregations
configuring on Alteon 2000 and 3000 series 117
BGP Peers
configuring on Alteon 2000 and 3000 series 115, 118
BGP Standard Peers Summary
monitoring on Alteon 2000 and 3000 series 331
BLOCKING (port state) 275
bridge
configuring general properties 56
configuring spanning tree protocol 57
spanning tree groups 59
BWM 18
BWM Contract Rates
monitoring on Alteon 180 or AD series 410
BWM Contract Rates Per Port
monitoring on Alteon 180 or AD series 411
BWM Contracts
monitoring on Alteon 180 or AD series 407
BWM contracts
configuring on Alteon 2000 and 3000 series 222
BWM Contracts Per Port
monitoring 408
BWM policies
configuring on Alteon 180 or AD series 218
configuring on Alteon 2000 and 3000 series 220

C

Configuring general switch properties
2000 and 3000 series 21
configuring on Alteon 2000 and 3000 series 172
Confirm row deletion 15
Contact 19, 21
Current Date 19, 21
Current Time 19, 21

D

Device Manager
setting poll interval 14
DISABLED (port state) 275

DNS
configuring 77
monitoring on Alteon 180 or AD series 349
monitoring on Alteon 2000 and 3000 series 350

E

enabling 18

F

filter
membership on ports 241
filter membership on ports, configuring 241
filtering
configuring on ports 240
Filters
configuring advanced layer 4 125
filters
configuring IP 130
configuring L7 deny 131
configuring TCP 129
configuring URL BWM 136
IP network 86
Forwarding Database
monitoring 271
monitoring on Alteon 2000 and 3000 series application switches 272
Forwarding Statistics
monitoring on Alteon 2000 and 3000 series 273
Front Middle Sensor Temperature 20
Front Right Sensor Temperature 20
FTP
monitoring on Alteon 180 or AD series 347
monitoring on Alteon 2000 and 3000 series 348

G

general ip settings
configuring on Alteon 2000 and 3000 series 73
general properties for ports
configuring 236
general switch properties 14
Global SLB
configuring general settings on Alteon 2000 and 3000 series 185
configuring Lookups 189, 191, 192, 193
configuring Network Lookups 190
configuring Remote Sites 184
monitoring General on Alteon 2000 and 3000 series 369
monitoring Geographical Regions on Alteon 2000 and 3000 series 379
monitoring Networks on Alteon 2000 and 3000 series 377
monitoring Remote Real Groups on Alteon 2000 and 3000 series 371
monitoring Remote Real Servers Information on Alteon 2000 and 3000 series 374
monitoring Remote Real Servers on Alteon 2000 and 3000 series 370
monitoring Remote Site Information on Alteon 2000 and 3000 series 376
monitoring Remote Sites on Alteon 2000 and 3000 series 373
monitoring Remote Virtual Servers on Alteon 2000 and 3000 series 372
monitoring Rules on Alteon 2000 and 3000 series 378
monitoring Virtual Server Information on Alteon 2000 and 3000 series 375
GSLB
enabling 18
GUI front panel view 250

H

Hardware Revision 20
HTTP server port 19, 21

I

ICMP In
monitoring 302
ICMP message types 127
ICMP Out

monitoring 303
IP Addresses
monitoring on Alteon 180 or AD series 293
IP Filters
configuring 130
IP forwarding 81
IP gateways
configuring 76
IP Interface Statistics
monitoring on Alteon 180 or AD series 291
IP Interfaces
monitoring on Alteon 180 or AD series 290
IP interfaces
configuring on Alteon 180 or AD series 75
IP network filters 86
IP Properties
monitoring on Alteon 180 or AD series 298
monitoring on Alteon 2000 and 3000 series 300
IP Routes
monitoring on Alteon 180 or AD series web switches 284
monitoring on Alteon 2000 and 3000 series 285

L

L7 Deny Filters
configuring 131
Layer 4 Filters
configuring 120
Layer 4 Filters statistics
monitoring 338
Layer 7 URL Parsing
configuring SLB strings 201, 203
configuring WCR redirect 199
Layer 7 URL Parsing Expressions
configuring 198
LDAP version 163
LEARNING (port state) 275
Listen for Traps 14
LISTENING (port state) 275
local route cache 78
Location 19, 21
login banner 19, 21

M

MAC address 19, 21
Management Port
configuring on Alteon 2000 and 3000 series 25
monitoring on Alteon 2000 and 3000 series 263
monitoring SONMP 264
MP CPU Stats
monitoring on Alteon 180 or AD series 256
monitoring on Alteon 2000 and 3000 series 257

N

Network Time Protocol (NTP)
configuring on Alteon 180 or AD series 38

O

OSPF Administration
configuring 91
OSPF Administrative Status
monitoring 306, 307
OSPF Area
monitoring 308
OSPF Area Aggregates
configuring 103
OSPF Area Info
monitoring 322
OSPF Area Interface
monitoring 311
OSPF Area Nbr
monitoring on Alteon 180 or AD series 309
monitoring on Alteon 2000 and 3000 series 310
OSPF Area SPF
configuring 95
OSPF Areas
configuring 93
OSPF External BGP

configuring on Alteon 2000 and 3000 series application switches 106
OSPF External Link-State DB
monitoring 325
OSPF Fixed Routes
configuring 104
OSPF General Settings
configuring 92
OSPF Host Areas on Alteon 2000 and 3000 series
configuring 98
OSPF Hosts
configuring 97
OSPF Interface Info
monitoring 323
OSPF Interface Metrics
configuring 101
OSPF Interface Nbr
monitoring 313
OSPF Interface Transmissions
monitoring 312
OSPF Interfaces
configuring 99
OSPF Internal BGP
configuring on Alteon 2000 and 3000 series 107
OSPF Link-State DB
monitoring 324
OSPF MD5
configuring on Alteon 2000 and 3000 series 108
OSPF MD5-Interface
configuring on Alteon 2000 and 3000 series 109
OSPF MD5-Virtual Interface
configuring on Alteon 2000 and 3000 series application switches 110
OSPF Static Routes
configuring on Alteon 2000 and 3000 series 105
OSPF Stats
monitoring on Alteon 180 or AD series 315
monitoring on Alteon 2000 and 3000 series 318
OSPF Stats 2
monitoring 321
OSPF Stub Areas
configuring 96
OSPF Virtual Interfaces
configuring 102

P

Part Number 19
Port Bridge
monitoring 420
Port CPU Statistics
monitoring 422
Port Ethernet Statistics
monitoring 418
Port Interfaces
monitoring on Alteon 180 or AD series 416
port mirroring
configuring 52
configuring (version 10.0 and higher) 53
port properties
configuring on Alteon 180 or AD series web switches 237
port statistics 423
ports
configuring filter membership 241
configuring general properties on 236
Power Supply 20
proxy IP (pip) addresses 167, 170

R

Radius Accounting
monitoring on Alteon 180 or AD series 386
monitoring on Alteon 2000 and 3000 series 387
RADIUS server
configuring 35
Rate Limiting 339
real server groups
configuring on Alteon 2000 and 3000 series 147
Real Server Ports
configuring 146

Real Servers
configuring 142
monitoring on Alteon 180 or AD series 342
Real Servers by SP
monitoring on Alteon 180 or AD series 343
Real Servers State
monitoring 346
Real Time Streaming Protocol (RTSP) Load Balancing
configuring 171
Rear Left Sensor Temperature 20
Rear Middle Sensor Temperature 20
Register for Traps 14
Remote URL Buffers
monitoring 388
Remote URL Destination Port
configuring 183
Remote URL Errors
monitoring 389
Remote URL General settings
configuring 182
Remote URL Maintenance
monitoring 390
Remote URL Miscellaneous
monitoring 391
Remote URL Sessions
monitoring 392
Remote URL Tables
monitoring 393
Retry Count 14
RIP
monitoring 304
route map access list 85
route maps 83
Route Statistics
monitoring 287
routing information protocol
configuring 79
RTSP
monitoring on Alteon 180 or AD series 380
monitoring on Alteon 2000 and 3000 series 381

S

scriptable health checks 172
Selection Dialog windows, using 17
Services
configuring on Alteon 180 or AD series 154
configuring on Alteon 2000 and 3000 series 160
SLB
configuring general settings on Alteon 180 or AD series 137, 139
SLB Groups
monitoring 344
SLB Maintenance
monitoring on Alteon 180 or AD series 351
monitoring on Alteon 2000 and 3000 series 352
SLB on ports
configuring on Alteon 180 or AD series 165
monitoring 421
SLB Strings
configuring 201, 203
SLB summary view 335
SMTP host 217
SNMP
monitoring 252
snmp 14
software images
configuring on Alteon 180 or AD series 27
SP Filters
monitoring on Alteon 2000 and 3000 series 341
SP Maintenance
monitoring on Alteon 2000 and 3000 series 260, 354
SP Maintenance Receive
monitoring on Alteon 2000 and 3000 series 261
SP Maintenance Send
monitoring on Alteon 2000 and 3000 series 262
spanning tree groups
configuring on the bridge 59

spanning tree protocol
configuring on ports 239
configuring on ports (Alteon 2000 and 3000 series) 62
Spanning-Tree Protocol
root bridge 59, 61
SSL 126
SSL processor 23
SSL Statistics
monitoring on Alteon 2000 and 3000 series 357
state information, client system 126
static routes 82
Routing Information Protocol (RIP) 79
Status Poll Interval 14
Switch HTTP Server Port 19, 21
switch summary view 245
item descriptions 245, 248
switch telnet server port 21
SYN attack prevention
configuring 176
syslog
configuring 30
listen for 15
syslog traps
configuring on Alteon 180 or AD series 34
System Description 19, 21
System Name 19, 21
System Up Since 19, 21

T

TCP
monitoring on Alteon 180/AD series 294
TCP Connection
monitoring 295
TCP filters
configuring 129
TCP rate limiting
monitoring 339
TFTP server
configuring 28
Timeout 14
time-to-live, DNS response (global SLB menu option) 192
TP Ports
monitoring 276
trace routes, enabling 14
Tracking
VRRP 213
trap hosts
configuring 32, 33
traps
designating a port 14
listening for 14
max number in log 14
registering for 14
trunk groups
configuring 41

U

UDP
monitoring 296
UDP Local
monitoring 297
URL BWM Filtering
configuring 136
URL Parsing
Parsing Information
monitoring 402
URL Parsing Maintenance
monitoring on Alteon 180 or AD series 398
monitoring on Alteon 2000 and 3000 series 400
URL SLB Strings
monitoring 397
URL-Based BWM
configuring 181

V

Virtual Routing
configuring general 205

configuring peers 215
configuring routers 207
Synchronizing to a Peer Switch 214
Virtual Routing Groups
configuring 210, 212
Virtual Routing Interfaces
configuring 209
Virtual Routing State
monitoring 405
Virtual Routing Statistics
monitoring 404
Virtual Server Service State
monitoring on Alteon 2000 and 3000 series 358
Virtual Server Services
configuring on Alteon 180 or AD series 154
configuring on Alteon 2000 and 3000 series 160
Virtual Servers
configuring on Alteon 180 or AD series 152
configuring on Alteon 2000 and 3000 series 158
monitoring 345
VLAN membership
configuring on Alteon 180 or AD series 64
VRRP
tracking 213

W

WAP
monitoring Add Sessions on Alteon 180 or AD series 382
monitoring Add Sessions on Alteon 2000 and 3000 series 383
monitoring Delete Sessions on Alteon 180 or AD series 384
monitoring Delete Sessions on Alteon 2000 and 3000 series 385
WAP General Properties
configuring 194
web cache redirection
configuring L7 URL parsing 199
monitoring on Alteon 180 or AD series 395
monitoring on Alteon 2000 and 3000 series 396
Web OS Statistics
monitoring 254