RELEASE NOTES:

WebOS Switch Software

Release 8.0

Alteon WebSystems
Web Speed for e-Business

50 Great Oaks Boulevard
San Jose, California 95119
408-360-5500 Main
408-360-5501 Fax
www.alteonwebsystems.com

Part Number: 050092, Revision A, May 2000

Release Notes

These release notes provide the latest information regarding your Alteon Web switch with WebOS 8.0 software. This supplement modifies information found in the complete documentation:

- *WebOS 8.0 Command Reference* (part number 050081, Revision A)
- *WebOS 8.0 Application Guide* (part number 050087, Revision A)

Please keep this information with your Alteon WebSystems product manuals.

Installing WebOS 8.0

Upgrade Procedure

Use the following procedure when upgrading your Alteon Web switch software:

1. **Be sure that your Web switch is currently running WebOS 6.0.**

   If running WebOS or ACElerate software prior to version 6.0, obtain and follow the upgrade instructions found in the *WebOS 6.0 Release Supplement* (part 050056B). The switch must be running WebOS 6.0 prior to continuing with the upgrade.

2. **Backup the current WebOS 6.0 configuration (optional, but recommended).**

   You may obtain a configuration backup though tftp configuration upload to a file, or by copying the contents of the configuration dump to a file.

3. **Perform a tftp download of the WebOS 8.0 software code onto the switch.**

4. **Select the new WebOS 8.0 image for use upon reboot, and reset the switch.**

5. **Virtual Matrix Architecture (Optional)**

   If any port is configured with a proxy IP address, VMA will be initially disabled. To enable VMA, see “Virtual Matrix Architecture” on page 4.

Retrograde Notes

Before retrograding to an WebOS 6.0, it is recommended that you create a backup of the WebOS 8.0 switch configuration.

Because the WebOS 8.0 configuration format has changed, retrograding to WebOS 6.0 will cause the switch configuration to revert to the WebOS 6.0 factory default settings.

To restore the WebOS 6.0 configuration to pre-8.0 settings, you can use the backup created during the upgrade procedure. Otherwise, if substantial configuration changes make this inappropriate, an 8.0 to 6.0 configuration conversion utility is available. Please contact Alteon WebSystems Customer Support for assistance if you need to convert a WebOS 8.0 configuration dump to the WebOS 6.0 format.

Feature Configuration Notes

Virtual Matrix Architecture

Virtual Matrix Architecture (VMA) is a hybrid architecture that takes full advantage of the distributed processing capability in the Alteon Web switches. It combines the strengths of central and distributed processing to deliver improvements in processing power and port capacity.

It is recommended to enable the VMA feature for better performance and higher session capacities, especially when using Bandwidth Management and Content Intelligent Switching for multiple frames processing (up to 4,500 bytes).

Proxy IP Addresses and VMA

By default, VMA is enabled on the Web switch. If upgrading to WebOS 8.0 from a previous release, however, VMA will be initially disabled if there is a proxy IP address configured for any port on the switch. This is because VMA requires that if any port is configured with a proxy IP address, then all ports (except port 9) must be configured with a proxy IP address prior to enabling VMA.

FWLB and VMA

Also note that VMA is required to be enabled in certain Firewall Load Balancing (FWLB) situations. When setting up FWLB with clean-side switches performing SLB or URL-based SLB, if Direct Access Mode (DAM) is enabled, then VMA must be also be enabled.

URL Parsing and VRRP Active/Active Setup

When URL-based SLB is used in an active/active redundant setup, do not use Direct Access Mode (DAM). Instead, use a proxy IP address.

TOS Rewrite

TOS rewrite is only applicable when defining a filter with the `allow` action.

Bandwidth Management

The following tips and restrictions apply for the Bandwidth Management (BWM) feature:

- VMA is recommended when Bandwidth Management is enabled.
- When both Filter TOS and Bandwidth Management TOS are applied, the BWM TOS has precedence.
- Bandwidth Management configurations will not be synchronized during VRRP synchronization.
- The maximum hard limit for a bandwidth policy is 1 Gbps, even when multiple Gigabit ports are trunked.

Script-Based Health Check

Health check scripts can only be configured through the CLI, but once entered can be assigned as the health check method using SNMP or the Browser-Based Interface.

GSLB Static Client Proximity

The following tips and restrictions apply for the GSLB Static Client Proximity feature:

- The switch supports only a single domain.
- No health checks or pings for virtual servers in the network table.
- Switch replies with only one virtual server IP address, based on response time and `min-con` value.

VRRP with GSLB

When using both VRRP and GSLB, you must change the `/cfg/sys/wport` (BBI port) value of the target switch (the switch that is being synchronized to) to a port other than port 80 before VRRP synchronization begins.

URL Parsing with Content Intelligent Persistence

Tips and Limitations

The following tips and restrictions apply when using URL-based SLB or WCR with cookie-based or SSL session ID persistence:

- VMA is recommended when using any Content Intelligent switching feature.
- You must use either Direct Access Mode (DAM) or a proxy IP address.
- Precedence for load balancing/persistence algorithms are:
  - Persistence-based load balancing (Cookie, SSL Session ID or Client IP-based persistence)
  - HTTP Header or URL based load balancing (cookie-based preferential service or host header-based load balancing for virtual hosting or load balancing based on the URLs)

Capacity Summary

- Supports up a maximum of 4,500 bytes in a single request
- Cookie information

  Cookie name = up to 20 bytes with support of wildcard “*”

  Cookie value for hashing = up to 64 bytes
- URL based and HTTP header based SLB

  # of sub string = 128

  Maximum length of sub string = 40 bytes
- URL based WCR

  # of filter = 32

  Maximum length of filter = 8 bytes
- Hashing based on URL

  Maximum # of bytes to hash = 255

SecurID

There is no SNMP pr Browser-Based Interface (BBI) support for SecurID, since the SecurID server, ACE is a one-time password authentication and requires an interactive session.

SSH and SCP

The following tips and restrictions apply for the SSH and SCP features:

- SSH and SCP are supported on the Alteon AD4 and Alteon 184 platforms only.
- These features have been tested with the following SSH clients:
  - SSH client version SSH 1.2.27 and 1.2.23 for Linux (freeware)
  - SecureCRT 3.0.2 and 3.0.3 for Win NT
  - F-Secure SSH 1.1 for Windows from Data Fellow. (It will accept all clients which has version identification “SSH-1.5-1.X”.)
- The Web switch SSH daemon uses TCP port 22 only and is not configurable.
- The configuration of SSH/SCP parameters can only be performed using the console port.
- The maximum number of simultaneous Telnet/SSH/SCP connections is 4.
- The Web switch will perform only one session of key/cipher generation at a time. Thus, an SSH/SCP client will not be able to login if the switch is performing key generation at that time, or, if another client has logged in immediately prior. Also, key generation will fail if an SSH/SCP client is logging in at that time.
- Sessions connected via the `/cfg/sys/radius/telnet` command count toward SSH/SCP connections.
- The `scpadmin` login is only useful when the `scp` command is to be used with RADIUS and SecurID authentication.
- The `scpadmin` login should not be given the same password as any of the other user, admin, or oper passwords. Users login in with a password which is the same as the `scpadmin` will be logged in as `scpadmin`.

Advanced Packet Filtering

The following tips and restrictions apply for advanced packet filtering for IP Options, TCP Flags, ICMP Message Type and IP TOS:

- These features work only with Cache disabled filtering.
- Care must be taken when applying cache enabled and cache disabled filters to the same switch port. This is because cache enabled filter creates a session entry in the switch so that the switch can bypass checking for subsequent frames that matches the same criteria. This can potentially cause cache disable filters applying to the same switch port to be bypassed too.

Load Balancing Enhancements for Passive FTP servers

The following tips and restrictions apply when using the enhancements for passive FTP:

- You must use either Direct Access Mode (DAM) or a proxy IP address.
- This feature does not support different FTP modes within a single session. That is, the user cannot switch from active to passive or vise versa in the same FTP session.

Configuration dump

The output file from the `ptcfg` command is formatted with line-breaks without carriage returns and cannot be viewed with editors that require carriage returns (such as MS Notepad).

BBI Limitations

Alteon Web switches provide a variety of methods for gathering switch information and performing switch configuration. The two main interactive methods are the Browser-Based Interface available through any standard Web-browser, and the Command-Line Interface (CLI) available from the console and through Telnet.

Although the BBI and CLI are both meant to provide the same level of function, they are not identical. The following CLI menus and commands are not available in the BBI at this time:

`/info/slb/sess`	Session table information menu
`/stats/port/link`	Show link stats
`/stats/port/rmon`	Show RMON stats
`/stats/port/maint`	Show maintenance stats
`/stats/slb/port/clear`	Clear port stats
`/stats/slb/url/maint`	Show URL SLB/Redir Maintenance stats
`/stats/slb/ssl`	Show SSL SLB stats
`/stats/slb/ftp`	Show FTP SLB parsing and NAT stats
`/stats/slb/clear`	Clear non-operational Server Load Balancing stats
`/stats/mp`	MP-specific Stats Menu
`/stats/fdb`	Show FDB stats
`/stats/route`	Show route stats

`/stats/arp`	Show ARP stats
`/cfg/sys/radius/telnet`	Enable/disable RADIUS backdoor for telnet
`/cfg/sys/ntp`	NTP Server Menu
`/cfg/sys/idle`	Set timeout for idle CLI sessions
`/cfg/sys/snmp`	Set SNMP access control
`/cfg/sys/wport`	Set Web server port number
`/cfg/sys/bannr`	Set login banner
`/cfg/sys/tnet`	Enable/disable Telnet access
`/cfg/sys/http`	Enable/disable HTTP (Web) access
`/cfg/sys/user`	User Access Control Menu (passwords)
`/cfg/ip/bgp`	Border Gateway Protocol menu
`/cfg/slb/adv/script`	Scriptable Health Check Menu
`/cfg/setup`	Step by step configuration set up
`/cfg/dump`	Dump current configuration to script file
`/oper/port/rmon`	Enable/Disable RMON for port
`/oper/mirr`	Operational Mirroring Menu
`/oper/slb/synch`	Synchronize SLB, FILT, and VRRP configuration on peers
`/oper/slb/clear`	Clear session table
`/oper/vrrp vrrp`	Operational Virtual Router Redundancy Menu
`/oper/maint/sys`	System Maintenance Menu
`/oper/main/debug`	Debugging Menu