# Release Notes:

## User's Guide

# Release 5.2

Alteon WebSystems
Web Speed for e-Business

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

Part Number: 050045, Revision D, October 1999

# Release Notes

These release notes provide the latest information regarding your WebOS switch software. This supplement covers new features and known issues for WebOS Release 5.2.21 (and above), and modifies information found in the complete documentation: *WebOS* Release 5.2 *User's Guide* (Part Number 050044, Revision B). Please keep this information with your Alteon WebSystems manuals.

The following list summarizes the topics covered in this document:

# VRRP: The New Switch Failover Method

Release 5.2 includes Virtual Router Redundancy Protocol (VRRP) for redundancy to routers within a LAN. In addition, Alteon WebSystems has extended VRRP to include virtual servers as well, allowing for full active/active redundancy between its Layer 4 switches. This allows for more efficient network resource allocation than the old hot-standby method. It also supports more complex failover topologies.

## VRRP Active/Active Replaces Hot-Standby for SLB

With the addition of VRRP, the hot-standby switch failover mode for Server Load Balancing has been removed. During the software upgrade process (see page 7), a switch configured with hot-standby failover will be converted to active/active failover, and VRRP will be automatically enabled.

## VRRP Active/Active Synchronization

The old hot-standby failover required the primary and secondary switches to have identical configurations and port topology. With VRRP and active/active failover, this is optional.

If desired, each switch can be configured individually with different port topology, Server Load Balancing, and filters.

If you would rather force two active/active switches to use identical settings, you can synchronize their configuration using the following command:

```
/oper/slb/sync IP_address
```

The `sync` command copies the following settings to the switch at the specified IP interface address:

- VRRP settings
- Server Load Balancing settings (including SLB port settings)
- Filter settings (including filter port settings)

If you perform the `sync` command, you should check the configuration on the target switch to ensure that the settings are correct.

**NOTE –** In WebOS version 5.2.21, the `sync` command also copies IP proxy settings to the target switch. This creates duplicate IP addresses on your network. To correct this problem, you must reconfigure each IP proxy on the target switch to use a unique IP address.

## VRRP, STP, and Failover Response Time

VRRP active/active failover is significantly different from the hot-standby failover method in previous releases. One important difference is that VRRP generally requires Spanning-Tree Protocol (STP) to be enabled in order to resolve bridge loops that usually occur in cross-redundant topologies like the one shown below.

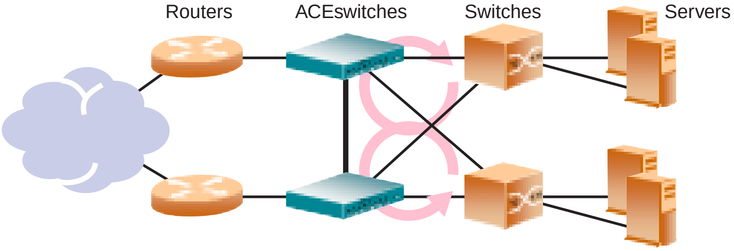

**Figure 1** Cross-redundancy creates loops, but STP resolves them

In this example, a number of loops are wired into the topology. STP resolves loops by blocking ports where looping is detected.

One drawback to using STP with VRRP is the failover response time. STP could take as long as 45 seconds to reestablish alternate routes after a switch or link failure.

When using VRRP in WebOS Release 5.2, you can decrease failover response time by using VLANs instead of STP to separate traffic into non-looping broadcast domains. For example:

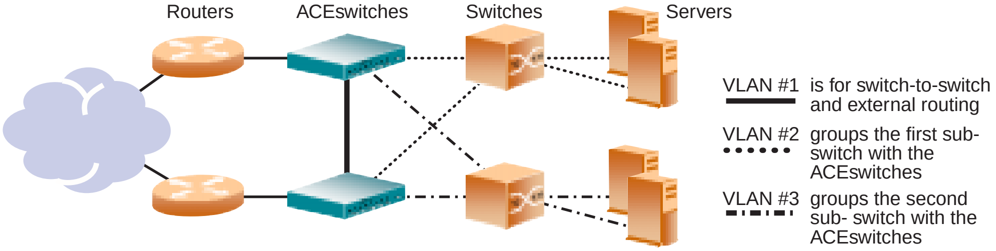
Routers
ACEswitches
Switches
Servers
VLAN #1
is for switch-to-switch and external routing
VLAN #2
groups the first sub-switch with the ACEswitches
VLAN #3
groups the second sub- switch with the ACEswitches

**Figure 2** VLANs can be used to create non-looping topologies.

The topology above allows STP to be disabled. On the ACEswitches, IP routing allows traffic to cross VLAN boundaries. The servers use the ACEswitches as default gateways. For port failure, traffic is rerouted to the alternate path within one health-check interval (configurable between 1 and 60 seconds, with a default of 2 seconds).

## VRRP Virtual Router ID Numbering

During the software upgrade process (see below), VRRP virtual router IDs will be automatically assigned if failover is enabled on the switch. When configuring VRRP virtual routers at any point after upgrade, virtual router ID numbers (`/cfg/vrrp/vr #/vrid`) must be assigned in accordance with the following restrictions:

- The virtual router ID may be configured as ***any number*** between 1 and 255 when the virtual router IP address is not assigned the same value as a virtual server IP address.
- The virtual router ID must be configured as an ***odd number*** between 1 and 255 under the following circumstance:
  - □ The virtual router uses Layer 4 services (its virtual router IP address is the same as assigned to a virtual server), *and*...
  - □ Layer 3 binding is turned on for the virtual server (by enabling the `layr3` option on the virtual server menu: `/cfg/slb/virt`)
- The virtual router ID must be configured as an ***even number*** between 2 and 254 under the following circumstance:
  - □ The virtual router uses Layer 4 services (its virtual router IP address is the same as assigned to a virtual server), *and*...
  - □ Layer 3 binding is turned off for the virtual server (by disabling the `layr3` option on the virtual server menu: `/cfg/slb/virt`)

# Upgrade Installation Notes

There are two major issues to consider when upgrading to WebOS Release 5.2:

- Before you can upgrade to WebOS Release 5.2, your switch must be running Release 4.0.42 (or above) with boot kernel version 5.0 (or above). The TFTP upgrade procedure below includes special steps for upgrading from older software.
- To prevent forwarding loops during VRRP failover conversion, STP must be enabled on both the active and standby switches. This is also covered in the TFTP procedure below.

There are two ways to upgrade switch software: TFTP software downloads which allow you to retain the switch configuration, or serial downloads which reset the configuration.

## TFTP Upgrade

Because TFTP software downloads retain the switch configuration throughout the upgrade process, this method is preferred when upgrading switch software.

**NOTE –** To avoid problems with configuration conversion during TFTP software download, please follow the procedure below carefully. Since some of the upgrade steps require resetting the switch, be sure to schedule appropriate network downtime for the upgrade process. Also, before upgrading the switch software, be sure to make a backup of the switch configuration.

1. **If failover is configured, turn Spanning-Tree Protocol (STP) on for both switches.**

   To prevent forwarding loops during failover conversion, STP must be enabled on both the active and standby switches. If failover is not configured, this step is not necessary and you may skip to step 3.

   If you're unsure whether switch failover is configured, use the `/info/slb` command to display failover information. For example:

   ```
   # /info/slb

   Failover state:
     primary   10.10.10.1,     up, STANDBY
     secondary 10.10.10.2,     up, ACTIVE (this switch)
   ...
   ```

   In the example above, we see that failover is configured and we must make sure that STP is on for both switches. If you're unsure about the status of STP, use the `/cfg/stp/cur` command to check.

For example:

```
# /cfg/stp/cur
------------------------------------------------------------------
Current operational Spanning Tree settings: globally turned OFF
...
```

In this example, we see that STP is globally turned off. Use the following commands to turn STP on, first on the standby switch, and then on the active switch. Both switches must be reset within 45 seconds of each other in order for STP to be properly resolved.

```
# /cfg/stp/on                         (Globally turn Spanning-Tree Protocol on)
>> Spanning Tree# save                (Save the configuration changes)
>> Spanning Tree# /boot/reset         (Reboot the switch with STP on)
```

**NOTE –** Turning STP on may increase the time required to reboot the switch. You can minimize reboot time by setting STP timer parameters to their lowest reasonable values before saving configuration parameters.

2. **If switch failover is configured, upgrade the software on the standby switch first.**

   If you're unsure which switch is in standby mode, use the `/info/slb` command to display failover information. For example:

```
# /info/slb

Failover state:
  primary   10.10.10.1,     up, ACTIVE
  secondary 10.10.10.2,     up, STANDBY (this switch)
...
```

   Here, we see that the secondary (10.10.10.2) switch is in failover standby mode and should be upgraded first. Follow steps 3 through 9 for the standby switch, then repeat the process for the active switch.

3. **If running ACElerate Release 4.0.41 (or below), upgrade to Release 4.0.50.**

   You can check the version level of your switch software by using the `/info/sys` command. If necessary, obtain the Release 4.0.50 software from your service agent and install it using the TFTP software download command (`/boot/tftp`). When prompted, specify **`image1`** as the software image to replace, then repeat the process for **`image2`**.

   The complete TFTP software download process is described in Chapter 9 of your *WebOS Release 5.2 User's Guide*.

4. **Make sure that the switch will boot using `image1`.**

   Issue the `/boot/image` command. Specify **`image1`** as the image to use upon next reset.

5. **Reboot the switch.**

   Use the `/boot/reset` command to reboot the switch.

6. **If running switch boot kernel 4.x (or below), upgrade to boot kernel 5.0 (or above).**

   The version of your switch boot code is displayed on the console when your switch first boots. If necessary, obtain the boot kernel 5.0 (or above) from your service agent and install it using the TFTP boot download command (`/boot/tftp`). When prompted, specify **`boot`** as the download target.

7. **Download WebOS Release 5.2.x to `image2` on your switch.**

   **NOTE –** Be sure to download Release 5.2.x into `image2` instead of `image1`.

   Use the TFTP download command (`/boot/tftp`) to install the Release 5.2.x software. Specify **`image2`** as the software image to be replaced.

8. **Make sure that the switch will boot using `image2`.**

   Issue the `/boot/image` command. Specify **`image2`** as the image to use upon next reset.

9. **Reboot the switch.**

   Use the `/boot/reset` command to reboot the switch with Release 5.2.

   If failover is configured on the switch, the following configuration conversions will be made when the switch reboots:

   - Virtual Router Redundancy Protocol (VRRP) will be enabled.
   - A VRRP virtual router will be configured for each virtual server to provide active/active redundancy. The virtual router IP address will be the same as the virtual server IP address.
   - The failover port will be reconfigured for Layer 4 client and server processing instead.

10. **After upgrading the standby switch of a failover pair, repeat the upgrade process (steps 3 through 9) for the active switch.**

    If failover is not configured on your switch, this step is not necessary.

## Direct Serial Upgrade

To upgrade directly to Release 5.2.x from any different switch software image, you can perform a serial download of the new switch software from the switch console port. However, this will reset the switch configuration back to its factory defaults.

The serial download procedure can be found in Chapter 18 of your *WebOS Release 5.2 User's Guide*.

**NOTE –** Serial download requires a software image designated specifically for serial download. The regular WebOs software files installed via TFTP are not compatible with the serial download method. Serial download of TFTP files will corrupt the switch software bank and require an additional serial download of the proper software.

## Down-Versioning to ACElerate Release 5.1.x or Prior

When moving from WebOS Release 5.2.x of the switch software back to Release 5.1.x or prior, the failover configuration will be lost and must be manually reconfigured or restored from a backup configuration dump.

# Other New Features

## UDP Stateless Load Balancing

A new UDP stateless option has been added to Server Load Balancing:

```
/cfg/slb/virt virtual_server_ID/udp UPD_port enable|disable|stateless
```

Normally, session time-out is governed using the real server time-out option (`/cfg/slb/real` *real_server_ID*`/tmout`) where the default is 10 minutes. When the `stateless` option is set, UDP sessions time-out immediately, ignoring the real server time-out value. This is useful for quick request/response traffic such as DNS and RADIUS where traffic flows are not required.

**NOTE –** When the `stateless` option is used, the switch does not record the current number of sessions. As a result, the `leastcons` Server Load Balancing metric (configured under the Real Server Group Menu) cannot be used. Instead, use `roundrobin`, `hash`, or `minmisses`.

## Persistent Mask for SLB

A new persistent mask option has been added to Server Load Balancing:

```
/cfg/slb/pmask IP_mask
```

Where *IP_mask* is an IP address mask in dotted decimal notation. The default value is 255.255.255.255 (off).

When a persistent mask is configured, all clients in the masked range will be load balanced to the same real server. This is useful in situations where client proxies are being used.

## GSLB Minimum Available Connections

A new minimum available connections option has been added to Global Server Load Balancing:

```
/cfg/slb/glsb/minco minimum_connections
```

Where *minimum_connections* is a value between 0 and 65535, with 0 as the default.

When a value is specified, remote global sites will stop redirecting (via HTTP) or handing-off (via DNS) clients to this site once the available connections on this site drops below the configured minimum.

## GSLB Real Server Name Redirection

A new real-name options has been added to Global Server Load Balancing:

```
/cfg/slb/gslb/usern enable|disable
```

When this option is enabled, the real server name and virtual server domain name are used in the HTTP redirect to remote sites. This option is cookie friendly. When disabled, the real server IP address is used instead and may not work with all cookies.

## Server Fragment Remap Disabling

A new fragment remap disable command has been added to Server Load Balancing:

```
/cfg/slb/virt virtual_server_ID/frag e|d
```

Specifying **d** disables remapping server fragments. The default is **e** (enabled). This option should be enabled when the switch is expected to load balance UDP applications that generate large UDP datagrams which are fragmented by the servers. When load balancing UDP applications that are generally unfragmented, such as DNS or RADIUS, this option should be disabled.

## 32-Bit Low/High Access to 64-Bit Counters

New SNMP MIB variables provide 32-bit access to 64-bit counters. All 64-bit counters now have equivalent 32-bit low and 32-bit high counters so that 32-bit SNMP applications can utilize them. These new counters are detailed within the MIB itself.

# Addendum, Errata, and Limitations

## Defining Host Names for Services

The following text clarifies material regarding host names that appears in your *WebOS Release 5.2 User's Guide* on pages 7-40, 17-10, and 17-14.

Host names can be assigned to services on virtual servers through the `hname` option on the Virtual Server Configuration Menu (`/cfg/slb/virt`). Host names are used in conjunction with the domain name (also assigned through the Virtual Server Configuration Menu) and provide support to the Global Server Load Balancing (GSLB) system.

For each virtual server, any particular host name can be assigned to only one service. If multiple services under the same virtual server require the same host name (for example "www" for both HTTP and HTTPS services), the host name in question should be defined for only one of those services, and the host name for the other should be left blank. Leaving duplicate host names blank does not harm the efficiency of the GSLB system.

**NOTE –** If you try to configure duplicate host names for any particular virtual server, the switch will not allow you to apply your configuration changes until the duplicate entries are cleared. You can clear a host name by defining it as "`none`".

## Health Checking in Large Server Farms

By default, health checking for each real server is performed every two seconds. When a very large number of real servers (over 250) is connected to the switch, attempting health checks on each real server every two seconds can degrade performance and health checking accuracy. If this becomes a problem, you can increase the time between health checks in order to gain system performance.

The following command is used for changing the health checking interval:

```
    /cfg/slb/real real_server_ID/intr time_interval
```

Where *time_interval* is an integer between 1 and 60 seconds. In large server farms, the recommended value is at least 10 seconds.

## Changing Filters in an Active Configuration

If when assigning a new filter to a switch port, the new filter has a higher order of precedence than filters currently firing on the port (the filter number of the new filter is lower than the filter number of existing filters), the new filter will not take effect until the binding table for the switch port is cleared. You can clear the binding table for a given switch port with the following command:

```
/oper/slb/clear port_number
```

**NOTE –** This command also clears all sessions cached on the specified port.

## Restrictions on Direct Access Mode

Direct Access Mode imposes the following restrictions:

- Topology: All frames coming back through the switch server port must egress the switch via the same client port where they were originally received. When DAM is enabled, it can create problems in address re-mapping for networks that have more than one active ingress router.
- VRRP sharing should be disabled.

## Remote Gateways Are Not Supported

When setting default gateways on the switch, the gateway device must be on the same IP subnet as one of the switch’s IP interfaces. The WebOS switch software does not support default gateways that must be reached remotely through an intermediate router.

## Port Trunking with Cisco 3.2.2 Not Supported

When STP is enabled on your WebOS switch, port trunking between the switch and a Cisco Catalyst with version 3.3.2 software is not supported.

## TFTP Software Downloads to Active Image

When performing software upgrades using the `/boot/tftp` command, you should not replace the active software image. If booting from `image1`, replace `image2`. Alternately, if you wish to replace `image1`, first boot using `image2`.

Use the `/boot/image` command to change the image from which you wish to boot, and use the `/boot/reset` command to reboot the switch using the specified software image.

## Serial Download of Non-Serial Software

Serial download requires a software image designated specifically for serial download. The regular WebOs software files installed via TFTP are not compatible with the serial download method. Serial download of TFTP files will corrupt the switch software bank and require an additional serial download of the proper software.

## Listing of Known Bugs and Fixes

Up-to-date information about the status of known software bugs, fixes, and work-arounds for each release of the WebOS switch software is available online. The following URL leads to our main webpage:

`http://www.alteon.com`

Follow the “Support” link to the “Field Notices,” where you will find the “Known Bug List.”

This information is available as part of your support contract and will require you to enter your support access name and password.

# Late-Breaking News and Support

Web access: `http://www.alteon.com`

Questions? Check the URL for Alteon WebSystems. This website includes product information, software updates, release notes, and white papers. The website also includes access to Alteon WebSystems Customer Support for accounts under warranty or that are covered by a maintenance contract.