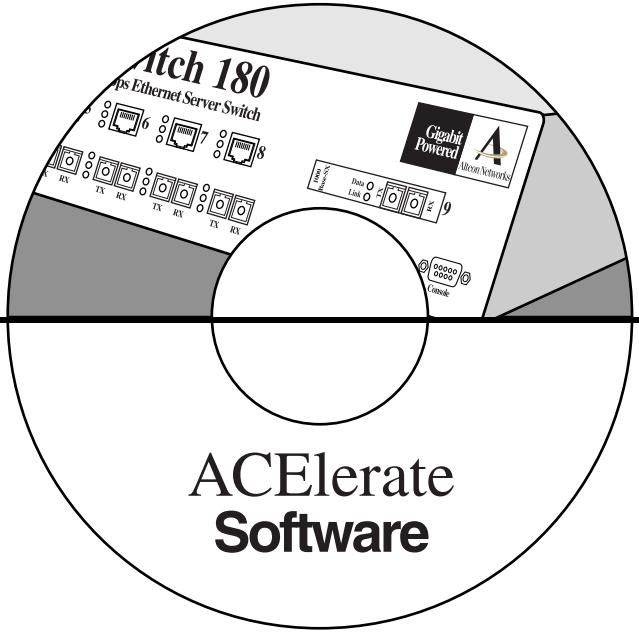
RELEASE NOTES:
User's Guide



Release 5.1

AlteonWebSystems
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 B, April 1999

Release Notes

These release notes provide the latest information regarding your ACElerate switch software. This supplement covers new features, bug fixes, and known issues for ACElerate Release 5.1.23 (and above), and modifies information found in the complete documentation: *ACElerate Switch Software User's Guide* for Release 5 (Part Number 050044, Revision A). Please keep this information with your Alteon WebSystems manuals.

Upgrade Installation Notes

There are two ways to upgrade switch software: TFTP software downloads which retains the switch configuration, and serial download which can be quicker but resets the configuration.

TFTP Upgrade

TFTP software download is the preferred method for upgrading your switch software. However, before you can upgrade to Release 5.1.23, your switch must be running Release 4.0.42 (or above) with boot kernel version 5.0 (or above). Here is the basic upgrade path:

1. **If running Release 4.0.41 or below, you must first upgrade to Release 4.0.42.**

   You can check the version level of your switch software by using the `/info/sys` command. If necessary, obtain the Release 4.0.42 software from your service agent and install it using the TFTP software download command (`/boot/tftp`).

2. **If running any Release 4.x software, you must upgrade to the version 5.0 (or above) boot kernel.**

   Once running version 4.0.42 (or above), the version of your switch boot code is displayed on the console when your switch first boots. If necessary, obtain the version 5.0 (or above) boot kernel from your service agent and install it using the TFTP boot download command (`/boot/tftp`).

3. **Once running Release 4.0.42 (or above) with the version 5.0 boot kernel, you can perform a TFTP software download of Release 5.1.23.**

   The TFTP software download process is described on page 9-2 of your *ACElerate Switch Software User's Guide* for Release 5.

Direct Serial Upgrade

To upgrade to Release 5.1.23 directly from any different image, you can perform a serial download of the new switch software. However, serial download will reset the switch configuration back to its factory defaults. The serial download procedure can be found on page 18-4 or your *ACElerate Switch Software User's Guide* for Release 5.

New Features & Enhancements

The following new features are covered in these release notes:

Command-Line History and Editing

Using the command-line interface has been made easier. You can retrieve and modify previously entered commands with just a few keystrokes. The following options are now available globally at the command line:

Table 1 Command-Line History and Editing Options

Option	Description
`history`	Display a numbered list of the last 10 previously entered commands.
`!!`	Repeat the last entered command.
`!`*n*	Repeat the *n*th command shown on the history list.
<Ctrl-p>	(Also the up arrow key.) Recall the *previous* command from the history list. This can be used multiple times to work backward through the last 10 commands. The recalled command can be entered as is, or edited using the options below.
<Ctrl-n>	(Also the down arrow key.) Recall the *next* command from the history list. This can be used multiple times to work forward through the last 10 commands. The recalled command can be entered as is, or edited using the options below.
<Ctrl-a>	Move the cursor to the beginning of command line.
<Ctrl-e>	Move cursor to the *end* of the command line.
<Ctrl-b>	(Also the left arrow key.) Move the cursor *back* one position to the left.
<Ctrl-f>	(Also the right arrow key.) Move the cursor *forward* one position to the right.
<Backspace>	Erase one character to the left of the cursor position.
<Ctrl-d>	(Also the Delete key.) *Delete* one character at the cursor position.
<Ctrl-k>	*Kill* (erase) all characters from the cursor position to the end of the command line.
<Ctrl-u>	Clear the entire line.
Other keys	Insert new characters at the cursor position.

Layer 4 Topology Restrictions Removed

The ACEvision Layer 4 Switching Port Configuration page and the command-line interface Server Load Balancing Port Menu (`/cfg/slb/port`) have been updated. They no longer require switch ports to be configured exclusively for one type of Layer 4 processing (client, server, or redirection). The `state` option, where the port processing type was defined, has been removed. In its place, new options allow you to enable or disable processing independently for each type of Layer 4 traffic, expanding your topology options.

To simplify configuration further, the redirection state has been removed. Instead, the function is automatically enabled when a filter with the `redir` action is applied on the port (see the Filtering sections of your *ACElerate Switch Software User's Guide*).

One topology restriction remains: Ports enabled for failover processing cannot be enabled for processing client or server traffic.

The new Server Load Balancing Port Menu (`/cfg/slb/port`) follows, with new commands shown in bold type:

```
[SLB port Menu]
        clien - Enable/disable client processing
        servr - Enable/disable server processing
        failv - Enable/disable failover processing
        pip   - Set Proxy IP address for port
        filt  - Enable/disable filtering
        add   - Add filter to port
        rem   - Remove filter from port
        cur   - Display current port configuration

>> SLB port#
```

Example: Consider the following network topology:

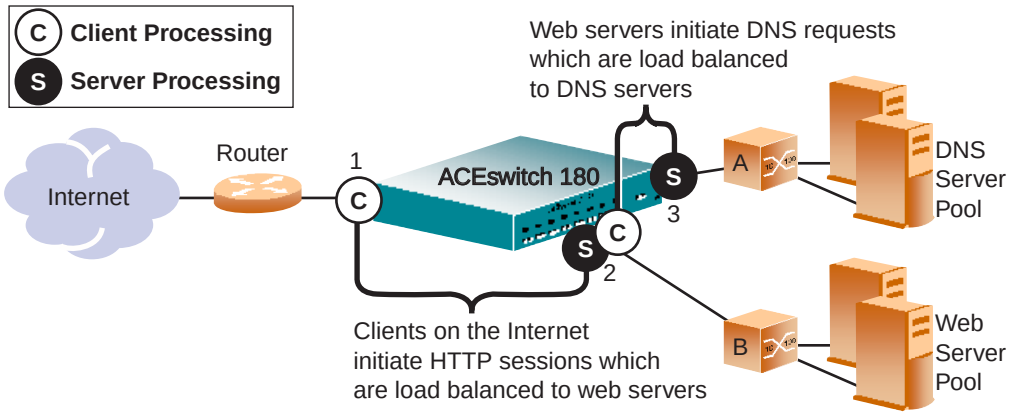


Figure 1 Example Network for Client/Server Port Configuration

In this example, the switch load balances Internet HTTP requests to the web server pool, and web server DNS requests to the DNS server pool. Layer 4 client processing is needed on port 1 and port 2 where HTTP and DNS service requests originate, and Layer 4 server processing is needed on port 2 and port 3 where server load balancing occurs. In this case, port 2 is asked to perform both server *and* client processing.

Under previous switch software releases, this example topology would be invalid since Layer 4 client and server processing could not both occur on the same switch port. As of Release 5.1, this restriction is removed and the port topology could be configured as follows:

```
>> # /cfg/slb/port 1                 (Select the port for Internet traffic)
>> SLB port 1# clien ena             (Enable client processing on the port)
>> SLB port 1# ../port 2             (Select the port for the web server pool)
>> SLB port 2# clien ena             (Enable client processing on the port)
>> SLB port 2# servr ena             (Enable server processing on the port)
>> SLB port 2# ../port 3             (Select the port for the DNS server pool)
>> SLB port 3# servr ena             (Enable server processing on the port)
>> SLB port 3# apply                 (Apply the configuration changes)
>> SLB port 3# save                  (Save the configuration changes)
```

NOTE – Only the Server Load Balancing switch port configuration has changed. All other switch configuration for this example remains the same, as covered in your *ACElerate Switch Software User's Guide.*

Some topologies require special configuration. For example, if clients were added to switch "B" in the example above, these clients could not access the web server pool using Layer 4 services except through a proxy IP address configured on port 2 of the ACEswitch 180.

Improved Switch Management Security

A new feature has been added which allows you to limit access to the switch's Management Processor without having to configure filters for each switch port. You can set a source IP address (or range) that will be allowed to connect to the switch IP interface through Telnet, SNMP, or the ACEvision web-interface. This will also help prevent spoofing or attacks on the switch's TCP/IP stack.

The allowed management IP address range is configured using the system `mnet` and `mmask` options available on the command-line interface System Menu (`/cfg/sys`) as shown in bold type below:

```
[System Menu]
        date  - Set system date
        time  - Set system time
        usrpw - Set user password
        admpw - Set administrator password
        idle  - Set timeout for idle CLI sessions
        bootp - Enable/disable use of BOOTP
        http  - Enable/disable HTTP (Web) access
        wport - Set Web server port number
        mnet  - Set management network
        mmask - Set management netmask
        cur   - Display current system-wide parameters

>> System#
```

Table 1 New System Menu Commands (/cfg/sys)

Option	Description
`mnet`	Sets the base source IP address allowed to access switch management through Telnet, SNMP, RIP, or the ACEvision web interface. A range of IP addresses is produced when used with `mmask` (below). Specify an IP address in dotted-decimal notation.
`mmask`	This IP address mask is used with `mnet` to set a range of source IP addresses allowed access to switch management functions. Specify the mask in dotted-decimal notation.

NOTE – These management security commands are found on the `/cfg/sys` menu. The `mnet` and `mmask` commands in the `/cfg/slb` menu are used for a different purpose.

When an IP packet reaches the Management Processor, the source IP address is checked against the range of addresses defined by `mnet` and `mmask`. If the source address of the host or hosts are within this range, then they are allowed to attempt to log in. Any packet addressed to a switch IP interface with a source IP address outside this range is discarded silently.

Example: Assume that the `mnet` is set to 192.192.192.0, and the `mmask` is set to 255.255.255.128. This defines the following range of IP addresses: 192.192.192.0 to 192.192.192.127.

- A host with a source IP address of 192.192.192.21 falls within the defined range and would be allowed to access the switch Management Processor.
- A host with a source IP address of 192.192.192.192 falls outside the defined range and is not granted access. To make this source IP address valid, you would need to shift the host to an IP address within the valid range specified by the `mnet` and `mmask`, or modify the `mnet` to be 192.192.192.128 and the `mmask` to be 255.255.255.128. This would put the 192.192.192.192 host within the valid range allowed by the `mnet` and `mmask` (192.192.192.128-255).

NOTE – When the `mnet` and `mmask` Management Processor filter is applied, RIP updates received by the switch will be discarded if the source IP address of the RIP packet(s) falls outside the specified range. This can be corrected by configuring static routes.

Layer 4 Administrator Account

Once you are connected to the switch via local console or Telnet, you are prompted to enter a password to access one of three accounts. In addition to the standard user and administrator accounts, a new account for Layer 4 switch administration is now available.

The Layer 4 administrator has limited access to the switch. He or she can view all switch information and statistics, but can make configuration changes only on the Server Load Balancing menus. The default password for the Layer 4 administrator account is `l4admin`.

It is recommended that you change switch passwords after initial configuration and as regularly as required under your network security policies.

Changing the Default Layer 4 Administrator Password

The default password for the Layer 4 administrator account is `l4admin`. To change the default password, follow this procedure:

1. **Connect to the switch and log in using the administrator account.**

   To change any switch password, you must login using the administrator password. Passwords cannot be modified from the Layer 4 administrator account or the user account.

2. **From the Main Menu, use the following command to access the System Menu:**

```
Main# /cfg/sys
```

The System Menu is displayed.

```
[System Menu]
        date  - Set system date
        time  - Set system time
        usrpw - Set user password
        admpw - Set administrator password
        l4apw - Set L4 administrator password
        idle  - Set timeout for idle CLI sessions
        tnet  - Enable/disable Telnet access
        bootp - Enable/disable use of BOOTP
        http  - Enable/disable HTTP (Web) access
        wport - Set Web server port number
        bannr - Set login banner
        mnet  - Set management network
        mmask - Set management netmask
        cur   - Display current system-wide parameters
>> System#
```

3. **Select the Layer 4 administrator password:**

```
System# l4apw
```

4. **Enter the current *administrator* password (not the Layer 4 administrator password) at the prompt:**

```
Changing L4 ADMINISTRATOR password; validation required...
Enter current administrator password:
```

NOTE – If you forget your administrator password, call your technical support representative for help using the password fix-up mode.

---

5. **Enter the new Layer 4 administrator password at the prompt:**

```
Enter new L4 administrator password:
```

6. **Enter the new administrator password, again, at the prompt:**

```
Re-enter new L4 administrator password:
```

7. **Apply and save your change by entering the following commands:**

```
System# apply
System# save
```

Enhanced Filter Logs

For additional troubleshooting and session inspection capability, packet source and destination IP addresses are now included in the filter log messages. Log messages are generated when a Layer 3/Layer 4 filter is triggered and has logging enabled. The messages are output to the console port, system host log (`syslog`), and the ACEvision message window.

Example: A network administrator has noticed a significant number of ICMP frames on one portion of the network, and wants to determine the specific sources of the ICMP messages. The administrator uses the command-line interface to create and apply the following filter:

```
>> # /cfg/slb/filt 15                (Select filter 15)
>> Filter 15# sip any                 (From any source IP address)
>> Filter 15# dip any                 (To any destination IP address)
>> Filter 15# proto icmp              (For the ICMP protocol)
>> Filter 15# log enabled             (Create a log entry when matched)
>> Filter 15# ena                     (Enable the filter)
>> Filter 15# /cfg/slb/port 7         (Select a port to filter)
>> SLB port 7# add 15                 (Add the filter to the port)
>> SLB port 7# filt ena               (Enable filtering on the port)
>> SLB port 7# apply                  (Apply the configuration changes)
>> SLB port 7# save                   (Save the configuration changes)
```

When applied to one or more switch ports, this simple filter rule will produce log messages that show when the filter is triggered, and what the IP source and destination addresses were for the ICMP frames traversing those ports.

Below is an example of the filter log message output, showing the filter number, port, source IP address, and destination IP address:

```
slb: filter 15 fired on port 7, 206.118.93.110 -> 20.10.1.10
```

High-Water Mark for Real Server Statistics

For more useful Server Load Balancing performance feedback, a new measurement has been added to the real server statistics. The new statistic appears in ACEvision and the command-line interface. It shows the highest number of simultaneous sessions recorded for each server. This statistic is a high-water mark, meaning that it is updated only when the current number of sessions bound to a server exceeds the previous record.

Example: The command-line interface real server statistics (`/stats/slb/real`) show the highest number of sessions bound to the real server IP address, as shown in bold type below:

```
>> /stats/slb/real 1
------------------------------------------------------------------
Real server 1 stats:
Current sessions:                34223
Total sessions:                64342344
Highest sessions:                43433
Octets:                     1546993843
Health check failures:                0
```

SLB Server Octet Counters

To provide additional information for Server Load Balancing tuning and accounting purposes, real server transmit/receive octet counters have been added to the Server Load Balancing statistics in ACEvision and the command-line interface. These new statistics are found anywhere the real server “current sessions” and “total sessions” are displayed.

Example:

```
>> # /stats/slb/virt 1
Virtual server 1 stats:
Real IP address      Current Sessions  Total Sessions         Octets
---- --------------- ----------------  --------------- -------------
   1 205.178.13.223              0            4031             93223
  10 20.10.1.100                44         6126090        30549746705
  13 20.10.2.100                46         6312397        10685250903
---- --------------- ----------------  --------------- -------------
  v1 20.10.1.10                 90        12442518        41236090831

>> Server Load Balancing Statistics#
```

For each load-balanced real server, the octet counter represents the combined number of transmit and receive frames. These counters are then added to report the total octets for each virtual server.

Per-Service Octet Counters

The octet counters are provided per server–not per service. If you need octet counters on a per-service basis, you can accomplish this through the following configuration:

1. **Configure a separate IP address for each service on each server being load balanced.**

   For instance, you can configure IP address 10.1.1.20 for HTTP services, and 10.1.1.21 for FTP services on the same physical server.

2. **On the switch, configure a real server with a real IP address for each service above.**

   Continuing the example above, two real servers would be configured for the physical server (representing each real service). If there were five physical servers providing the two services (HTTP and FTP), 10 real servers would have to be configured: five for the HTTP services on each physical server, and five for the FTP services on each physical server.

3. **On the switch, configure one real server group for each type of service, and group each appropriate real server IP address into the group that handles the specific service.**

   Thus, in keeping with our example, two groups would be configured: one for handling HTTP and one for handling FTP.

4. **Configure a virtual server for each server group and service.**

Information and Statistics Dumps

To help you gather data for tuning and debugging switch performance, two new dump commands have been added:

Command	Description
`/info/dump`	Dumps all switch information available from the Information Menu (10K or more, depending on your configuration).
`/stats/dump`	Dumps all switch statistics available from the Statistics Menu (40K or more, depending on your configuration).

If you want to capture dump data to a file, set your communication software on your workstation to capture session data prior to issuing the dump commands.

TCP ACK Matching for Filters

To provide greater filtering flexibility, the `ack` filter criteria has been added. The new criteria appears in the ACEvision web interface, and in the command line interface on the Filter Menu (`/cfg/slb/filt`) as shown in bold below:

```
[Filter 1 Menu]
        sip   - Set source IP address
        smask - Set source IP mask
        dip   - Set destination IP address
        dmask - Set destination IP mask
        proto - Set IP protocol
        sport - Set source TCP/UDP port or range
        dport - Set destination TCP/UDP port or range
        actio - Set action
        group - Set real server group for redirection
        rport - Set real server port for redirection
        proxy - Enable/disable client proxy
        inver - Enable/disable filter inversion
        ack   - Enable/disable TCP ack matching
        nat   - Set which addresses are network address translated
        cache - Enable/disable caching sessions that match filter
        log   - Enable/disable logging
        ena   - Enable filter
        dis   - Disable filter
        del   - Delete filter
        cur   - Display current filter configuration

>> Filter 1#
```

When `ack` is enabled, the filter matches only those frames set with the `TCP ACK` or `RST` flag.

Example: Consider the following network:

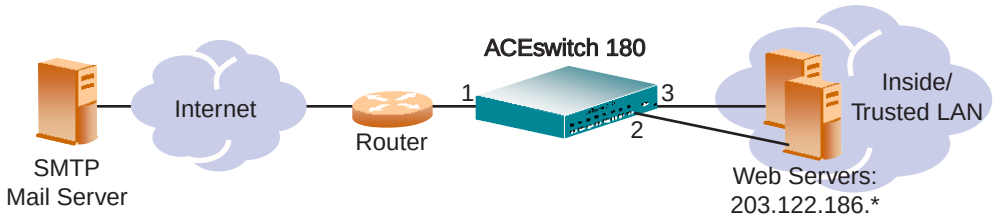


Figure 2 Example Filter TCP ACK Matching Network

In this network, the web servers inside the LAN must be able to transfer mail to any SMTP-based mail server out on the Internet. At the same time, we wish to prevent access to the LAN from the Internet, except for HTTP.

SMTP traffic uses well-known TCP port 25. The web servers will originate TCP sessions to the SMTP server using destination TCP port 25, and the SMTP server will acknowledge each TCP session and data transfer using source TCP port 25.

Filtering with the ACK flag closes one potential security hole. Without it, the switch would permit a TCP SYN connection request to reach any listening destination TCP port on the web servers inside the LAN, as long as it originated from TCP source port 25. The server would listen to the TCP SYN, allocate buffer space for the connection, and reply to the connect request. In some SYN attack scenarios, this could cause the server's buffer space to fill, crashing the server or at least making it unavailable.

This filter with the ACK flag requirement prevents external servers from beginning a TCP connection (with a TCP SYN) from source TCP port 25. The server will drop any frames that have the ACK flag "spoofed" in them, and will not allocate space for a new connection.

The following filters are required:

1. **One filter must allow the web servers to pass SMTP requests to the Internet.**

```
>> # /cfg/slb/filt 10                (Select a filter for trusted SMTP requests)
>> Filter 10# sip 203.122.186.0      (From the web servers' source IP address)
>> Filter 10# smask 255.255.255.0    (For the entire subnet range)
>> Filter 10# sport any              (From any source port)
>> Filter 10# proto tcp              (For TCP traffic)
>> Filter 10# dip any                (To any destination IP address)
>> Filter 10# dport smtp             (To well-known destination SMTP port)
>> Filter 10# actio allow            (Allow matching traffic to pass)
>> Filter 10# ena                    (Enable the filter)
```

2. **One filter must allow SMTP traffic from the Internet to pass through the switch *only* if the destination is one of the web servers and the frame is an acknowledgment (ACK) of a TCP session.**

```
>> Filter 10# ../filt 15             (Select a filter for Internet SMTP ACKs)
>> Filter 15# sip any                (From any source IP address)
>> Filter 15# sport smtp             (From well-known source SMTP port)
>> Filter 15# proto tcp              (For TCP traffic)
>> Filter 15# ack ena                (For acknowledgments only)
>> Filter 15# dip 203.122.186.0      (To the web servers' IP address)
>> Filter 15# dmask 255.255.255.0    (To the entire subnet range)
>> Filter 15# dport any              (To any destination port)
>> Filter 15# actio allow            (Allow matching traffic to pass)
>> Filter 15# ena                    (Enable the filter)
```

3. **One filter must allow trusted HTTP traffic from the Internet to pass through the switch to the web servers.**

```
>> Filter 15# ../filt 16                (Select a filter for incoming HTTP traffic)
>> Filter 16# sip any                   (From any source IP address)
>> Filter 16# sport http                (From well-known source HTTP port)
>> Filter 16# proto tcp                 (For TCP traffic)
>> Filter 16# dip 203.122.186.0         (To the web servers' IP address)
>> Filter 16# dmask 255.255.255.0       (To the entire subnet range)
>> Filter 15# dport http                (To well-known destination HTTP port)
>> Filter 16# actio allow               (Allow matching traffic to pass)
>> Filter 16# ena                       (Enable the filter)
```

4. **One filter must allow HTTP responses from the web servers to pass through the switch to the Internet.**

```
>> Filter 16# ../filt 17                (Select a filter for outgoing HTTP traffic)
>> Filter 17# sip 203.122.186.0         (From the web servers' source IP address)
>> Filter 17# smask 255.255.255.0       (From the entire subnet range)
>> Filter 17# sport http                (From well-known source HTTP port)
>> Filter 17# proto tcp                 (For TCP traffic)
>> Filter 17# dip any                   (To any destination IP address)
>> Filter 17# dport http                (To well-known destination HTTP port)
>> Filter 17# actio allow               (Allow matching traffic to pass)
>> Filter 17# ena                       (Enable the filter)
```

5. **One default filter is required to deny everything else:**

```
>> Filter 17# ../filt 224               (Select a default filter)
>> Filter 220# sip any                  (From any source IP address)
>> Filter 220# dip any                  (To any destination IP address)
>> Filter 220# actio deny               (Block matching traffic)
>> Filter 220# ena                      (Enable the filter)
```

6. **Next, the filters must be applied to the appropriate switch ports.**

```
>> Filter 220# ../port 1          (Select the Internet-side port)
>> SLB port 1# add 15             (Add the SMTP ACK filter to the port)
>> SLB port 1# add 16             (Add the incoming HTTPS filter)
>> SLB port 1# add 224            (Add the default filter to the port)
>> SLB port 1# filt ena           (Enable filtering on the port)
>> SLB port 1# ../port 2          (Select the first web server port)
>> SLB port 2# add 10             (Add the outgoing SMTP filter to the port)
>> SLB port 2# add 17             (Add the outgoing HTTP filter to the port)
>> SLB port 2# add 224            (Add the default filter to the port)
>> SLB port 2# filt ena           (Enable filtering on the port)
>> SLB port 2# ../port 3          (Select the other web server port)
>> SLB port 3# add 10             (Add the outgoing SMTP filter to the port)
>> SLB port 3# add 17             (Add the outgoing HTTP filter to the port)
>> SLB port 3# add 224            (Add the default filter to the port)
>> SLB port 3# filt ena           (Enable filtering on the port)
>> SLB port 3# apply              (Apply the configuration changes)
>> SLB port 3# save               (Save the configuration changes)
```

Hostname for HTTP Content Health Checks

HTTP-based health checks can now include hostname for `HOST:` headers. The `HOST:` header and health check URL are constructed from the following components:

Item	Option	Configured Under	Maximum Length
Virtual server hostname	`hname`	`/cfg/slb/virt`	9 characters
Domain name	`dname`	`/cfg/slb/virt`	34 characters
Server group health check field	`cntnt`	`/cfg/slb/group`	31 characters

If the `HOST:` header is required, an `HTTP/1.1 GET` will occur, otherwise an `HTTP/1.0 GET` will occur.

Example 1:

```
hname   = compute
dname   = alteon.com
cntnt   = index.html
```

Health check is performed using:

```
GET /index.html HTTP/1.1
Host: compute.alteon.com
```

Example 2:

```
hname   = (none)
dname   = raleighduram.cityguru.com
cntnt   = /page/gen/?_template=alteon
```

Health check is performed using:

```
GET /page/gen/?_template=alteon HTTP/1.1
Host: raleighduram.cityguru.com
```

Example 3:

```
hname   = (none)
dname   = compute
cntnt   = index.html
```

Health check is performed using:

```
GET /index.html HTTP/1.1
Host: compute
```

Example 4:

```
hname   = (none)
dname   = (none)
cntnt   = index.html
```

Health check is performed using:

`GET /index.html HTTP/1.0` (since no `HTTP HOST:` header is required)

Example 5:

```
hname   = (none)
dname   = (none)
cntnt   = //compute/index.html
```

Health check is performed using:

```
GET /index.html HTTP/1.1
Host: compute
```

DSLB Local Site Preference

For Distributed Server Load Balancing, a new feature has been added which allows the switch to always respond to DNS queries with a local virtual IP address. This feature is found in the ACEvision web interface, and in the command-line interface on the Distributed SLB Menu (`/cfg/slb/dist`) as shown in bold below:

```
[Distributed SLB Menu]
      site  - Remote Site menu
      dns   - Enable/disable DNS handoffs
      ttl   - Set Time To Live of DNS resource records
      local - Enable/disable DNS responses with only local addresses
      http  - Enable/disable HTTP redirects
      intr  - Set interval between remote site updates
      on    - Globally turn Distributed SLB ON
      off   - Globally turn Distributed SLB OFF
      cur   - Display current distributed SLB configuration
```

When enabled, the switch will always respond to DNS queries by providing a local virtual IP address as long as the virtual IP address has healthy real servers with an aggregate of at least 1024 available connections (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 IP addresses are unavailable or saturated, the switch will respond to DNS requests using normal DSLB rules.

Increased Granularity of DNS TTL

For Distributed Server Load Balancing (DSLB), the Domain Name System time-to-live (DNS TTL) value controls how long the switch's DNS response (indicating site of best service) remains in the DNS servers' caches. The granularity of the DNS TTL value (configured from ACEvision or the command-line interface Distributed Server Load Balancing Menu) has been increased to allow settings from 0-65535 seconds. The default is 60 seconds.

This value can be set from the switch command-line interface as follows:

```
>> # /cfg/slb/dist                      (select DSLB configuration menu)
>> Distributed SLB menu# ttl 120        (set DNS time-to-live to 120 seconds)
```

A lower value may increase the ability of the DSLB 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 DSLB's response to sudden traffic changes.

TFTP Configuration Put and Get

New commands allow you to `put` (save) or `get` (load) the active switch configuration via TFTP. These commands appear on the ACEvision Switch Image and Configuration Management page, and in the command-line interface Configuration Menu (`/cfg`) as shown in bold type below:

```
[Configuration Menu]
        sys   - System-wide parameter menu
        port  - Port configuration menu
        ip    - IP configuration menu
        vlan  - VLAN configuration menu
        stp   - Spanning Tree menu
        snmp  - SNMP menu
        setup - Step by step configuration set up
        dump  - Dump current configuration to script file
        ptcfg - Backup current configuration to tftp server
        gtcfg - Restore current configuration from tftp server
        mirr  - Mirroring menu
        slb   - Server Load Balancing configuration menu
        trunk - Trunk Group configuration menu

>> Configuration#
```

Saving the Active Switch Configuration via TFTP

The format for this command is as follows:

`ptcfg` *server filename*

Where *server* is the TFTP server IP address or hostname, and *filename* is the name of the target configuration file.

When the command is used, the switch's active configuration commands (as displayed using `/cfg/dump`) will be uploaded to the specified configuration file on the TFTP server.

NOTE – The specified `ptcfg` file must exist *prior* to executing the `ptcfg` command, and must be writable (set with proper permission, and not locked by any application). The contents of the specified file will be replaced with the current configuration data.

Loading the Active Switch Configuration via TFTP

The format for this command is as follows:

`gtcfg` *server filename*

Where *server* is the TFTP server IP address or hostname, and *filename* is the name of the target configuration file.

When the command is used, the active configuration will be replaced with the commands in the specified configuration file. The file can contain a full or partial switch configuration.

NOTE – The configuration loaded using `gtcfg` is not activated until the `apply` command is used. If the `apply` command is found in the configuration file loaded using this command, the apply action will be performed automatically.

TFTP System Dump Put

A new command allows you to `put` (save) the system dump via TFTP. The new command is found on the ACEvision Switch Image and Configuration Management page and in the command-line interface Maintenance Menu (`/maint`) as shown in bold type below:

```
[Maintenance Menu]
        uudmp - Uuencode FLASH dump
        ptdmp - tftp put FLASH dump to tftpserver
        cldmp - Clear FLASH dump
        panic - Dump state information to FLASH and reboot
        sys   - System Maintenance Menu
        fdb   - Forwarding Database Manipulation Menu
        debug - Debugging Menu
        arp   - ARP Cache Manipulation Menu
        route - IP Route Manipulation Menu

>> Maintenance#
```

The format for this command is as follows:

`ptdmp` *server filename*

Where *server* is the TFTP server IP address or hostname, and *filename* is the target dump file.

NOTE – The specified `ptdmp` file must exist *prior* to executing the `ptdmp` command, and must be writable (set with proper permission, and not locked by any application). The contents of the specified file will be replaced with the current dump data.

Resolved Issues

Following is a list of performance issues and bugs resolved since ACElerate Release 5.0.24:

- Load balancing of pop3 mail servers now works when using NAT with a virtual IP address. E-mail larger than 4K now downloads properly.
- A switch login prompt no longer appears unexpectedly at a client when that client session is NATed to the virtual IP address.
- SNMP query of `ipNetToMediaTable` no longer causes real server health checks to fail.
- SNMP trap host community string is now correctly set.
- Nestea/Nestea2 attacks on the switch using UDP fragments no longer cause switch resets.
- Setting a null string in certain SNMP fields (such as `AgNewTrapHostCommString`) no longer causes switch to reset.

Known Issues

Order of Precedence for Layer 4 Services

When Server Load Balancing and Application Redirection are both configured for the same TCP/UDP port on the same physical switch port, all traffic addressed to a virtual server will be redirected rather than load balanced.

To allow traffic addressed to a virtual server to be load balanced, add a filter before the redirection filter (that is, one with a lower filter number) which is configured to allow traffic addressed to the virtual server.

Incomplete Log Messages

Under some conditions where the switch experiences high levels of Layer 4 traffic, the console might display incomplete syslog messages. This is merely cosmetic.

Down-versioning to Release 5.0.x

When moving from Release 5.1.x back to a previous Release 5.0.x version of the switch software, Server Load Balancing port state configuration will be lost.

To correct this, note the Layer 4 services enabled on each port while the Release 5.1.x software is loaded. You can use the `/cfg/slb/port` *x*`/cur` command to collect port configuration information. Then, after loading and booting the switch with Release 5.0.x software, manually reconfigure the port state options for each port using the `/cfg/slb/port` *x*`/state` command.

Viewing Large Lists with ACEvision

ACEvision provides a convenient means for viewing switch configuration information and statistics in most web browsers. When using ACEvision to display information for switches with lengthy lists (such as configured filters or real servers), some web browsers may have difficulty due to the large number of web pages that are sent from the switch. If your browser has difficulty with long ACEvision lists, use the command-line interface instead.

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.