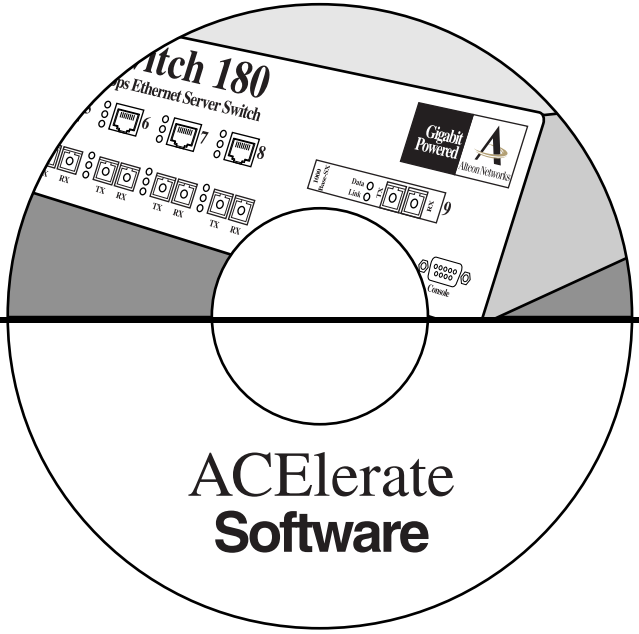
RELEASE NOTES:
User's Guide



Release 5

Alteon Networks
THE SERVER SWITCHING COMPANY
50 Great Oaks Boulevard
San Jose, California 95119
408-360-5500 Main
408-360-5501 Fax
www.alteon-networks.com

Part Number: 050045, Revision A
February 1999

Release Notes

These release notes provide the latest information regarding your ACElereate Switch Software. This supplement covers new features, bug fixes, and known issues for ACElereate Release 5.0.35 (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 Networks manuals.

New Features

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) which 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 `mnet` and `mmask` commands on the System Menu (`/cfg/sys`), 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 which is allowed to access switch management through Telnet, SNMP, 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 the `mnet` to select a range of source IP addresses which can access 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 the `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.

For 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).

CAUTION—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.

Disabling Gratuitous ARPs

A new command has been added for disabling gratuitous ARPs. Normally, a device uses ARP (Address Resolution Protocol) requests to determine the hardware addresses of network devices when only the IP address is known. A *gratuitous* ARP occurs when a device sends an ARP request for its own IP address (the source and destination IP address are identical). Gratu-

itous ARPs help routers and bridges learn the MAC addresses of the network devices, and provide an important mechanism for switch failover in redundant configurations. Every 30 seconds, the Alteon Networks switch sends gratiutious ARPs for each configured virtual IP address.

Gratuitous ARPs should normally be disabled for computers running FreeBSD that create a syslog entry each time they see a gratuitous ARP. If left enabled, gratuitous ARPs can result in needlessly large syslogs on such systems.

By default, gratuitous ARPs are enabled. To change the setting (disable or enable gratuitous ARPs), use the `garp` command on the Server Load Balancing Menu (`/cfg/slb`), shown in **bold** type below:

```
[Server Load Balancing Menu]
        real  - Real server menu
        group - Real server group menu
        virt  - Virtual server menu
        filt  - Filtering menu
        port  - Layer 4 port menu
        fail  - Layer 4 failover menu
        dist  - Distributed SLB menu
        on    - Globally turn Layer 4 processing ON
        off   - Globally turn Layer 4 processing OFF
        imask - Set virtual and real IP address mask
        mnet  - Set managment network
        mmask - Set management subnet mask
        garp  - Enable/disable gratuitous ARPs
        cur   - Display current Server Load Balancing configuration

>> Server Load Balancing#
```

NOTE – In failover/hotstandby mode, gratuitous ARPs must be enabled.

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

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 of configured filters, real servers, or such, 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.

Downloading Configuration Files to the Console Port

It is a common practice to capture and save switch configuration dumps created by the `/cfg/dump` command. Later, if you need to restore the switch configuration, you can paste the contents of the captured dump to the switch.

Under some conditions, when downloading a very long list of configuration commands to the switch console port, some input data may be lost, causing configuration errors. This problem does not occur on Telnet connections. If an IP interface is configured for the switch, you can use Telnet to establish an administrative connection and download the configuration file.

Late-Breaking News and Support

Web access: http://www.alteon-networks.com

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