Release Note for Cisco Wide Area Application Services Software Version 4.4.5x

October 29, 2012

Note The most current Cisco documentation for released products is available on Cisco.com.

Contents

These release notes apply to the following software versions for the Cisco Wide Area Application Services (WAAS) software:

- 4.4.5d
- 4.4.5c
- 4.4.5b
- 4.4.5a
- 4.4.5

For information on WAAS features and commands, see the WAAS documentation located at http://www.cisco.com/en/US/products/ps6870/tsd_products_support_series_home.html.

Note The WAAS Central Manager must be the highest version of all devices in your WAAS network. Upgrade the Central Manager first before upgrading any other devices.

These release notes contain the following sections:

New and Changed Features

The following section contains the new and changed features in software Version 4.4.5x:

Software Version 4.4.5 New and Changed Features

WAAS software version 4.4.5 includes the following new features and changes:

- Support for Intelligent Platform Management Interface (IPMI) over LAN—This feature provides remote platform management service for WAVE-294/594/694/7541/7571/8541 appliances. IPMI is an open standard technology that defines how administrators monitor system hardware and sensors, control system components, and retrieve logs of important system events to conduct remote management and recovery. IPMI runs on the Baseboard Management Controller (BMC) and operates independently of the WAAS OS. After IPMI over LAN is set up and enabled on WAAS, authorized users can access BMC remotely even when WAAS OS becomes unresponsive or the device is powered down but connected to a power source. You can use an IPMI v2 compliant management utility, such as ipmitool or OSA SMbridge, to connect to the BMC remotely to perform IPMI operations.

  The IPMI over LAN feature provides the following remote platform management services:

  – Supports the power on, power off, and power cycle of the WAAS appliance.

  – Monitors the health of the WAAS hardware components by examining Field Replaceable Unit (FRU) information and reading sensor values.

  – Retrieves logs of important system events to conduct remote management and recovery.

  – Provides serial console access to the WAAS appliance over the IPMI session.

- Support for IPMI Serial over LAN (SoL)—IPMI SoL enables a remote user to access a WAAS appliance through a serial console through an IPMI session.

IPMI over LAN and IPMI SoL features can be configured using CLI commands and include the following:

  - Configuring IPMI LAN interface
  - Configuring IPMI LAN users
  - Configuring security settings for remote IPMI access
  - Enabling/disabling IPMI over LAN
  - Enabling/disabling IPMI SoL
  - Restoring the default settings for the BMC LAN channel
  - Displaying the current IPMI over LAN and IPMI SoL configurations

  For more information on configuring IPMI over LAN using CLIs, see the "Software Version 4.4.5 Command Changes" section on page 21.

- CLI commands—For CLI command changes, see the "Software Version 4.4.5 Command Changes" section on page 21

BMC Firmware Update and Checking the Firmware Version

IPMI over LAN feature requires that a specific BMC firmware version be installed on the device. The minimum supported BMC firmware versions are:

- WAVE-294/594/694—48a
- WAVE-7541/7571/8541—26a

WAAS appliances shipped from the factory with WAAS version 4.4.5 or later do have the correct firmware installed. If you are updating a device that was shipped with an earlier version of WAAS software, you must update the BMC firmware, unless it was updated previously.

To determine if you are running the correct firmware version, use the **show bmc info** command. The following example displays the latest BMC firmware version installed on the device (48a here):

```
wave# show bmc info
Device ID                 : 32
Device Revision           : 1
Firmware Revision         : 0.48                    <<<<< version 48
IPMI Version              : 2.0
Manufacturer ID           : 5771
Manufacturer Name         : Unknown (0x168B)
Product ID                : 160 (0x00a0)
Product Name              : Unknown (0xA0)
Device Available          : yes
Provides Device SDRs      : no
Additional Device Support :
    Sensor Device
    SDR Repository Device
    SEL Device
    FRU Inventory Device
Aux Firmware Rev Info     :
    0x0b
    0x0c
    0x08
    0x0a                                            <<<<< a
. . .
```

If a BMC firmware update is needed, you can download it from cisco.com at the Wide Area Application Service (WAAS) Firmware download page (registered customers only). The firmware binary image is named waas-bmc-installer-48a-48a-26a-k9.bin.

You can use the following command to update the firmware from the image file that is available through FTP on your network:

copy ftp install *ip-address remotefiledir* **waas-bmc-installer-48a-48a-26a-k9.bin**

The update process can take several minutes and the device may appear unresponsive but do not interrupt the process or power cycle the device. After the update is complete, you must reload the device.

After the device reboots, you can verify the firmware version by using the **show bmc info** command.

BMC recovery and BMC firmware update restores the factory defaults on the BMC and all the current IPMI over LAN configurations are erased.

Software Version 4.4.5 Filenames

This section describes the WAAS software Version 4.4.5 software image files for use on WAAS appliances and modules and contains the following topics:

- Standard Image Files, page 4
- No Payload Encryption (NPE) Image Files, page 5

Standard Image Files

WAAS software Version 4.4.5 includes the following standard primary software image files for use on WAAS appliances and modules:

- waas-universal-4.4.5.*x*-k9.bin—Universal software image that includes Central Manager and Application Accelerator functionality. You can use this type of software file to upgrade either a Central Manager or an Application Accelerator device.
- waas-accelerator-4.4.5.*x*-k9.bin—Application Accelerator software image that includes Application Accelerator functionality only. You can use this type of software file to upgrade only an Application Accelerator device, including those devices on an SM-SRE module. This software image file is significantly smaller than the Universal image. Kdump analysis functionality is not included in the Accelerator-only image.
- waas-sre-installer-4.4.5.*x*-k9.zip—SM-SRE install .zip file that includes all the files necessary to install WAAS on the SM-SRE module.

The following additional files are also included:

- waas-rescue-cdrom-4.4.5.*x*-k9.iso—WAAS software recovery CD image.
- waas-x86_64-4.4.5.*x*-k9.sysimg—Flash memory recovery image for 64-bit platforms (WAVE-274/294/474/574/594/694/7541/7571/8541 and WAE-674/7341/7371 devices).
- waas-4.4.5.*x*-k9.sysimg—Flash memory recovery image for 32-bit platforms (all other devices).
- waas-kdump-4.4.5.*x*-k9.bin—Kdump analysis component that you can install and use with the Application Accelerator software image. The Kdump analysis component is intended for troubleshooting specific issues and should be installed following the instructions provided by Cisco TAC.
- waas-alarm-error-books-4.4.5.*x*.zip—Contains the alarm and error message documentation.

- virtio-drivers.iso—Virtual blade paravirtualized network drivers for Windows. (Available at the Cisco Wide Area Application Services (WAAS) Software > Tools directory on Cisco.com.)

No Payload Encryption (NPE) Image Files

WAAS software Version 4.4.5 includes NPE primary software image files that have the disk encryption feature disabled. These images are suitable for use in countries where disk encryption is not permitted. NPE primary software image files include the following:

- waas-universal-4.4.5.*x*-npe-k9.bin—Universal NPE software image that includes Central Manager and Application Accelerator functionality. You can use this type of software file to upgrade either a Central Manager or an Application Accelerator device.
- waas-accelerator-4.4.5.*x*-npe-k9.bin—Application Accelerator NPE software image that includes Application Accelerator functionality only. You can use this type of software file to upgrade only an Application Accelerator device, including those on a SM-SRE module. This software image file is significantly smaller than the Universal image. Kdump analysis functionality is not included in the Accelerator-only image.
- waas-sre-installer-4.4.5.*x*-npe-k9.zip—SM-SRE install .zip file that includes all the NPE files necessary to install WAAS on the SM-SRE module.

The following additional files are also included:

- waas-rescue-cdrom-4.4.5.*x*-npe-k9.iso—WAAS NPE software recovery CD image.
- waas-x86_64-4.4.5.*x*-npe-k9.sysimg—Flash memory NPE recovery image for 64-bit platforms (WAVE-274/294/474/574/594/694/7541/7571/8541 and WAE-674/7341/7371 devices).
- waas-4.4.5.*x*-npe-k9.sysimg—Flash memory NPE recovery image for 32-bit platforms (all other devices).
- waas-kdump-4.4.5.*x*-npe-k9.bin—NPE Kdump analysis component that you can install and use with the Application Accelerator software image. The Kdump analysis component is intended for troubleshooting specific issues and should be installed following the instructions provided by Cisco TAC.
- waas-alarm-error-books-4.4.5.*x*-npe.zip— Alarm and error message documentation.
- virtio-drivers.iso—Virtual blade paravirtualized network drivers for Windows. (Available at the Cisco Wide Area Application Services (WAAS) Software > Tools directory on Cisco.com.)

Upgrading from WAFS to WAAS

WAFS to WAAS Version 4.4.1 (or later) migration is not supported. You must first migrate to a WAAS version prior to Version 4.4.1, then upgrade to Version 4.4.1 or later, and migrate from the legacy WAFS mode to the transparent CIFS accelerator.

Upgrading and Interoperability

This section contains the following topics:

WCCP Interoperability

Central Managers running Version 4.4.5x can manage WAEs running software Versions 4.0.19 and later. However, we recommend that all WAEs in a given WCCP service group run the same version.

Note The default value for the WCCP source IP mask changed to 0xF00 in Version 4.2.1. If you are upgrading a WAE that previously used the default WCCP source IP mask of 0x1741, its WCCP mask is not changed. Note that all WAEs in a WCCP service group must have the same mask.

To upgrade the WAEs in your WCCP service group, follow these steps:

Step 1 You must disable WCCP redirection on the Cisco IOS router first. To remove the global WCCP configuration, use the following **no ip wccp** global configuration commands:

```
Router(config)# no ip wccp 61
Router(config)# no ip wccp 62
```

Step 2 Perform the WAAS software upgrade on all WAEs using the WAAS Central Manager GUI.

Step 3 Verify that all WAEs have been upgraded in the Devices pane of the WAAS Central Manager GUI. Choose **My WAN > Manage Devices** to view the software version of each WAE.

Step 4 If mask assignment is used for WCCP, ensure that all WAEs in the service group are using the same WCCP mask value.

If you have upgraded any WAEs from a version earlier than 4.2.1, and the WAEs were using the default mask value, the mask value is not changed by the upgrade.

Step 5 Reenable WCCP redirection on the Cisco IOS routers. To enable WCCP redirection, use the **ip wccp** global configuration commands:

```
Router(config)# ip wccp 61
Router(config)# ip wccp 62
```

Prepositioning Interoperability

Note When a Central Manager running Version 4.1.5c or later is managing a WAE running a previous version (4.1.5b or earlier), you must use the Central Manager to create, modify, delete, and schedule preposition tasks.

This requirement is necessary because of preexisting behavior in WAE software Versions 4.1.5b or earlier that causes schedule information, from a preposition task created on the WAE, to be discarded by the 4.1.5c or later Central Manager. Because the Central Manager cannot create a preposition task successfully without schedule information, the preposition task is automatically removed from the WAE.

In this case, although the Central Manager GUI indicates that the preposition schedule is NOW and the WAE has been assigned to the task, this information is misleading.

To recover from this scenario, for preposition tasks that were created on WAE software Versions 4.1.5b or earlier to be successful with a Central Manager running Version 4.1.5c or later, follow these steps:

Step 1 Modify the schedule as required using the Central Manager GUI, even if you want the preposition schedule as NOW, and click **Submit**.

Step 2 Wait two data feed poll cycles for the configuration to synchronize between the Central Manager and the WAE (the default data feed poll cycle is 300 seconds).

The preposition task is then created on the WAE and the Central Manager, and the WAE is assigned to the preposition task with the required schedule changes.

In addition to GUI changes, any preposition changes made using the CLI on a WAE running Version 4.1.5b or earlier are also discarded by the 4.1.5c or later Central Manager.

Therefore, you must also use the Central Manager to perform the following preposition CLI tasks:

- Create, modify, or delete a schedule
- Delete a pattern
- Modify or delete a root-share

Upgrading from a Prerelease Version to Version 4.4.5x

To upgrade from WAAS prerelease software to Version 4.4.5x, you must perform the following tasks to ensure a successful upgrade:

- Restore the factory default settings by using the **restore factory-default** command.
- Perform a fresh install from the rescue CD.

Upgrading from a Release Version to Version 4.4.5x

This section contains the following topics:

For additional upgrade information and detailed procedures, see to the *Cisco Wide Area Application Services Upgrade Guide*.

Requirements and Guidelines

When you upgrade to Version 4.4.5x, observe the following guidelines and requirements:

- Upgrading to Version 4.4.5x is supported only from Versions 4.1.1d, 4.1.3, 4.1.3b, 4.1.5c, 4.1.5f, 4.1.7, 4.1.7b, 4.2.1, 4.2.3, 4.2.3c, 4.3.1, 4.3.3, 4.3.5, 4.4.1, 4.4.3c, 4.4.5, 4.4.5a, 4.4.5b, 4.4.5c, and 4.5.1. If you want to upgrade a WAAS device running a different version, first upgrade to the next supported version in the list, and then upgrade to the current 4.4.5 version.
- Upgrading to Version 4.4.5x is not supported on the following platforms: WAE-511, WAE-611, and WAE-7326. WAAS Version 4.4.5x does not operate on these appliances.
- To take advantage of new features and bug fixes, we recommend that you upgrade your entire deployment to the latest version.
- If you operate a network with devices that have different software versions, the WAAS Central Manager must be the highest version.
- Upgrade the WAAS Central Manager devices first, and then upgrade the WAE devices. If you have a standby WAAS Central Manager, upgrade it first, before upgrading the primary WAAS Central Manager. After upgrading, restart any active browser connections to the WAAS Central Manager.
- Before upgrading a WAAS Central Manager to Version 4.4.5, make a database backup by using the **cms database backup** EXEC command. This command creates a backup file in /local1/. In case of any problem during the upgrade, you can restore the database backup that you made before upgrading by using the **cms database restore** *backup-file* EXEC command, where *backup-file* is the one created by the **backup** command.
- After upgrading application accelerator WAEs, verify that the proper licenses are installed by using the **show license** EXEC command. The Transport license is enabled by default. If CIFS was enabled on the device before the upgrade, then the Enterprise license should be enabled. Configure any additional licenses (Video and Virtual-Blade) as needed by using the **license add** EXEC command. For more information on licenses, see the "Managing Software Licenses" section in the *Cisco Wide Area Application Services Configuration Guide*.
- After upgrading application accelerator WAEs, verify that the proper application accelerators, policies, and classifiers are configured. For more information on configuring accelerators, policies, and classifiers, see the "Configuring Application Acceleration" chapter in the *Cisco Wide Area Application Services Configuration Guide*.
- If you are upgrading a WAAS Central Manager to Version 4.4.1 or later and have the secure store enabled, you must reopen the secure store after the device reloads (and after any reload). From the WAAS Central Manager GUI, choose **Admin > Secure Store** or use the **cms secure-store open** EXEC command. After upgrading to Version 4.4.1 or later, you can change to an auto-generated passphrase mode and you will no longer need to manually open the secure store after each reload. For more information on using the secure store, see the "Configuring Secure Store Settings" section in the *Cisco Wide Area Application Services Configuration Guide*.
- If you have two Central Managers that have secure store enabled and you have switched primary and standby roles between the two Central Managers, before upgrading the Central Managers to Version 4.4.5, you must reenter all passwords in the primary Central Manager GUI. The passwords that need to be reentered include user passwords and CIFS file server passwords. If you do not reenter the passwords, after upgrading to Version 4.4.5, the Central Manager fails to send configuration updates to WAEs and the standby Central Manager until after the passwords are reentered.
- Central Manager support for configuring the Initial Slow Start Threshold TCP/IP setting was removed in Version 4.2.1. If your Central Manager is managing devices earlier than Version 4.2.1, you may see repeated device configuration change updates for the Initial Slow Start Threshold configuration parameter coming from these devices when this parameter is assigned a nondefault

value in the devices. To avoid these repeated updates, use the **no tcp init-ss-threshold** global configuration command to set the default value on the devices, which is the recommended value for most networks.

- If you are upgrading a Central Manager from Version 4.2.3x or earlier to Version 4.4.5, and you have any scheduled reports that are configured for more than 100 recurrences, after the upgrade only 100 recurrences are retained.
- If you use the setup utility for basic configuration after upgrading to 4.4.5, wccp router list 7 is used. Because the setup utility is designed for use on new installations, any existing configuration for wccp router list 7 is replaced with the new configuration.
- If you have disk encryption enabled and are upgrading to Version 4.4.5 NPE from Version 4.2.1 or earlier, disk encryption configuration as well as disk cached data are lost. There is no impact when upgrading to standard Version 4.4.5 (non-NPE).
- Beginning with Version 4.3.1, the print admin role is no longer assigned to all admin user accounts by default. However, if you are upgrading from an earlier version, the print admin role is not automatically removed from all admin user accounts. To manually remove the print admin role from an account, edit the admin user from the Admin > AAA > Users page, uncheck the **Print Admin** check box, and click **Submit**.
- After upgrading a Central Manager from Version 4.2.3x or earlier, the AllDevicesGroup device group is renamed to the AllWAASGroup. Additionally, an AllWAASExpressGroup is created for all WAAS Express devices.
- In Version 4.4.1, application aware DRE changes the way the DRE cache is populated and managed. When upgrading to Version 4.4.5x from Version 4.3.x or earlier, the existing DRE cache is preserved, but all new cache entries are written in a new cache format. The two formats coexist until the old cache is evicted through the normal eviction processes.

  Application policies do not change, but the new “bidirectional” term is introduced, which is the mode used prior to Version 4.4.1.

  DRE on a Version 4.4.5x device is compatible with all Version 4.1.x, 4.2.x, 4.3.x, and 4.4.x peers, but is not compatible with 4.0.x peers.
- After upgrading WAE devices to Version 4.4.1 or later, you may be able to improve DRE disk performance by deleting and recreating disk data partitions by using the **disk delete-data-partitions** EXEC command. This command deletes the DRE and CIFS caches and all installed virtual blade images. If you want to keep virtual blade images, back them up before using this command by using the **copy virtual-blade** EXEC command.

  After using the **disk delete-data-partitions** command, you must reload the device and the data partitions are automatically recreated and the caches are initialized, which can take several minutes. DRE optimization is not done until the DRE cache has finished initializing. The **show statistics dre** EXEC command reports “TFO: Initializing disk cache” until then.
- After upgrading a Central Manager to Version 4.4.5x from Version 4.3.x or earlier, the secure store may be in one of two states:
  - If the secure store was previously initialized, the secure store is in user-passphrase mode and is not open. You must manually open it by supplying the passphrase.
  - If the secure store was previously uninitialized, the secure store is in auto-passphrase mode and is open. After a reboot, no user intervention is required to open the secure store.
- When upgrading a device to Version 4.4.1 or later, the WCCP load balancing assignment method is always strictly enforced and must match the farm assignment method or the WAAS device is not allowed to join the farm. The nonstrict assignment method is no longer an option.

When upgrading a Central Manager to Version 4.4.1 or later, the Only Use Selected Assignment Method check box is no longer available in the device group WCCP Settings window. Any WAEs in a device group that are running a version earlier than 4.4.1 and getting their WCCP settings from the device group will not use strict assignment method enforcement. This does not affect the WCCP farm.

- The method for associating virtual blade interfaces to physical interfaces changed in Version 4.4.1 to use bridge groups and Bridge Virtual Interfaces (BVIs). When upgrading a device with a virtual blade to Version 4.4.1 or later, any virtual interface configurations are converted to use the new bridging method.
- Legacy mode WAFS is no longer supported in Version 4.4.1 or later and upgrading to Version 4.4.1 or later is prevented if legacy mode WAFS is enabled (edge or core services). Legacy WAFS users must migrate to the transparent CIFS accelerator before upgrading. For details on CIFS migration, see the *Cisco Wide Area Application Services Upgrade Guide*.
- Legacy mode print services is no longer supported in Version 4.4.1 or later. On upgrade to Version 4.4.1 or later, legacy print services functionality is removed and users must use the Windows Print accelerator. The print role and print admin privileges are removed from all user accounts, and the functionality of the Central Manager acting as a print repository is removed. Any legacy print services jobs that are spooled are lost if an upgrade to Version 4.4.1 or later is done before the data is printed.

  A Version 4.4.1 or later Central Manager can continue to manage earlier version WAEs that have legacy print services enabled, but print services can be configured on these WAEs only through the device CLI. The Central Manager can also display print services alarms from earlier version WAEs that are running legacy print services.
- In WAAS versions before 4.4.5, you were able to configure more memory for virtual blades on a 294-4G platform than was supported for virtual blades. To maintain stability, after upgrading to version 4.4.5 all memory allocated to virtual blades on the 294-4G platform is limited to 1 GB. This change affects any existing 294-4G virtual blade configurations.

Upgrading From Version 4.1.x

The following guidelines and requirements apply only if you are upgrading from Version 4.1.x:

- WAAS Versions 4.1.3 and later support SSL application definition, which is enabled for monitoring by default. However, if you are upgrading from Version 4.1.1 to Version 4.4.5x and already have 20 applications enabled for monitoring, the new SSL application has monitoring disabled because a maximum of 20 monitored applications are allowed. In order to enable monitoring of the SSL application, you must disable monitoring of a different application and then enable monitoring of the SSL application. You can enable and disable monitoring by using the Enable Statistics check box in the Modifying Application page of the WAAS Central Manager (Configure > Acceleration > Applications > *Application Name*).

  If the SSL Bandwidth Optimization chart has no data, monitoring may be disabled for the SSL application definition. Check that monitoring is enabled for the SSL application.
- The device group and role naming conventions changed in Version 4.1.3. Device group and role names cannot contain characters other than letters, numbers, period, hyphen, underscore, and space. (In Version 4.1.1, other characters were allowed.) If you upgrade from Version 4.1.1 to Version 4.4.5x, disallowed characters in device group and role names are retained, but if you try to modify the name, you must follow the new naming conventions.
- The standby interface configuration changed in Version 4.1.3. If multiple standby groups are configured before upgrading from Version 4.1.1, only the group with the lowest priority and a valid member interface remains after the upgrade and it becomes standby interface 1. If the errors option was configured, it is removed.

- If you have a Version 4.1.1x Central Manager where secure store has been initialized but not opened (such as after a reload) and the Central Manager has sent configuration updates containing user account, CIFS core password, preposition, or dynamic share changes to WAEs before the secure store was opened, then before upgrading the Central Manager to Version 4.4.5x, you must reenter all passwords in the primary Central Manager GUI. The passwords that need to be reentered include user passwords, CIFS file server passwords, and WAFS core passwords. If you do not reenter the passwords, after upgrading to Version 4.4.5x, the Central Manager fails to send configuration updates to WAEs and the standby Central Manager until after the passwords are reentered.
- If you have a Version 4.1.1x Central Manager, are using external/remote users that have the admin role, and have edited one or more of these users on the Central Manager, you might encounter caveat CSCsz24694, which causes the Central Manager not to send updates to WAEs after upgrading to Version 4.1.5x. To work around this caveat, from the Central Manager, manually edit the external users (without changing anything) after the upgrade. If you have a large number of external users defined, contact Cisco TAC for a script to run before or after the upgrade.
- If you are upgrading a Central Manager from Version 4.1.1x to Version 4.4.5x, before you upgrade, save all scheduled default reports that exist in Version 4.1.1x to avoid failed scheduled reports. To save a default report that you want to schedule, display the report and click the **Save** button. This requirement does not apply if you are upgrading from 4.1.3 or later because default reports are automatically saved.
- After upgrading a Central Manager from Version 4.1.x to Version 4.4.5x, any scheduled reports that contain the following charts are removed from the Manage Reports and Scheduled Reports lists: Managed Devices Information, CPU Utilization, and any CIFS charts. You can reschedule the CPU Usage report for a device if you want. The Managed Devices and CIFS charts are not applicable as part of a scheduled report.
- The default value for the WCCP source IP mask changed to 0xF00 in Version 4.2.1. If you are upgrading a Version 4.1.x WAE that previously used the default WCCP source IP mask of 0x1741, its WCCP mask is not changed. Note that all WAEs in a WCCP service group must have the same mask. For the recommended upgrade procedure for WAEs in a service group, see the "WCCP Interoperability" section on page 6.
- The SNMP username and remote entity ID constraints changed in Version 4.2.1. SNMP usernames are limited to 32 characters. (In Version 4.1.x and earlier, 64 characters were allowed.) SNMP remote entity IDs must be between 10 to 32 hexadecimal characters. (In Version 4.1.x and earlier, 1 to 64 characters were allowed.) If you upgrade from Version 4.1.x or earlier to Version 4.4.5x, invalid settings in these fields are deleted.

Ensuring a Successful RAID Pair Rebuild

RAID pairs rebuild on the next reboot after you use the **restore factory-default** command, replace or add a hard disk drive, delete disk partitions, or reinstall WAAS from the booted recovery CD-ROM.

Caution You must ensure that all RAID pairs are done rebuilding before you reboot your WAE device. If you reboot while the device is rebuilding, you risk corrupting the file system.

To view the status of the drives and check if the RAID pairs are in the "NORMAL OPERATION" or in "REBUILDING" status, use the **show disk details** command in EXEC mode. When you see that RAID is rebuilding, you must let it complete that rebuild process. This rebuild process may take several hours.

If you do not wait for the RAID pairs to complete the rebuild process before you reboot the device, you may see the following symptoms that could indicate a problem:

- The device is offline in the Central Manager GUI.
- CMS cannot be loaded.
- Error messages say that the file system is read-only.
- The syslog contains errors such as “Aborting journal on device md2,” “Journal commit I/O error,” “Journal has aborted,” or “ext3_readdir: bad entry in directory.”
- Other unusual behaviors occur that are related to disk operations or the inability to perform them.

If you encounter any of these symptoms, reboot the WAE device and wait until the RAID rebuild finishes normally.

Downgrading from Version 4.4.5x to a Previous Version

Note the following guidelines and considerations for downgrading:

- A downgrade is supported only to Versions 4.5.1, 4.4.5c, 4.4.5b, 4.4.5a, 4.4.5, 4.4.3c, 4.4.1, 4.3.5, 4.3.1, 4.2.3c, 4.2.3, 4.2.1, 4.1.7b, 4.1.7, 4.1.5f, 4.1.5c, 4.1.3b, 4.1.3, and 4.1.1d. A downgrade is not supported to Version 4.0.x.
- On a vWAAS device, you cannot downgrade to a version earlier than 4.3.1.
- On WAVE-294/594/694/7541/7571/8541 models you cannot downgrade to a version earlier than 4.4.1.
- When downgrading WAAS devices, first downgrade application accelerator WAEs, then the standby WAAS Central Manager (if you have one), and lastly the primary WAAS Central Manager.
- If you have a standby WAAS Central Manager, it must be registered to the primary WAAS Central Manager before the downgrade.
- When downgrading from a WAAS NPE version to a version earlier than 4.2.3, the **show version last** command does not display NPE in the version output.
- If two Cisco WAE Inline Network Adapters are installed in a WAE, you must remove one of the adapters before you downgrade the WAE to a version earlier than 4.2.1. Two Cisco WAE Inline Network Adapters are not supported in WAAS versions earlier than Version 4.2.1.
- If downgrading to Version 4.2.1, you must first change the password for WCCP, SNMP user, RADIUS, TACACS, or transaction log modules before the downgrade if any of the special characters !@#$%\ were used in the password for the module. Otherwise, the related CLI commands for those modules fail.
- Due to stricter security implemented in Version 4.2.1 and later, when downgrading to a version earlier than 4.2.1, any configuration settings that contain passwords or security keys are discarded and must be reconfigured. Affected CLI commands include the following: **ntp**, **radius-server**, **snmp-server user**, **tacacs**, **transaction-logs**, and **wccp tcp-promiscuous router-list-num**. After the downgrade, discarded configurations are listed in the file /local1/discarded_cli.

  Additionally, the following Central Manager settings are affected:

  – All SNMP users are deleted.
  – The RADIUS encryption key is deleted.
  – The TACACS security word is deleted.
  – The Email notification server password is deleted.
  – The transaction log and video acceleration transaction log export server configurations are deleted.

  - The WCCP password is set to null.
  - The username and password (if defined) associated with all software image files is set to anonymous/anonymous.

- Locked-out user accounts are reset upon a downgrade.
- If extended object cache is enabled, all CIFS cache data, DRE cache data, and virtual blade data is lost when downgrading to a version earlier than 4.2.1.
- Any new reports and charts that were introduced in Version 4.4.5 are removed from managed reports and scheduled reports when downgrading to an earlier version.
- The default value for the WCCP source IP mask changed in Version 4.2.1 to 0xF00. If you are downgrading a 4.4.5x WAE that uses the default WCCP source IP mask, its WCCP mask is not changed on a downgrade to a version earlier than 4.2.1. Note that all WAEs in a WCCP service group must have the same mask.
- If you use the setup utility for a basic configuration after downgrading to a version earlier than 4.2.3x, WCCP router list 8 is used. Because the setup utility is designed for use on new installations, any existing configuration for WCCP router list 8 is replaced with the new configuration.
- After downgrading a Central Manager to a version earlier than 4.3.1, the AllWAASGroup device group is renamed to the AllDevicesGroup. Additionally, the AllWAASExpressGroup is removed.
- After downgrading a Central Manager to a version earlier than 4.3.1, all registered WAAS Express devices are deleted from the Central Manager. If the Central Manager is later upgraded to 4.3.1, WAAS Express devices must be registered again.
- When downgrading to a version earlier than 4.4.1, the DRE cache is cleared and the DRE caching mode for all application policies is changed to bidirectional (the only available mode prior to 4.4.1). Before downgrading a WAE, we recommend that you use the Central Manager GUI to change all policies that are using the new Unidirectional or Adaptive caching modes to the Bidirectional caching mode.
- When downgrading a Central Manager to a version earlier than 4.4.1, if the secure store is in auto-passphrase mode, a downgrade is not allowed. You must switch to user-passphrase mode before you can downgrade to a software version that does not support auto-passphrase mode.
- Prior to downgrading to a version earlier than 4.4.1, we recommend that you change the WCCP service IDs back to their default values of 61 and 62, and change the failure detection timeout back to the default value of 30 seconds, if you have changed these values. Only these default values are supported in versions prior to 4.4.1 and any other values are lost after the downgrade. If a WAE is registered to a Central Manager, it is configured with the default service IDs of 61 and 62 after it is downgraded and comes back online.
- Current BMC settings are erased and restored to factory-default when downgrading WAAS to a version earlier than 4.4.5.

To downgrade the WAAS Central Manager (not required for WAE devices), follow these steps:

Step 1 (Optional) From the Central Manager CLI, create a database backup by using the **cms database backup** EXEC command. Move the backup file to a separate device.

```
CentralManager# cms database backup
```

Step 2 Install the downgrade WAAS software image by using the **copy ftp install** EXEC command.

Step 3 Reload the device.

Downgrading the database may trigger full updates for registered devices. In the Central Manager GUI, ensure that all previously operational devices come online.

Cisco WAE and WAVE Appliance Boot Process

To monitor the boot process on Cisco WAE and WAVE appliances, connect to the serial console port on the appliance as directed in the *Cisco Wide Area Application Engine Hardware Installation Guide*.

Cisco WAE and WAVE appliances have video connectors that should not be used in a normal operation. The video output is for troubleshooting purposes only during BIOS boot and stops displaying output as soon as the serial port becomes active.

Cisco WAE-674, WAE-7341, and WAE-7371 RAID Controller Firmware Upgrade

Under rare circumstances, the RAID controller firmware used in the WAE-674, WAE-7341, and WAE-7371 appliances can cause the disk storage subsystem to go offline and the affected devices to stop optimizing connections. The symptoms are as follows:

- Syslog output contains several instances of the following message: "WAAS-SYS-3-900000: sd 0:0:0:0: rejecting I/O to offline device."
- A sysreport and running-config cannot be generated and copied to /local/local1.
- Both of these symptoms are an indication of the file system becoming read-only during traffic flow.
- An increasing number of pending connections appear in the output of the **show statistics tfo** command, indicating that new connections cannot be optimized. You can use this command to proactively check the functionality of the system.

The solution is to upgrade to the 5.2-0 (17002) RAID Controller Firmware, which can be found on cisco.com at the Wide Area Application Service (WAAS) Firmware download page (registered customers only). The firmware binary image is named L4_*xxxxx*_FIRMWARE.bin.

Instructions on how to apply the firmware update are posted on cisco.com together with the firmware in the file named L4_*xxxxx*_FIRMWARE.pdf, which you can see when you mouse over the firmware file.

Cisco WAE-612 Hard Disk Drive Replacement Notification

This notice applies to the WAE-612 and all WAAS versions previous to 4.0.19 that support the hot-swap replacement of drives while the appliance is running.

A problem may occur while replacing the drives while the unit is running. Occasionally after a drive hot-swap procedure, the WAE-612 may stop operating and require a reboot.

To avoid this problem, upgrade your WAAS software to Version 4.0.19 or later.

This notice does not apply to the WAE-674, WAE-7341, or WAE-7371.

Operating Considerations

This section includes operating considerations that apply to software Version 4.4.5x and contains the following topics:

Interoperability

This section discusses operating considerations when operating a WAAS network that mixes Version 4.4.5x devices with devices running earlier software versions.

- WAAS Version 4.4.5x does not support running in a mixed version WAAS network where any WAAS device is running a software version lower than 4.0.19. If you have any WAAS devices running Version 4.0.17 or earlier, you must first upgrade them to Version 4.0.19 (or a later version), before you install Version 4.4.5. You should first upgrade any WAEs to Version 4.0.19 (or a later version) and then upgrade any WAAS Central Managers to Version 4.0.19 (or a later version).
- In a mixed version WAAS network with Version 4.4.5x, the WAAS Central Manager must be running the highest version of the WAAS software.

Central Manager Report Scheduling

In the WAAS Central Manager, we recommend running system-wide reports in device groups of 250 devices or less, or scheduling these reports at different time intervals, so multiple system-wide reports are not running simultaneously.

WAAS Express Policy Changes

Making policy changes to large numbers of WAAS Express devices from the Central Manager may take longer than making policy changes to WAAS devices.

Virtual Blade Configuration From File

If you copy the device configuration to the running configuration from a file (for example, with the **copy startup-config running-config** command), configuration changes from the file are applied to the device without confirmation. If a virtual blade disk configuration exists in the configuration file and it is different from the actual device configuration, the device virtual blade disk configuration is removed and replaced with the disk configuration from the file. You lose all data on the virtual blade disks.

Device Group Default Settings

When you create a device group in WAAS Version 4.4.5x, the Configure > Acceleration > DSCP Marking page is automatically configured for the group, with the default DSCP marking value of copy.

Using Autoregistration with Port-Channel and Standby Interfaces

Autoregistration is designed to operate on the first network interface and will not work if this interface is part of a port-channel or standby interface. Do not enable the auto-register global configuration command when the interface is configured as part of a port-channel or standby.

CIFS Support of FAT32 File Servers

The CIFS accelerator does not support file servers that use the FAT32 file system. You can use the policy engine rules to exclude from CIFS acceleration any file servers that use the FAT32 file system.

Using the HTTP Accelerator with the Cisco ASR 1000 Series Router and WCCP

When using the Cisco ASR 1000 Series router and WCCP to redirect traffic to a WAE that is using WCCP GRE return as the egress method and the HTTP accelerator is enabled, there may be an issue with HTTP slowness due to the way the ASR router handles proxied HTTP connections (see CSCtj41045). To work around this issue, on the ASR router, create a web cache service in the same VRF as that of the 61/62 service by entering the following command: **ip wccp** [**vrf** *vrf-name*] **web-cache** command.

Disabling WCCP from the Central Manager

If you use the Central Manager to disable WCCP on a WAAS device, the Central Manager immediately shuts down WCCP and closes any existing connections, ignoring the setting configured by the **wccp shutdown max-wait** global configuration command. If you want to gracefully shut down WCCP connections, use the **no wccp version 2** global configuration command on the WAAS device.

Internet Explorer Certificate Request

If you use Internet Explorer to access the Central Manager GUI version 4.3.1 or later and Internet Explorer has personal certificates installed, the browser prompts you to choose a certificate from the list of those installed in the personal certificate store. The certificate request occurs to support WAAS

Express registration and is ignored by Internet Explorer if no personal certificates are installed. Click **OK** or **Cancel** in the certificate dialog to continue to the Central Manager log in page. To avoid this prompt, remove the installed personal certificates or use a different browser.

Software Version 4.4.5d Resolved Caveats and Open Caveats

This section contains the resolved caveats, open caveats, and command changes in software Version 4.4.5d and contains the following topics:

Software Version 4.4.5d Resolved Caveats

The following caveats were resolved in software Version 4.4.5d.

Caveat ID Number	Description
CSCtt17284	standby CM OutofMem due to growing ao_stats_collection_info table
CSCtx27549	Slow CIFS performance due to connections not terminated appropriately
CSCtx27970	WAAS CIFS error when server sending a NT notify after a NT Cancel
CSCtz65773	BBU related logs seen on 7541,7571,8541;may indicate low disk throughput
CSCua98279	Role incorrect behavior as WAAS device is accessed via PeerID link

Software Version 4.4.5d Open Caveats

The open caveats for software Version 4.4.5d are the same as those for software Version 4.4.5, except for those that are resolved in Version 4.4.5, Version 4.4.5a, Version 4.4.5b, and Version 4.4.5c. For details, see the "Software Version 4.4.5 Open Caveats" section on page 20.

Software Version 4.4.5c Resolved Caveats and Open Caveats

This section contains the resolved caveats, open caveats, and command changes in software Version 4.4.5c and contains the following topics:

Software Version 4.4.5c Resolved Caveats

The following caveats were resolved in software Version 4.4.5c.

Caveat ID Number	Description
CSCtr27619	Disabling print accelerator from CM is not shown in running config
CSCtt99933	WAAS HTTP AO restarted while making DNS requests
CSCtz55888	Core file is generated while deleting user with password policy enabled.
CSCua00552	Device Settings overridden after upgrade from pre-4.3.x to post-4.3.x

Software Version 4.4.5c Open Caveats

The open caveats for software Version 4.4.5c are the same as those for software Version 4.4.5, except for those that are resolved in Version 4.4.5, Version 4.4.5a, and Version 4.4.5b. For details, see the "Software Version 4.4.5 Open Caveats" section on page 20.

Software Version 4.4.5b Resolved Caveats and Open Caveats

This section contains the resolved caveats, open caveats, and command changes in software Version 4.4.5b and contains the following topics:

Software Version 4.4.5b Resolved Caveats

The following caveats were resolved in software Version 4.4.5b.

Caveat ID Number	Description
CSCtx85628	"***" as a password creates core dump
CSCty70150	CMS accounting sends the no form of Tacacs/Radius key in clear text
CSCtz41283	SNMP OID mismatch SRE900 and CISCO-PRODUCTS-MIB for sysObjectID

Software Version 4.4.5b Open Caveats

The open caveats for software Version 4.4.5b are the same as those for software Version 4.4.5, except for those that are resolved in Version 4.4.5 and Version 4.4.5a. For details, see the "Software Version 4.4.5 Open Caveats" section on page 20.

Software Version 4.4.5a Resolved Caveats and Open Caveats

This section contains the resolved caveats, open caveats, and command changes in software Version 4.4.5a and contains the following topics:

Software Version 4.4.5a Resolved Caveats

The following caveats were resolved in software Version 4.4.5a.

Caveat ID Number	Description
CSCts99372	Deadlock in CIFS AO Causes Clients to Experience Slowness
CSCtx34265	Get operation for ifTable Mib's does not retrieve for inline interface
CSCty26359	DRE cache history progressively gets shorter and shorter

Software Version 4.4.5a Open Caveats

The open caveats for software Version 4.4.5a are the same as those for software Version 4.4.5, except for those that are resolved in Version 4.4.5a. For details, see the "Software Version 4.4.5 Open Caveats" section on page 20.

Software Version 4.4.5 Resolved Caveats, Open Caveats, and Command Changes

This section contains the resolved caveats, open caveats, and command changes in software Version 4.4.5 and contains the following topics:

Software Version 4.4.5 Resolved Caveats

The following caveats were resolved in software Version 4.4.5.

Caveat ID Number	Description
CSCto68524	LSI Controller not detected after all HDDs replaced on 7571, 8541
CSCtq41222	Virtual Blades could be created on 294-4G with the wrong memory size
CSCtr57511	WAAS - NFS AO to be restarted for generating a file
CSCtr83165	clear cache dre command reloads the system in a rare case scenario
CSCtr94024	Printer installation fails between Win2k8 SP1 64 bit and Win7 64bit
CSCts26831	Autoregistration gets disabled when BVI Interface is configured
CSCts67890	TFO/PT performance with GRE redirect/L2-ret and GRE-return is very low
CSCts71225	WAE Appliance crashed with HTTPS/THSDL session
CSCtu00021	DRE optimization process terminated with a core dump
CSCtu43274	Exceeding SNMP interface name index causes process restart
CSCtw58778	WAVE694 raised alarm for missing PSU
CSCtw77600	so_dre restarts and core created when the peer WAE so_dre goes to KDB/Core
CSCtw94637	Site map browsing do not work for both PP & DS in CIFSAO
CSCtw98937	vWAAS - all VM's from the same .ova file have the same dre-peer-id
CSCtx12250	CDPD core dumps generated when CDP update does ont contain hostname
CSCtx15689	Primary interface configuration lost on inline interface after reload
CSCtx22355	so_dre service is dead & so_dre core files found in the OE

Software Version 4.4.5 Open Caveats

The following open caveats apply to software Version 4.4.5.

Caveat ID Number	Description
CSCsi65522	CIFS related statistics graphs are not populated
CSCtw69937	Unable to set power-on operation on some WAVE platforms
CSCtx45526	MAPI core waas - memory corruption in the session shutdown path
CSCtw66559	winbindd causes 100% CPU load on WAAS
CSCtu10066	WAAS w/ACS does not always assign appropriate roles

The additional open caveats for software Version 4.4.5 are the same as those for software Version 4.4.3, except for those that are resolved in Version 4.4.5. For details, see The *Release Note for Cisco Wide Area Application Services (Software Version 4.4.3x).*

Software Version 4.4.5 Command Changes

This section lists the new and modified commands in WAAS software Version 4.4.5.

Table 1 lists the new commands and options added in WAAS Version 4.4.5.

Table 1 New Commands and Options in WAAS Version 4.4.5

Mode	Command and Syntax
EXEC	**restore bmc-factory-defaults** For details, see restore bmc-factory-defaults, page 25.
Global Configuration	[**no**] **bmc lan** {**ip address** {**dhcp** [**vlan** *vlan-id*] |*ipaddr netmask* **defaultgw** *ipaddr* [**vlan** *vlan-id*] **set-to-factory-default** [**force**]}| **user** *userid* {**username** *username* | **password** | **privilege** *privilege-level* | **IPMI-session-version** | **enable** | **disable** } | **cipher-privilege** *cipher-suite-number max-privilege-level* | **enable**} For details, see (config) bmc lan, page 22.
	[**no**] **bmc serial-over-lan enable** For details, see (config) bmc serial-over-lan enable, page 24.

Table 2 lists existing commands that have been modified in WAAS version 4.4.5.

Table 2 CLI Commands Modified in Version 4.4.5

Mode	Command	Description
EXEC	**copy sysreport**	Added the **usb** *filename* option to allow you to copy a system troubleshooting report to the specified file on a USB drive installed in a WAVE-294/594/694/7541/7571/8541 device.
	show bmc lan {**access** | **users** | **serial-over-lan** | **all**}	The **show bmc** command is enhanced with the following options to display the current IPMI over LAN and IPMI SoL configurations. • **access**—Displays IPMI over LAN settings. • **all**—Displays IPMI over LAN, SoL, and BMC users settings • **serial-over-lan**—Displays IPMI SoL settings • **users**—Lists all the configured BMC users
	show running-config	Enhanced to show BMC configurations.
	show tech-support	Enhanced to show IPMI over LAN, BMC users, and SoL settings.

Command Reference

The following commands are added in WAAS version 4.4.5:

- (config) bmc lan
- (config) bmc serial-over-lan enable
- restore bmc-factory-defaults

(config) bmc lan

To enable the IPMI over LAN feature and configure the BMC LAN settings, use the **bmc lan** global configuration command. To disable this feature, use the **no** form of this command.

bmc lan {**ip address** {**dhcp** [**vlan** *vlan-id*] | *ipaddr netmask* **defaultgw** *ipaddr* [**vlan** *vlan-id*] **set-to-factory-default** [**force**]}| **user** *userid* {**username** *username* **| password** | **privilege** *privilege-level* **| IPMI-session-version | enable | disable}** | **cipher-privilege** *cipher-suite-number max-privilege-level* **| enable**}

no bmc lan enable

Syntax Description

ip address	Configures the network settings for the BMC LAN interface statically or dynamically. Although the BMC LAN interface is connected through GigabitEthernet 0/0 to the outside, these two interfaces have their own MAC addresses, thus, the IP configurations for IPMI LAN interface and GigabitEthernet 0/0 are independent.
dhcp	Sets the IP address to the address that is negotiated over DHCP for the BMC LAN channel.
vlan *vlan-id*	(Optional) Uses VLAN configurations to set up the BMC LAN interface if the BMC is deployed in a separate network from the GigabitEthernet 0/0 interface. By default, *vlan-id* is 0, which means that the BMC LAN channel resides in the same subnet as that of GigabitEthernet 0/0. Note the following: • The previous VLAN setting is retained if **vlan** *vlan-id* is not specified. • If a previous configuration sets **vlan** to be nonzero for the BMC LAN channel, **vlan** must be explicitly set to 0 to deploy the BMC in the same subnet as GigabitEthernet 0/0.
ipaddr netmask	Configures the IP address and netmask for the BMC LAN interface.
defaultgw *ipaddr*	Configures the default gateway IP address.
set-to-factory-default [**force**]	Configures the BMC LAN IP address to factory-default values. This option also disables IPMI over LAN, IPMI SoL, and Webserver. The **force** option sets the default values without prompting.
user *userid*	Configures a user with the specified user ID.
username *username*	Configures the user name. The maximum length is 16 bytes.
password	Configures the user password. You are prompted for the password when you specify this option.
enable | **disable**	Enables or disables the user.

privilege *privilege-level*	Sets the user privilege level to one of these values (from lowest to highest): Callback User Operator Administrator A user's privilege level determines the type of IPMI operations that can be performed through the LAN. For example, only an operator level user and above can power cycle the device through a remote IPMI session.
IPMI-session-version	Specifies the minimum IPMI session version supported. You are prompted to change the version when you specify this option. This setting toggles between v1.5 and v2.0.
cipher-privilege *cipher-suite-number max-privilege-level*	This option sets the maximum BMC user privilege level that is allowed to use the specified cipher suite. There are 15 cipher suites numbered from 0 to 14 (for details see the IPMI v2.0 specification). The maximum user privilege level is specified as follows: Callback User Operator Administrator NONE (cipher suite is unused)
enable	Enables IPMI over LAN.

Defaults

IPMI over LAN is disabled on a WAAS device. There is only one enabled IPMI user whose user ID is 2, username is USERID, password is PASSWORD, privilege level is Administrator, and IPMI-session-version is v2.0. The BMC IP address and netmask are statically configured as 192.168.1.1/255.255.255.0. The BMC default gateway is 0.0.0.0. The VLAN is 0. The cipher privilege list is caaaaaaaaaaaaaa. (Each letter corresponds to a cipher suite from 0–14 and specifies the first letter of the maximum user privilege level that can use that cipher suite.)

Command Modes

Global configuration

Device Modes

application-accelerator

central-manager

Usage Guidelines

We recommend that a stronger cipher suite number be assigned to the network administrators than is used for normal users.

A user password must to be configured before the IPMI-session-version can be configured.

The default IPMI-session-version for a newly created users is v1.5, which means that both IPMI session v1.5 and v2.0 are supported. Setting a new password the first time sets the IPMI-session-version to v1.5.

If the BMC LAN IP address is to be configured dynamically, it is your responsibility to ensure a correct DHCP setup. Although the BMC LAN interface is connected through GigabitEthernet 0/0 to the outside, the DHCP configuration on the router are completely independent for the BMC LAN interface and

GigabitEthernet 0/0. The physical identifiers sent in the DHCPDISCOVER message by the BMC LAN interface and GigabitEthernet 0/0 are different. The BMC LAN interface sends its physical identifier in the format of "01" followed by MAC. For example, if the BMC LAN interface's MAC address is 588d.0990.8b43, its physical identifier as DHCP client is 0158.8d09.908b.43. GigabitEthernet 0/0 sends its MAC address as its physical identifier. For example, if you use manual binding on a Cisco router to assign a fixed IP to each interface, here is the correct DHCP pool configuration on the router:

```
ip dhcp pool bmclan
host 2.17.74.166 255.255.255.224
client-identifier 0158.8d09.908b.43
default-router 2.17.74.161

ip dhcp pool giga00
host 2.17.74.165 255.255.255.224
hardware-address 588d.0990.8b42
default-router 2.17.74.161
```

Examples

The following examples show how to configure a VLAN in the BMC interface settings:

Given the default BMC setting, the following two commands are equivalent:

```
WAVE(config)# bmc lan ip address 192.168.1.14 255.255.255.0 defaultgw 192.168.1.2
WAVE(config)# bmc lan ip address 192.168.1.14 255.255.255.0 defaultgw 192.168.1.2 vlan 0
```

The following command configures BMC LAN in a separate VLAN from GigabitEthernet 0/0:

```
WAVE(config)# bmc lan ip address 192.168.1.14 255.255.255.0 defaultgw 192.168.1.2 vlan 3
```

The following command configures the BMC LAN back into the same subnet as GigabitEthernet 0/0:

```
WAVE(config)# bmc lan ip address 192.168.1.14 255.255.255.0 defaultgw 192.168.1.2 vlan 0
```

The following command shows how to configure the BMC LAN IP settings to the factory defaults:

```
WAVE(config)# bmc lan ip address set-to-factory-default
Setting BMC IP to factory-default will disable IPMI over LAN, IPMI SoL, and Embedded
Webserver. Would you like to proceed?(Y/N)[N]
```

To set the maximum privilege level a BMC user needs to have to use cipher suites 1, 2 and 3 to User, Operator, and Administrator, respectively, use the following commands:

```
WAVE(config)# bmc lan cipher-privilege 1 User
WAVE(config)# bmc lan cipher-privilege 2 Operator
WAVE(config)# bmc lan cipher-privilege 3 Administrator
```

For more information on configuring the BMC LAN, see the "Configuring BMC for Remote Platform Management" section on page 26.

(config) bmc serial-over-lan enable

To enable the IPMI Serial over LAN (SoL) feature, use the **bmc serial-over-lan enable** global configuration command. To disable this feature, use the **no** form of this command.

bmc serial-over-lan enable

[**no**] **bmc serial-over-lan enable**

Syntax Description This command has no arguments or keywords.

Defaults By default, the IPMI SoL is disabled on a WAAS device.

Command Modes Global configuration

Device Modes application-accelerator

central-manager

Usage Guidelines IPMI SoL can only be enabled when IPMI over LAN is enabled. The baud rate of the WAAS serial console (whose baud rate is 9600 bps), IPMI SoL, and the remote terminal, must match for IPMI SoL to function correctly.

Examples The following example shows how to enable the IPMI SoL:

```
WAVE(config)# bmc serial-over-lan enable
```

restore bmc-factory-defaults

To restore the default settings for the BMC LAN channel, use the **restore bmc-factory-defaults** EXEC command.

restore bmc-factory-defaults

Syntax Description This command has no arguments or keywords.

Command Modes EXEC

Device Modes application-accelerator

central-manager

Examples The following example shows how to restore default settings for the BMC LAN channel:

```
WAVE# restore bmc-factory-defaults
```

Configuring BMC for Remote Platform Management

This section describes the minimum steps needed to enable IPMI over LAN and IPMI SoL to conduct remote platform management. This section includes the following topics:

Enabling IPMI Over LAN

To enable IPMI over LAN, perform the following steps using the **bmc lan** command:

1. Change the default BMC LAN IP address.
2. Change the password for the BMC default user, which is user 2.
3. Enable IPMI over LAN.
4. Access the BMC from a remote client over IPMI session v2.0 using the username and password for the number 2 user. The default cipher suite used to access the BMC is 3, which specifies RAKP-HMAC-SHA1 authentication, HMAC-SHA1-96 integrity, and AES-CBC-128 encryption algorithms.
5. To access the BMC over a IPMI session v1.5, change the user 2 IPMI-session-version setting from v2.0 to v1.5.

Enabling IPMI SoL

To enable IPMI SoL, perform the following steps:

1. On the WAAS device, configure and enable IPMI over Lan (IoL).
2. On the remote client make sure that the BMC user can do IoL operations successfully over IPMI session v2.0.
3. On the remote client, change the baud-rate of the terminal to match the WAAS console baud rate of 9600 bps.
4. On the WAAS device, enable IPMI SoL.
5. On the remote client, if the IPMI management tool is ipmitool, execute the command **ipmitool -I lanplus -H** *bmc-ip-address* **-U** *bmc-user-name* **sol activate** to open the serial console to the WAAS device.
6. On the remote client, you have now entered the console session of the WAAS device. When you are done, use the ~. escape character to terminate the connection.

WAAS Documentation Set

In addition to this document, the WAAS documentation set includes the following publications:

- *Cisco Wide Area Application Services Upgrade Guide*
- *Cisco Wide Area Application Services Quick Configuration Guide*
- *Cisco Wide Area Application Services Configuration Guide*
- *Cisco Wide Area Application Services Command Reference*

- *Cisco Wide Area Application Services API Reference*
- *Cisco Wide Area Application Services Monitoring Guide*
- *Cisco Wide Area Application Services vWAAS Installation and Configuration Guide*
- *Cisco WAAS Installation and Configuration Guide for Windows on a Virtual Blade*
- *Cisco WAAS Troubleshooting Guide for Release 4.1.3 and Later*
- *Cisco WAAS on Service Modules for Cisco Access Routers*
- *Cisco SRE Service Module Configuration and Installation Guide*
- *Configuring Cisco WAAS Network Modules for Cisco Access Routers*
- *WAAS Enhanced Network Modules*
- *Cisco Wide Area Application Services Online Help*
- *Using the Print Utilities to Troubleshoot and Fix Samba Driver Installation Problems*
- *Regulatory Compliance and Safety Information for the Cisco Wide Area Virtualization Engines*
- *Cisco Wide Area Virtualization Engine 294 Hardware Installation Guide*
- *Cisco Wide Area Virtualization Engine 594 and 694 Hardware Installation Guide*
- *Cisco Wide Area Virtualization Engine 7541, 7571, and 8541 Hardware Installation Guide*
- *Cisco Wide Area Virtualization Engine 274 and 474 Hardware Installation Guide*
- *Cisco Wide Area Virtualization Engine 574 Hardware Installation Guide*
- *Regulatory Compliance and Safety Information for the Cisco Content Networking Product Series*
- *Cisco Wide Area Application Engine 512 and 612 Hardware Installation Guide*
- *Cisco Wide Area Application Engine 7341, 7371, and 674 Hardware Installation Guide*
- *Installing the Cisco WAE Inline Network Adapter*

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS Version 2.0.

This document is to be used in conjunction with the documents listed in the "WAAS Documentation Set" section.