



Cisco Wide Area Application Services Upgrade Guide

Published: April 30, 2013

Software Versions 5.0, 5.1, and 5.2

This document describes how to upgrade Cisco Wide Area Application Services (WAAS) to software version 5.0, 5.1, or 5.2, which includes optionally migrating from the Common Internet File System (CIFS) application accelerator to the new Server Message Block (SMB) application accelerator.



Note

The procedures in this note contain CLI command examples. For more information about the commands used in the procedures, see the [Cisco Wide Area Application Services Command Reference](#).

This document contains the following sections:

- [Information About Upgrading to Version 5.0, 5.1, or 5.2, page 1](#)
- [Upgrading Your WAAS Software, page 3](#)
- [Migrating from CIFS Application Accelerator to the SMB Application Accelerator, page 12](#)
- [Validity Testing and Rollbacks, page 22](#)
- [Additional Resources, page 30](#)
- [Obtaining Documentation and Submitting a Service Request, page 31](#)

Information About Upgrading to Version 5.0, 5.1, or 5.2

This section provides general information about upgrading your WAAS software to version 5.0, 5.1, or 5.2 and contains these topics:

- [Upgrade Paths, page 2](#)
- [Upgrade Restrictions and Prerequisites, page 2](#)
- [Capacity Planning, page 3](#)



Upgrade Paths

Upgrading to version 5.0, 5.1, or 5.2 is supported from certain older versions only. If you have a WAAS device that is running a version from which upgrading directly to version 5.0, 5.1, or 5.2 is not supported, first upgrade the device to the next highest supported intermediate version and then upgrade to the desired 5.0, 5.1, or 5.2 version.

[Table 1](#) specifies which WAAS software versions can be directly upgraded to version 5.0, 5.1, or 5.2 and which versions require an intermediate upgrade.

Table 1 WAAS Versions and Upgrade Paths

Current WAAS Software Version	Upgrade Path
Earlier than 4.2.1	Upgrade to one of the directly upgradeable versions shown in this table first, and then upgrade to version 5.0, 5.1, or 5.2
4.2.x	Upgrade directly to version 5.0
4.3.x, 4.4.x, 4.5.x	Upgrade directly to version 5.0, 5.1, or 5.2
5.0.x	Upgrade directly to version 5.1 or 5.2
5.1.x	Upgrade directly to version 5.2

Upgrade Restrictions and Prerequisites

The following list includes prerequisites and restrictions that you need to know about before upgrading your software:

- Upgrading to version 5.0, 5.1, or 5.2 requires that your devices have been upgraded to the transparent CIFS application accelerator that was introduced in version 4.4. If you are running legacy mode CIFS, you must first upgrade to version 4.4 or later, as described in the [Cisco Wide Area Application Services Upgrade Guide for Version 4.4](#).



Note If you have to upgrade from CIFS legacy mode to the transparent CIFS application accelerator, make sure that you do so in a separate change window.

- You must upgrade the Central Manager software to version 5.0, 5.1, or 5.2 prior to upgrading other Wide Area Application Engine (WAE) devices in your network.
- Make sure the Cisco IOS release on the router or switch has been scrubbed for WCCP issues for your specific platform. You must do this action only on routers and switches that participate in transparent redirection and is not applicable to policy-based routing (PBR) or inline deployments. If you do not do this action and there is a current active WAAS network, disable WCCP in the routers and switches in the data center and all branches before the software upgrade to 5.0, 5.1, or 5.2.
- You may need to update firmware or BIOS on some or all of your devices; see the [Release Notes](#) for the latest information on firmware requirements and updates.
- The following device platform is no longer supported on WAAS version 5.1 or later: NME-502. WAAS version 5.1 or later does not operate or install on this device.
- The following device platforms are no longer supported on WAAS version 5.0 or later: NME-302, NME-522, WAE-512, and WAE-612 platforms. WAAS version 5.0 or later does not operate or install on these devices. Additionally, the NME-502 platform is not supported in WAAS version 5.1.

- If you are using NTLM Windows domain authentication or are using a nonstandard port (other than port 88) for Kerberos authentication, you must change these configurations and ensure that your domain controller is configured for Kerberos authentication before proceeding with an upgrade to WAAS version 5.1 or later, which does not support NTLM or nonstandard ports. For more details on the procedure, see the WAAS [Release Note for Cisco Wide Area Application Services](#).

**Note**

If you are using WCCP, the default value for the WCCP source IP mask changed in version 4.2.1 and later to 0xF00. However, if you are upgrading a WAE that used the previous default WCCP source IP mask of 0x1741 (or any custom mask), its WCCP mask will not be changed. If you are downgrading a WAE to a version earlier than 4.2.1, its WCCP source IP mask will not be changed. By not changing the mask during an upgrade or downgrade, the WAE avoids unexpected mask changes and WCCP farm disruptions. All WAEs in a WCCP farm must have the same mask or they will not participate in the farm.

For important upgrade details, including to which software version you want to upgrade, see the WAAS [Release Note for Cisco Wide Area Application Services](#).

Capacity Planning

Capacity planning is an ongoing process as branches and applications are added. Check the WAE devices to make sure that they are providing adequate caching and optimization and that connection limits are not exceeded.

If you determine that you need more processing capacity, contact your Cisco representative.

Upgrading Your WAAS Software

This section contains the following topics:

- [Information About Upgrade Methods, page 3](#)
- [Upgrading Your Firmware, page 4](#)
- [Selecting a WAAS Upgrade Software Image, page 4](#)
- [Upgrading Sequence, page 5](#)
- [Creating a Backup of the Primary Central Manager, page 5](#)
- [Upgrading the Standby Central Manager, page 6](#)
- [Upgrading the Primary Central Manager, page 6](#)
- [Upgrading the Branch WAAS Software, page 7](#)
- [Upgrading the Data Center WAAS Software, page 8](#)

Information About Upgrade Methods

You can use one of the following methods to perform the WAAS upgrade and transfer the new software image onto the WAE devices in the WAAS network:

- Use the Central Manager Software Update feature to distribute the WAAS software image to WAAS devices.

- Install the software image directly using the Software Recovery CD or USB method to perform a clean install (not an upgrade), which deletes the previous WAAS software image, deletes any cache and so forth.
- Use FTP or TFTP directly on the WAE through the command-line interface (CLI).

The remainder of this document assumes that you are using FTP or TFTP and the CLI to upgrade your software.

If you are using one of the other methods, see the “Maintaining Your WAAS System” chapter of the *Cisco Wide Area Application Services Configuration Guide*.

Upgrading Your Firmware

On WAE and WAVE appliances, before proceeding with your software upgrade, we recommend that you update the following three types of system firmware to the latest versions to best support new WAAS features:

- BIOS on the WAVE-594/694/7541/7571/8541 models—The latest BIOS is required for the AppNav operation in WAAS version 5.0 and later.
- BMC firmware on the WAVE-294/594/694/7541/7571/8541 models—The latest BMC firmware is required for the Intelligent Platform Management Interface (IPMI) over LAN feature in WAAS version 5.0 and later.
- RAID controller firmware on the WAE-674/7341/7371 and WAVE-7541/7571/8541—The latest RAID controller firmware is recommended to avoid some rarely encountered RAID controller issues.

See the [Release Notes](#) for the latest information on firmware requirements and updates.

Selecting a WAAS Upgrade Software Image

Two different WAAS software images are available. One provides only accelerator and AppNav Controller (ANC) functionality, while the other provides all (universal) functionality, as shown in [Table 2](#).


Table 2 WAAS Software Images

Image Type	Descriptions
Accelerator	Includes Application Accelerator and ANC functionality only. This image is smaller than the Universe image, which makes it the preferred software image to use for upgrading your WAE devices.
Universal	Includes Central Manager, Application Accelerator functionality and ANC functionality. You can use this type of software file to upgrade either a Central Manager or an Application Accelerator device. This image is considerably larger than the Accelerator-only software image.

Additionally, a separate set of No Payload Encryption (NPE) images are provided that have the disk encryption feature disabled. These images are suitable for use in countries where disk encryption is not permitted. Be sure to use the standard or NPE software images as required. You can recognize the NPE images by the “-npe” designation in the image filenames.

Upgrading Sequence

Use this procedure to upgrade your WAAS network to version 5.0, 5.1, or 5.2.

-
- Step 1** Create a backup of the Central Manager database and save it to an external hard drive, as described in the [“Creating a Backup of the Primary Central Manager”](#) section on page 5.
 - Step 2** Upgrade the Secondary Central Manager, if present, as described in the [“Upgrading the Standby Central Manager”](#) section on page 6.
 - Step 3** Upgrade the primary Central Manager, as described in the [“Upgrading the Primary Central Manager”](#) section on page 6.
-  **Note** You must upgrade your Central Manager(s) before you upgrade the rest of the WAE devices in your WAAS network.
-
- Step 4** Upgrade the other WAE network devices, as described in the [“Upgrading the Branch WAAS Software”](#) section on page 7 and the [“Upgrading the Data Center WAAS Software”](#) section on page 8.
 - Step 5** If you are migrating some or all of your devices from the CIFS application accelerator to the new SMB application accelerator, follow the migration steps described in the [“Migrating from CIFS Application Accelerator to the SMB Application Accelerator”](#) section on page 12.
-

Creating a Backup of the Primary Central Manager

Use this procedure to back up the primary Central Manager (CM) database and copy the backup file to an FTP server.

Procedure

-
- Step 1** Telnet to the primary CM.
`telnet cm_ip_address`
 - Step 2** Create the database backup.
`cms database backup`
 - Step 3** Copy the backup file to a remote FTP server.
`copy disk ftp ftpserver / waas-db-filename.dump remote_filename`
 - Step 4** Verify that the backup file copied correctly by checking the file for correct size and timestamp.
-

Upgrading the Standby Central Manager

Use this procedure to upgrade the WAAS software on the standby CM.

Procedure

-
- Step 1** Telnet to the standby CM IP address.

```
telnet standby_cm_ip_address
```

- Step 2** Copy the new software image to the standby CM.

```
copy ftp install ftpserver / waas-image.bin
```

This example assumes that the file is in the root directory of the FTP server. Provide the correct path if needed.

- Step 3** Reload the standby CM.

```
reload
```

- Step 4** Verify that the new image loaded correctly.

```
show version
```

- Step 5** Ping the primary CM and branch WAE devices to confirm connectivity.

- Step 6** Wait at least 5 minutes and then confirm the database last synchronization time to ensure that the database has been synchronized.

```
show cms info
```

- Step 7** From the primary CM, confirm that the status indicator for the standby CM is online and green.
-

Upgrading the Primary Central Manager

Use this procedure to upgrade the WAAS software on the primary CM.

Prerequisites

Upgrade the standby CM before you upgrade the primary CM, as described in the [“Upgrading the Standby Central Manager”](#) section on page 6.

Procedure

-
- Step 1** Telnet to the primary CM IP address.

```
telnet primary_cm_ip_address
```

- Step 2** Copy the new software image to the primary CM.

```
copy ftp install ftpserver / waas-image.bin
```

This example assumes that the file is in the root directory of the FTP server. Provide the correct path if needed.

- Step 3** Reload the primary CM.

```
reload
```

- Step 4** Verify that the new image loaded correctly.
- ```
show version
```
- Step 5** Ping the standby CM and branch WAE devices to confirm connectivity.
- Step 6** Confirm that the CMS services are running.
- ```
show cms info
```
- Step 7** Verify that all the WAE devices are online and in the AllWAASGroup.
- Choose **Devices > All Devices** and verify that all the WAE devices are online and have a green device status.
 - Choose **Device Groups > AllWAASGroup > Assign Devices** and verify that all WAEs are listed with a green check mark.
-

Checkpoint

The CMs are updated with the new WAAS software version 5.0, 5.1, or 5.2. The standby CM was upgraded first followed by the primary CM.

Upgrading the Branch WAAS Software

Use this procedure to upgrade each WAAS branch WAE to version 5.0, 5.1, or 5.2.

Prerequisites

- Make sure that you have already upgraded the secondary and primary CM(s)
- Use FTP to copy the WAAS software image to a local server or push the software image to your WAE devices through the CM, as described in the “Maintaining Your WAAS System” chapter of the [Cisco Wide Area Application Services Configuration Guide](#).

Procedure

- Step 1** Access the CM GUI.
- ```
https://cm_ip_address:8443
```
- Step 2** Verify that all the WAE devices are online (green).
- Step 3** Address any alarm conditions that may exist.
- Step 4** Open a console or Telnet session to the branch WAE.
- Step 5** Copy the software image to the WAE.
- ```
copy ftp install ftpserver / waas-image.bin
```
- This example assumes that the file is in the root directory of the FTP server. Provide the correct path if needed. You can use either the Universal or Accelerator-only images.
- Step 6** Reload the WAE.
- ```
reload
```
- Step 7** Verify that the image installed correctly.
- ```
show version
```

Step 8 Verify that the correct licenses are installed.

```
show license
```

If an Enterprise license has been purchased and not enabled, go to Steps 9 and 10. Otherwise, go to Step 11.

Step 9 (Optional) Clear the Transport license.

```
clear license Transport
```

Step 10 (Optional) Add the Enterprise license.

```
license add Enterprise
```

Step 11 Save the configuration.

```
copy running-config startup-config
```

Step 12 From the WAAS CM GUI, choose **Devices** > *branchWAE* and verify that the WAE is online and has a green device status.

Step 13 Verify the WAE device functionality as follows:

a. Assuming that WCCP is used for the traffic interception method, verify the WCCP is functioning properly.

```
show run | include wccp
```

b. (Optional) Confirm that flows are being optimized.

```
show statistics connection
```

c. Confirm that the Enterprise license is enabled.

```
show license
```

If the Enterprise license is not enabled, proceed with Steps d through f.

d. Clear the Transport license.

```
clear license Transport
```

e. Add the Enterprise license.

```
license add Enterprise
```

f. Save the changed configuration.

```
copy running-config startup-config
```

Checkpoint

All the branch WAE devices within the active WAAS network are upgraded to version 5.0, 5.1, or 5.2.

Upgrading the Data Center WAAS Software

Use this procedure to prepare for and upgrade the data center WAAS Software to version 5.0, 5.1, or 5.2.

Procedure

-
- Step 1** Access the CM GUI.
`https://cm_ip_address:8443`
- Step 2** Verify that all the WAE devices are online (green).
- Step 3** Address any alarm conditions that may exist.
- Step 4** Follow the procedure in the [“Upgrading Each Data Center WAE” section on page 9](#), for each data center device.



Note

This procedure removes the WAE from the interception path while the upgrade is done and applies to deployments that use WCCP for redirection in the data center. If you are not using WCCP interception in the data center, you should use another method to remove the WAE from the interception path. For an inline deployment, use the **interface InlineGroup slot/group shutdown** global configuration command to bypass the traffic on the active inline groups. In a serial inline cluster, shut down the interfaces on the intermediate WAE first, then on the optimizing WAE in the cluster. For a deployment using Cisco ACE for interception, gracefully shut down the ACE real server by using the **no inservice** command in either real server host or real server redirect configuration mode.

Upgrading Each Data Center WAE

Use this procedure to upgrade the data center WAE software.

Procedure

-
- Step 1** Disable WCCP on the WAE as follows to allow a graceful termination of existing TCP flows that are optimized by WAAS:
- a. Disable WCCP.


```
config
wccp tcp-promiscuous service-pair x x
no enable
exit
```
 - b. Wait until the countdown expires or press **Ctrl-C** to skip waiting for a graceful WCCP shutdown.
 - c. Verify that WCCP is disabled.


```
show wccp status
```
 - d. Save the changed configuration.


```
copy running-config startup-config
```
- Step 2** (Optional) Disable WCCP on the intercepting router or switch. This step is recommended only if the Cisco IOS release on the router or switch has not been scrubbed for WCCP issues for your specific platform.
- ```
config t
no ip wccp 61
no ip wccp 62
exit
```
- Step 3** (Optional) Verify that WCCP is disabled. This step is needed only if you disabled WCCP in Step 2.

```
show ip wccp
```

**Step 4** Upgrade the data center WAE software as follows:

- a. Open a console or Telnet session to the data center WAE.
- b. Copy the software image to the WAE.

```
copy ftp install ftpserver / waas-image.bin
```

This example assumes that the file is in the root directory of the FTP server. Provide the correct path if needed. You can use either the Universal or Accelerator only images.

- c. Reload the WAE.

```
reload
```

- d. Verify that the image installed correctly.

```
show version
```

- e. Confirm that WCCP is disabled.

```
show wccp status
```

- f. Save the changed configuration.

```
copy running-config startup-config
```

**Step 5** From the WAAS CM GUI, choose **Devices** > *dataCenterWAE* and verify that the WAE is online and has a green device status.

**Step 6** (Optional) Enable WCCP on all intercepting routers or switches in the router list as follows:

- a. Telnet to each core router or switch.
- b. Enable WCCP.

```
config t
ip wccp 61 redirect-list ACL_name
ip wccp 62 redirect-list ACL_name
```

See the [“Enabling WCCP on WAE Devices in a Cluster”](#) section on page 11 for an example ACL template.

This step is needed only if you disabled WCCP in [Step 2](#).

**Step 7** Verify WAE device functionality as follows:

- a. Enable WCCP.

```
config
wccp tcp-promiscuous service-pair x x
enable
exit
```

If you are using wccp single service, use these commands instead:

```
config
wccp tcp-promiscuous y
enable
exit
```

- b. Confirm that redirecting intercepting router IDs are seen.

```
show wccp routers
```

- c. Confirm that all WAE devices in the cluster are seen.

```
show wccp clients
```

- d. Confirm that the packet count to the WAE is increasing and no loops are detected.

```
show wccp statistics
```

- e. Verify that the buckets assigned for Service Group 61 match those of Service Group 62 and are assigned to the WAE.

```
show wccp flows tcp-promiscuous detail
```

- f. Confirm that flows are being optimized.

```
show statistics connection
```

### Checkpoint

All WAE devices in the data center are upgraded to version 5.0, 5.1, or 5.2 and have WCCP enabled.

## Enabling WCCP on WAE Devices in a Cluster

Use this procedure to enable WCCP on WAE devices in a cluster.

### Procedure

- Step 1** Validate your Cisco IOS release with a bug scrub for WCCP-related issues for your specific platform.
- Step 2** Enable WCCP on the WAEs in the cluster
- Step 3** Enable WCCP on the intercepting routers or switches; you can use or modify the following router ACL template for running WCCP in your network.

```
!
ip access-list extended WCCPLIST
remark ** ACL used for WCCP redirect-list **
remark **WAAS WCCP Mgmt ports **
deny tcp any any eq telnet
deny tcp any any eq 22
deny tcp any any eq 161
deny tcp any any eq 162
deny tcp any any eq 123
deny tcp any any eq bgp
deny tcp any any eq tacacs
deny tcp any eq telnet any
deny tcp any eq 22 any
deny tcp any eq 161 any
deny tcp any eq 162 any
deny tcp any eq 123 any
deny tcp any eq bgp any
deny tcp any eq tacacs any
remark ** Allow only explicit traffic **
permit tcp x.x.x.x 0.0.0.255 y.y.y.y 0.0.0.255
permit tcp y.y.y.y 0.0.0.255 x.x.x.x 0.0.0.255
remark **
remark ** Deny all other traffic
deny ip any any
!
```

# Migrating from CIFS Application Accelerator to the SMB Application Accelerator

After you upgrade your WAAS software to version 5.0, 5.1, or 5.2, you have the option of migrating file sharing acceleration on devices in your WAAS network from using the CIFS application accelerator to using the SMB application accelerator. These accelerators perform similar optimizations using different techniques.

This section assumes that you have already upgraded your devices to Version 5.0, 5.1, or 5.2, as described in the previous sections of this document.

No matter which option you use, the basic migration steps are as follows:

- 
- Step 1** Upgrade your CM and any devices on which you want to use the SMB application accelerator to Version 5.0, 5.1, or 5.2, as described in the previous sections of this document.
  - Step 2** Review the [“Information About Migrating to the SMB Application Accelerator” section on page 12](#) and decide which devices you want to migrate to the SMB application accelerator.
  - Step 3** Decide on your migration options by reviewing the information in these topics:
    - [Performing an All at Once Migration to SMB Acceleration, page 14](#)—Describes the option for migrating all of the devices in your WAAS network to use the SMB application accelerator.
    - [Performing a Phased-In Migration to SMB Acceleration, page 15](#)—Describes the option for migrating some of your devices to use the SMB application accelerator while continuing to use the CIFS application accelerator on other devices.
  - Step 4** Follow the migration steps in the section for the option you have selected.
  - Step 5** If you had dynamic shares on a device that you migrated to the SMB application accelerator, you need to recreate those shares, as described in the [“Migrating Dynamic Shares” section on page 21](#).
- 

## Information About Migrating to the SMB Application Accelerator

Version 5.0 of WAAS introduced the new SMB application accelerator, which is briefly summarized in this section, and AppNav, which is described in the “Configuring AppNav” chapter of the [Cisco Wide Area Application Services Configuration Guide](#).

This section contains the following topics:

- [Information About the SMB and CIFS Application Accelerators, page 12](#)
- [Migration Considerations, page 13](#)

## Information About the SMB and CIFS Application Accelerators

The CIFS and SMB application accelerators mostly support the same features, although they use different techniques to perform their optimizations. [Table 3](#) shows the main features supported by each accelerator for file sharing.

**Table 3** *SMB and CIFS Application Accelerator Feature Comparison*

| File Sharing Acceleration Feature                     | SMB Accelerator     | CIFS Accelerator |
|-------------------------------------------------------|---------------------|------------------|
| Optimization of SMBv1 traffic                         | Yes                 | Yes              |
| Optimization of CIFS traffic                          | Yes                 | Yes              |
| Optimization of print traffic                         | Yes                 | Yes              |
| Optimization of signed traffic                        | Yes                 | Yes              |
| Optimization of SMBv2.x traffic                       | Yes                 | Yes              |
| Native SMBv2.x acceleration                           | Yes                 | No               |
| Performance tuned for high throughput and low latency | Yes                 | No               |
| Support for object prepositioning                     | Not yet             | Yes              |
| Supports advanced print acceleration                  | In WAAS version 5.2 | Yes              |

The CIFS application accelerator is enabled by default, except in ISR-WAAS, which does not support the CIFS accelerator and where the SMB accelerator is enabled by default. The SMB accelerator provides native support for SMBv2 signing and higher throughput with low latency times than the CIFS accelerator.

**Note**

You can enable either the CIFS application accelerator or the SMB application accelerator on a WAE. Enabling one automatically disables the other on the device.

Peer WAEs must both use the same application accelerator (CIFS or SMB) because the two different accelerators do not interoperate. They can coexist in the same WAAS network but only on separate devices that are not peers.

Note that the SMB application accelerator provides options for fine-tuning the optimizations you want it to perform. For more information about configuring the accelerators, see the “Configuring File Services” chapter of the [Cisco Wide Area Application Services Configuration Guide](#).

You can use either AppNav or WAAS groups to migrate from the CIFS application accelerator to the SMB application accelerator, as described in the [“Performing a Phased-In Migration to SMB Acceleration”](#) section on page 15.

## Migration Considerations

When you upgrade to version 5.0, 5.1, or 5.2 from a 4.x version, you can continue to optimize file sharing traffic with the CIFS application accelerator, or you can migrate some or all of your devices to optimize with the SMB application accelerator instead.

If you are migrating some or all of your file share traffic to the SMB application accelerator, be aware of these considerations:

- The SMB and CIFS application accelerators are mutually exclusive: they cannot be enabled on a device at the same time.
- If you only have SMB and CIFS application accelerators running on the same path, the flow is not optimized.

- You can migrate some of your devices to the SMB application accelerator while continuing to use the CIFS application accelerator on other devices by following one of the migration options outlined in the [“Performing a Phased-In Migration to SMB Acceleration”](#) section on page 15. You can also choose the all at once migration option to switch your entire WAAS network to the SMB accelerator; see the [“Performing an All at Once Migration to SMB Acceleration”](#) section on page 14.
- Enabling SMB automatically disables CIFS; enabling CIFS automatically disables SMB.
- Policy classifiers are identical for the SMB and CIFS accelerators.
- The SMB accelerator does not support prepositioning; when you switch from the CIFS accelerator to the SMB accelerator, your preposition directives are deactivated.

Before starting any migration, make sure that the current CIFS traffic load can be supported without the CIFS object cache for the time required to perform the migration.

## Performing an All at Once Migration to SMB Acceleration

The all at once option is the simplest way to migrate. All you need to do is update all devices to version 5.0, 5.1, or 5.2 and enable SMB acceleration on all devices. After you are done, the file share traffic is optimized by the SMB application accelerator.



**Note**

When you use this option, CIFS connections are not accelerated during the migration; the connections continue to be optimized with TFO and DRE during the migration but acceleration does not restart until you complete the migration to SMB.

**Procedure**

- Step 1** Upgrade the data center and remote devices to Version 5.0, 5.1, or 5.2, as described in the [“Upgrading Your WAAS Software”](#) section on page 3.
- Step 2** Log in to the primary CM GUI.  
`https://cm_ip_address:8443`
- Step 3** Verify that all the WAE devices are online (green).
- Step 4** Address any existing alarm conditions before proceeding.
- Step 5** Choose **Device Groups** > *AllWAASGroup* > **Configure** > **Acceleration** > **Enabled Features** and check the **SMB Accelerator** check box.



**Note**

The SMB accelerator is enabled by default on ISR-WAAS devices and the CIFS accelerator is not supported.

- Step 6** Open a Telnet session to the data center WAE CLI.
- Step 7** Verify proper WAE functionality as follows:
  - a. Verify that only the SMB accelerator is enabled.  
`show accelerators`
  - b. Confirm that other flows are optimized.  
`show statistics connection`

You know that a connection is being optimized when you see the letter C in the Accel column for that connection in the output of the **show statistics connection** command.

### Checkpoint

All filing sharing requests received from remote accelerators running SMB receive full TFO, DRE and SMB optimization; however, if any remote accelerators continue to run the CIFS accelerator, their traffic receives only TFO optimization.

## Performing a Phased-In Migration to SMB Acceleration

With the phased-in (mixed deployment) migration, you separate your devices into two groups. One group is migrated to the SMB application accelerator, while the other group continues to use the CIFS accelerator.

You can isolate SMB and CIFS traffic to the data center devices by separating those devices into groups in two ways:

- Using AppNav—This method uses a phased-in or mixed deployment in which AppNav automatically distributes traffic to a device that runs either the SMB accelerator or the CIFS accelerator, depending on application policy configurations. For more information, see the [“Using AppNav with Mixed SMB and CIFS Application Accelerators”](#) section on page 15.
- Using WCCP—This method uses a phased-in or mixed deployment in which branch traffic is distributed to a device that runs the SMB accelerator or to a device that runs the CIFS accelerator, depending on its WCCP Service Group ID. For more information, see the [“Using WCCP Service Groups With Mixed SMB and CIFS Application Accelerators”](#) section on page 18.

When you perform a phased migration, the traffic flows for CIFS and SMB are separated and sent to one or more dedicated WAAS accelerators. You can either add additional data center devices or separate the devices in the data center; we strongly recommend that you perform a sizing estimate before you migrate any branch nodes. You can use WAAS Central Manager reports to help determine sizing metrics such as traffic volume, connections, and pass-through traffic.

Initially, when the WAE servers are assigned for each accelerator, the traffic load is increased on the device that handles the existing CIFS traffic. As soon as branches are updated to use the SMB accelerator, that traffic load drops, and the load on the designated SMB accelerator(s) begins to increase. At some point, the designated SMB accelerator(s) optimizes all traffic until the CIFS accelerator in the data center is updated for SMB with traffic distributed to it by AppNav or WCCP.

If you are adding additional WAE devices in your data center to add capacity or enhance the migration, see the [Cisco Wide Area Application Services Quick Configuration Guide](#).

## Using AppNav with Mixed SMB and CIFS Application Accelerators

This section describes how to use AppNav for a mixed SMB and CIFS application accelerator deployment.



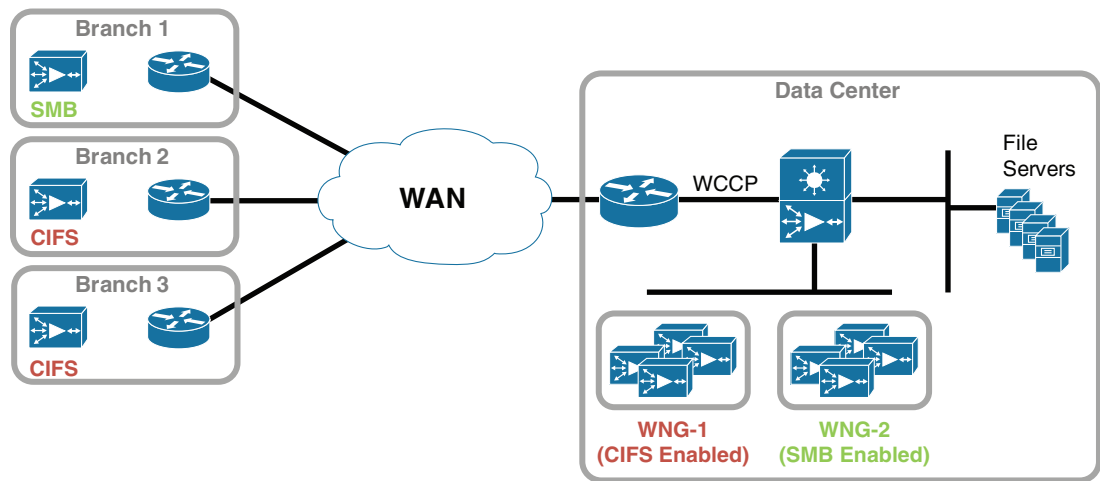
**Note**

See the “Configuring AppNav” chapter in the [Cisco Wide Area Application Services Quick Configuration Guide](#) for information about AppNav.

[Figure 1](#) shows an overview of using AppNav to control a mixed deployment of the SMB and CIFS application accelerators.

**Figure 1** Using an AppNav Cluster for Mixed SMB and CIFS Accelerator Deployment

### Phased-in SMB Migration Using AppNav



This section describes the steps required to migrate some of your branches to SMB acceleration with AppNav. This approach creates a WNG for the branch nodes you want to migrate to SMB acceleration, and uses branch affinity to distribute traffic from those branches to SMB accelerator nodes in the data center. Unmigrated nodes are left unchanged.



**Note**

You can use this migration method with either in-path (inline) or off-path (WCCP) devices.

### Mixed SMB and CIFS Migration Sequence Using AppNav

Follow the procedure below to use AppNav to migrate some of your WAAS system to the SMB application accelerator.

#### Procedure for Using AppNav for a Mixed Deployment Migration

- Step 1** Identify the number of connections you want to migrate and how to fit those connections into your WAAS network, as described in the [“Planning Your Migration”](#) section on page 17.
- Step 2** Determine which branches you want to migrate to SMB and create a WAAS node group (WNG) for those branch nodes, as described in the [“Configuring a WAAS Node Group for SMB Acceleration”](#) section on page 17.
- Step 3** Configure AppNav to distribute SMB traffic to the new WNG, as described in the [“Configuring AppNav Traffic for SMB Acceleration”](#) section on page 17.
- Step 4** Enable the SMB accelerator, as described in the [“Enabling SMB for Nodes in the New WNG”](#) section on page 17.
- Step 5** Verify that traffic is being optimized, as described in the [“Verifying That Both Accelerators are Working”](#) section on page 18.



## Planning Your Migration

Before migrating some of your branch nodes to the SMB accelerator, plan your migration by performing a sizing estimate and deciding if you have enough capacity to support a phased migration.

### Procedure

- 
- Step 1** Identify the number of branch devices that you want to migrate to the SMB accelerator.
  - Step 2** Determine how many file sharing connections those branches are handling.
  - Step 3** Decide whether your data center capacity supports accelerating those connections with SMB on existing devices, or if you need additional capacity.

If you determine that you need additional capacity, contact your Cisco representative.

---

## Configuring a WAAS Node Group for SMB Acceleration

After you determine how many branch devices you are migrating, configure a WAAS Node Group (WNG) for those devices.

### Procedure

- 
- Step 1** Select the group of target branches that you want to migrate to SMB acceleration.
  - Step 2** Create and configure a new SMB acceleration WNG for the devices you want to migrate, as described in the “Configuring AppNav” chapter of the [Cisco Wide Area Application Services Configuration Guide](#).
- 

## Configuring AppNav Traffic for SMB Acceleration

Next, configure AppNav to distribute traffic from those branch devices to the new SMB acceleration WNG. See the “Configuring AppNav” chapter of the [Cisco Wide Area Application Services Configuration Guide](#).

## Enabling SMB for Nodes in the New WNG

After you configure the WNG and AppNav, enable SMB on each branch device in the new WNG.

### Procedure

- 
- Step 1** Log in to the primary CM GUI.  
`https://cm_ip_address:8443`
  - Step 2** Choose **Device > WAEDevice > Configure > Acceleration > Enabled Features**.
  - Step 3** Check the **SMB Accelerator** check box.
-

## Verifying That Both Accelerators are Working

Finally, verify that the SMB application accelerator is working for your new WNG, and that the CIFS application accelerator is still working for the nodes you did not migrate.

### Procedure

**Step 1** Log in to the primary CM GUI.

```
https://cm_ip_address:8443
```

**Step 2** Verify that the correct accelerator is enabled for each group of nodes in your network.

```
show accelerators
```

**Step 3** Verify that the connections are being optimized.

```
show statistics connection
```

You know that a connection is being optimized when you see the letter C in the Accel column for that connection in the output of the **show statistics connection** command.

## Using WCCP Service Groups With Mixed SMB and CIFS Application Accelerators

This section describes using WCCP Service Groups for a mixed SMB and CIFS application accelerator deployment.



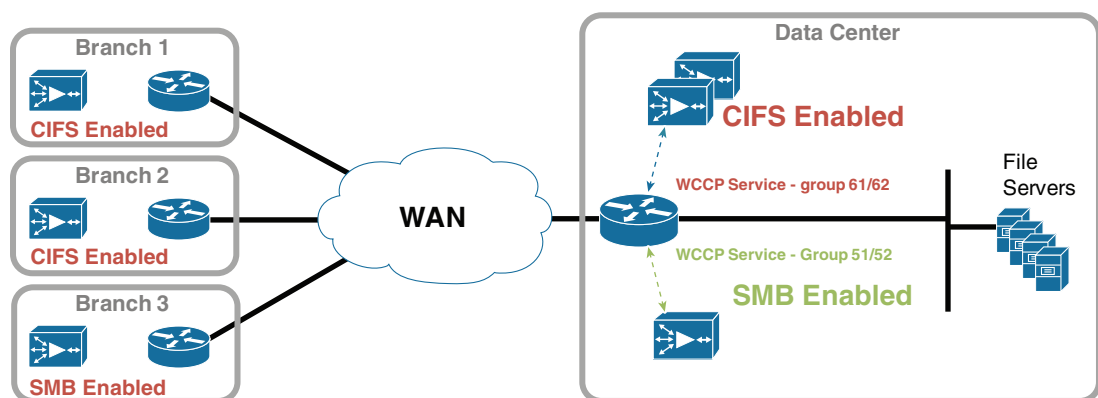
### Note

See the “Configuring Traffic Interception” chapter in the [Cisco Wide Area Application Services Quick Configuration Guide](#) for information about WCCP service groups.

Figure 2 shows an overview of using WCCP Service Groups to control a mixed deployment of SMB and CIFS application accelerators.

**Figure 2** Using WCCP Service Groups for a Mixed SMB and CIFS Accelerator Deployment

### Phased-in SMB Migration Using WCCP Service Groups



## Mixed SMB and CIFS Migration Sequence Using WCCP Service Groups

Follow the procedure below to use WCCP service groups to migrate some of your WAAS system to the SMB application accelerator.

### Procedure for Using WCCP Service Groups for a Mixed Deployment Migration

- 
- Step 1** Identify the number of connections you want to migrate and how to fit those connections into your WAAS network, as described in the [“Planning Your Migration” section on page 19](#).
  - Step 2** Configure the redirection devices in the data center for an additional set of WCCP Service IDs, as described in the [“Configuring Your Switches and Routers for the Migration”](#).
  - Step 3** Configure the new Service IDs to handle the subnets of the branches you are migrating to SMB acceleration, as described in the [“Setting the Access Control Lists on the Redirect Devices in the Data Center” section on page 20](#).
  - Step 4** Enable the SMB accelerator on the data center devices, as described in the [“Enabling SMB and Reconfiguring WCCP on the WAAS Devices in the Data Center” section on page 20](#).
  - Step 5** Enable the SMB accelerator on the branch devices, as described in the [“Enabling SMB on the Remote Accelerators in the Branch Subnets” section on page 21](#).
- 

## Planning Your Migration

Before migrating some of your branch nodes to the SMB accelerator, plan your migration by performing a sizing estimate and deciding if you have enough capacity to support a phased migration.

### Procedure

- 
- Step 1** Identify the number of branch devices that you want to migrate to the SMB accelerator.
  - Step 2** Determine how many file sharing connections those branches are handling.
  - Step 3** Decide whether your data center capacity supports accelerating those connections with SMB on existing devices or if you need additional capacity.  
If you determine that you need additional capacity, contact your Cisco representative.
  - Step 4** Plan to perform the migration during a maintenance window; existing traffic will be processed with less acceleration during the migration process.
- 

## Configuring Your Switches and Routers for the Migration

To start migrating your selected branch nodes to the SMB accelerator, you must add new service IDs 51 and 52 to each switch and router in the data center that performs redirection using WCCP Service IDs 61 and 62.

Use this procedure to set up the recommended services 51 and 52 on a router by configuring the data center router to separate the traffic flow for the CIFS and SMB accelerators.

**Procedure**

**Step 1** Create an access list to identify the branch subnets that you want to redirect to the SMB accelerator:

```
ip access-list extended bypass_branch_local
deny ip any any
```

**Step 2** Create the WCCP service groups and use the access list that you just created for the redirect list.

```
ip wccp 51 redirect-list bypass_branch_local
ip wccp 52 redirect-list bypass_branch_local
```

When you then add branch subnets to the access list, those subnets are redirected to the SMB accelerator.

**Step 3** Add the corresponding WCCP redirect commands to the router interfaces.

```
ip wccp 51 redirect in
ip wccp 52 redirect in
```

The new service groups do not yet intercept traffic, because none of the branch subnets are listed in the access list. Follow the remaining topics in this section to complete the migration.

See the “Configuring Traffic Interception” chapter of the [Cisco Wide Area Application Services Configuration Guide](#) for information about configuring WCCP services.

**Setting the Access Control Lists on the Redirect Devices in the Data Center**

After you create the new service IDs, set the access control lists (ACLs) on each of the redirect devices for those IDs to handle the subnets of the target branches you are migrating to SMB acceleration.

This example ACL template shows how to configure a router for WCCP Service Groups 51 and 52:

```
permit ip <Branch1> any
permit ip any <Branch1>
permit ip <Branch2> any
permit ip any <Branch2>
permit ip <Branch3> any
permit ip any <Branch3>
deny ip any any
```

See the “Configuring Traffic Interception” chapter of the [Cisco Wide Area Application Services Configuration Guide](#) for information about setting up ACLs on your routers and switches.

**Enabling SMB and Reconfiguring WCCP on the WAAS Devices in the Data Center**

Enable the SMB accelerator and reconfigure WCCP on the Data Center devices that you are migrating.

**Procedure**

**Step 1** Log in to the primary CM GUI.

```
https://cm_ip_address:8443
```

**Step 2** Choose **Devices > EdgeDevice > Configure > Acceleration > Enabled Features**.

- Step 3** Check the **SMB Accelerator** check box.
- Step 4** Reconfigure WCCP on the WAAS device to use the new 51 and 52 service IDs:
- Choose **Devices > EdgeDevice > Configure > Interception > Interception Configuration**.
  - Change the Service ID1 field value to 51.
  - Click **Submit**.

**Step 5** Verify that the accelerator has registered for the new IDs on the redirect devices:

- Verify that the correct accelerator is enabled for the redirect devices.

```
show accelerators
```

- Verify that the connections are being optimized.

```
show statistics connection
```

You know that a connection is being optimized when you see the letter C in the Accel column for that connection in the output of the **show statistics connection** command.



**Note** For more information about configuring WCCP, see the “Configuring Traffic Interception” chapter of the [Cisco Wide Area Application Services Configuration Guide](#).

## Enabling SMB on the Remote Accelerators in the Branch Subnets

Use this procedure to enable the SMB accelerator on the branch subnets for which you set up ACLs.

- Step 1** Log in to the primary CM GUI.
- ```
https://cm_ip_address:8443
```
- Choose **Device > RemoteDevice > Configure > Acceleration > Enabled Features**.

Step 2 Check the **SMB Accelerator** check box.

Step 3 Verify that the accelerator has registered for the new IDs on the redirect devices:

- Verify that the correct accelerator is enabled for the remote devices.

```
show accelerators
```

- Verify that the connections are being optimized.

```
show statistics connection
```

You know that a connection is being optimized when you see the letter C in the Accel column for that connection in the output of the **show statistics connection** command.

Migrating Dynamic Shares

If you migrate a device with dynamic shares on it from the CIFS application accelerator to the SMB application accelerator, you must recreate those dynamic shares after the migration.

Follow the instructions in the “Configuring File Services” chapter of the [Cisco Wide Area Application Services Configuration Guide](#).

Validity Testing and Rollbacks

This section describes specific actions that are related to backing up your software, restoring your software from a backup, registering upgrades, and testing different aspects of your network affected by the upgrade.

- [Backing Up the Central Manager Database, page 22](#)
- [Restoring the Central Manager Databases, page 22](#)
- [Registering an Upgraded WAE with the Central Manager, page 24](#)
- [Performing a WAE Software Downgrade, page 25](#)
- [Performing WCCP Validity Testing, page 25](#)
- [Performing SMB Validity Testing and Performing a Rollback, page 26](#)

Backing Up the Central Manager Database

Use this procedure to back up the databases of the primary and standby CMs.

Procedure

-
- Step 1** From the primary CM, create a backup of the database.
- ```
cms database backup
```
- Step 2** Copy the primary CM backup file to a remote location.
- ```
cd /local1
copy disk ftp ftp_ip_address remote_directory remote_file_name local_file_name
```
- Step 3** From the standby CM, create a backup of the database.
- ```
cms database backup
```
- Step 4** Copy the standby CM backup file to a remote location.
- ```
cd /local1
copy disk ftp ftp_ip_address remote_directory remote_file-name local_file_name
```
-

Restoring the Central Manager Databases

This section describes how to restore the databases on the primary and standby CMs using their database backup files (see the [“Backing Up the Central Manager Database” section on page 22](#)).

Guidelines and Restrictions

Use the following guidelines when restoring the CM databases:

- Ensure that the CM is using the same software version as when the database backup file was created.
- Restore the standby CM first and then restore the primary CM.

- If you are restoring a backup from a CM where the secure store was in user-provided passphrase mode when the backup was made, you may be asked to provide the secure store password during the restore process. For more information on the secure store, see the “Configuring Other System Settings” chapter of the *Cisco Wide Area Application Services Configuration Guide*.

This section contains the following topics:

- [Restoring the Standby Central Manager Database, page 23](#)
- [Restoring the Primary Central Manager Database, page 23](#)

Restoring the Standby Central Manager Database

Use this procedure to restore the standby CM database.

Procedure

-
- Step 1** From the standby CM, disable the Centralized Management System (CMS) service.

```
config
no cms enable
exit
```

- Step 2** Delete the existing CMS database.

```
cms database delete
```

- Step 3** Initialize the CMS database.

```
cms database create
```

- Step 4** Restore the CMS database contents from the backup file.

```
cms database restore bkup_file_name
```

- Step 5** Enable the CMS service.

```
config
cms enable
exit
```

- Step 6** Verify that the CMS services are running and that the database has synchronized.

```
show cms info
```

Wait at least 5 minutes and then confirm that the database last synchronization time is current. If the time is not current, wait another 5 minutes.

- Step 7** Check the current date and time on the standby CM.

```
show clock
```

- Step 8** Verify the CMS status in the running configuration.

```
show running-config | include cms
```

Restoring the Primary Central Manager Database

Use this procedure to restore the primary CM database.

Prerequisites

Restore the standby CM database before you restore the primary CM database (see the [“Restoring the Standby Central Manager Database”](#) section on page 23).

Procedure

Step 1 From the primary CM, disable the CMS service.

```
config
no cms enable
exit
```



Note Stopping the CMS service disables the CM GUI. All users logged in to this GUI are logged out when the CMS service is disabled.

Step 2 Delete the existing CMS database.

```
cms database delete
```

Step 3 Initialize the CMS database.

```
cms database create
```

Step 4 Restore the CMS database contents from the backup file.

```
cms database restore bkup_file_name
```

Step 5 Enable the CMS service.

```
config
cms enable
exit
```

Step 6 Verify that the CMS services are running.

```
show cms info
```

Step 7 Check the current date and time on the standby CM.

```
show clock
```

Step 8 Confirm that you see “Ready to accept incoming RPC requests” in the log file (errorlog/cms_log.current), which indicates that the WAE is ready to establish connections with the Central Manager.

Look for the timestamp from the output and compare it with the current time.

Step 9 Verify the CMS status in the running configuration.

```
show running-config | include cms
```

Step 10 Access the CM GUI from a browser.

Registering an Upgraded WAE with the Central Manager

If you cannot set a WAE in the Central Manager after upgrading the device, you must register the upgraded WAE, as shown in the following procedure.

Procedure

-
- Step 1** From the CM, delete the branch WAE.
- Step 2** From the branch WAE, enter the following commands:
- ```
cms deregister force
cms enable
```
- Step 3** From the CM, choose **Devices > branchWAE > Activation** to activate the branch WAE.
- 

## Performing a WAE Software Downgrade

Use this procedure to install a previous version of software on a branch WAE if you encounter a problem during the upgrade.

**Procedure**

- 
- Step 1** Determine the previously installed version.
- ```
show version last
```
- Step 2** Install the previous WAAS software version as follows:
- a. Telnet to the branch WAE.
 - b. Install the previous version software image.
- ```
copy ftp install ftpserver / waas-image.bin
```
- Step 3** Reload the branch WAE.
- ```
reload
```
- Step 4** Verify that the software image installed correctly.
- ```
show version
```
- 

If you want to downgrade your entire WAAS network software to a previous version, see the [Release Note for Cisco Wide Area Application Services](#).

## Performing WCCP Validity Testing

This section lists the commands that you can use for WCCP validity testing.

Enter the commands three to four times in succession to determine if counters are incrementing.

The commands are as follows:

- WAE commands:
  - **show clock detail**
  - **show wccp statistics**
  - **show wccp routers**

- **show wccp clients**
- **show wccp flows tcp-promiscuous detail**
- Router and switch commands (for each service group where applicable):
  - **show ip wccp**
  - **show ip wccp *service* *service***
  - **show ip wccp *service* *detail***
  - **show ip wccp *service* *internal*** (available in most recent releases only)
  - **show ip wccp *interface* *detail*** (available in most recent releases only)
- Router and switch commands (when hashing is used):
  - **show tcam counts**
  - **show mls stat**
  - **show mls netflow table detail**
  - **show mls netflow ip count**
  - **show mls netflow ip sw-installed count**
  - **show mls netflow ip sw-installed detail**
  - **show fm interface *interface\_name***
- Router and switch commands (when masking is used):
  - **show ip wccp *service* *mask***
  - **show ip wccp *service* *merge***
  - **show tcam interface *interface name* *acl* {in | out} ip**
  - **show tcam interface *interface name* *acl* {in | out} ip detail**

For possible Cisco IOS issues, capture the following debug output to either the console or a Telnet session:

- **debug ip wccp events**
- **debug ip wccp packets**

## Performing SMB Validity Testing and Performing a Rollback

This section describes the methods that you can use for SMB validity testing, which includes manual procedures and automation tools.

### Guidelines and Restrictions

Use the following guidelines when performing SMB validity testing and performing a rollback:

- Choose a single file or a variety of files for the test. You must use the same file or files for all the tests (base, cold, hot).
- Use an existing share or create a directory structure on the file server. Verify that the share has permissions set for domain users. We recommend that you test or create a share that has multiple nested directories (at least 2 to 3 levels deep) that contain files of various types (such as PowerPoint, Excel or Word) and sizes.

This section contains the following topics:

- [Preparing the Shared Server and Client for SMB Validity Testing, page 27](#)
- [Performing a Manual SMB Performance Test with WAAS, page 27](#)
- [Evaluating the Manual Test Results, page 28](#)
- [Rolling Back from the SMB Application Accelerator to the CIFS Application Accelerator, page 30](#)

## Preparing the Shared Server and Client for SMB Validity Testing

Use this procedure to prepare the shared server and client for SMB validity testing.

### Procedure

- 
- Step 1** On the server, create a share directory that contains several subfolders and files.
- Step 2** Verify the following items on the shared server:
- Adequate permissions for domain users used in the testing.
  - Domain users can access the share before testing WAAS.
  - SMB signing (digital signature) is disabled on the server.
- Step 3** Verify the following items on the client:
- PC clients are part of the tested domain environment.
  - A domain user exists for each PC client.
  - Tested shares do not rely on local user and groups but rather have permissions for domain users and groups.
  - Microsoft Office (Word, Excel, PowerPoint) is installed.
- 

## Performing a Manual SMB Performance Test with WAAS

Use this procedure to manually perform a SMB performance test.

### Procedure

- 
- Step 1** Verify operation by opening some Microsoft Office documents from the shared server. Record the filename, size, and open time.

| Filename | File Size | Time to Open |
|----------|-----------|--------------|
|          |           |              |
|          |           |              |
|          |           |              |
|          |           |              |
|          |           |              |
|          |           |              |

**Step 2** Modify the files by adding some text and saving.  
Record the time it takes to save.

| Filename | File Size | Time to Save |
|----------|-----------|--------------|
|          |           |              |
|          |           |              |
|          |           |              |
|          |           |              |
|          |           |              |
|          |           |              |

**Step 3** Open the files again to inspect response time and data integrity.  
Record the time it took to open them and get to the place where your changes were made.

| Filename | File Size | Time to Open |
|----------|-----------|--------------|
|          |           |              |
|          |           |              |
|          |           |              |
|          |           |              |
|          |           |              |
|          |           |              |

**Step 4** Evaluate the results of the testing (see the [“Evaluating the Manual Test Results”](#) section on page 28).

## Evaluating the Manual Test Results

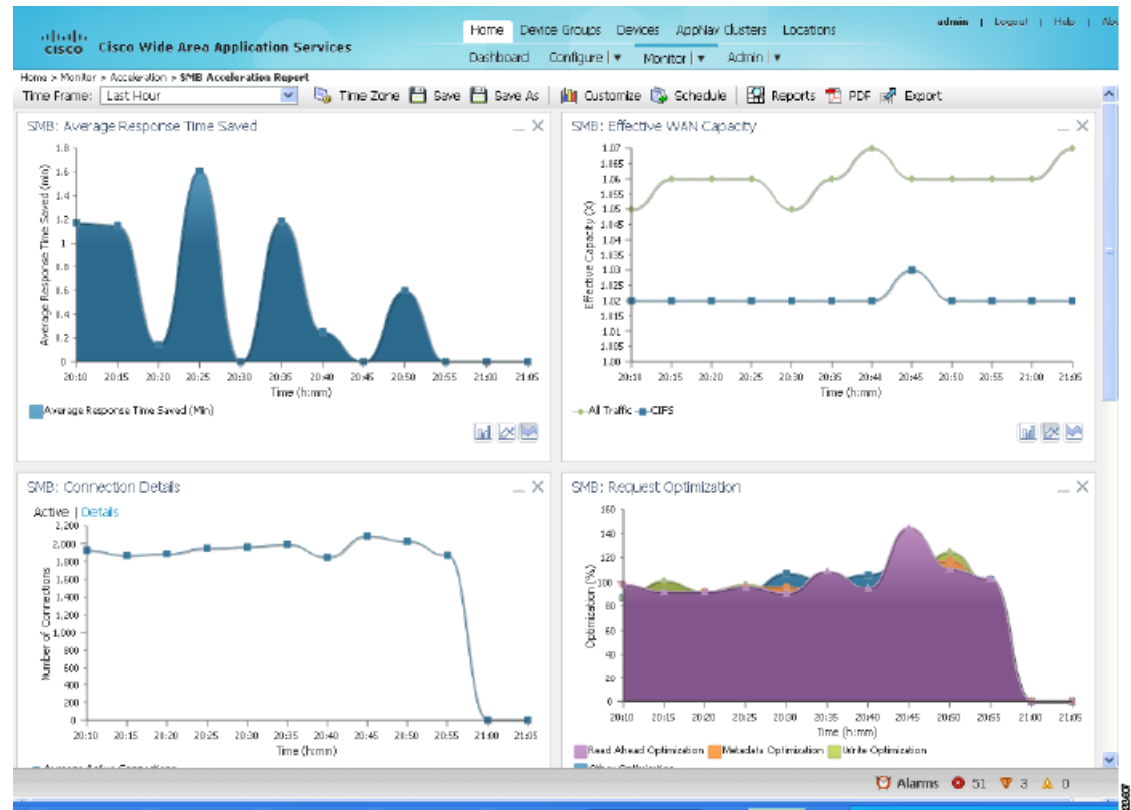
This section describes the expected results of the manual SMB performance test (see the [“Performing a Manual SMB Performance Test with WAAS”](#) section on page 27).

The test should show significant improvement in the time to open and time to save operations. The same behavior should also be observed with the modified file.

The Central Manager provides real-time statistics and a summary report for SMB connections (**Devices > branchWAE > Monitor > Acceleration > SMB Acceleration Report**).

[Figure 3](#) shows some of the SMB charts.

Figure 3 SMB Acceleration Report



From the CLI, the following information appears:

```
WAE674# show statistics connection optimized
```

```
Current Active Optimized Flows: 1
 Current Active Optimized TCP Plus Flows: 1
 Current Active Optimized TCP Only Flows: 0
 Current Active Optimized TCP Preposition Flows: 0
Current Active Auto-Discovery Flows: 0
Current Active Pass-Through Flows: 0
Historical Flows: 100
```

D:DRE,L:LZ,T:TCP Optimization,

A:AcceleratorIM,C:CIFS,E:EPM,G:GENERIC,H:HTTP,M:MAPI,N:NFS,S:SSL,V:VIDEO

| ConnID | Source IP:Port  | Dest IP:Port  | PeerID            | Accel |
|--------|-----------------|---------------|-------------------|-------|
| 214682 | 2.8.35.100:2122 | 2.8.1.200:445 | 00:23:7d:06:6e:08 | TCDL  |

To display detailed information about any SMB connection, enter the **show statistics connection optimized smb detail** command.

To display overall SMB accelerator statistics, enter the **show statistics accelerator smb detail** command as follows:

```
WAE674# show statistics accelerator smb detail
```

```
CIFS:
```

```
Global Statistics
```

```

```

```
Time Accelerator was started:
```

```
Sun May 17
```

```
06:11:00 2009
```

```

Time Statistics were Last Reset/Cleared: Sun May 17
06:11:00 2009
Total Handled Connections: 10565
Total Optimized Connections: 0
Total Connections Handed-off with Compression Policies Unchanged: 0
Total Dropped Connections: 0
Current Active Connections: 0
Current Pending Connections: 0
Maximum Active Connections: 5
Number of local reply generating requests: 13266
Number of remote reply generating requests: 13266
The Average time to generate a local reply (msec): 0
Average time to receive remote reply (ms): 1

```

## Rolling Back from the SMB Application Accelerator to the CIFS Application Accelerator

Use this procedure to roll back from the SMB application accelerator to the CIFS application accelerator if a failure occurs when upgrading to the SMB application accelerator or if SMB is not optimized. The SMB application accelerator can be rolled back to the CIFS application accelerator by reenabling the CIFS Accelerator feature on the WAE devices.

### Procedure

- 
- Step 1** Perform the following tasks on the branch WAE devices:
- Choose **Devices** > *BranchWAE* > **Configure** > **Acceleration** > **Enabled Features** and check the **CIFS Accelerator** check box. This automatically unchecks the SMB Accelerator check box.
- Step 2** Perform the following tasks on the data center WAE devices:
- Choose **Devices** > *DataCenterWAE* > **Configure** > **Acceleration** > **Enabled Features** and check the **CIFS Accelerator** check box. This automatically unchecks the SMB Accelerator check box.
- 

## Additional Resources

For additional information on the Cisco WAAS software, see the following documentation:

- [Release Note for Cisco Wide Area Application Services](#)
- [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 Wide Area Application Services Upgrade Guide](#) (this manual)
- [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*
- *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 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 *What's New in Cisco Product Documentation* at:

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

Subscribe to *What's New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation, as an RSS feed and deliver content directly to your desktop using a reader application. The RSS feeds are a free service.

---

This document is to be used in conjunction with the documents listed in the “Additional Resources” section.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2010-2013 Cisco Systems, Inc. All rights reserved.