This article introduces the basic concepts, methodology, and general troubleshooting guidelines for problems that may occur when you configure and use your WAAS system.

Guide Contents
Main Article
Understanding the WAAS Architecture and Traffic Flow
Preliminary WAAS Troubleshooting
Troubleshooting Optimization
Troubleshooting Application Acceleration
Troubleshooting the CIFS AO
Troubleshooting the HTTP AO
Troubleshooting the EPM AO
Troubleshooting the MAPI AO
Troubleshooting the NFS AO
Troubleshooting the SSL AO
Troubleshooting the Video AO
Troubleshooting the Generic AO
Troubleshooting Overload Conditions
Troubleshooting WCCP
Troubleshooting AppNav
Troubleshooting Disk and Hardware Problems
Troubleshooting Serial Inline Clusters
Troubleshooting vWAAS
Troubleshooting WAAS Express
Troubleshooting NAM Integration

Contents

Overview of the WAAS Troubleshooting Process

To troubleshoot your WAAS system, follow these general guidelines:

1. Maintain a consistent and recommended software version across all your WAAS devices. If versions must differ, the Central Manager must be running the highest version. See the "Verifying the WAAS Image" section to determine the version in use.
2. See the WAAS release notes for your software version for the latest features, operating considerations, caveats, and CLI command changes.
3. Before you introduce configuration changes on the WAAS Central Manager, use the CMS backup feature to save your configuration. If you run into problems with the new configuration, you can restore the previous configuration. See the *Backing Up and Restoring your WAAS System* section in the *Cisco Wide Area Application Services Configuration Guide*. Troubleshoot any problems with new configuration changes immediately after making them.
4. Verify that your configuration is correct for your network application. Make any required changes to the running-config file, and then test the configuration. If it is satisfactory, save it to the startup-config file using the **copy running-config startup-config** command.
5. Enable system message logging. See the "Enabling WAAS Logging" section.
6. Run the diagnostic tool to verify device functionality and connectivity. See the "Running Diagnostics" section.
7. Verify the physical connectivity between WAAS peers and to the application servers. See the "Verifying the Physical Connectivity Between Peer WAAS Devices and to Application Servers" section.
8. Gather information that defines the specific symptoms. See the "Gathering WAAS Troubleshooting Information" section.
9. Refer to one of the other articles in this WAAS Troubleshooting Guide for information on troubleshooting specific problems:
    - If the system appears to be having hardware or disk problems, see the article Troubleshooting Disk and Hardware Problems.
    - If the system is having trouble receiving traffic, see the article Troubleshooting WCCP. This problem also could be due to a firewall issue.
    - If the system is passing through traffic instead of optimizing it or is having problems optimizing specific kinds of application traffic (HTTP, MAPI, SSL, and so on), see the articles Troubleshooting Optimization and Troubleshooting Application Acceleration.
    - If the system is passing through more traffic than expected instead of optimizing it, see the article Troubleshooting Overload Conditions.
10. After you have determined that your troubleshooting attempts have not resolved the problem, contact the Cisco Technical Assistance Center (TAC) or your technical support representative. See the "Contacting Cisco Technical Support" section.

Verifying the WAAS Image

To display the version of the software image that is currently running in your WAAS device, enter the following command:

```
wae# show version
Cisco Wide Area Application Services Software (WAAS)
Copyright (c) 1999-2009 by Cisco Systems, Inc.
Cisco Wide Area Application Services Software Release 4.1.3a (build b25 May 23 2  <--------
009)
Version: oe7341-4.1.3a.25
```

```
Compiled 10:10:47 May 23 2009 by cnbuild

System was restarted on Wed May 27 14:45:28 2009.
The system has been up for 6 weeks, 2 hours, 35 minutes, 48 seconds.
```

This command provides other useful information, for example:

- Device model (the numbers in the first part of the Version string encode the device model number; a WAE-7341 is shown here.)
- WAE uptime

To verify that there is no pending software upgrade (waiting for a device reboot), enter the following command:

```
wae# show version pending
No pending version
```

You should see the message "No pending version".

Enabling WAAS Logging

General system error logging to the disk file /local1/syslog.txt is enabled by default. You can check that logging is enabled by entering the following command:

```
wae# show logging
Syslog to host is disabled.

Syslog to console is disabled
Priority for console logging is set to:  warning

Syslog to disk is enabled                                    <------------
Priority for disk logging is set to:  notice
Filename for disk logging is set to:  /local1/syslog.txt

Syslog facility is set to *

Syslog disk file recycle size is set to 10000000
```

To enable logging to the console, enter the following global configuration command:

```
wae(config)# logging console enable
```

NOTE: Setting the logging priority to a level lower than notice can be CPU intensive and can generate a large amount of output. Use it judiciously and sparingly in a production environment.

The following directories are used by WAAS for log files:

- /local1 ? Root directory for all log files and location of syslog.txt
- /local1/logs ? Service log files (admin and transaction logs)
- /local1/errorlog ? Service log files (debug logs)
- /local1/errorlog/cifs ? CIFS internal log files
- /local1/core_dir ? Process core dump files

You can use the following file system navigation commands to navigate and view the log files:

- **cd**
- **pwd**
- **dir**
- **type-tail** *filename lines* [| | **follow**]
- **find-pattern**

Running Diagnostics

The WAAS Central Manager includes a built-in diagnostic tool that can help you troubleshoot many device problems, including the following:

- Network configuration
- Interface configuration
- Connectivity to hosts
- WCCP configuration
- Inline configuration
- TFO configuration
- WAFS configuration

We recommend that you run the diagnostic tool first before taking other troubleshooting actions. The tool reports on the status and configuration of many system functions.

To run the diagnostic tool from the Central Manager, follow these steps:

1. From the WAAS Central Manager GUI navigation pane, choose **My WAN > Manage Devices** (or **Manage Device Groups**).
2. Click the **Edit** icon next to the name of the device (or device group) for which you want to perform diagnostic tests.
3. In the navigation pane, choose **Troubleshoot > Diagnostics Tests**. The Diagnostic Tool window appears.
4. Check the check box next to each diagnostic test that you want to run, or check the top check box to run all tests.
5. Click **Run**.
6. View the test results in the lower part of the window. You may have to scroll the window to see all results.

For tests that fail, error messages describe the problem and provide recommended solutions. You can find error message descriptions in the **test** command in the *Cisco Wide Area Application Services Command Reference*.

You can run the same diagnostic tests again and refresh the results by clicking the **Refresh** icon in the taskbar.

To print the results, click the **Print** icon in the taskbar.

To run the diagnostic tests from the CLI, use the **test** EXEC command.

Verifying the Physical Connectivity Between Peer WAAS Devices and to Application Servers

To verify the physical connectivity of the peer WAAS device, follow these steps:

1. Check all cable connections on the switch or router that may impact the WAAS device.
2. Use the **ping** command to send an ICMP Echo request to the peer WAE.

```
wae# ping 10.1.1.2
PING 10.1.1.2 (10.1.1.2) 56(84) bytes of data.
64 bytes from 10.1.1.2: icmp_seq=1 ttl=37 time=83.9 ms
64 bytes from 10.1.1.2: icmp_seq=2 ttl=37 time=80.6 ms
64 bytes from 10.1.1.2: icmp_seq=3 ttl=37 time=79.2 ms
64 bytes from 10.1.1.2: icmp_seq=4 ttl=37 time=79.3 ms
64 bytes from 10.1.1.2: icmp_seq=5 ttl=37 time=79.4 ms

--- 10.1.1.2 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3997ms
rtt min/avg/max/mdev = 79.274/80.538/83.904/1.793 ms
```

If a device is one hop away and you are unable to reach the device, then ping the intermediary gateway. If the gateway is not reachable, enter the **show ip routes** command and check to make sure that the correct route is displayed. For example, enter:

```
wae# show ip routes
Destination      Gateway          Netmask
---------------- ---------------- ----------------
10.10.10.1       0.0.0.0          255.255.255.255
10.43.62.4        0.0.0.0          255.255.255.255
10.43.62.0        0.0.0.0          255.255.255.192
10.10.10.0       0.0.0.0          255.255.255.0
0.0.0.0          10.43.62.1        0.0.0.0
```

If necessary, enter a static route for the gateway.

You can use a similar ping command to verify connectivity between the WAAS data center device and the application server hosts.

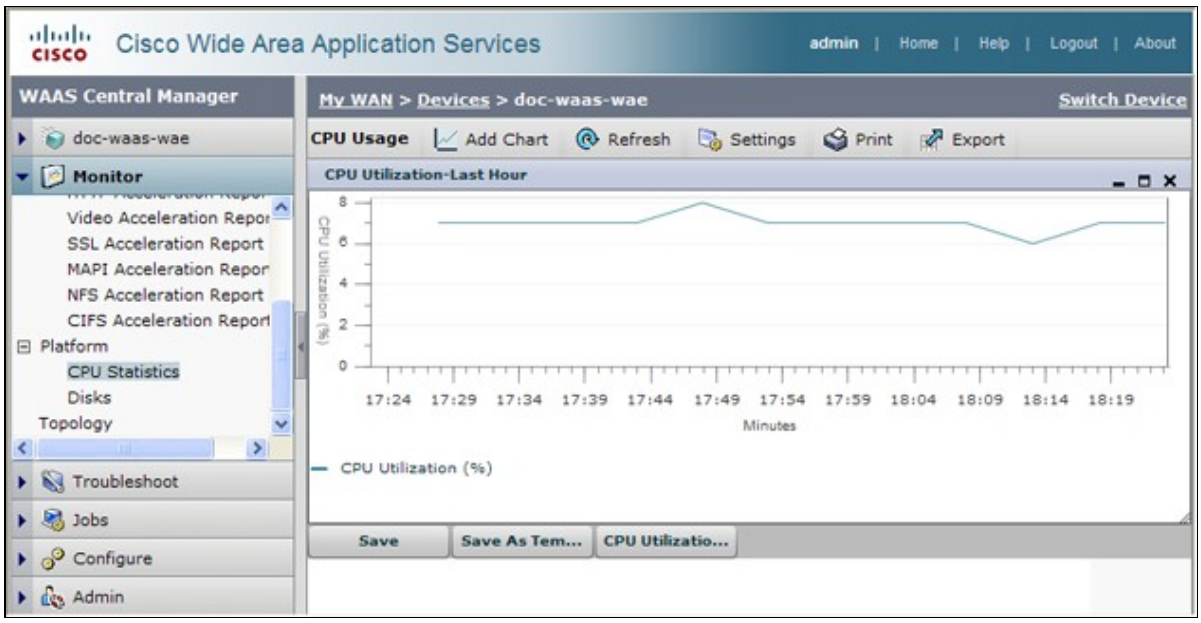
Note that firewalls might block ICMP traffic and ICMP traffic does not follow the WCCP redirection path, so using the **ping** command does not verify redirection or acceleration. As an alternative you could use a third party tool that performs a TCP-based ping.

Checking CPU Load

To check the CPU load of a WAAS device, follow these steps:

1. From the WAAS Central Manager GUI navigation pane, choose **My WAN > Manage Devices**.
2. Click the **Edit** icon next to the name of the device on which you want to check the CPU load.
3. In the navigation pane, choose **Monitor > Platform > CPU Statistics**.

Figure 1. CPU Statistics



You may want to adjust the time period of the chart, since the default is Last Hour. To adjust the time period, click the **Settings** icon in the task bar and choose a different Time Frame such as Last Day or Last Week.

It is common for a WAAS device to show spikes or even longer durations of high CPU utilization during high user activity periods. When the CPU remains at a high CPU level for significantly long durations, further troubleshooting or resizing of the device may be indicated.

Gathering WAAS Troubleshooting Information

The following sections recommend ways to gather information that is relevant to the problem that is occurring and that is necessary before contacting the Cisco Technical Assistance Center (TAC).

Rebooting the WAAS Device

Do not reboot the WAAS device unless it is absolutely necessary. Some information that is important to troubleshooting your problem may not survive a reboot. Try to gather as much information as possible before rebooting.

Using show Commands

You can use several **show** commands in Exec mode to gather information specific to the symptoms you are observing in your device. In most cases, you can gather the information you need to troubleshoot the device by entering the **copy tech-support** command. This command runs many **show** commands that are useful for troubleshooting and gathers the output into a single file. You can redirect the output of the **copy tech-support** command to a disk file, an FTP server, or a TFTP server. The command syntax is as follows:

copy tech-support {**disk** *filename* | **ftp** {*hostname* | *ip-address*} *remotedirectory remotefilename* | **tftp** {*hostname* | *ip-address*} *remotefilename*}

For example, to copy the output of the command to a disk file on the local system, specify the command as follows:

```
wae# copy tech-support disk ts-report.txt
```

Other useful **show** commands include the following:

- **show alarms**: Displays alarms.
- **show accelerator**: Displays application accelerator status.
- **show license**: Displays license status.
- **show statistics connection**: Displays statistics for all TCP connections.
- **show statistics tfo**: Displays TFO statistics.
- **show interface**: Displays interface information and status. Verify that the speed and duplex match with the switch.

- For WCCP deployments, use the following commands on the WAE:
  - **show wccp gre**
  - **show wccp routers**
  - **show wccp wide-area-engine**
  - **show wccp flows**
  - **show egress-methods**

- For WCCP deployments, use the following commands on the router or switch (for each service group, where applicable):
  - **show ip wccp**
  - **show ip wccp interfaces detail**
  - **show ip wccp** *service*
  - **show ip wccp** *service* **detail**

- For WCCP deployments, use the following commands on the router or switch 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 inteface** *interface_name*

- For WCCP deployments, use the following commands on the router or switch 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**

Generating a System Report

A system report (sysreport) is a comprehensive report that you will need before you contact Cisco technical support. You can generate a sysreport by running the **copy sysreport** command. The system report contains the output from many commands and logs on the system, including show commands, network statistics, graphs, log contents, configuration settings, statistics, and so on. It can take some time to generate a system report and it can be from 30 - 100 MB in size or larger. The system report contains many more elements than are included in the **copy tech-support** command, and is generally needed when contacting Cisco technical support.

Before generating a system report, use the **test** command to run the diagnostic tests so that this information is included in the system report. When generating a system report on a Central Manager (or standby Central Manager), you should first make a database backup by using the **cms database backup** command.

To generate a sysreport and store it to an FTP server, use this form of the command: **copy sysreport ftp** *server-ip remote-directory remote-file-name*

For example:

```
wae# copy sysreport ftp 10.10.10.5 /reports wae1report
```

When generating a system report, do not use any command options that limit the report to a specific time period, as this could cause information even within that time period not to be included.

Capturing and Analyzing Packets

Capturing packets (sometimes referred to as a "TCP dump") is a useful aid in troubleshooting connectivity problems with the WAAS device or for monitoring suspicious activity. The WAAS device can track packet information for network traffic that passes through it. The attributes of the packet are defined by an ACL. The WAAS device buffers the captured packets, and you can copy the buffered contents to a file or to a remote server. You can also display the captured packet information on your console or terminal.

Two packet capture utilities are available: **tcpdump** and **tethereal**. These commands require admin privileges.

By default, these commands capture only the first 64 bytes of each packet. We recommend that you use the **-s 1600** option to capture full packet data.

If you will be taking large traces, use **tcpdump** to create rolling packet captures in multiple files. (The **-C** option sets the maximum size of each captured file in KB and the **-M** option sets the maximum number of log files to create.)

If you need to filter the packets captured, use **tethereal** with the **-R** read filter option. You can use **tcpdump** to create a large packet capture, then use **tethereal** against the captured file to perform filtering.

Be careful when using **tcpdump** in a WCCP environment because **tcpdump** filters do not look within the GRE wrapper. You will need to use **tethereal** if you need to do that.

With both commands, use the **-i any** option to capture all interfaces, or separate telnet sessions to capture on separate interfaces. Use **^c** (CTRL+c) to stop the packet capture.

There are several packet analysis tools that you can use to analyze packet capture files after you have captured them:

- Wireshark: A free packet analysis tool with extensive capabilities (recommended over Ethereal).
- Ethereal: Another free packet analysis tool with extensive capabilities.
- Microsoft Netmon: Included with Windows server software.
- Sniffer Pro

Using tcpdump

For the full tcpdump syntax, see **tcpdump** in the *Cisco Wide Area Application Services Command Reference*.

The most useful tcpdump options are as follows:

- -i *interface* : The interface where you want to capture packets, for example:
  - ♦ lo : localhost

    - eth0 : GigabitEthernet 1/0
    - eth1 : GigabitEthernet 2/0
    - eth2 : InlinePort 1/1/wan
    - eth3 : InlinePort 1/1/lan
    - eth4 : InlinePort 1/0/wan
    - eth5 : InlinePort 1/0/lan
    - any : All available Ethernet ports. Be aware that the "any" interface cannot capture in promiscuous mode, so it may miss some outgoing packets. For more information, see the Linux man page on tcpdump(8). Note: This option is not available on WAAS version 4.1.5 and later.
    - bond0 : Logical interface that combines all physical interfaces.
- -s *snaplen*: The maximum size that will be captured for each packet.
- -w *file*: The name of the file where the captured packets will be written in their raw form.
- -C *count*: The maximum size of the capture file, specified in thousands of bytes. If the -M option is also specified, additional capture files are created.
- -M *num*: The maximum number of log files created by rollover when the maximum file size is reached. This specifies how many capture files to make before stopping the capture.
- -D: Dumps the list of interfaces available for capturing.

The following example captures all packets to the file packets1.cap:

```
wae# tcpdump -i bond0 -s 1600 -w packets1.cap
```

Using tethereal

For the full tethereal syntax, see **tethereal** in the *Cisco Wide Area Application Services Command Reference*.

Useful tethereal options are as follows:

- -R *read_filter*: Filtering can be very useful. Use the same filtering syntax as you would use with Ethereal or Wireshark, so you can use one of those tools to help you compose a filter. tethereal is also useful for file conversion and filtering of a packet capture file that has already been captured (for example, from tcpdump).
- -F *output_filetype*: The default filetype is a libpcap file; however, the following options are available:
    - libpcap - libpcap (tcpdump, Ethereal, etc.)
    - rh6_1libpcap - RedHat Linux 6.1 libpcap (tcpdump)
    - suse6_3libpcap - SuSE Linux 6.3 libpcap (tcpdump)
    - modlibpcap - modified libpcap (tcpdump)
    - nokialibpcap - Nokia libpcap (tcpdump)
    - lanalyzer - Novell LANalyzer
    - ngsniffer - Network Associates Sniffer (DOS-based)
    - snoop - Sun snoop
    - netmon1 - Microsoft Network Monitor 1.x
    - netmon2 - Microsoft Network Monitor 2.x
    - ngwsniffer_1_1 - Network Associates Sniffer (Windows-based) 1.1
    - ngwsniffer_2_0 - Network Associates Sniffer (Windows-based) 2.00x
    - nettl - HP-UX nettl trace
    - visual - Visual Networks traffic capture
    - 5views - Accellent 5Views capture
    - niobserverv9 - Network Instruments Observer version 9

The following examples show various options used for filtering and conversion:

To convert from one file format to another, use a command similar to the following:

```
wae# tethereal -r test-netmon.cap -F libpcap -w test-libpcap.cap
```

To use a read filter for the SYN flag, use a command similar to the following:

```
wae# tethereal -R "tcp.flags.syn eq 1"
```

To use a read filter for specific hosts (and look inside GRE packets), use a command similar to the following:

```
wae# tethereal -s 1600 -w dump1.cap ?R "ip.addr eq 2.43.183.254 and ip.addr eq 2.43.182.165"
```

Note: The tethereal command has some usage caveats that you should be aware of:

- A filter defined using the -R option is ignored when it is combined with the -w option (writing to a file) in WAAS 4.1.1 and 4.1.3. To filter captured traffic and write to a disk file, use -f option to specify a capture filter. This issue is resolved in version 4.1.5.
- When using the -a option to print heavy traffic to the screen, it can take significantly longer than the autostop duration to display the information on the screen. Wait for the command to finish. Displaying output to the console can take significantly longer than through telnet or SSH, so console display is not recommended.
- When using the -f option with the "host" or "not host" filter expression, the wrong traffic may be captured with WCCP GRE encapsulated or VLAN traffic. With WCCP GRE traffic, tethereal sees only the outermost IP address, not the original IP address inside the encapsulated packets. Add the "proto 47" keyword into the -f filter expression to capture the correct traffic. Additionally, for VLAN traffic, add the "vlan" keyword into the -f filter expression to let the command parse VLAN traffic correctly.
- When using the -a filesize option together with the -R option, tethereal may stop unexpectedly and print the message "Memory limit is reached" before reaching the specified autostop file size. In this case, the maximum memory limit for the command was reached before the autostop file size limit.

Contacting Cisco Technical Support

If you are unable to resolve a problem after using the troubleshooting suggestions in the articles in this wiki, contact the Cisco Technical Assistance Center (TAC) for assistance and further instructions. Before you call, have the following information ready to help your TAC engineer assist you as quickly as possible:

- Date that you received the WAAS hardware
- Chassis serial number
- Type of software and release number (if possible, enter the **show version** command)
- Maintenance agreement or warranty information
- A good problem description including:
    - ♦ What is the problem and what are the user visible symptoms?
    - ♦ Where and when it occurs
    - ♦ Error messages, alerts, and alarms seen
    - ♦ Steps to duplicate the problem
- Brief explanation of the steps that you have already taken to isolate and resolve the problem
- The diagnostic test output (see the "Running Diagnostics" section)
- A Central Manager database backup (use the **cms database backup** command)
- Information gathered in the "Gathering WAAS Troubleshooting Information" section.
- Topology diagrams, including network/wiring diagrams and logical diagrams
- Any other evidence of the problem such as packet captures, transaction logs, core files, WCCP show command output from routers/switches and WAEs, and other log files.

You can reach TAC in one of these ways:

- Create a service request online
- Call the TAC at the telephone numbers on this page.
- Contact the Cisco Small Business Support Center