

# Cisco WAAS-Fehlerbehebungsleitfaden für Version 4.1.3 und höher

## Kapitel: Vorläufige WAAS-Fehlerbehebung

In diesem Artikel werden die grundlegenden Konzepte, die Methodik und die allgemeinen Richtlinien zur Fehlerbehebung für Probleme vorgestellt, die bei der Konfiguration und Verwendung des WAAS-Systems auftreten können.

- [1 Übersicht über den Fehlerbehebungsprozess für WAAS](#)
- [2 Überprüfen des WAAS-Images](#)
- [1 Aktivieren der WAAS-Protokollierung](#)
- [4 Diagnosen ausführen](#)
- [5 Überprüfen der physischen Verbindung zwischen Peer-WAAS-Geräten und Anwendungsservern](#)
- [6 Überprüfen der CPU-Last](#)
- [7 Sammeln von Informationen zur WAAS-Fehlerbehebung](#)
  - [7,1 Neustarten des WAAS-Geräts](#)
  - [7,2 Verwenden von Show-Befehlen](#)
  - [7,3 Erstellen eines Systemberichts](#)
  - [7,4 Erfassen und Analysieren von Paketen](#)
    - [7,4/1 Verwenden von tcpdump](#)
    - [7,4/2 Verwendung von Tetheral](#)

Inh

Ha

An

Da

Vo

Op

Pro

Fel

Fel

Fel

Fel

Fel

Fel

Fel

Fel

Fel

Fel

Fel

Fel

Ha

Fel

vW

Fel

Fel

- [8 Kontaktieren des technischen Supports von Cisco](#)

## Übersicht über den Fehlerbehebungsprozess für WAAS

Um eine Fehlerbehebung für Ihr WAAS-System durchzuführen, befolgen Sie die folgenden allgemeinen Richtlinien:

1. Beibehaltung einer konsistenten und empfohlenen Softwareversion für alle WAAS-Geräte. Wenn sich die Versionen unterscheiden müssen, muss der Central Manager die höchste Version ausführen. Im Abschnitt "[Verifying the WAAS Image](#)" (Überprüfen des WAAS-Images) können Sie die verwendete Version ermitteln.
2. In den [WAAS-Versionshinweisen](#) finden Sie Informationen zu den neuesten Funktionen, Überlegungen zum Betrieb, Vorbehalte und Änderungen an CLI-Befehlen.
3. Bevor Sie Konfigurationsänderungen in WAAS Central Manager einführen, speichern Sie Ihre Konfiguration mithilfe der CMS-Sicherungsfunktion. Wenn bei der neuen Konfiguration Probleme auftreten, können Sie die vorherige Konfiguration wiederherstellen. Weitere Informationen finden Sie im Abschnitt [Sichern und Wiederherstellen Ihres WAAS-Systems](#) im *Konfigurationshandbuch für Cisco Wide Area Application Services*. Fehlerbehebung bei Problemen mit neuen Konfigurationsänderungen unmittelbar nach deren Durchführung.
4. Überprüfen Sie, ob Ihre Konfiguration für Ihre Netzwerkanwendung korrekt ist. Nehmen Sie alle erforderlichen Änderungen an der Datei running-config vor, und testen Sie dann die Konfiguration. Wenn sie zufriedenstellend ist, speichern Sie sie mithilfe des Befehls `copy running-config startup-config` in der Datei startup-config.
5. Aktivieren Sie die Protokollierung der Systemmeldungen. Weitere Informationen finden Sie im Abschnitt "[Aktivieren der WAAS-Protokollierung](#)".
6. Führen Sie das Diagnosetool aus, um die Gerätefunktionalität und -anbindung zu überprüfen. Siehe Abschnitt "[Diagnosetests durchführen](#)".
7. Überprüfen Sie die physische Verbindung zwischen WAAS-Peers und den Anwendungsservern. Weitere Informationen finden Sie im Abschnitt "[Überprüfen der physischen Verbindung zwischen Peer-WAAS-Geräten und Anwendungsservern](#)".
8. Sammeln Sie Informationen, die die spezifischen Symptome definieren. Weitere Informationen finden Sie im Abschnitt "[Informationen zur WAAS-Fehlerbehebung sammeln](#)".
9. Informationen zur Behebung spezifischer Probleme finden Sie in einem der anderen Artikel in diesem WAAS-Leitfaden zur Fehlerbehebung:
  - Wenn im System Hardware- oder Festplattenprobleme auftreten, lesen Sie den Artikel [Fehlerbehebung bei Festplatten- und Hardwareproblemen](#).
  - Wenn das System Probleme beim Empfangen von Datenverkehr hat, lesen Sie den Artikel [Fehlerbehebung bei WCCP](#). Dieses Problem kann auch auf ein Firewall-Problem zurückzuführen sein.
  - Wenn das System Datenverkehr durchläuft, statt ihn zu optimieren, oder Probleme bei der Optimierung bestimmter Arten von Anwendungsdatenverkehr (HTTP, MAPI, SSL usw.) hat, lesen Sie die Artikel [Fehlerbehebung Optimierung](#) und [Problembehandlung Anwendungsbeschleunigung](#).
  - Wenn das System mehr Datenverkehr als erwartet durchläuft, anstatt ihn zu optimieren, lesen Sie den Artikel [Beheben von Überlastungsbedingungen](#).
10. Wenn Sie festgestellt haben, dass Ihre Fehlerbehebungsversuche das Problem nicht behoben haben, wenden Sie sich an das Cisco Technical Assistance Center (TAC) oder Ihren technischen Support-Mitarbeiter. Weitere Informationen finden Sie im Abschnitt "[Kontakt mit dem technischen Support von Cisco](#)".

# Überprüfen des WAAS-Images

Geben Sie den folgenden Befehl ein, um die Version des Software-Image anzuzeigen, das derzeit auf dem WAAS-Gerät ausgeführt wird:

```
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.
```

Dieser Befehl stellt weitere nützliche Informationen bereit, z. B.:

- Gerätemodell (die Zahlen im ersten Teil der Version-Zeichenfolge codieren die Gerätemodellnummer; hier wird WAE-7341 angezeigt.)
- WAE-Verfügbarkeit

Geben Sie den folgenden Befehl ein, um zu überprüfen, ob kein ausstehender Software-Upgrade vorliegt (wartet auf einen Neustart des Geräts):

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

Sie sollten die Meldung "Keine ausstehende Version" sehen.

## Aktivieren der WAAS-Protokollierung

Die allgemeine Systemfehlerprotokollierung in der Datenträgerdatei /local1/syslog.txt ist standardmäßig aktiviert. Sie können überprüfen, ob die Protokollierung aktiviert ist, indem Sie den folgenden Befehl eingeben:

```
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
```

Um die Protokollierung in der Konsole zu aktivieren, geben Sie den folgenden globalen Konfigurationsbefehl ein:

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

**HINWEIS:** Das Festlegen der Protokollierungspriorität auf eine niedrigere Ebene als die vorherige Ankündigung kann CPU-intensiv sein und eine große Menge an Ausgabe generieren. Verwenden Sie sie sorgfältig und sparsam in einer Produktionsumgebung.

Die folgenden Verzeichnisse werden von WAAS für Protokolldateien verwendet:

- /local1 - Stammverzeichnis für alle Protokolldateien und den Speicherort von syslog.txt
- /local1/logs - Service-Protokolldateien (Admin- und Transaktionsprotokolle)
- /local1/errorlog — Dienstprotokolldateien (Debug-Protokolle)
- /local1/errorlog/cifs - interne CIFS-Protokolldateien
- /local1/core\_dir: Verarbeiten von Core-Dump-Dateien

Mithilfe der folgenden Befehle für die Dateisystemnavigation können Sie die Protokolldateien navigieren und anzeigen:

- **CD**
- **Pwd**
- **Verzeichnis**
- **type-tail** *filename lines* [| **folgen**]
- **Suchmuster**

## Diagnosen ausführen

Der WAAS Central Manager enthält ein integriertes Diagnose-Tool, mit dem Sie zahlreiche Geräteprobleme beheben können. Dazu gehören:

- Netzwerkkonfiguration
- Schnittstellenkonfiguration
- Verbindung zu Hosts
- WCCP-Konfiguration
- Inline-Konfiguration
- TFO-Konfiguration
- WAFS-Konfiguration

Wir empfehlen, dass Sie das Diagnosetool zuerst ausführen, bevor Sie andere Fehlerbehebungsmaßnahmen durchführen. Das Tool berichtet über den Status und die Konfiguration vieler Systemfunktionen.

So führen Sie das Diagnosetool über den zentralen Manager aus:

1. Wählen Sie im Navigationsbereich der GUI von WAAS Central Manager **My WAN > Manage Devices (Mein WAN > Geräte verwalten (oder Gerätegruppen verwalten))** aus.
2. Klicken Sie auf das Symbol **Bearbeiten** neben dem Namen des Geräts (oder der Gerätegruppe), für das Sie Diagnosetests durchführen möchten.
3. Wählen Sie im Navigationsbereich **Troubleshoot > Diagnostics Tests (Fehlerbehebung > Diagnosetests)**. Das Fenster Diagnosetool wird angezeigt.
4. Aktivieren Sie das Kontrollkästchen neben jedem Diagnosetest, den Sie ausführen möchten, oder aktivieren Sie das obere Kontrollkästchen, um alle Tests auszuführen.

5. Klicken Sie auf **Ausführen**.

6. Zeigen Sie die Testergebnisse im unteren Bereich des Fensters an. Möglicherweise müssen Sie im Fenster einen Bildlauf durchführen, um alle Ergebnisse anzuzeigen.

Bei fehlgeschlagenen Tests beschreiben Fehlermeldungen das Problem und bieten empfohlene Lösungen. Sie finden eine Beschreibung von Fehlermeldungen im [Test](#)-Befehl in der *Befehlsreferenz für Cisco Wide Area Application Services*.

Sie können dieselben Diagnosetests erneut ausführen und die Ergebnisse aktualisieren, indem Sie in der Taskleiste auf das Symbol **Aktualisieren** klicken.

Um die Ergebnisse zu drucken, klicken Sie auf das Symbol **Drucken** in der Taskleiste.

Um die Diagnosetests über die CLI auszuführen, verwenden Sie den Befehl **test EXEC**.

## Überprüfen der physischen Verbindung zwischen Peer-WAAS-Geräten und Anwendungsservern

Um die physische Verbindung des Peer-WAAS-Geräts zu überprüfen, gehen Sie wie folgt vor:

1. Überprüfen Sie alle Kabelverbindungen am Switch oder Router, die sich auf das WAAS-Gerät auswirken können.
2. Verwenden Sie den Befehl **ping**, um eine ICMP-Echoanfrage an die Peer-WAE zu senden.

```
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
```

Wenn ein Gerät nur einen Hop entfernt ist und Sie das Gerät nicht erreichen können, senden Sie einen Ping an das zwischengeschaltete Gateway. Wenn das Gateway nicht erreichbar ist, geben Sie den Befehl **show ip routes** ein, und überprüfen Sie, ob die richtige Route angezeigt wird. Geben Sie z. B. Folgendes ein:

```
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
```

Geben Sie ggf. eine statische Route für das Gateway ein.

Sie können einen ähnlichen Ping-Befehl verwenden, um die Verbindung zwischen dem Gerät des WAAS-Rechenzentrums und den Hosts des Anwendungsservers zu überprüfen.

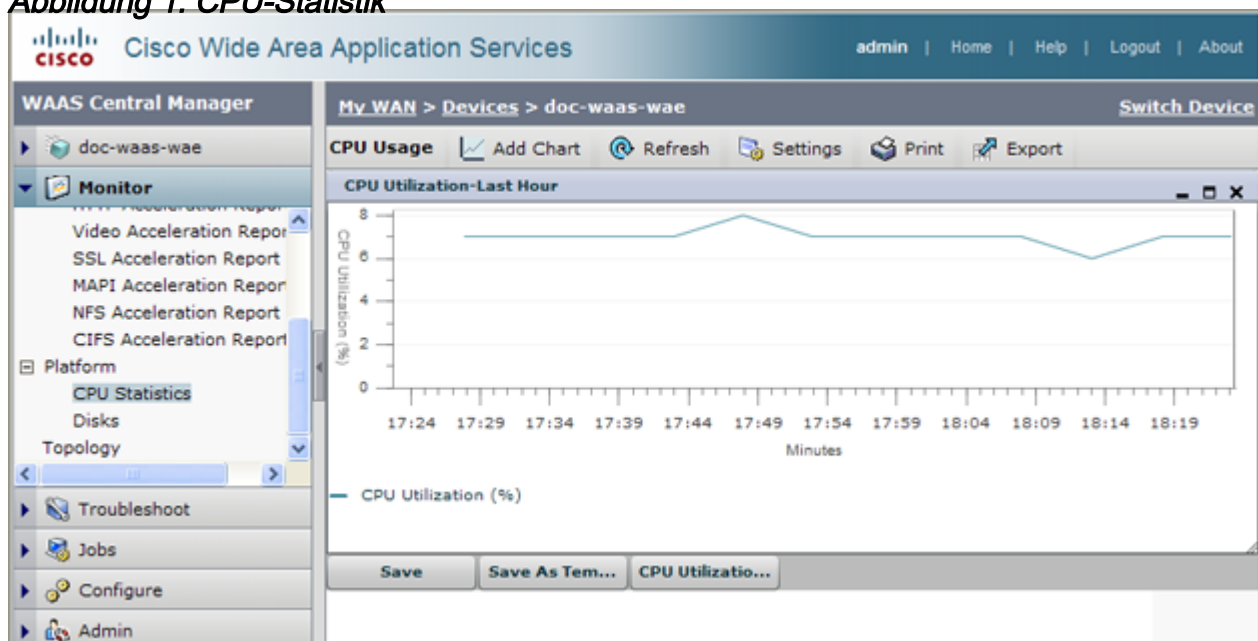
Beachten Sie, dass Firewalls möglicherweise ICMP-Datenverkehr blockieren und ICMP-Datenverkehr nicht dem WCCP-Umleitungspfad folgt. Daher überprüft der Befehl **ping** keine Umleitung oder Beschleunigung. Alternativ können Sie ein Drittanbieter-Tool verwenden, das einen TCP-basierten Ping ausführt.

## Überprüfen der CPU-Last

So prüfen Sie die CPU-Last eines WAAS-Geräts:

1. Wählen Sie im Navigationsbereich der GUI von WAAS Central Manager **My WAN > Manage Devices (Mein WAN > Geräte verwalten)** aus.
2. Klicken Sie auf das Symbol **Bearbeiten** neben dem Namen des Geräts, auf dem Sie die CPU-Last prüfen möchten.
3. Wählen Sie im Navigationsbereich **Monitor > Platform > CPU Statistics** aus.

**Abbildung 1: CPU-Statistik**



Sie können die Zeitspanne des Diagramms anpassen, da die Standardeinstellung "Letzte Stunde" ist. Um den Zeitraum anzupassen, klicken Sie auf das Symbol **Settings** (Einstellungen) in der Taskleiste und wählen einen anderen Zeitrahmen aus, z. B. Last Day (Letzter Tag) oder Last Week (Letzte Woche).

Bei WAAS-Geräten ist es üblich, Spitzen oder sogar längere Zeiträume mit hoher CPU-Auslastung bei hoher Benutzeraktivität anzuzeigen. Wenn sich die CPU während einer sehr langen Dauer auf einem hohen CPU-Level befindet, kann eine weitere Fehlerbehebung oder Größenanpassung des Geräts angezeigt werden.

## Sammeln von Informationen zur WAAS-Fehlerbehebung

In den folgenden Abschnitten werden Möglichkeiten empfohlen, um Informationen zu sammeln, die für das auftretende Problem relevant sind und vor der Kontaktaufnahme mit dem Cisco Technical Assistance Center (TAC) erforderlich sind.

### Neustarten des WAAS-Geräts

Starten Sie das WAAS-Gerät nur dann neu, wenn es unbedingt erforderlich ist. Einige

Informationen, die für die Problembeseitigung wichtig sind, überleben einen Neustart möglicherweise nicht. Versuchen Sie, so viele Informationen wie möglich zu sammeln, bevor Sie neu starten.

## Verwenden von Show-Befehlen

Im Exec-Modus können Sie mehrere **show**-Befehle verwenden, um Informationen zu den Symptomen zu sammeln, die Sie auf Ihrem Gerät beobachten. In den meisten Fällen können Sie die Informationen zur Fehlerbeseitigung für das Gerät sammeln, indem Sie den Befehl **copy tech-support** eingeben. Dieser Befehl führt viele **show**-Befehle aus, die zur Fehlerbeseitigung nützlich sind, und sammelt die Ausgabe in einer einzigen Datei. Sie können die Ausgabe des Befehls **copy tech-support** auf eine Festplattendatei, einen FTP-Server oder einen TFTP-Server umleiten. Die Befehlsyntax ist wie folgt:

```
copy tech-support {disk filename | ftp {Hostname | ip address} remotedirectory-remotefilename. | tftp {Hostname | ip address} remotefilename}
```

Um beispielsweise die Ausgabe des Befehls in eine Datenträgerdatei auf dem lokalen System zu kopieren, geben Sie den Befehl wie folgt an:

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

Weitere nützliche **show**-Befehle sind:

- **Alarme anzeigen:** Zeigt Alarme an.
- **Show Accelerator:** Zeigt den Status der Anwendungsbeschleuniger an.
- **Lizenz anzeigen:** Zeigt den Lizenzstatus an.
- **Statistikverbindung anzeigen:** Zeigt Statistiken für alle TCP-Verbindungen an.
- **Statistiken anzeigen für:** Zeigt TFO-Statistiken an.
- **Schnittstelle anzeigen:** Zeigt Schnittstelleninformationen und -status an. Überprüfen Sie, ob Geschwindigkeit und Duplex mit dem Switch übereinstimmen.
- Verwenden Sie für WCCP-Bereitstellungen die folgenden Befehle in der WAE:
  - **show wccp gre**
  - **show wccp-Router**
  - **show wccp wide-area-engine**
  - **show wccp flows**
  - **Ausgangsmethoden anzeigen**
- Verwenden Sie für WCCP-Bereitstellungen die folgenden Befehle auf dem Router oder Switch (ggf. für jede Servicegruppe):
  - **show ip wccp**
  - **show ip wccp interfaces detail**
  - **show ip wccp Dienst**
  - **show ip wccp Dienst Details**
- Verwenden Sie bei WCCP-Bereitstellungen die folgenden Befehle auf dem Router oder Switch, wenn das Hashing verwendet wird:
  - **Show-Tcam-Zähler**
  - **mls stat anzeigen**

- **Anzeige mls netflow detaillierter Tabelle**
  - **show mls netflow icount**
  - **show mls netflow ip sw-installed count**
  - **show mls netflow ip sw-installierte Details**
  - **show fm-Schnittstelle *interface\_name***
- Verwenden Sie bei WCCP-Bereitstellungen die folgenden Befehle auf dem Router oder Switch, wenn die Masking-Funktion verwendet wird:
    - **show ip wccp *Dienst Maske***
    - **show ip wccp *Dienst zusammenführen***
    - **show tcam interface *interface\_name* acl {in | out} ip**
    - **show tcam interface *interface\_name* acl {in | out} ip detail**

## Erstellen eines Systemberichts

Ein Systembericht (Sysreport) ist ein umfassender Bericht, den Sie benötigen, bevor Sie sich an den technischen Support von Cisco wenden. Sie können einen Sysreport erstellen, indem Sie den Befehl [copy sysreport](#) ausführen. Der Systembericht enthält die Ausgabe vieler Befehle und Protokolle im System, einschließlich Befehle anzeigen, Netzwerkstatistiken, Diagramme, Protokollinhalte, Konfigurationseinstellungen, Statistiken usw. Es kann einige Zeit dauern, einen Systembericht zu erstellen, und der Wert kann zwischen 30 und 100 MB oder größer sein. Der Systembericht enthält viel mehr Elemente als im **Text** des **technischen Support**-Befehls enthalten sind und wird in der Regel bei der Kontaktaufnahme mit dem technischen Support von Cisco benötigt.

Verwenden Sie vor dem Generieren eines Systemberichts den Befehl **test**, um die Diagnosetests so auszuführen, dass diese Informationen im Systembericht enthalten sind. Beim Generieren eines Systemberichts in einem zentralen Manager (oder Standby Central Manager) sollten Sie zuerst eine Datenbanksicherung mit dem Befehl **cms database backup** durchführen.

Um einen Sysreport zu generieren und auf einem FTP-Server zu speichern, verwenden Sie das folgende Formular: **copy sysreport ftpserver-ip remote-directory remote-file-name**

Beispiel:

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

Verwenden Sie beim Generieren eines Systemberichts keine Befehlsoptionen, die den Bericht auf einen bestimmten Zeitraum beschränken, da dies dazu führen kann, dass Informationen auch innerhalb dieses Zeitraums nicht eingeschlossen werden.

## Erfassen und Analysieren von Paketen

Das Erfassen von Paketen (manchmal auch als "TCP-Dump" bezeichnet) ist eine nützliche Hilfe bei der Behebung von Verbindungsproblemen mit dem WAAS-Gerät oder bei der Überwachung verdächtiger Aktivitäten. Das WAAS-Gerät kann Paketinformationen für den Netzwerkverkehr verfolgen, der durch das Gerät geleitet wird. Die Attribute des Pakets werden durch eine ACL definiert. Das WAAS-Gerät puffert die erfassten Pakete, und Sie können den gepufferten Inhalt in eine Datei oder auf einen Remote-Server kopieren. Sie können die erfassten Paketinformationen auch auf Ihrer Konsole oder Ihrem Terminal anzeigen.

Es stehen zwei Dienstprogramme zur Paketerfassung zur Verfügung: **tcpdump** und **tethereal**.



Diese Befehle erfordern Administratorberechtigungen.

Standardmäßig erfassen diese Befehle nur die ersten 64 Byte jedes Pakets. Wir empfehlen, die Option **-s 1600** zu verwenden, um vollständige Paketdaten zu erfassen.

Wenn Sie große Traces verwenden, verwenden Sie **tcpdump**, um rollende Paketerfassungen in mehreren Dateien zu erstellen. (Die Option **-C** legt die maximale Größe jeder erfassten Datei in KB und die Option **-M** legt die maximale Anzahl der zu erstellenden Protokolldateien fest.)

Wenn Sie die erfassten Pakete filtern müssen, verwenden Sie **Tethereal** mit der Lesefilteroption **-R**. Sie können **tcpdump** verwenden, um eine große Paketerfassung zu erstellen, und dann **Tethereal** für die Filterung der erfassten Datei verwenden.

Seien Sie vorsichtig, wenn Sie **tcpdump** in einer WCCP-Umgebung verwenden, da **tcpdump**-Filter nicht im GRE-Wrapper angezeigt werden. Sie müssen den **Tethereal** verwenden, wenn Sie dies tun müssen.

Verwenden Sie bei beiden Befehlen die Option **-i any**, um alle Schnittstellen zu erfassen, oder trennen Sie Telnet-Sitzungen, um diese an separaten Schnittstellen zu erfassen. Verwenden Sie **^c** (STRG+c), um die Paketerfassung zu stoppen.

Es gibt mehrere Paketanalyse-Tools, mit denen Sie Dateien zur Paketerfassung analysieren können, nachdem Sie sie erfasst haben:

- [Wireshark](#): Ein kostenloses Paketanalyse-Tool mit umfassenden Funktionen (empfohlen gegenüber Ethereal).
- [Ätherisch](#): Ein weiteres kostenloses Paketanalyse-Tool mit umfassenden Funktionen.
- Microsoft Netmon: Im Lieferumfang der Windows-Serversoftware enthalten.
- Sniffer Pro

## Verwenden von tcpdump

Die vollständige tcpdump-Syntax finden Sie unter [tcpdump](#) in der *Befehlsreferenz für Cisco Wide Area Application Services*.

Die nützlichsten tcpdump-Optionen sind:

- **-i Schnittstelle**: Die Schnittstelle, über die Sie Pakete erfassen möchten, z. B.:
  - **an** 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
  - **an**: Alle verfügbaren Ethernet-Ports. Beachten Sie, dass die "Any"-Schnittstelle im Promiscuous-Modus nicht erfasst werden kann, sodass sie möglicherweise einige ausgehende Pakete verpasst. Weitere Informationen finden Sie auf der Linux-Man-Page unter tcpdump(8). Hinweis: Diese Option ist für WAAS ab Version 4.1.5 nicht verfügbar.
  - **Anleihe0**: Logische Schnittstelle, die alle physischen Schnittstellen kombiniert.
- **-s Momentlen**: Die maximale Größe, die für jedes Paket erfasst wird.
- **-w-Datei**: Der Name der Datei, in der die erfassten Pakete in ihrer Rohform geschrieben

werden.

- **-C Anzahl:** Die maximale Größe der Erfassungsdatei, die in Tausenden von Byte angegeben ist. Wenn auch die Option **-M** angegeben ist, werden weitere Erfassungsdateien erstellt.
- **-M Num:** Die maximale Anzahl von Protokolldateien, die durch das Rollover bei Erreichen der maximalen Dateigröße erstellt werden. Gibt an, wie viele Erfassungsdateien vor dem Beenden der Erfassung erstellt werden sollen.
- **D:** Fügt die Liste der Schnittstellen, die zum Erfassen verfügbar sind, aus.

Im folgenden Beispiel werden alle Pakete in die Datei `packages1.cap` erfasst:

```
wae# tcpdump -i bond0 -s 1600 -w packages1.cap
```

## Verwendung von Tetheral

Die vollständige Tethereal-Syntax finden Sie in der *Cisco Wide Area Application Services Command Reference*.

Nützliche Tethereal-Optionen sind:

- **-R read\_filter:** Filterung kann sehr nützlich sein. Verwenden Sie dieselbe Filtersyntax wie bei Ethernet oder Wireshark, sodass Sie eines dieser Tools verwenden können, um einen Filter zu erstellen. tethereal ist auch für die Dateikonvertierung und Filterung einer Paketerfassungsdatei nützlich, die bereits erfasst wurde (z. B. von tcpdump).
- **-F output\_filetype:** Der Standard-Dateityp ist eine libpcap-Datei. Folgende Optionen sind jedoch verfügbar:
  - Libpcap - Libpcap (tcpdump, Ethernet usw.)
  - rh6\_1libpcap - RedHat Linux 6.1 libpcap (tcpdump)
  - suse6\_3libpcap - SuSE Linux 6.3 libpcap (tcpdump)
  - Modlibpcap - modifizierte Libpcap (tcpdump)
  - nokialibpcap - Nokia libpcap (tcpdump)
  - lalyzer - Novell LANalyzer
  - ngsniffer - Network Associates Sniffer (DOS-basiert)
  - snoop - Sun Snoop
  - netmon1 - Microsoft Network Monitor 1.x
  - netmon2 - Microsoft Network Monitor 2.x
  - ngwsniffer\_1\_1 - Network Associates Sniffer (Windows-basiert) 1.1
  - ngwsniffer\_2\_0 - Network Associates Sniffer (Windows-basiert) 2,00x
  - nettl - HP-UX nettl trace
  - Visual Networks Traffic Capture
  - 5 Ansichten - Akzente 5 Ansichten erfassen
  - niobserver 9 - Network Instruments Observer Version 9

Die folgenden Beispiele zeigen verschiedene Optionen, die für Filterung und Konvertierung verwendet werden:

Um ein Dateiformat in ein anderes zu konvertieren, verwenden Sie einen Befehl, der dem folgenden ähnelt:

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

Um einen Lesefilter für das SYN-Flag zu verwenden, verwenden Sie einen Befehl, der dem folgenden ähnelt:

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

Um einen Lesefilter für bestimmte Hosts zu verwenden (und in GRE-Paketen zu suchen), verwenden Sie einen Befehl, der dem folgenden ähnelt:

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

**Hinweis:** Der Befehl "tethereal" weist einige Verwendungseinschränkungen auf, die Sie beachten sollten:

- Ein mit der Option -R definierter Filter wird ignoriert, wenn er mit der Option -w (in eine Datei schreiben) in WAAS 4.1.1 und 4.1.3 kombiniert wird. Um erfassten Datenverkehr zu filtern und in eine Datenträgerdatei zu schreiben, verwenden Sie die Option -f, um einen Erfassungsfiler anzugeben. Dieses Problem wurde in Version 4.1.5 behoben.
- Wenn Sie die -a-Option zum Drucken von starkem Datenverkehr auf dem Bildschirm verwenden, kann es erheblich länger dauern, bis die Informationen auf dem Bildschirm angezeigt werden. Warten Sie, bis der Befehl abgeschlossen ist. Die Anzeige der Ausgabe in der Konsole kann erheblich länger dauern als über Telnet oder SSH, sodass die Konsolanzeige nicht empfohlen wird.
- Wenn die -f-Option mit dem Filterausdruck "host" oder "not host" verwendet wird, kann der falsche Datenverkehr mit gekapseltem WCCP GRE- oder VLAN-Datenverkehr erfasst werden. Beim WCCP GRE-Datenverkehr sieht der Tethereal nur die äußerste IP-Adresse, nicht die ursprüngliche IP-Adresse innerhalb der gekapselten Pakete. Fügen Sie das Schlüsselwort "proto 47" in den -f-Filterausdruck ein, um den korrekten Datenverkehr zu erfassen. Fügen Sie außerdem für den VLAN-Datenverkehr das Schlüsselwort "vlan" in den -f-Filterausdruck ein, damit der Befehl den VLAN-Datenverkehr korrekt parsen kann.
- Wenn Sie die -a filesize-Option zusammen mit der -R-Option verwenden, wird der Teekal möglicherweise unerwartet beendet und die Meldung "Memory limit is erreicht" ausgegeben, bevor die angegebene autostop-Dateigröße erreicht wird. In diesem Fall wurde die maximale Speicherbeschränkung für den Befehl vor der Größenbeschränkung der autostop-Datei erreicht.

## Kontaktieren des technischen Supports von Cisco

Wenn Sie ein Problem nicht beheben können, nachdem Sie die Vorschläge zur Fehlerbehebung in den Artikeln in diesem Wiki verwendet haben, wenden Sie sich an das Cisco Technical Assistance Center (TAC), um Hilfe und weitere Anweisungen zu erhalten. Halten Sie vor Ihrem Anruf die folgenden Informationen bereit, damit Ihr TAC-Techniker Ihnen so schnell wie möglich behilflich sein kann:

- Datum, an dem Sie die WAAS-Hardware erhalten haben
- Chassis-Seriennummer
- Art der Software und Versionsnummer (wenn möglich, geben Sie den Befehl **show version** ein)

- Wartungsvertrag oder Garantieinformationen
- Eine gute Problembeschreibung, einschließlich:
  - Was ist das Problem, und welche Symptome sind für den Benutzer sichtbar?
  - Wo und wann
  - Anzeige von Fehlermeldungen, Warnmeldungen und Alarmen
  - Schritte zur Verdopplung des Problems
- Kurze Erläuterung der Schritte, die Sie bereits unternommen haben, um das Problem zu isolieren und zu beheben
- Die Ausgabe des Diagnosetests (siehe Abschnitt "[Diagnosetests durchführen](#)")
- Sicherung der Datenbank in Central Manager (verwenden Sie den Befehl **cms database backup**)
- Informationen im Abschnitt "[Sammeln von Informationen zur WAAS-Fehlerbehebung](#)".
- Topologiediagramme, einschließlich Netzwerk-/Verkabelungsdiagramme und logische Diagramme
- Alle anderen Anzeichen für das Problem, wie Paketerfassung, Transaktionsprotokolle, Kerndateien, WCCP zeigen Befehlsausgabe von Routern/Switches und WAEs sowie andere Protokolldateien an.

Sie können das TAC auf eine der folgenden Arten erreichen:

- [Erstellen Sie online eine Serviceanfrage.](#)
- [Rufen Sie das TAC unter den Telefonnummern auf dieser Seite an.](#)
- [Wenden Sie sich an das Cisco Small Business Support Center](#)