

WAAS - voorlopige WAAS-probleemoplossing

Hoofdstuk: Voorlopige WAAS-probleemoplossing

Dit artikel voert de basisconcepten, methodologie en algemene richtlijnen voor het opsporen en verhelpen van problemen in die kunnen voorkomen wanneer u uw WAAS-systeem configureren en gebruikt.

- [1 Overzicht van het WAAS-proces voor probleemoplossing](#)
- [2 De WAAS-afbeelding controleren](#)
- [3 WAAS-vastlegging inschakelen](#)
- [4 Diagnostiek uitvoeren](#)
- [5 Verifieer de fysieke connectiviteit tussen peer WAAS-apparaten en toepassings servers](#)
- [6 CPU-lading controleren](#)
- [7 Informatie over WAAS-probleemoplossing verzamelen](#)
 - [7.1 Het WAAS-apparaat herstarten](#)
 - [7.2 Weergaven-opdrachten gebruiken](#)
 - [7.3 Een systeemrapport genereren](#)
 - [7.4 Packets opnemen en analyseren](#)
 - [7.4.1 Gebruik van een pomp](#)
 - [7.4.2 Het gebruik van theeaal](#)
- [8 Contact opnemen met technische ondersteuning van Cisco](#)

Overzicht van het WAAS-proces voor probleemoplossing

Inh

Ho

De

Vo

Op

To

Pro

Pro

Pro

Pro

Pro

Pro

Pro

Pro

Pro

Pro

Pro

Pro

Pro

Pro

Pro

Pro

Pro

Pro

Pro

Pro

Pro

Pro

Pro

Pro

Pro

Pro

Pro

Pro

Pro

Pro

Pro

Pro

Pro

Pro

Pro

Pro

Pro

Pro

Pro

Pro

Om uw WAAS-systeem te kunnen oplossen, volgt u deze algemene richtlijnen:

1. Houd een consistente en aanbevolen softwareversie in al uw WAAS-apparaten. Als versies moeten verschillen, moet de Central Manager de hoogste versie uitvoeren. Zie het gedeelte ["De WAAS-afbeelding controleren"](#) voor informatie over de gebruikte versie.
2. Zie de [WAAS release notes](#) voor uw softwareversie voor de nieuwste functies, operationele overwegingen, voorbehouden en CLI-opdrachtwijzigingen.
3. Voordat u configuratiewijzigingen in de WAAS Central Manager invoert, gebruikt u de CMS back-upfunctie om de configuratie op te slaan. Als u problemen met de nieuwe configuratie hebt, kunt u de vorige configuratie herstellen. Zie het gedeelte [Backing Up en Restore van uw WAAS System](#) in de *Cisco Wide Area Application Services Configuration Guide*. Probleemoplossing voor problemen met nieuwe configuratiewijzigingen direct nadat u deze hebt gemaakt.
4. Controleer dat de configuratie juist is voor uw netwerktoepassing. Breng om het even welke vereiste veranderingen in het in werking stellen-configuratiebestand aan, en test dan de configuratie. Als het bevredigend is, bewaar het in het opstartende-configuratiebestand met behulp van het **kopie in werking stellen-configuratie opstartende-klaar** opdracht.
5. Toegang voor systeemmeldingen. Zie het gedeelte ["WAAS-vastlegging inschakelen"](#).
6. Start het diagnostische gereedschap om de functionaliteit van het apparaat en de connectiviteit te controleren. Zie het gedeelte ["Start diagnostiek"](#).
7. Controleer de fysieke connectiviteit tussen WAAS-peers en de toepassings servers. Zie het gedeelte ["Verificatie van de fysieke connectiviteit tussen peer WAAS-apparaten en toepassings servers"](#).
8. Verzamel informatie die de specifieke symptomen definieert. Zie het gedeelte ["Informatie over WAAS-probleemoplossing verzamelen"](#).
9. Raadpleeg een van de andere artikelen in deze WAAS-handleiding voor probleemoplossing voor informatie over specifieke problemen bij het oplossen van problemen:
 - Als het systeem hardware- of diskproblemen lijkt te hebben, raadpleegt u het artikel [Problemen oplossen en hardwareproblemen](#).
 - Als het systeem problemen heeft met het ontvangen van verkeer, zie het artikel [Problemen oplossen WCCP](#). Dit probleem kan ook worden veroorzaakt door een firewallprobleem.
 - Als het systeem door verkeer gaat in plaats van het te optimaliseren, of problemen heeft met het optimaliseren van specifieke soorten toepassingsverkeer (HTTP, MAPI, SSL, enzovoort), zie de artikelen [Optimization](#) and [Troubleshooter Application Acceleration Application](#).
 - Als het systeem meer verkeer doorgeeft dan verwacht in plaats van het te optimaliseren, raadpleegt u het artikel [Voorwaarden voor probleemoplossing](#).
10. Nadat u hebt vastgesteld dat uw pogingen om problemen op te lossen niet het probleem hebben opgelost, neemt u contact op met het Cisco Technical Assistance Center (TAC) of uw technische ondersteuningsvertegenwoordiger. Zie het gedeelte ["Contact opnemen met Cisco Technical Support"](#).

De WAAS-afbeelding controleren

Als u de versie van het softwarebeeld wilt weergeven die momenteel op uw WAAS-apparaat actief is, voert u de volgende opdracht in:

```
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.

Deze opdracht bevat andere nuttige informatie, bijvoorbeeld:

- Apparaatmodel (de getallen in het eerste deel van de Versiereeks coderen het apparaatmodelnummer; hier is een WAE-7341 afgebeeld.)
- WAE-uptime

Om te verifiëren dat er geen hangende software upgrade is (wachten op een apparaat dat opnieuw is opgestart), voert u de volgende opdracht in:

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

U dient het bericht "Geen hangende versie" te zien.

WAAS-vastlegging inschakelen

De algemene systeemfoutmelding /local1/syslog.txt is standaard ingeschakeld. U kunt controleren of loggen is ingeschakeld door de volgende opdracht in te voeren:

```
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
```

Om houtkap aan de console toe te laten, voer de volgende globale configuratieopdracht in:

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

OPMERKING: Het instellen van de logprioriteit op een lager niveau dan kennisgeving kan CPU-intensief zijn en kan een grote hoeveelheid output genereren. Gebruik het voorzichtig en spaarzaam in een productieomgeving.

De volgende directories worden door WAAS gebruikt voor logbestanden:

- /local1 — Root folder voor alle logbestanden en de locatie van syslog.txt
- /local1/logs — Service-logbestanden (beheer- en transactielogboeken)
- /local1/errorlog — Service-logbestanden (debug-bestanden)
- /local1/errorlog/cifs — CIFS interne logbestanden
- /local1/core_dir — Stortingsbestanden

U kunt de volgende opdrachten voor het navigeren van het bestandssysteem gebruiken om door de logbestanden te navigeren en te bekijken:

- **cd**
- **pwd**
- **dir**
- **type-tail** *bestandsnaam regels* [| **opvolgen**]
- **zoekpatroon**

Diagnostiek uitvoeren

WAAS Central Manager bevat een ingebouwde diagnostische tool die u kan helpen bij het oplossen van veel apparaatproblemen, waaronder het volgende:

- Netwerkconfiguratie
- Interfaceconfiguratie
- Connectiviteit met hosts
- WCCP-configuratie
- Inline configuratie
- TFO-configuratie
- WAFS-configuratie

We raden u aan om het diagnostische gereedschap eerst te gebruiken voordat u andere probleemoplossing uitvoert. De tool rapporteert over de status en configuratie van veel systeemfuncties.

Als u het diagnostische gereedschap vanuit de Central Manager wilt uitvoeren, volgt u de volgende stappen:

1. Kies in het navigatiedeelvenster WAAS Central Manager GUI **Mijn WAN > Apparaten beheren** (of **Apparaatgroepen beheren**).
2. Klik op het pictogram **Bewerken** naast de naam van het apparaat (of de apparaatgroep) waarvoor u diagnostische tests wilt uitvoeren.
3. Selecteer in het navigatiedeelvenster de optie **Problemen oplossen > Diagnostische tests**. Het venster Diagnostic Tool verschijnt.
4. Controleer het aankruisvakje naast elke diagnostische test die u wilt uitvoeren of controleer het aanvinkvakje bovenaan om alle tests uit te voeren.
5. Klik op **Uitvoeren**.
6. Bekijk de testresultaten in het onderste gedeelte van het venster. Het kan nodig zijn om in het venster te bladeren om alle resultaten te zien.

Voor testen die falen, beschrijven de foutmeldingen het probleem en bieden ze de aanbevolen oplossingen aan. U kunt foutmeldingen vinden in de [testopdracht](#) in de *Cisco Wide Area Application Services Opdracht*.

U kunt dezelfde diagnostische tests opnieuw uitvoeren en de resultaten verfrissen door op het pictogram Vernieuwen in de taakbalk te klikken.

Als u de resultaten wilt afdrukken, klikt u op het pictogram **Afdrukken** in de taakbalk.

Om de diagnostische tests van de CLI uit te voeren, gebruikt u de **test EXEC** opdracht.

Verifieer de fysieke connectiviteit tussen peer WAAS-apparaten en toepassingsservers

Om de fysieke connectiviteit van het peer WAAS apparaat te verifiëren, volg deze stappen:

1. Controleer alle kabelverbindingen op de switch of router die het WAAS-apparaat kunnen beïnvloeden.
2. Gebruik de opdracht **ping** om een ICMP Echo-aanvraag naar de peer WAE te verzenden.

```
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
```

Als een apparaat één hop weg is en u niet het apparaat kunt bereiken, dan pingelt u de intermediaire gateway. Als de gateway niet bereikbaar is, voer de opdracht **ip-routes** in en controleer of de juiste route wordt weergegeven. Voer bijvoorbeeld in:

```
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
```

Voer indien nodig een statische route voor de poort in.

U kunt een soortgelijk ping-opdracht gebruiken om de connectiviteit tussen het WAAS-datacenter-apparaat en de toepassingsserverhosts te controleren.

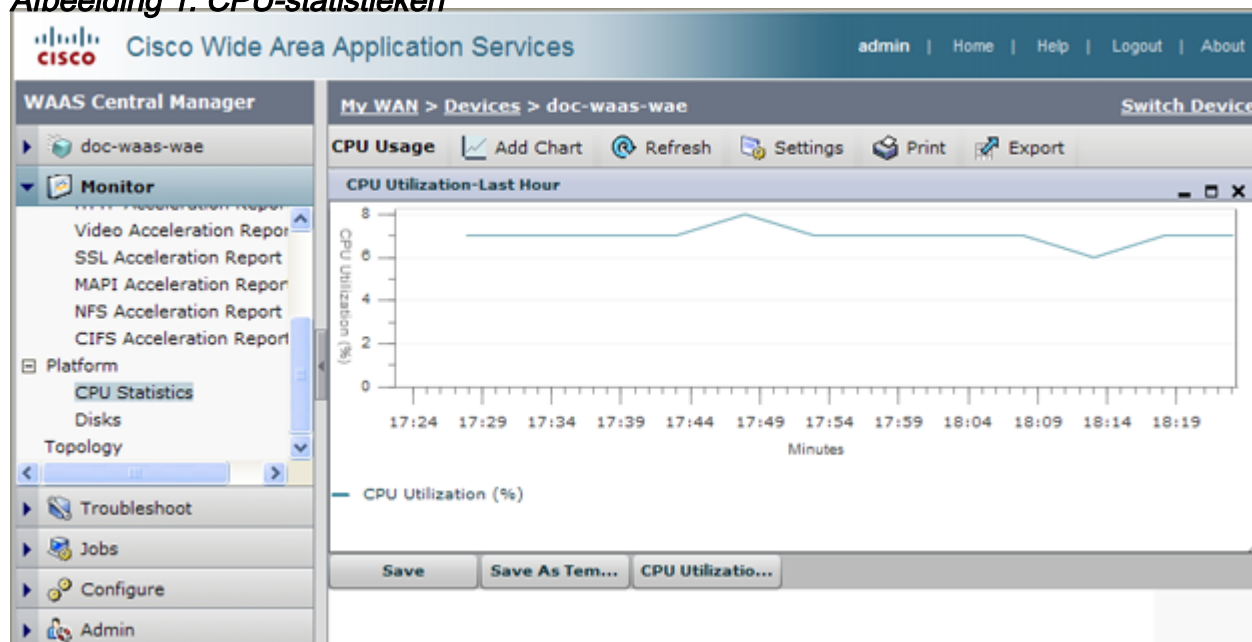
Merk op dat firewalls ICMP-verkeer kunnen blokkeren en dat ICMP-verkeer niet het WCCP-omleidingspad volgt, zodat het **ping**-opdracht niet de omleiding of versnelling controleert. Als alternatief kunt u een derde-partijgereedschap gebruiken dat een TCP-gebaseerde ping uitvoert.

CPU-lading controleren

Om de CPU-lading van een WAAS-apparaat te controleren, volgt u de volgende stappen:

1. Kies **Mijn WAN > Apparaten beheren** in het navigatiedeelvenster WAAS Central Manager GUI.
2. Klik op het pictogram **Bewerken** naast de naam van het apparaat waarop u de CPU-lading wilt controleren.
3. Kies in het navigatiedeelvenster de optie **Monitor > Platform > CPU-statistieken**.

Afbeelding 1. CPU-statistieken



U kunt de tijdsperiode van de tabel aanpassen, omdat de standaardinstelling "Laatste uur" is. Als u de tijdsperiode wilt aanpassen, klikt u op het pictogram **Instellingen** in de taakbalk en vervolgens kiest u een ander tijdframe zoals vorige dag of vorige week.

Het is gebruikelijk dat een WAAS-apparaat spikes of zelfs langere duur van een hoog CPU-gebruik tijdens perioden met hoge gebruikersactiviteit laat zien. Wanneer de CPU gedurende een aanzienlijk lange periode op een hoog CPU-niveau blijft, kan worden aangegeven hoe het apparaat moet worden opgelost of gerepareerd.

Informatie over WAAS-probleemoplossing verzamelen

De volgende secties bevelen aan om informatie te verzamelen die relevant is voor het probleem dat zich voordoet en die nodig is voordat u contact opneemt met het Cisco Technical Assistance Center (TAC).

Het WAAS-apparaat herstarten

Start het WAAS-apparaat niet opnieuw op, tenzij dit echt nodig is. Sommige informatie die belangrijk is voor het oplossen van uw probleem kan geen herstart overleven. Probeer zoveel mogelijk informatie te verzamelen voordat u het programma herstart.

Weergaven-opdrachten gebruiken

U kunt in de Exec-modus meerdere opdrachten gebruiken om informatie te verzamelen die specifiek is voor de symptomen die u in uw apparaat waarneemt. In de meeste gevallen kunt u de informatie verzamelen die u nodig hebt om de oplossing van het apparaat te problemen, door de opdracht **technische ondersteuning kopiëren** in te voeren. Deze opdracht **voert** veel **tonen** opdrachten uit die nuttig zijn voor het oplossen van problemen en verzamelt de uitvoer in één

bestand. U kunt de uitvoer van de opdracht voor **ondersteuning van kopieertechnologie** opnieuw richten op een diskbestand, een FTP-server of een TFTP-server. De opdrachtsyntax is als volgt:

Copyright-ondersteuning {**disk filename** | **ftp** {*hostname* | *ip-adres*} *remotefolder remotefilename* | **tftp** {*hostname* | *ip-adres*} *remotefilename*}

Als u de uitvoer van de opdracht naar een diskbestand in het lokale systeem wilt kopiëren, specificeert u de opdracht als volgt:

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

Andere nuttige **tonen** opdrachten omvatten het volgende:

- **alarmen tonen:** Waarschuwingen.
- **show accelerator:** Status toepassing versneller weergeven.
- **vergunning tonen:** Licentiestatus wordt weergegeven.
- **verbinding statistieken tonen:** Statistieken van displays voor alle TCP-verbindingen.
- **statistische gegevens weergeven:** TFO-statistieken van displays.
- **interface tonen:** Informatie over gebruikersinterface en status worden weergegeven. Controleer dat de snelheid en de duplex met de switch overeenkomen.

- Gebruik voor WCCP-implementaties de volgende opdrachten in WAE:
 - **WCCP-gr tonen**
 - **WCCP-routers tonen**
 - **WCCP-motor met groot gebied tonen**
 - **WCCP-stromen weergeven**
 - **tonen grasmethodes**

- Gebruik voor WCCP-implementaties de volgende opdrachten op de router of switch (voor elke servicegroep, indien van toepassing):
 - **ip wcp tonen**
 - **ip wcp-interfacetekening**
 - **ip wcp tonen dienst**
 - **ip wcp tonen dienst detail**

- Gebruik voor WCCP-implementaties de volgende opdrachten op de router of switch wanneer hashing wordt gebruikt:
 - **aantal getcam's weergeven**
 - **mls staat tonen**
 - **details in netflow-tabel tonen**
 - **tonen het aantal nevenstromen**
 - **tonen mls netflow ip sw-geïnstalleerd aantal**
 - **tonen het aantal mls netflow-ip sw-geïnstalleerd detail**
 - **show fm inteface *interface_naam***

- Gebruik voor WCCP-implementaties de volgende opdrachten op de router of switch wanneer maskeren wordt gebruikt:
 - **ip wcp tonen dienst masker**
 - **ip wcp tonen dienst samenvoegen**

- **toon tcam interface** *interface_name* **acl** {in | out} **ip**
- **toon tcam interface** *interface_name* **acl** {in | **Uitgaande**} **ip-details**

Een systeemrapport genereren

Een systeemrapport (systeemrapport) is een uitgebreid rapport dat u nodig hebt voordat u contact opneemt met de technische ondersteuning van Cisco. U kunt een systeemrapport genereren door de opdracht [kopieersysteem uit](#) te voeren. Het systeemrapport bevat de output van veel opdrachten en logbestanden op het systeem, waaronder showopdrachten, netwerkstatistieken, grafieken, loginhoud, configuratie instellingen, statistieken, enz. Het kan enige tijd duren om een systeemrapport te genereren en het kan van 30 tot 100 MB in grootte of groter zijn. Het systeemrapport bevat veel meer elementen dan in de opdracht **technische ondersteuning van kopiëren** zijn opgenomen en is over het algemeen nodig wanneer u contact opneemt met de technische ondersteuning van Cisco.

Alvorens een systeemrapport te genereren, gebruikt u de **testopdracht** om de diagnostische tests uit te voeren, zodat deze informatie in het systeemrapport wordt opgenomen. Wanneer u een systeemrapport genereert op een Central Manager (of stand-by Central Manager), moet u eerst een back-up maken van de database door de opdracht **voor de back-up van de cms** te gebruiken.

Om een systeemrapport te genereren en op een FTP server op te slaan, gebruik deze vorm van de opdracht: **FTP-rapport van het kopieersysteem** *server-ip afstandsbediening-bestand-naam*

Bijvoorbeeld:

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

Gebruik bij het genereren van een systeemrapport geen opdracht-opties die het rapport beperken tot een specifieke periode, aangezien dit zelfs binnen die periode informatie zou kunnen opleveren die niet wordt opgenomen.

Packets opnemen en analyseren

Het opnemen van pakketten (soms aangeduid als een "TCP-dumpen") is een nuttige hulp bij het oplossen van problemen met de connectiviteit van het WAAS-apparaat of bij het controleren van verdachte activiteit. Het WAAS-apparaat kan pakketinformatie volgen voor netwerkverkeer dat erdoor gaat. De eigenschappen van het pakket worden gedefinieerd door een ACL. Het WAAS-apparaat buffert de opgenomen pakketten en u kunt de gebufferde inhoud naar een bestand of naar een externe server kopiëren. U kunt de opgenomen pakketinformatie ook op uw console of terminal weergeven.

Er zijn twee hulpprogramma's voor pakketvastlegging beschikbaar: **vob** en **tetheraal**. Deze opdrachten hebben beheerrechten nodig.

Standaard nemen deze opdrachten alleen de eerste 64 bytes van elk pakket op. We raden u aan om de optie **1600** te gebruiken om alle pakketgegevens op te nemen.

Als u grote sporen zal nemen, gebruik **tcpdf** om het rollen van pakketvastlegging in meerdere bestanden te creëren. (De optie **-C** stelt de maximale grootte van elk opgenomen bestand in KB in en de optie **-M** stelt het maximale aantal te maken logbestanden in.)

Als u de opgenomen pakketten moet filteren, gebruikt u **de thermische studie** met de optie **-R** leesfilter. U kunt **tcPDump** gebruiken om een grote pakketvastlegging te maken en vervolgens

tegen het opgenomen bestand tratheraal gebruiken om filtering uit te voeren.

Wees voorzichtig met het gebruik van **tcpdf** in een WCCP-omgeving, omdat de filters **van** de **tcpdf**-pomp niet in de GRE-wikkeler kijken. Je moet **tetheraal** gebruiken als je dat nodig hebt.

Met beide opdrachten gebruikt u de **-i**-optie om alle interfaces op te nemen, of afzonderlijke telnet-sessies om op afzonderlijke interfaces op te nemen. Gebruik **^c** (CTRL+c) om de pakketvastlegging te stoppen.

Er zijn verschillende tools voor pakketanalyse die u kunt gebruiken om pakketvastlegging bestanden te analyseren nadat u ze hebt opgenomen:

- [Wireshark](#): Een gratis pakketanalysetool met uitgebreide functies (aanbevolen via Ether).
- [Etheraal](#): Een ander gratis pakketanalysetool met uitgebreide mogelijkheden.
- Microsoft Netmon: Inclusief Windows serversoftware.
- Sniffer Pro

Gebruik van een pomp

Voor de volledige syntaxis van het [vobp](#), zie [tcpdf](#) in de *Cisco Wide Area Application Services opdrachtreferentie*.

De meest bruikbare opties voor de tabbladen zijn:

- **-i interface** : De interface waar u pakketten wilt opnemen, bijvoorbeeld:
 - blz . : localhost
 - 0e eeuw : Gigabit Ethernet 1/0
 - 1 . : Gigabit Ethernet 2/0
 - 2 . : Inline poort 1/1/wan
 - 3 . : Inline poort 1/1/LAN
 - 4 : Inline poort 1/0/00/000
 - 0e vijfde : Inline poort 1/0/LAN
 - elke : Alle beschikbare Ethernet poorten. Let erop dat de "enige" interface niet in de veelbelovende modus kan opnemen, zodat er een aantal uitgaande pakketten mis kan gaan. Zie de Linux man pagina op de tabump(8) voor meer informatie. Opmerking: Deze optie is niet beschikbaar voor WAAS versie 4.1.5 en hoger.
 - obligatie 0 : Logische interface die alle fysieke interfaces combineert.
- **-s momentopname**: De maximale grootte die voor elk pakket wordt opgenomen.
- **-w bestand**: De naam van het bestand waarin de opgenomen pakketten in hun ruwe vorm worden geschreven.
- **-C telling**: De maximale grootte van het opnamebestand, gespecificeerd in duizenden bytes. Als de optie **-M** ook wordt gespecificeerd, worden er extra opnamebestanden gecreëerd.
- **-M num**: Het maximum aantal logbestanden dat wordt gemaakt door te verplaatsen wanneer de maximale bestandsgrootte is bereikt. Hiermee wordt aangegeven hoeveel opnamebestanden u moet maken voordat u de opname stopt.
- **-D**: Maakt de lijst met interfaces beschikbaar voor het opnemen.

In het volgende voorbeeld worden alle pakketten naar het bestand Packet1.cap opgenomen:

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

Het gebruik van theeal

Zie [de thermische](#) syntaxis van [Cisco](#) in de *Cisco Wide Area Application Services Opdracht Referentie*.

De nuttige tetheropties zijn als volgt:

- `-R read_filter`: Filtering kan zeer nuttig zijn. Gebruik de zelfde syntaxis die u met Ethereal of Wireshark zou gebruiken, zodat u één van die tools kunt gebruiken om u te helpen een filter te vormen. tetheral is ook handig voor het converteren en filteren van bestanden van een pakketvastlegging die al is opgenomen (bijvoorbeeld vanaf de tcPDump).
- `-F output_filetype`: Het standaard filetype is een libpcap-bestand. de volgende opties zijn echter beschikbaar :
 - libpcap - libpcap (tcpdf, etherisch, enz.)
 - rh6_1libpcap - RedHat Linux 6.1 libpcap (tcpdf)
 - suse6_3libpcap - SuSE Linux 6.3 libpcap (tcpdf)
 - modulair glb - gewijzigde libpcap (tcpdf)
 - nokialibpcap - Nokia libpcap (tcpdf)
 - Analyzer - Novell LAN-analyzer
 - ngsniffer - Network Associates Sniffer (DOS-gebaseerd)
 - snoop - Sun snoop
 - mon1 - Microsoft Network Monitor 1.x
 - mon2 - Microsoft Network Monitor 2.x
 - NGWNF_1_1 - Sniffer van netwerkasociaties (op Windows gebaseerd) 1.1
 - NGWNER_2_0 - Network Associates Sniffer (Windows-gebaseerd) 2.00x
 - nett - HP-UX nette trace
 - visueel - verkeersopnamen via visuele netwerken
 - 5 beelden - Accelerated 5 views-opname
 - niobserver v9 - Network Instruments Observer versie 9

De volgende voorbeelden tonen verschillende opties die voor het filteren en converteren worden gebruikt:

Om van één bestandsindeling naar een andere te converteren, gebruikt u een opdracht vergelijkbaar met de volgende:

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

Gebruik een opdracht vergelijkbaar met de volgende om een leesfilter voor de SYN-vlag te gebruiken:

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

Als u een leesfilter voor specifieke hosts wilt gebruiken (en naar een GRE-pakket wilt kijken), gebruikt u een opdracht die vergelijkbaar is met het volgende:

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

Opmerking: De tetherische opdracht heeft een aantal gebruiksvoorbehouden die u bewust moet zijn van:

- Een filter dat is gedefinieerd met de optie -R wordt genegeerd wanneer deze wordt gecombineerd met de optie -w (schrijven naar een bestand) in WAAS 4.1.1 en 4.1.3. Gebruik -f optie om een opnamefilter te specificeren om opgenomen verkeer te filteren en naar een diskbestand te schrijven. Dit probleem wordt opgelost in versie 4.1.5.
- Wanneer u de optie -a gebruikt om zwaar verkeer naar het scherm af te drukken, kan het aanzienlijk langer duren dan de automatische stop-duur om de informatie op het scherm weer te geven. Wacht tot de opdracht klaar is. Het weergeven van uitvoer naar de console kan aanzienlijk langer duren dan via telnet of SSH, zodat de weergave van de console niet wordt aanbevolen.
- Wanneer u de optie -f gebruikt met de filterexpressie "host" of "not host", kan het verkeerde verkeer worden opgenomen met WCCP GRE ingekapseld of VLAN-verkeer. Met WCCP GRE-verkeer ziet Tetheral alleen het ultraperifere IP-adres, niet het oorspronkelijke IP-adres in de ingekapselde pakketten. Voeg het "autoprotoocol 47" sleutelwoord toe in de -f filteruitdrukking om het juiste verkeer op te nemen. Voeg daarnaast, voor VLAN verkeer, het "VLAN"sleutelwoord in de - f filteruitdrukking toe om het commando te laten om het verkeer van VLAN correct te parsen.
- Wanneer u de optie -a bestand gebruikt samen met de optie -R, kan de theorie onverwachts stoppen en het bericht "Memory Limiet wordt bereikt" afdrukken voordat u de gespecificeerde grootte van het autostop bestand bereikt. In dit geval is de maximale geheugenlimiet voor de opdracht bereikt voordat de maximale grootte van het automatische stop-bestand is bereikt.

Contact opnemen met technische ondersteuning van Cisco

Als u geen probleem kunt oplossen na het gebruiken van de suggesties voor probleemoplossing in de artikelen in deze wiki, neem dan contact op met het Cisco Technical Assistance Center (TAC) voor ondersteuning en verdere instructies. Voordat u belt, hebt u de volgende informatie bij de hand om uw TAC-ontwerper zo snel mogelijk te helpen:

- Datum waarop u WAAS-hardware hebt ontvangen
- Serienummer chassis
- Type software en releasenummer (indien mogelijk, voer de opdracht **show versie in**)
- Onderhoudsovereenkomst of garantieinformatie
- Een goede probleembeschrijving, met inbegrip van:
 - Wat is het probleem en wat zijn de door de gebruiker zichtbare symptomen?
 - Waar en wanneer
 - Weergave van foutmeldingen, signaleringen en alarmen
 - Stappen om het probleem te dupliceren
- Korte uitleg over de stappen die u al hebt ondernomen om het probleem te isoleren en op te lossen
- De diagnostische testuitvoer (zie het gedeelte "[Werken diagnostiek](#)")
- Een back-up van de centrale Manager-database (gebruik de opdracht **voor back-up van de cms-database**)
- Informatie die is verzameld in het gedeelte "[Bezig met verzamelen van informatie over WAAS-probleemoplossing](#)".

- Topologische diagrammen, met inbegrip van netwerk-/bedradingsschema's en logische diagrammen
- Elk ander bewijs van het probleem zoals pakketvastlegging, transactielogboeken, kernbestanden, WCCP-show toont opdrachtoutput van routers/switches en WAE's, en andere logbestanden.

U kunt TAC op een van deze manieren bereiken:

- [Maak online een serviceaanvraag](#)
- [Neem contact op met de TAC-nummers op deze pagina.](#)
- [Neem contact op met het Cisco Small Business Support Center](#)