WAAS - 예비 WAAS 트러블슈팅

장:예비 WAAS 문제 해결

이 문서에서는 WAAS 시스템을 구성하고 사용할 때 발생할 수 있는 문제에 대한 기본 개념, 방법론 및 일반적인 트러블슈팅 지침을 소개합니다.

WAAS 트러블슈팅 프로세스 개요

WAAS 시스템의 문제를 해결하려면 다음 일반 지침을 따르십시오.

1. 모든 WAAS 장치에서 일관되고 권장되는 소프트웨어 버전을 유지합니다.버전이 다를 경우 Central Manager에서 가장 높은 버전을 실행해야 합니다.사용 중인 버전을 확인하려면 "WAAS 이미지 확인" 섹션을 참조하십시오.
2. 최신 기능, 운영 고려 사항, 주의 사항 및 CLI 명령 변경에 대한 소프트웨어 버전의 WAAS 릴리스 정보를 참조하십시오.
3. WAAS Central Manager에 컨피그레이션 변경 사항을 적용하기 전에 CMS 백업 기능을 사용하여 컨피그레이션을 저장합니다.새 컨피그레이션에 문제가 발생하면 이전 컨피그레이션을 복원할 수 있습니다.*Cisco Wide Area Application Services 컨피그레이션 가이드*의 *WAAS 시스템 백업 및 복원* 섹션을 *참조하십시오*.새 컨피그레이션을 변경한 후 즉시 문제를 해결합니다.
4. 네트워크 애플리케이션에 대한 컨피그레이션이 올바른지 확인합니다.running-config 파일을 필요에 따라 변경한 다음 컨피그레이션을 테스트합니다.만족스러우면 copy running-config startup-**config** 명령을 사용하여 startup-config 파일**에** 저장합니다.
5. 시스템 메시지 로깅을 활성화합니다."WAAS 로깅 활성화" 섹션을 참조하십시오.
6. 진단 도구를 실행하여 장치 기능 및 연결을 확인합니다."진단 실행" 섹션을 참조하십시오.
7. WAAS 피어와 애플리케이션 서버 간의 물리적 연결을 확인합니다."피어 WAAS 장치와 애플리케이션 서버 간 물리적 연결 확인" 섹션을 참조하십시오.
8. 특정 증상을 정의하는 정보를 수집합니다."WAAS 문제 해결 정보 수집" 섹션을 참조하십시오.
9. 특정 문제 해결에 대한 자세한 내용은 이 WAAS 문제 해결 가이드의 다른 문서 중 하나를 참조하십시오.
   - 시스템에 하드웨어 또는 디스크 문제가 있는 것 같으면 디스크 및 하드웨어 문제 해결 문서를 참조하십시오.
   - 시스템에서 트래픽을 수신하는 데 문제가 있는 경우 WCCP 문제 해결 문서를 참조하십시오.이 문제는 방화벽 문제 때문일 수도 있습니다.
   - 시스템이 트래픽을 최적화하지 않고 통과하거나 특정 종류의 애플리케이션 트래픽(HTTP, MAPI, SSL 등)을 최적화하는 데 문제가 있는 경우 최적화 문제 해결 및 애플리케이션 가속화 문제 해결을 참조하십시오.
   - 시스템이 트래픽을 최적화하지 않고 예상보다 많은 트래픽을 통과하고 있는 경우 오버로드 조건 트러블슈팅 문서를 참조하십시오.
10. 문제 해결 시도에 문제가 해결되지 않았음을 확인한 후 Cisco TAC(Technical Assistance Center) 또는 기술 지원 담당자에게 문의하십시오."Cisco 기술 지원 문의" 섹션을 참조하십시오.

WAAS 이미지 확인

WAAS 디바이스에서 현재 실행 중인 소프트웨어 이미지의 버전을 표시하려면 다음 명령을 입력합니다.

```
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.
```

이 명령은 다음과 같은 기타 유용한 정보를 제공합니다.

- 장치 모델(버전 문자열의 첫 부분에 있는 숫자는 장치 모델 번호를 인코딩합니다.여기에 WAE-7341이 표시되어 있습니다.)
- WAE 가동 시간

보류 중인 소프트웨어 업그레이드가 없는지(디바이스 재부팅 대기 중) 확인하려면 다음 명령을 입력합니다.

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

"No pending version" 메시지가 표시됩니다.

WAAS 로깅 활성화

디스크 파일 /local1/syslog.txt에 대한 일반 시스템 오류 로깅은 기본적으로 활성화되어 있습니다.다음 명령을 입력하여 로깅이 활성화되었는지 확인할 수 있습니다.

```
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
```

콘솔에 대한 로깅을 활성화하려면 다음 전역 컨피그레이션 명령을 입력합니다.

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

참고:로깅 우선순위를 알림 레벨보다 낮은 수준으로 설정하면 CPU 사용량이 많으며 많은 양의 출력을 생성할 수 있습니다.생산 환경에서 현명하게 그리고 드물게 사용하십시오.

WAAS에서 로그 파일에 사용하는 디렉토리는 다음과 같습니다.

- /local1 — 모든 로그 파일 및 syslog.txt의 위치에 대한 루트 디렉토리
- /local1/logs — 서비스 로그 파일(관리자 및 트랜잭션 로그)
- /local1/errorlog — 서비스 로그 파일(디버그 로그)
- /local1/errorlog/cifs — CIFS 내부 로그 파일
- /local1/core_dir — 코어 덤프 파일을 처리합니다.

다음 파일 시스템 탐색 명령을 사용하여 로그 파일을 탐색하고 볼 수 있습니다.

- cd
- pwd
- 디렉터리

- **type-tail** *파일 이름 줄* [| | **팔로우**]
- **찾기 패턴**

진단 실행

WAAS Central Manager에는 다음을 포함한 여러 장치 문제를 해결하는 데 도움이 되는 내장 진단 도구가 포함되어 있습니다.

- 네트워크 구성
- 인터페이스 구성
- 호스트에 연결
- WCCP 컨피그레이션
- 인라인 구성
- TFO 컨피그레이션
- WAFS 구성

다른 문제 해결 작업을 수행하기 전에 먼저 진단 도구를 실행하는 것이 좋습니다.이 도구는 여러 시스템 기능의 상태 및 컨피그레이션에 대해 보고합니다.

중앙 관리자에서 진단 도구를 실행하려면 다음 단계를 수행하십시오.

1. WAAS Central Manager GUI 탐색 창에서 **My WAN > Manage Devices**(또는 Manage **Device Groups**)를 선택합니다.
2. 진단 테스트를 수행할 디바이스(또는 디바이스 그룹) 이름 옆에 있는 **Edit**(수정) 아이콘을 클릭합니다.
3. 탐색 창에서 Troubleshoot(문제 해결) **> Diagnostics Tests(진단 테스트)를** 선택합니다.진단 도구 창이 나타납니다.
4. 실행할 각 진단 테스트 옆의 확인란을 선택하거나, 모든 테스트를 실행하려면 위쪽 확인란을 선택합니다.
5. Run(**실행)을 클릭합니다**.
6. 창 하단에서 테스트 결과를 봅니다.모든 결과를 보려면 창을 스크롤해야 할 수 있습니다.

실패한 테스트의 경우 오류 메시지는 문제를 설명하고 권장 솔루션을 제공합니다.*Cisco Wide Area Application Services 명령 참조*의 test 명령에서 오류 메시지 설명을 찾을 수 있습니다.

동일한 진단 테스트를 다시 실행하고 작업 표시줄에서 **새로 고침** 아이콘을 클릭하여 결과를 새로 고칠 수 있습니다.

결과를 인쇄하려면 작업 표시줄에서 **인쇄** 아이콘을 클릭합니다.

CLI에서 진단 테스트를 실행하려면 **test** EXEC 명령을 사용합니다.

피어 WAAS 장치와 애플리케이션 서버 간의 물리적 연결 확인

피어 WAAS 장치의 물리적 연결을 확인하려면 다음 단계를 수행하십시오.

1. WAAS 장치에 영향을 줄 수 있는 스위치 또는 라우터의 모든 케이블 연결을 확인합니다.
2. ping 명령을 사용하여 피어 WAE에 ICMP 에코 요청을 전송합니다.

```
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
```

디바이스가 한 홉에 떨어져 있고 디바이스에 연결할 수 없는 경우 중간 게이트웨이를 ping합니다.게이트웨이에 연결할 수 없는 경우 **show ip routes** 명령을 입력하고 올바른 경로가 표시되는지 확인합니다.예를 들어 다음을 입력합니다.

```
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
```

필요한 경우 게이트웨이의 고정 경로를 입력합니다.

유사한 ping 명령을 사용하여 WAAS 데이터 센터 디바이스와 애플리케이션 서버 호스트 간의 연결을 확인할 수 있습니다.

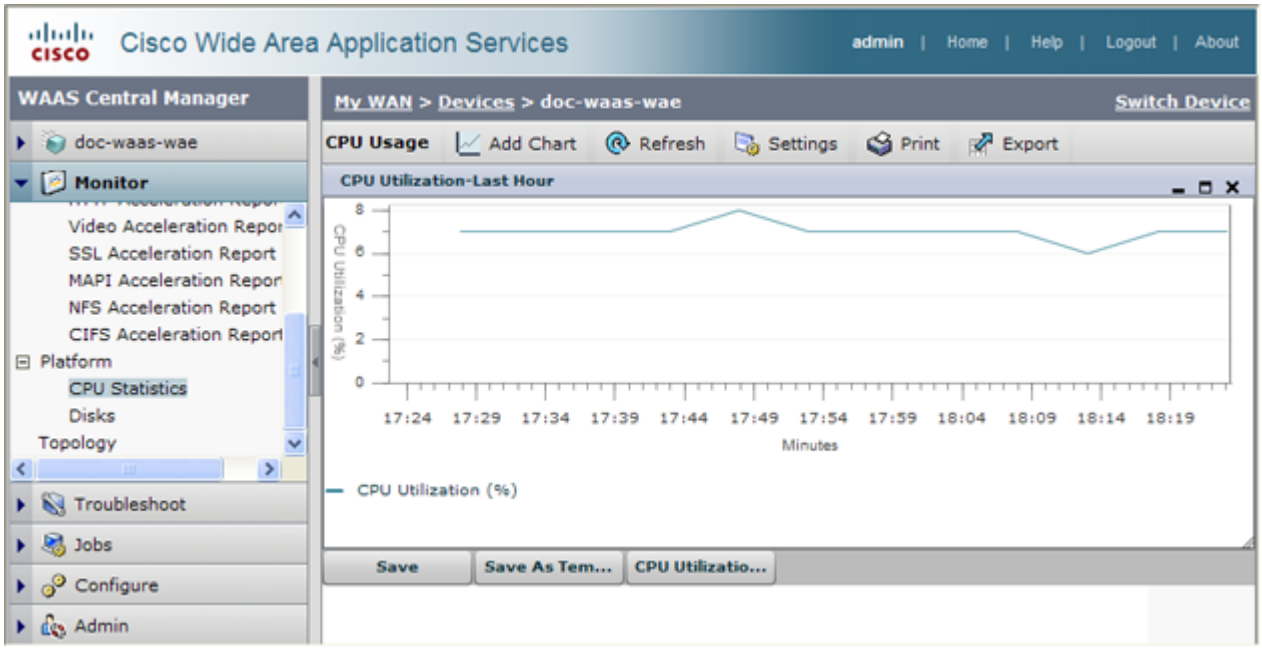
방화벽이 ICMP 트래픽을 차단할 수 있으며 ICMP 트래픽은 WCCP 리디렉션 경로를 따르지 않으므로 ping 명령을 사용해도 리디렉션 또는 가속화를 확인하지 않습니다.대안으로 TCP 기반 ping을 수행하는 서드파티 툴을 사용할 수 있습니다.

CPU 로드 확인

WAAS 장치의 CPU 로드를 확인하려면 다음 단계를 수행하십시오.

1. WAAS Central Manager GUI 탐색 창에서 **My WAN > Manage Devices**를 선택합니다.
2. CPU 로드를 확인할 디바이스 이름 옆에 있는 Edit(수정) 아이콘을 클릭합니다.
3. 탐색 창에서 Monitor(모니터) **> Platform(플랫폼) > CPU Statistics(CPU 통계)**를 선택합니다.

그림 1. CPU 통계



기본값은 마지막 시간이므로 차트의 기간을 조정할 수 있습니다.기간을 조정하려면 작업 표시줄에서 **Settings**(설정) 아이콘을 클릭하고 Last Day(마지막 날) 또는 Last Week(마지막 주)와 같은 다른 Time Frame(시간 프레임)을 선택합니다.

WAAS 장치가 높은 사용자 활동 기간 동안 CPU 사용률이 급증하거나 더 긴 기간을 표시하는 것은 일반적입니다.CPU가 상당히 오랜 기간 동안 높은 CPU 레벨에 남아 있을 경우, 디바이스의 문제 해결 또는 크기 조정을 추가로 표시할 수 있습니다.

WAAS 문제 해결 정보 수집

다음 섹션에서는 Cisco TAC(Technical Assistance Center)에 문의하기 전에 발생하는 문제와 관련된 정보를 수집하는 방법을 권장합니다.

WAAS 장치 재부팅

반드시 필요한 경우가 아니면 WAAS 장치를 재부팅하지 마십시오.문제를 해결하는 데 중요한 일부 정보는 재부팅해도 유지되지 않을 수 있습니다.재부팅하기 전에 최대한 많은 정보를 수집하십시오.

show 명령 사용

디바이스에서 관찰하는 증상과 관련된 정보를 수집하려면 Exec 모드에서 여러 **show** 명령을 사용할 수 있습니다.대부분의 경우 **copy tech-support** 명령을 입력하여 디바이스 문제를 해결하는 데 필요한 정보를 수집할 수 있습니다.이 명령은 문제 해결에 유용한 많은 **show** 명령을 실행하며 출력을 단일 파일로 수집합니다.copy tech-support 명령의 출력을 디스크 파일, FTP 서버 또는 TFTP 서버로 리디렉션할 수 있습니다.명령 구문은 다음과 같습니다.

기술 지원 {**disk** filename *복사* | **ftp** {*hostname* | *ip-address*} remotedirectory *remotefilename.* | **tftp** { *hostname* | *ip-address*} *remotefilename*}

예를 들어, 명령의 출력을 로컬 시스템의 디스크 파일에 복사하려면 다음과 같이 명령을 지정합니다.

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

기타 유용한 **show** 명령은 다음과 같습니다.

- **show alarms**:경보를 표시합니다.
- **show accelerator**:응용 프로그램 가속기 상태를 표시합니다.
- **show license**:라이센스 상태를 표시합니다.
- **통계 연결 표시**:모든 TCP 연결에 대한 통계를 표시합니다.
- **통계 정보 표시**:TFO 통계를 표시합니다.
- **show interface**:인터페이스 정보 및 상태를 표시합니다.속도와 듀플렉스가 스위치와 일치하는지 확인합니다.

- WCCP 구축의 경우 WAE에서 다음 명령을 사용합니다.
  - **wccp gre 표시**
  - **wccp 라우터 표시**
  - **show wccp wide-area-engine**
  - **wccp 흐름 표시**
  - **show egress 메서드**

- WCCP 구축의 경우 라우터 또는 스위치에서 다음 명령을 사용합니다(해당하는 경우 각 서비스 그룹에 대해).
  - **show ip wccp**
  - **ip wccp 인터페이스 세부 정보 표시**
  - **show ip wccp** *서비스*
  - **show ip wccp** *서비스* **세부 정보**

- WCCP 구축의 경우 해싱을 사용할 때 라우터 또는 스위치에서 다음 명령을 사용합니다.
  - **tcam 수 표시**
  - **mls 상태 표시**
  - **show mls netflow table detail**
  - **show mls netflow ip count**
  - **show mls netflow ip sw installed count**
  - **show mls netflow ip sw installed detail**
  - **fm 인터페이스 표시** *인터페이스 이름*

- WCCP 구축의 경우 마스킹을 사용할 때 라우터 또는 스위치에서 다음 명령을 사용합니다.
  - **show ip wccp** *서비스* **mask**
  - **show ip wccp** *서비스* **병합**
  - **show tcam interface** *interface_name* **acl** {**in** | **out**} **ip**
  - **show tcam interface** *interface_name* **acl** {**in** | **out**} **ip 세부 정보**

시스템 보고서 생성

시스템 보고서(sysreport)는 Cisco 기술 지원에 문의하기 전에 필요한 종합적인 보고서입니다.copy sysreport 명령을 실행하여 sysreport를 생성할 수 있습니다.시스템 보고서에는 show 명령, 네트워크 통계, 그래프, 로그 내용, 컨피그레이션 설정, 통계 등 시스템의 여러 명령 및 로그의 출력이 포함됩니다.시스템 보고서를 생성하는 데 다소 시간이 걸릴 수 있으며 크기는 30~100MB 이상일 수 있습니다.시스템 보고서에는 **copy tech-support** 명령에 포함된 것보다 많은 요소가 포함되며, 일반적으로 Cisco 기술 지원 팀에 문의할 때 필요합니다.

시스템 보고서를 생성하기 전에 **test** 명령을 사용하여 진단 테스트를 실행하여 이 정보가 시스템 보고서에 포함되도록 합니다.중앙 관리자(또는 대기 중앙 관리자)에서 시스템 보고서를 생성할 때는

먼저 cms **database backup** 명령을 사용하여 데이터베이스를 백업해야 합니다.

sysreport를 생성하여 FTP 서버에 저장하려면 다음 명령의 형식을 사용합니다.**sysreport ftp** *server-ip remote-directory remote-file-name 복사*

예를 들면 다음과 같습니다.

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

시스템 보고서를 생성할 때 보고서를 특정 기간으로 제한하는 명령 옵션을 사용하지 마십시오. 이 경우 해당 기간 내에도 정보가 포함되지 않을 수 있습니다.

패킷 캡처 및 분석

패킷 캡처("TCP 덤프"라고도 함)는 WAAS 디바이스와의 연결 문제를 해결하거나 의심스러운 활동을 모니터링하는 데 유용합니다.WAAS 장치는 이를 통과하는 네트워크 트래픽에 대한 패킷 정보를 추적할 수 있습니다.패킷의 특성은 ACL에 의해 정의됩니다.WAAS 디바이스는 캡처된 패킷을 버퍼링하며, 버퍼링된 내용을 파일이나 원격 서버에 복사할 수 있습니다.또한 콘솔 또는 터미널에 캡처된 패킷 정보를 표시할 수 있습니다.

두 개의 패킷 캡처 유틸리티를 사용할 수 있습니다.**tcpdump**와 **테테테테알**.이러한 명령에는 관리자 권한이 필요합니다.

기본적으로 이러한 명령은 각 패킷의 처음 64바이트만 캡처합니다.전체 패킷 데이터를 캡처하려면 **-s 1600** 옵션을 사용하는 것이 좋습니다.

큰 추적을 가져올 경우 tcpdump를 사용하여 여러 파일**에** 롤링 패킷 캡처를 생성합니다.(**-C** 옵션은 캡처된 각 파일의 최대 크기를 KB 단위로 설정하고 **-M** 옵션은 생성할 최대 로그 파일 수를 설정합니다.)

캡처된 패킷을 필터링해야 하는 경우 **-R** 읽기 필터 옵션과 함께 **테테테일레**를 사용합니다 .tcpdump를 사용하여 큰 패킷 캡처를 생성한 다음 캡처된 파일에 대해 테테얼을 사용하여 필터링을 수행할 수 있습니다.

tcpdump **필터**가 GRE 래퍼를 찾지 않으므로 WCCP 환경에서 tcpdump를 사용할 때 주의하십시오 .그렇게 해야 한다면 **테테레알**을 사용해야 합니다.

두 명령을 모두 사용할 경우 모든 인터페이스를 캡처하려면 **-i any** 옵션을 사용하고 개별 인터페이스에서 캡처할 별도의 텔넷 세션을 사용합니다.^**c**(Ctrl+c)를 사용하여 패킷 캡처를 중지합니다.

패킷 캡처 파일을 캡처한 후 패킷 캡처 파일을 분석하는 데 사용할 수 있는 몇 가지 패킷 분석 도구가 있습니다.

- Wireshark:광범위한 기능을 갖춘 무료 패킷 분석 툴(Ethereal보다 권장)
- 이더넷:광범위한 기능을 갖춘 또 다른 무료 패킷 분석 툴
- Microsoft 네트워크:Windows 서버 소프트웨어에 포함되어 있습니다.
- 스니퍼 프로

tcpdump 사용

전체 tcpdump 구문은 *Cisco* Wide Area *Application Services 명령 참조*의 tcpdump*를* 참조하십시오 .

가장 유용한 tcpdump 옵션은 다음과 같습니다.

- -i *인터페이스*:패킷을 캡처할 인터페이스(예:
  - lo:로컬 호스트
  - eth0:기가비트 이더넷 1/0
  - eth1 :기가비트 이더넷 2/0
  - eth2 :InlinePort 1/1/wan
  - eth3 :InlinePort 1/1/lan
  - eth4 :InlinePort 1/0/wan
  - eth5:InlinePort 1/0/lan
  - any :사용 가능한 모든 이더넷 포트."any" 인터페이스는 프로미스큐어스 모드에서 캡처할 수 없으므로 일부 발신 패킷을 놓칠 수 있습니다.자세한 내용은 tcpdump(8)의 Linux 매뉴얼 페이지를 참조하십시오. 참고:이 옵션은 WAAS 버전 4.1.5 이상에서는 사용할 수 없습니다.
  - 채권0:모든 물리적 인터페이스를 결합하는 논리적 인터페이스입니다.
- -s *스냅*:각 패킷에 대해 캡처될 최대 크기입니다.
- -w *파일*:캡처된 패킷이 원시 형식으로 기록될 파일의 이름입니다.
- -C *개수*:캡처 파일의 최대 크기(1,000바이트)입니다.-M 옵션도 지정하면 추가 캡처 파일이 생성됩니다.
- -M *번호*:최대 파일 크기에 도달할 때 롤오버로 생성된 최대 로그 파일 수입니다.캡처를 중지하기 전에 만들 캡처 파일 수를 지정합니다.
- -D:캡처할 수 있는 인터페이스 목록을 덤프합니다.

다음 예에서는 모든 패킷을 packets1.cap 파일에 캡처합니다.

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

테테레알 사용

전체 테레알 구문은 *Cisco* Wide Area *Application Services 명령 참조*의 *테레알을* 참조하십시오.

유용한 테일 옵션은 다음과 같습니다.

- -R *read_filter*:필터링은 매우 유용할 수 있습니다.Ethereal 또는 Wireshark에서 사용할 것과 동일한 필터링 구문을 사용하여 이러한 도구 중 하나를 사용하여 필터를 작성할 수 있습니다.또한 tcpdump에서 이미 캡처된 패킷 캡처 파일의 파일 변환 및 필터링에 유용합니다.
- -F *output_filetype*:기본 파일 유형은 libpcap 파일입니다.그러나 다음 옵션을 사용할 수 있습니다.
  - libpcap - libpcap(tcpdump, Ethereal 등)
  - rh6_1libpcap - RedHat Linux 6.1 libpcap(tcpdump)
  - suse6_3libpcap - SuSE Linux 6.3 libpcap(tcpdump)
  - modlibpcap - 수정된 libpcap(tcpdump)
  - nokialibpcap - Nokia libpcap(tcpdump)
  - Lanalyzer - Novell LANalyzer
  - ngsniffer - Network Associates 스니퍼(DOS 기반)
  - 스누프 - Sun 스누프
  - netmon1 - Microsoft Network Monitor 1.x
  - netmon2 - Microsoft Network Monitor 2.x
  - ngwsniffer_1_1 - Network Associates 스니퍼(Windows 기반) 1.1
  - ngwsniffer_2_0 - Network Associates 스니퍼(Windows 기반) 2.00x

    - nettl - HP-UX nettl 추적
    - visual - 비주얼 네트워크 트래픽 캡처
    - 5가지 보기 - 고급 5보기 캡처
    - niobserverv9 - Network Instruments Observer 버전 9

다음 예에서는 필터링 및 변환에 사용되는 다양한 옵션을 보여줍니다.

한 파일 형식에서 다른 파일 형식으로 변환하려면 다음과 유사한 명령을 사용합니다.

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

SYN 플래그에 대해 읽기 필터를 사용하려면 다음과 유사한 명령을 사용합니다.

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

특정 호스트에 대해 읽기 필터를 사용하고 GRE 패킷 내부를 보려면 다음과 유사한 명령을 사용합니다.

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

참고:tele 명령에는 다음 사항에 유의해야 할 몇 가지 사용 주의 사항이 있습니다.

- -R 옵션을 사용하여 정의된 필터는 WAAS 4.1.1 및 4.1.3의 -w 옵션(파일에 쓰기)과 결합되면 무시됩니다. 캡처된 트래픽을 필터링하고 디스크 파일에 쓰려면 -f 옵션을 사용하여 캡처 필터를 지정합니다.이 문제는 버전 4.1.5에서 해결되었습니다.
- -a 옵션을 사용하여 대량의 트래픽을 화면에 인쇄할 경우, 자동 중지 기간보다 훨씬 오래 걸려 화면에 정보를 표시할 수 있습니다.명령이 완료될 때까지 기다립니다.텔넷 또는 SSH를 통해서보다 콘솔에 출력을 표시하는 데 훨씬 오래 걸릴 수 있으므로 콘솔 표시는 권장되지 않습니다.
- "host" 또는 "not host" 필터 표현식과 함께 -f 옵션을 사용할 경우 WCCP GRE 캡슐화 또는 VLAN 트래픽으로 잘못된 트래픽을 캡처할 수 있습니다.WCCP GRE 트래픽에서는 캡슐화된 패킷 내에서 원래 IP 주소가 아니라 가장 바깥쪽의 IP 주소만 표시합니다."proto 47" 키워드를 -f 필터 식에 추가하여 올바른 트래픽을 캡처합니다.또한 VLAN 트래픽의 경우 "vlan" 키워드를 -f 필터 식에 추가하여 명령이 VLAN 트래픽을 올바르게 구문 분석하도록 합니다.
- -a filesize 옵션을 -R 옵션과 함께 사용할 경우 예기치 않게 중지되고 지정된 자동 중지 파일 크기에 도달하기 전에 "메모리 제한에 도달함"이라는 메시지를 인쇄할 수 있습니다.이 경우 자동 중지 파일 크기 제한 이전에 명령에 대한 최대 메모리 제한에 도달했습니다.

Cisco 기술 지원 문의

이 Wiki의 문서에서 문제 해결 제안을 사용한 후 문제를 해결할 수 없는 경우 Cisco TAC(Technical Assistance Center)에 도움을 받고 추가 지침을 문의하십시오.전화를 걸기 전에 TAC 엔지니어가 가능한 한 신속하게 지원을 받을 수 있도록 다음 정보를 준비하십시오.

- WAAS 하드웨어를 받은 날짜
- 섀시 일련 번호
- 소프트웨어 유형 및 릴리스 번호(가능한 경우 **show version** 명령 입력)
- 유지 보수 계약 또는 보증 정보
- 다음과 같은 좋은 문제 설명:
    - 문제는 무엇이며, 사용자에게 표시되는 증상은 무엇입니까?

    - 언제 어디서
    - 오류 메시지, 경고 및 경보가 표시됨
    - 문제 복제 단계
- 문제를 격리 및 해결하기 위해 이미 수행한 단계에 대한 간략한 설명
- 진단 테스트 출력("Running Diagnostics" 섹션 참조)
- 중앙 관리자 데이터베이스 백업(cms **database backup** 명령 사용)
- "WAAS 문제 해결 정보 수집" 섹션에 수집된 정보
- 네트워크/배선 다이어그램 및 논리적 다이어그램을 포함한 토폴로지 다이어그램
- 패킷 캡처, 트랜잭션 로그, 코어 파일, WCCP show command output from router/switches and WAEs, 기타 로그 파일과 같은 문제에 대한 다른 증거입니다.

다음 방법 중 하나로 TAC에 연결할 수 있습니다.

- 온라인 서비스 요청 생성
- 이 페이지의 전화 번호로 TAC에 문의하십시오.
- Cisco Small Business Support Center에 문의