WAAS:WAASの事前トラブルシューティング

章：WAASの事前トラブルシューティング

この記事では、WAASシステムを設定して使用するときに発生する可能性がある問題の基本的な概念、方法、および一般的なトラブルシューティングのガイドラインについて説明します。

WAASトラブルシューティングプロセスの概要

WAASシステムのトラブルシューティングを行うには、次の一般的なガイドラインに従ってください。

1. すべてのWAASデバイスで一貫した推奨ソフトウェアバージョンを維持します。バージョンが異なっている必要がある場合は、Central Managerが最新バージョンを実行している必要があります。使用中のバージョンを確認するには、「WAASイメージの確認」セクションを参照してください。
2. 最新の機能、オペレーティング上の考慮事項、注意、およびCLIコマンドの変更については、使用しているソフトウェアバージョンのWAASリリースノートを参照してください。
3. WAAS Central Managerで設定を変更する前に、CMSバックアップ機能を使用して設定を保存します。新しい設定で問題が発生した場合は、前の設定を復元できます。『*Cisco Wide Area Application Services*構成ガイド』の「WAASシステムのバックアップと復元」セクションを参照してください。新しい設定変更を行った直後に、問題をトラブルシューティングします。
4. ネットワークアプリケーションの設定が正しいことを確認します。running-configファイルに必要な変更を加え、設定をテストします。問題がなければ、**copy running-config startup-config**コマンドを使用して、スタートアップコンフィギュレーション**ファイルに保存**します。
5. システムメッセージロギングを有効にします。「WAASロギングの有効化」セクションを参照してください。
6. 診断ツールを実行して、デバイスの機能と接続を確認します。「診断の実行」セクションを参照してください。
7. WAASピアとアプリケーションサーバ間の物理接続を確認します。「ピアWAASデバイスとアプリケーションサーバ間の物理接続の確認」セクションを参照してください。
8. 特定の症状を定義する情報を収集します。「WAASのトラブルシューティング情報の収集」セクションを参照してください。
9. 特定の問題のトラブルシューティングについては、このWAASトラブルシューティングガイドの他の記事を参照してください。
   - システムにハードウェアまたはディスクの問題がある場合は、「ディスクおよびハードウェアの問題のトラブルシューティング」を参照してください。
   - システムでトラフィックの受信に問題がある場合は、「WCCPのトラブルシューティング」を参照してください。この問題は、ファイアウォールの問題が原因である可能性もあります。
   - システムがトラフィックを最適化する代わりに通過するか、特定の種類のアプリケーショントラフィック（HTTP、MAPI、SSLなど）の最適化に問題がある場合は、「アプリケーション高速化のトラブルシューティング」を参照してください。
   - システムが予想よりも多くのトラフィックを通過する場合は、「過負荷状態のトラブルシューティング」を参照してください。
10. トラブルシューティングの試みが問題を解決していないと判断した後、Cisco Technical Assistance Center(TAC)またはテクニカルサポート担当者に連絡してください。「シスコテクニカルサポートへの連絡」セクションを参照してください。

WAASイメージの確認

WAASデバイスで現在実行されているソフトウェアイメージのバージョンを表示するには、次のコマンドを入力します。

```
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.
```

このコマンドは、次のような他の有用な情報を提供します。

- デバイスモデル(バージョン文字列の最初の部分の番号は、デバイスモデル番号をエンコードします。WAE-7341を次に示します)。
- WAEアップタイム

保留中のソフトウェアアップグレードがないことを確認するには（デバイスのリブートを待つ）、次のコマンドを入力します。

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

「No pending version」というメッセージが表示されます。

WAASロギングの有効化

ディスクファイル/local1/syslog.txtへの一般的なシステムエラーロギングは、デフォルトで有効になっています。次のコマンドを入力して、ロギングが有効になっていることを確認できます。

```
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
```

コンソールへのロギングを有効にするには、次のグローバルコンフィギュレーションコマンドを入力します。

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

注：ロギングの優先度を通知より低いレベルに設定すると、CPUに負荷がかかり、大量の出力が生成される可能性があります。実稼働環境では慎重に慎重に使用してください。

WAASでは、ログファイルに次のディレクトリが使用されます。

- /local1：すべてのログファイルとsyslog.txtの場所のルートディレクトリ
- /local1/logs – サービスログファイル（管理ログとトランザクションログ）
- /local1/errorlog：サービスログファイル（デバッグログ）
- /local1/errorlog/cifs:CIFS内部ログ・ファイル
- /local1/core_dir – コアダンプファイルを処理する

次のファイルシステムナビゲーションコマンドを使用して、ログファイルを移動および表示できます。

- **cd**
- **pwd**
- **dir**
- **type-tail** *filename行*[| |**フォロー**]
- **find-pattern**

診断の実行

WAAS Central Managerには、次のようなデバイスの問題のトラブルシューティングに役立つ診断ツールが組み込まれています。

- ネットワーク構成
- インターフェイス設定
- ホストへの接続
- WCCPの設定
- インライン設定
- TFOの設定
- WAFSの設定

他のトラブルシューティングを行う前に、診断ツールを最初に実行することをお勧めします。このツールは、多くのシステム機能のステータスと設定を報告します。

Central Managerから診断ツールを実行するには、次の手順を実行します。

1. WAAS Central ManagerのGUIナビゲーションペインで、[**My WAN**] > [**Manage Devices**](または[**Manage Device Groups**])を選択します。
2. 診断テストを実**行する**デバイス（またはデバイスグループ）の名前の横にある[編集]アイコンをクリックします。
3. ナビゲーションペインで**Troubleshoot** > **Diagnostics Tests**の順に選択します。診断ツールウィンドウが表示されます。
4. 実行する各診断テストの横にあるチェックボックスをオンにするか、すべてのテストを実行する上部のチェックボックスをオンにします。
5. [Run] をクリックします。
6. ウィンドウの下部にテスト結果を表示します。すべての結果を表示するには、ウィンドウをスクロールする必要があります。

失敗したテストでは、エラーメッセージで問題を説明し、推奨される解決策を提供します。エラーメッセージの説明については、『*Cisco* Wide Area Application Servicesコマンドリ[ファレンス』](#)のtestコマンドを*参照してください*。

タスクバーの[更新]アイコンをクリックすると、同じ診断テストを再度実行し、結果を**更新**することができます。

結果を印刷するには、タスクバーの[**印刷**]アイコンをクリックします。

CLIから診断テストを実行するには、**test EXECコマンドを**使用します。

ピアWAASデバイスとアプリケーションサーバ間の物理接続の確認

ピアWAASデバイスの物理接続を確認するには、次の手順を実行します。

1. WAASデバイスに影響する可能性があるスイッチまたはルータのすべてのケーブル接続を確認します。
2. **ping**コマンドを使用して、ピアWAEにICMPエコー要求を送信します。

```
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
```

デバイスが1ホップ離れていて、デバイスに到達できない場合は、中間ゲートウェイにpingを実行します。ゲートウェイに到達できない場合は、**show ip routes**コマンドを入力し、正しいルートが表示されていることを確認します。たとえば、enter: の場合です。

```
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
```

必要に応じて、ゲートウェイのスタティックルートを入力します。

同様のpingコマンドを使用して、WAASデータセンターデバイスとアプリケーションサーバホスト間の接続を確認できます。

ファイアウォールはICMPトラフィックをブロックする可能性があり、ICMPトラフィックはWCCPリダイレクトパスに従わないため、**pingコマンドを使用する**と、リダイレクションやアクセラレーションは確認されません。代わりに、TCPベースのpingを実行するサードパーティツールを使用することもできます。

CPU負荷のチェック

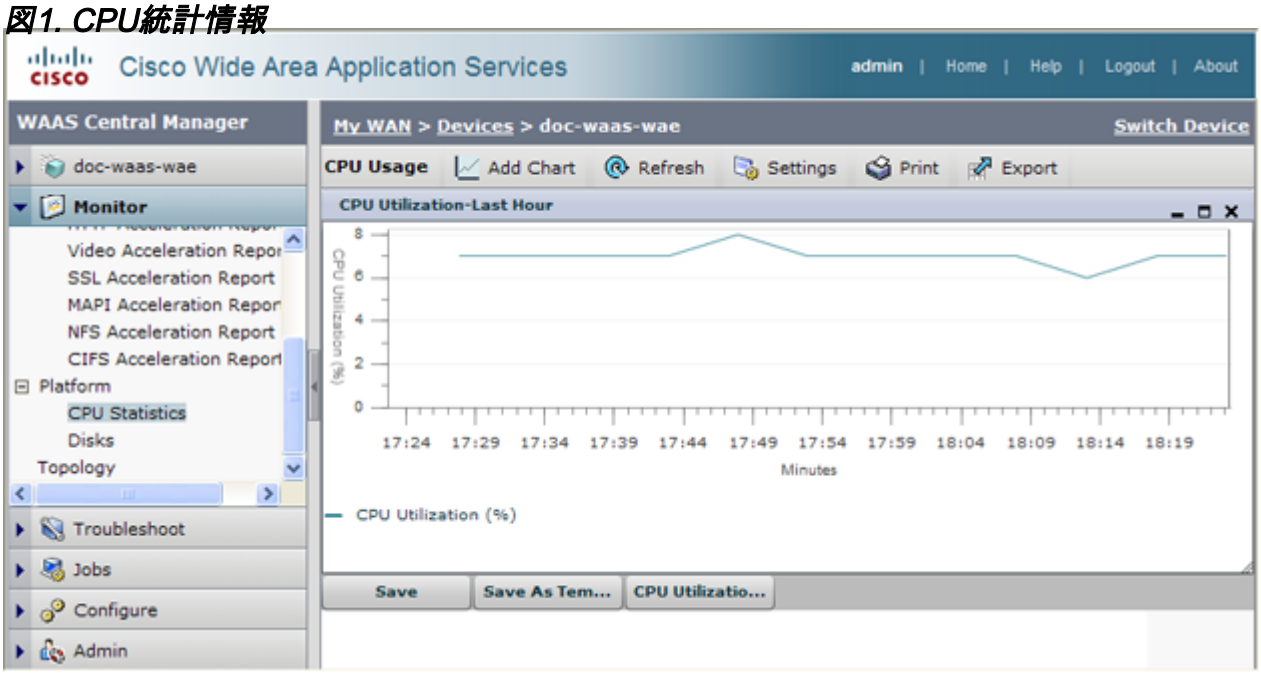
WAASデバイスのCPU負荷を確認するには、次の手順を実行します。

1. WAAS Central ManagerのGUIナビゲーションペインで、[**My WAN**] > [**Manage Devices**]を選

択します。

2. CPUの負荷を確認するデバイスの名前の横にある[Edit]アイコンをクリックします。
3. ナビゲーションペインでMonitor > Platform > CPU Statisticsの順に選択します。

図1. CPU統計情報



グラフの期間を調整することもできます。これは、既定値が[前回]であるためです。期間を調整するには、タスクバーの[設定]アイコンをクリックし、[前日]や[先週]など別の期間を選択します。

WAASデバイスでは、ユーザのアクティビティが多い時間帯にCPU使用率が高くなるスパイクや長い期間が発生することがよくあります。CPUが長時間にわたって高いCPUレベルのままになる場合は、デバイスのトラブルシューティングやサイズ変更の詳細を示すことができます。

WAASのトラブルシューティング情報の収集

次のセクションでは、Cisco Technical Assistance Center(TAC)に連絡する前に発生している問題に関連する情報を収集する方法を推奨します。

WAASデバイスのリブート

WAASデバイスは、絶対に必要でない限り、リブートしないでください。問題のトラブルシューティングに重要な情報の一部は、リブート後も残らない可能性があります。リブートする前に、できるだけ多くの情報を収集してください。

showコマンドの使用

Execモードで複数のshowコマンドを使用して、デバイスで観察している症状に固有の情報を収集できます。ほとんどの場合、copy tech-supportコマンドを入力すると、デバイスのトラブルシューティングに必要な情報を収集することができます。このコマンドは、トラブルシューティングに役立つ多くのshowコマンドを実行し、出力を1つのファイルに収集します。copy tech-supportコマンドの出力は、ディスク、ファイル、FTPサーバ、またはTFTPサーバにリダイレクトできます。コマンド構文は次のとおりです。

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

たとえば、コマンドの出力をローカルシステムのディスクファイルにコピーするには、次のようにコマンドを指定します。

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

その他の便利なshowコマンドには、次のものがあります。

- show alarms:アラームを表示します。
- show accelerator:アプリケーションアクセラレータのステータスを表示します。
- show license:ライセンスステータスを表示します。
- show statistics connection:すべてのTCP接続の統計情報を表示します。
- show statistics tfo:TFO統計情報を表示します。
- show interface:インターフェイス情報とステータスを表示します。速度とデュプレックスがスイッチと一致していることを確認します。

- WCCPの展開では、WAEで次のコマンドを使用します。
  - show wccp gre
  - show wccp routers
  - show wccp wide-area-engine
  - show wccp flows
  - show egress-methods

- WCCPの導入では、ルータまたはスイッチで次のコマンドを使用します（該当する場合は各サービスグループに対して）。
  - show ip wccp ：グローバルな WCCP 統計情報を表示します。
  - show ip wccp interfaces detail
  - show ip wccp ：グローバルな WCCP 統計情報を表示します。 *サービス*
  - show ip wccp ：グローバルな WCCP 統計情報を表示します。 *サービス* detail

- WCCP展開では、ハッシングを使用する場合に、ルータまたはスイッチで次のコマンドを使用します。
  - 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*

- WCCPの導入では、マスキングを使用する際に、ルータまたはスイッチで次のコマンドを使用します。
  - show ip wccp ：グローバルな WCCP 統計情報を表示します。 *サービス* mask
  - show ip wccp ：グローバルな WCCP 統計情報を表示します。 *サービス* マージ
  - show tcam interface *interface_name* acl {in | out} ip
  - show tcam interface *interface_name* acl {in | out} ip detail

システムレポートの生成

システムレポート(sysreport)は、シスコのテクニカルサポートに連絡する前に必要となる包括的

なレポートです。copy sysreportコマンドを実行すると、sysreportを生成することができます。システムレポートには、showコマンド、ネットワーク統計情報、グラフ、ログの内容、設定、統計情報など、システム上のさまざまなコマンドとログの出力が含まれます。システムレポートの生成に時間がかかることがあり、サイズが30 ~ 100 MB以上である場合があります。システムレポートには、**copy tech-support**コマンドに含まれる以上の要素が含まれ、通常はシスコのテクニカルサポートに問い合わせる際に必要となります。

システムレポートを生成する前に、**test**コマンドを使用して診断テストを実行し、この情報がシステムレポートに含まれるようにします。Central Manager（またはスタンバイCentral Manager）でシステムレポートを生成する場合は、まず**cms database backup**コマンドを使用してデータベースバックアップを作成する必要があります。

sysreportを生成してFTPサーバに保存するには、次の形式のコマンドを使用します。**copy sysreport ftp** *server-ip remote-directory remote-file-name*

以下に、いくつかの例を示します。

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

システムレポートを生成する際には、レポートを特定の期間に制限するコマンドオプションを使用しないでください。特定の期間内でも情報が含まれない可能性があります。

パケットのキャプチャと分析

パケットのキャプチャ（「TCPダンプ」とも呼ばれる）は、WAASデバイスの接続問題のトラブルシューティングや、疑わしいアクティビティの監視に役立ちます。WAASデバイスは、通過するネットワークトラフィックのパケット情報を追跡できます。パケットの属性はACLによって定義されます。WAASデバイスは、キャプチャされたパケットをバッファに格納し、バッファされた内容をファイルまたはリモートサーバにコピーできます。キャプチャされたパケット情報をコンソールまたは端末に表示することもできます。

次の2つのパケットキャプチャユーティリティを使用できます。**tcpdump**とteethereal**です**。これらのコマンドには管理者権限が必要です。

デフォルトでは、これらのコマンドは各パケットの最初の64バイトのみをキャプチャします。完全なパケットデータをキャプチャする**には、-s 1600オ**プションを使用することをお勧めします。

大規模なトレースを実行する場合は、tcpdumpを使用してローリング・**パケット**・キャプチャを複数のファイルに作成します。(-Cオプシ**ョンはキャプチャ**された各ファイルの最大サイズをKB単位で設定し、-**Mオプショ**ンは作成するログファイルの最大数を設定します)。

キャプチャされたパケットをフィルタする必要がある場合は、**-R読み取りフ**ィルタオプション**を指定して**telethereal**を使用します。tcpdumpを使用して大きな**パケットキャプチャを作成し、キャプチャされたファイルに対して**teethereal**を使用してフィルタリングを実行できます。

WCCP環境でtcpdumpを使用**する場合は**、tcpdumpフィルタは**GREラッパー**内に見えないので注意してください。必要な場合は**teethereal**を使用する必要があります。

両方のコマンドを使用する場合は、**-i anyオプションを使用して**すべてのインターフェイスをキャプチャするか、個別のTelnetセッションを使用して個別のインターフェイスでキャプチャします。**^c** (Ctrl+C)を使用してパケットキャプチャを停止します。

キャプチャ後にパケットキャプチャファイルを分析するために使用できるいくつかのパケット分析ツールがあります。

- Wireshark：広範な機能を備えた無料のパケット分析ツール（Etherealよりも推奨）。
- Ethereal:広範な機能を備えたもう1つの無料パケット分析ツール。
- Microsoft Netmon:Windowsサーバソフトウェアに含まれています。
- Sniffer Pro

tcpdumpの使用

tcpdump構文の詳細については、『*Cisco* Wide Area Application Servicesコマンドリファレンス』の「*tcpdump*」を参照してください。

最も便利なtcpdumpオプションは次のとおりです。

- -iインターフェイス:パケットをキャプチャするインターフェイス。例：
  - lo:localhost
  - eth0:GigabitEthernet1/0
  - eth1:GigabitEthernet2/0
  - eth2:インラインポート1/1/wan
  - eth3:InlinePort 1/1/lan
  - eth4:インラインポート1/0/wan
  - eth5:InlinePort 1/0/lan
  - 任意:使用可能なすべてのイーサネットポート。「any」インターフェイスは無差別モードではキャプチャできないため、一部の発信パケットが失われる可能性があることに注意してください。詳細は、tcpdump(8)のLinuxのマニュアルページを参照してください。注：このオプションは、WAASバージョン4.1.5以降では使用できません。
  - bond0:すべての物理インターフェイスを結合する論理インターフェイス。
- -s *snaplen*:各パケットでキャプチャされる最大サイズ。
- -wファイル:キャプチャされたパケットがraw形式で書き込まれるファイルの名前。
- -C数:キャプチャファイルの最大サイズ（単位：千バイト）。-Mオプションも指定すると、追加のキャプチャファイルが作成されます。
- -M番号:最大ファイルサイズに達したときにロールオーバーによって作成されたログファイルの最大数。これは、キャプチャを停止する前に実行するキャプチャファイルの数を指定します。
- -D:キャプチャに使用可能なインターフェイスのリストをダンプします。

次の例では、packets1.capファイルへのすべてのパケットをキャプチャします。

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

Teletherealの使用

完全なTeethereal構文については、『*Cisco Wide Area Application Servicesコマンドレフェレンス*』の**teetherealを参照してください**。

便利なTeetherealオプションは次のとおりです。

- -R *read_filter*:フィルタリングは非常に便利です。EtherealまたはWiresharkで使用するのと同じフィルタリング構文を使用して、これらのツールのいずれかを使用してフィルタを作成できます。tetherealは、すでにキャプチャされているパケットキャプチャファイル（tcpdumpなど）のファイル変換とフィルタリングにも役立ちます。

- -F *output_filetype*:デフォルトのファイルタイプはlibpcapファイルです。ただし、次のオプションを使用できます。
  - libpcap - libpcap（tcpdump, Etherealなど）
  - rh6_1libpcap - RedHat Linux 6.1 libpcap (tcpdump)
  - suse6_3libpcap - SuSE Linux 6.3 libpcap (tcpdump)
  - modlibpcap - modified libpcap (tcpdump)
  - nokialibpcap - Nokilibpcap (tcpdump)
  - lanalyzer:Novell LANalyzer
  - ngsniffer:Network Associates Sniffer（DOSベース）
  - snoop – 太陽のスヌープ
  - netmon1:Microsoft Network Monitor 1.x
  - netmon2:Microsoft Network Monitor 2.x
  - ngwsniffer_1_1 - Network Associates Sniffer（Windowsベース）1.1
  - ngwsniffer_2_0 - Network Associates Sniffer（Windowsベース）2.00x
  - nettl - HP-UX nettlトレース
  - ビジュアル：ビジュアルネットワークトラフィックキャプチャ
  - 5Views - Acqualive 5Viewsキャプチャ
  - obncserverv9 - Network Instruments Observerバージョン9

次の例は、フィルタリングと変換に使用されるさまざまなオプションを示しています。

あるファイル形式から別のファイル形式に変換するには、次のようなコマンドを使用します。

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

SYNフラグに読み取りフィルタを使用するには、次のようなコマンドを使用します。

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

特定のホスト（およびGREパケットの内部）に読み取りフィルタを使用するには、次のようなコマンドを使用します。

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

注：telethereal コマンドには、注意が必要な使用上の注意があります。

- WAAS 4.1.1および4.1.3の – wオプション（ファイルへの書き込み）と組み合わせると、-Rオプションを使用して定義されたフィルタは無視されます。キャプチャされたトラフィックをフィルタし、ディスクファイルに書き込むには、-fオプションを使用します。この問題はバージョン4.1.5で解決されています。
- -aオプションを使用して大量のトラフィックを画面に印刷する場合、画面に情報を表示するために自動停止時間よりも大幅に長い時間がかかることがあります。コマンドが終了するのを待ちます。コンソールへの出力の表示は、telnetまたはSSHを使用する場合よりも大幅に長くなる可能性があるため、コンソール表示は推奨されません。
- 「host」または「not host」フィルタ式で – fオプションを使用すると、WCCP GREカプセル化またはVLANトラフィックで誤ったトラフィックがキャプチャされる可能性があります。WCCP GREトラフィックでは、カプセル化されたパケット内の元のIPアドレスではなく、最も外側のIPアドレスだけが検出されます。正しいトラフィックをキャプチャするには、-fフィ

ルタ式に「proto 47」キーワードを追加します。さらに、VLANトラフィックの場合は、-fフィルタ式に「vlan」キーワードを追加して、コマンドでVLANトラフィックを正しく解析できるようにします。
- -a filesizeオプションを – Rオプションとともに使用すると、予期せず停止し、指定したautostopファイルサイズに達する前に「Memory limit is reached」というメッセージが表示されることがあります。この場合、コマンドの最大メモリ制限に達してから、ファイルの自動ストップサイズの制限に達しました。

シスコテクニカルサポートへの連絡

このWikiの記事にあるトラブルシューティングの提案を使用しても問題を解決できない場合は、Cisco Technical Assistance Center(TAC)に連絡して、サポートと詳細な手順を確認してください。電話をかける前に、TACエンジニアが可能な限り迅速にサポートできるように、次の情報を用意しておいてください。

- WAASハードウェアを受け取った日付
- シャーシのシリアル番号
- ソフトウェアのタイプとリリース番号(可能な場合は、**show version**コマンド**を入力**します)
- 保守契約または保証情報
- 次のような問題の説明が適切です。
  - 問題とユーザに見られる症状は何ですか。
  - いつ、どこで
  - 表示されるエラーメッセージ、アラート、アラーム
  - 問題を複製する手順
- 問題の切り分けと解決のために既に行った手順の簡単な説明
- 診断テスト出力(「診断の実行」セクションを参照)
- Central Managerデータベースのバックアップ(**cms database backupコマンドを**使用)
- 「WAASのトラブルシューティング情報の収集」セクションで収集された情報です。
- トポロジ図（ネットワーク/配線図、論理図など）
- パケットキャプチャ、トランザクションログ、コアファイル、ルータ/スイッチおよびWAEからのWCCP showコマンド出力、その他のログファイルなど、問題のその他の証拠。

次のいずれかの方法でTACに連絡できます。

- オンラインでサービスリクエストを作成
- このページの電話番号でTACに連絡してください。
- Cisco Small Business Support Centerに連絡する