CHAPTER 33

トラブルシューティング

この章では、ASA 1000V のトラブルシューティングの方法について説明します。次の項目を取り上げます。

コンフィギュレーションのテスト

この項では、接続性のテスト方法、ASA 1000V イーサネット インターフェイスを ping する方法、およびあるインターフェイスにあるホストが他のインターフェイスのホストに ping できるようにする方法について説明します。

ping メッセージおよびデバッグ メッセージはトラブルシューティング時に限りイネーブルにしてください。ASA 1000V のテストが終了したら、「テスト コンフィギュレーションのディセーブル化」（P.33-7）の手順に従ってください。

この項は、次の内容で構成されています。

ICMP デバッグ メッセージと Syslog メッセージのイネーブル化

デバッグ メッセージと syslog メッセージは、ping が成功しない理由をトラブルシューティングするのに役立ちます。ASA 1000V では、ASA 1000V イーサネット インターフェイスへの ping に対する ICMP デバッグ メッセージだけが表示されます。ASA 1000V を経由する他のホストへの ping に対する ICMP デバッグ メッセージは表示されません。デバッグ メッセージと syslog メッセージをイネーブルにするには、次の手順を実行します。

	コマンド	目的
ステップ 1	**debug icmp trace** **例：** `hostname(config)# debug icmp trace`	ASA 1000V イーサネット インターフェイスへの ping の ICMP パケット情報を表示します。
ステップ 2	**logging monitor debug** **例：** `hostname(config)# logging monitor debug`	Telnet セッションまたは SSH セッションに送信する syslog メッセージを設定します。 **（注）** あるいは、**logging buffer debug** コマンドを使用してログ メッセージをバッファに送信してから、**show logging** コマンドを使用してそれらを表示することもできます。
ステップ 3	**terminal monitor** **例：** `hostname(config)# terminal monitor`	Telnet セッションまたは SSH セッションに syslog メッセージを送信します。
ステップ 4	**logging on** **例：** `hostname(config)# logging on`	syslog メッセージの生成をイネーブルにします。

デフォルト グローバル ポリシーへの ICMP インスペクションをイネーブルにするには、次の手順を実行します。

	コマンド	目的
ステップ 1	**policy-map** name **例：** `hostname(config)# policy-map global_policy`	ポリシー マップを設定し、アクションをトラフィック クラスに関連付けます。
ステップ 2	**class** classmap_*name* **例：** `hostname(config-pmap)# class inspection_default`	クラス マップ トラフィックにアクションを割り当てることができるように、クラス マップをポリシー マップに割り当てます。
ステップ 3	**inspect icmp** **例：** `hostname(config)# inspect icmp`	ICMP インスペクションをイネーブルにします。

例

次に、外部ホスト（209.165.201.2）から ASA 1000V の外部インターフェイス（209.165.201.1）への ping が成功した例を示します。

```
hostname(config)# debug icmp trace
Inbound ICMP echo reply (len 32 id 1 seq 256) 209.165.201.1 > 209.165.201.2
Outbound ICMP echo request (len 32 id 1 seq 512) 209.165.201.2 > 209.165.201.1
Inbound ICMP echo reply (len 32 id 1 seq 512) 209.165.201.1 > 209.165.201.2
Outbound ICMP echo request (len 32 id 1 seq 768) 209.165.201.2 > 209.165.201.1
Inbound ICMP echo reply (len 32 id 1 seq 768) 209.165.201.1 > 209.165.201.2
Outbound ICMP echo request (len 32 id 1 seq 1024) 209.165.201.2 > 209.165.201.1
Inbound ICMP echo reply (len 32 id 1 seq 1024) 209.165.201.1 > 209.165.201.2
```

この出力では、ICMP パケット長（32 バイト）、ICMP パケット識別子（1）、および ICMP シーケンス番号（ICMP シーケンス番号は 0 から始まり、要求が送信されるたびに増分されます）が示されています。

ASA 1000V のインターフェイスへの ping の実行

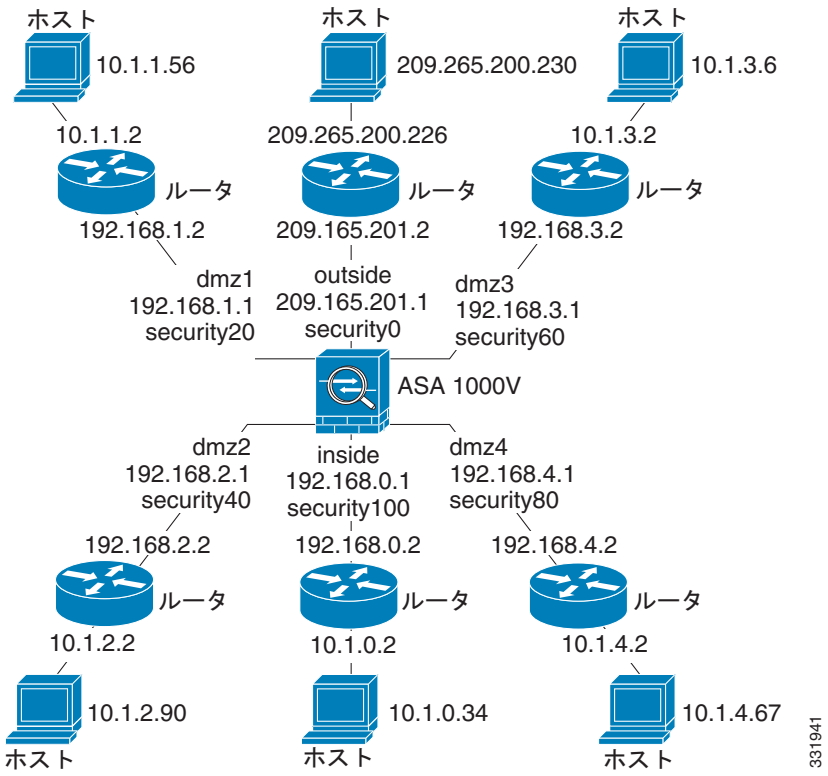
ASA 1000V インターフェイスが起動して動作しているかどうか、および ASA 1000V と接続ルータが正しく動作しているかどうかをテストするには、ASA 1000V インターフェイスを ping します。ASA 1000V インターフェイスを ping するには、次の手順を実行します。

ステップ 1　インターフェイス名、セキュリティ レベル、および IP アドレスを示す ASA 1000V の図を作成します。

（注）　この手順では IP アドレスを使用しますが、**ping** コマンドでは、DNS 名および **name** コマンドを使用してローカル IP アドレスに割り当てられた名前もサポートされます。

図には、直接接続されたすべてのルータ、および ASA 1000V を ping するルータの反対側にあるホストも含める必要があります。この情報はこの手順と「ASA 1000V 上のトラフィックの通過」（P.33-5）の手順で使用します。（図 33-1 を参照）。

図 33-1　インターフェイス、ルータ、およびホストを含むネットワーク図



ステップ 2　直接接続されたルータから各 ASA 1000V インターフェイスを ping します。このテストは、ASA 1000V インターフェイスがアクティブであること、およびインターフェイス コンフィギュレーションが正しいことを確認します。

ASA 1000V インターフェイスがアクティブではない場合、インターフェイス コンフィギュレーションが正しくない場合、または ASA 1000V とルータの間でスイッチがダウンしている場合、ping は失敗する可能性があります（図 33-2 を参照）。この場合、パケットが ASA 1000V に到達しないので、デバッグ メッセージや syslog メッセージは表示されません。

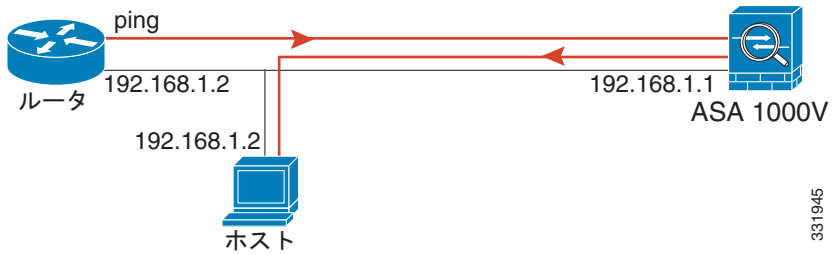
図 33-2　ASA 1000V インターフェイスへの ping の失敗

ping が ASA 1000V に到達し、応答があると、次のようなデバッグ メッセージが表示されます。

```
ICMP echo reply (len 32 id 1 seq 256) 209.165.201.1 > 209.165.201.2
ICMP echo request (len 32 id 1 seq 512) 209.165.201.2 > 209.165.201.1
```

ping 応答がルータに戻されない場合は、スイッチ ループまたは冗長 IP アドレスが存在する可能性があります（図 33-3 を参照）。

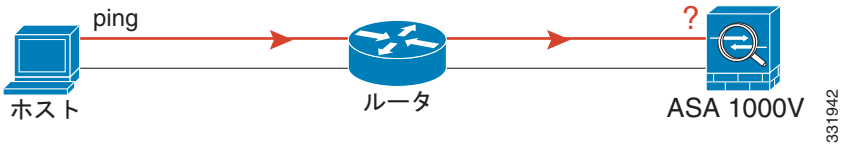
図 33-3　IP アドレッシングの問題による ping の失敗



ステップ 3　リモート ホストから各 ASA 1000V インターフェイスを ping します。このテストは、直接接続されたルータがホストと ASA 1000V の間でパケットをルーティングできるかどうか、および ASA 1000V がパケットを正確にルーティングしてホストに戻せるかどうかを確認します。

中間ルータを通ってホストに戻るルートが ASA 1000V にない場合、ping は失敗する可能性があります（図 33-4 を参照）。この場合、デバッグ メッセージには ping が成功したことが示されますが、ルーティングの失敗を示す syslog メッセージ 110001 が表示されます。

図 33-4　ASA 1000V の戻りルート未設定による ping の失敗



ASA 1000V 上のトラフィックの通過

ASA 1000V インターフェイスを正常に ping した後で、トラフィックが ASA 1000V を正常に通過できることを確認します。このテストによって、NAT が正しく動作していることが示されます（設定されている場合）。

異なるインターフェイス上のホスト間で ping するには、次の手順を実行します。

	コマンド	目的
ステップ 1	**access-list ICMPACL extended permit icmp any any** **例：** `hostname(config)# access-list ICMPACL extended permit icmp any any`	発信元ホストから ICMP トラフィックを許可するアクセス リストを追加します。 **（注）** デフォルトでは、ホストが低セキュリティ インターフェイスにアクセスすると、すべてのトラフィックが通過を許可されます。ただし、高セキュリティ インターフェイスにアクセスするには、先行するアクセス リストが必要です。

ステップ 2	**access-group ICMPACL in interface** *interface_name* **例：** `hostname(config)# access-group ICMPACL in interface inside`	各発信元インターフェイスにアクセス リストを割り当てます。各発信元インターフェイスに対してこのコマンドを繰り返します。 *interface_name* 引数は、イーサネット インターフェイスの名前です。

ステップ 3	**class-map ICMP-CLASS**
	match access-list ICMPACL
	policy-map ICMP-POLICY
	class ICMP-CLASS
	inspect icmp
	service-policy ICMP-POLICY global
	
	例：
	`hostname(config)# class-map ICMP-CLASS`
	`hostname(config-cmap)# match access-list ICMPACL`
	`hostname(config)# policy-map ICMP-POLICY`
	`hostname(config-pmap)# class ICMP-CLASS`
	`hostname(config-pmap)# inspect icmp`
	`hostname(config)# service-policy ICMP-POLICY global`
		ICMP インスペクション エンジンをイネーブルにして、ICMP 応答が発信元ホストに戻されるようにします。
		
		低セキュリティ インターフェイスにアクセスする場合は、ICMP インスペクションをイネーブルにする必要があります。ただし、高セキュリティ インターフェイスにアクセスするには、ICMP インスペクションおよび先行するアクセス リストをイネーブルにする必要があります。
		
		（注） あるいは、ICMP アクセス リストを宛先インターフェイスに適用し、ASA 1000V を介して ICMP トラフィックを戻すこともできます。

ステップ 4	**logging on** **例：** `hostname(config)# logging on`	syslog メッセージの生成をイネーブルにします。 ping が成功すると、アドレス変換（305009 または 305011）と ICMP 接続が確立されたこと（302020）を確認する syslog メッセージが表示されます。**show xlate** コマンドまたは **show conns** コマンドを入力してこの情報を表示することもできます。 NAT が正しく設定されていないために ping が失敗することがあります（図 33-5 を参照）。この場合、NAT が失敗したことを示す syslog メッセージが表示されます（305005 または 305006）。外部ホストから内部ホストに ping し、スタティック変換がない場合は、次の syslog メッセージが表示されます。 `%ASA-3-106010: deny inbound icmp.` **（注）** ASA 1000V では、ASA 1000V イーサネット インターフェイスへの ping に対する ICMP デバッグ メッセージだけが表示されます。ASA 1000V を経由する他のホストへの ping に対する ICMP デバッグ メッセージは表示されません。

図 33-5　ASA 1000V のアドレス変換の問題による ping の失敗

テスト コンフィギュレーションのディセーブル化

テストの完了後、ICMP の ASA 1000V への送信および通過を許可し、デバッグ メッセージを表示するテスト コンフィギュレーションをディセーブルにします。このコンフィギュレーションをそのままにしておくと、深刻なセキュリティ リスクが生じる可能性があります。また、デバッグ メッセージは ASA 1000V のパフォーマンスを低下させます。

テスト コンフィギュレーションをディセーブルにするには、次の手順を実行します。

	コマンド	目的
ステップ 1	**no debug icmp trace** **例：** `hostname (config)# no debug icmp trace`	ICMP デバッグ メッセージをディセーブルにします。
ステップ 2	**no logging on** **例：** `hostname (config)# no logging on`	ロギングをディセーブルにします。
ステップ 3	**no access-list ICMPACL** **例：** `hostname (config)# no access-list ICMPACL`	ICMPACL アクセス リストを削除し、関連する **access-group** コマンドを削除します。
ステップ 4	**no service-policy ICMP-POLICY** **例：** `hostname (config)# no service-policy ICMP-POLICY`	（任意）ICMP インスペクション エンジンをディセーブルにします。

トレースルートによるパケット ルーティングの決定

パケットのルートは、トレースルート機能を使用してトレースできます。この機能には、**traceroute** コマンドでアクセスできます。トレースルートは、無効なポート上の宛先に UDP パケットを送信することで機能します。ポートが有効ではないため、宛先までの間にあるルータから ICMP Time Exceeded メッセージが返され、ASA 1000V にエラーが報告されます。

パケット トレーサによるパケットの追跡

パケット トレーサ ツールは、パケット スニフィングとネットワーク障害箇所特定のためのパケット追跡を実現するとともに、パケットに関する詳細情報と ASA 1000V によるパケットの処理方法を示します。コンフィギュレーション コマンドが原因でパケットがドロップしたのではない場合、パケット トレーサ ツールにより、原因に関する詳細な情報が読みやすい形式で表示されます。

また、パケットが正しく動作しているかどうかを確認するために、パケット トレーサ ツールを使用して、ASA 1000V を通過するパケットのライフスパンをトレースできます。このツールでは、次の処理を行うことができます。

- ネットワーク内にドロップするすべてのパケットをデバッグする。
- コンフィギュレーションが意図したとおりに機能しているかを確認する。
- パケットに適用可能なすべてのルール、およびルールが追加される原因となった CLI コマンドを表示する。
- データ パス内でのパケット変化を時系列で表示する。
- データ パスにトレーサ パケットを挿入する。
- ユーザ ID と FQDN に基づく IP アドレスを検索します。

パケットを追跡するには、次のコマンドを入力します。

コマンド	目的
packet-tracer input [*ifc_name*] [**icmp** [*sip* | **user** *username* | **fqdn** *fqdn-string*] *type code ident* [*dip* | **fqdn** *fqdn-string*]] | [**tcp** [*sip* | **user** *username* | **fqdn** *fqdn-string*] *sport* [*dip* | **fqdn** *fqdn-string*] *dport*] | [**udp** [*sip* | **user** *username* | **fqdn** *fqdn-string*] *sport* [*dip* | **fqdn** *fqdn-string*] *dport*] | [**rawip** [*sip* | **user** *username* | **fqdn** *fqdn-string*] [*dip* | **fqdn** *fqdn-string*]] [**detailed**] [**xml**] **例：** `hostname# packet-tracer input inside tcp 10.2.25.3 www 209.165.202.158 aol detailed`	パケットに関する詳細情報と ASA 1000V によるパケットの処理方法を示します。詳細情報を出力し、内部ホスト 10.2.25.3 から外部ホスト 209.165.202.158 にパケット トレーシングをイネーブルにする例を示します。

TCP パケット損失の処理

TCP パケット損失のトラブルシューティングの詳細については、「TCP マップを使用した TCP ノーマライザのカスタマイズ」（P.24-6）を参照してください。

ASA 1000V のリロード

ASA 1000V をリロードするには、次のコマンドを入力します。

コマンド	目的
reload **例：** `hostname (config)# reload`	ASA 1000V を再起動します。

パスワード回復の実行

この項は、次の内容で構成されています。

ASA 1000V のパスワードまたはイメージの回復

ASA 1000V のパスワードまたはイメージを回復するには、次の手順を実行します。

	コマンド	目的
ステップ 1	**copy running-config** *filename* **例：** hostname# copy running-config backup.cfg	実行コンフィギュレーションを ASA 1000V のバックアップ ファイルにコピーします。
ステップ 2	**reload** **例：** hostname# reload	ASA 1000V を再起動します。
ステップ 3	GNU GRUB version 2.0(12)4 bootflash:/asa100123-20-smp-k8.bin **bootflash: /asa100123-20-smp-k8.bin with no configuration load** **例：** GNU GRUB version 2.0(12)4 **bootflash: /asa100123-20-smp-k8.bin with no configuration load**	[GNU GRUB] メニューから、下矢印を押し、**コンフィギュレーションをロードしない**オプションで <**filename**> を選択し、Enter キーを押します。filename は ASA 1000V のデフォルトのブート イメージ ファイル名です。デフォルトのブート イメージは、**fallback** コマンドによって自動的にブートされることはありません。 選択したブート イメージをブートします。
ステップ 4	**copy** *filename* **running-config** **例：** hostname (config)# copy backup.cfg running-config	バックアップ コンフィギュレーション ファイルを実行コンフィギュレーションにコピーします。
ステップ 5	**enable password** **例：** hostname (config)# enable password cisco123	パスワードをリセットします。
ステップ 6	**write mem** **例：** hostname (config)# write mem	新しいコンフィギュレーションを保存します。

パスワード回復のディセーブル化

ASA 1000V 上でパスワード回復をディセーブルにすることはできません。

フラッシュ ファイル システムの消去

フラッシュ ファイル システムを消去するには、次の手順を実行します。

ステップ 1　「ASA 1000V コマンドライン インターフェイスへのアクセス」（P.2-2）の手順に従って、ASA 1000V のコンソール ポートに接続します。

ステップ 2　次のように、特権 EXEC モードで **format** コマンドを入力します。

```
hostname# format disk0: disk1:
```

その他のトラブルシューティング ツール

ASA 1000V には、使用できるその他のトラブルシューティング ツールがあります。この項は、次の内容で構成されています。

デバッグ メッセージの表示

デバッグ出力は CPU プロセスで高プライオリティが割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。このため、特定の問題のトラブルシューティングを行う場合や、Cisco TAC とのトラブルシューティング セッションの間に限り **debug** コマンドを使用してください。さらに、**debug** コマンドはネットワーク トラフィックとユーザが少ないときに使用することをお勧めします。このような時間帯を選んでデバッグを実行すると、**debug** コマンドの処理の負担によってシステム利用が影響を受ける可能性が少なくなります。デバッグ メッセージをイネーブルにするには、コマンド リファレンスの **debug** コマンドを参照してください。

パケットの取得

パケットの取得は、接続障害のトラブルシューティングや不審なアクティビティのモニタを行う場合に便利です。パケット取得機能を使用する場合は、Cisco TAC に連絡することをお勧めします。コマンド リファレンスの **capture** コマンドを参照してください。

クラッシュ ダンプの表示

ASA 1000V がクラッシュした場合に、クラッシュ ダンプ情報を表示できます。クラッシュ ダンプの内容を調べる必要がある場合は、Cisco TAC に連絡することをお勧めします。コマンド リファレンスの **show crashdump** コマンドを参照してください。

コアダンプ

コア ダンプは、プログラムが異常終了（クラッシュ）した場合の実行中のプログラムのスナップショットです。コア ダンプは、エラーを診断またはデバッグするため、および障害を後からオフサイトで分析できるよう、クラッシュを保存するために使用されます。Cisco TAC では、ユーザがコア ダ

ンプ機能をイネーブルにして、ASA 1000V でのアプリケーションまたはシステムのクラッシュをトラブルシューティングする必要がある場合があります。コマンド リファレンスの **coredump** コマンドを参照してください。

プロセスごとの CPU 使用率のモニタリング

CPU 上で実行されているプロセスをモニタリングできます。特定のプロセスに使用する CPU 使用率に関する情報を取得できます。CPU 使用率に関する統計情報は、最も高い使用率を最上部に表示する降順にソートされます。また、ログ時刻の 5 秒、1 分、5 分前の、プロセスごとの CPU 負荷に関する情報も含まれます。この情報は 5 秒おきに自動的に更新され、リアルタイムの統計情報が表示されます。