NAT のモニタリングおよびメンテナンス

このモジュールでは、次の内容について説明します。

- 変換情報と統計を使用した Network Address Translation（NAT; ネットワーク アドレス変換）のモニタリング。
- タイムアウトの期限切れ前に NAT 変換をクリアすることによる、NAT のメンテナンス。
- システム エラー メッセージ、例外、他の情報の syslog によるログとトラッキングを利用した、NAT 変換のロギングのイネーブル化。

機能情報の検索

ご使用のソフトウェア リリースが、このモジュールで説明している機能の一部をサポートしていない場合があります。最新の機能情報および警告については、ご使用のプラットフォームおよびソフトウェア リリースのリリースノートを参照してください。このモジュールに記載されている機能に関する情報を検索したり、各機能がサポートされているリリースに関するリストを参照したりするには、「NAT のモニタリングとメンテナンスの機能情報」（P.12）を参照してください。

プラットフォームのサポートと、Cisco IOS および Catalyst OS ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスしてください。Cisco.com のアカウントは必要ありません。

目次

NAT のモニタリングおよびメンテナンスの前提条件

このモジュールの作業を実行する前に、「IP アドレス節約のための NAT 設定」モジュールに記載された概念を理解し、NAT を設定しておく必要があります。

NAT のモニタリングとメンテナンスについて

このモジュールに記載されている作業を実行する前に、次の概念について理解しておく必要があります。

NAT の表示内容

IP NAT 変換情報には、基本的に 2 つのタイプがあります。

変換エントリ

次の内容を含む、変換エントリ情報。

- アドレスを識別するポートのプロトコル。
- 1 つ以上の内部のローカル IP アドレスを外部に対して表すために使用できる合法的な IP アドレス。
- 内部ネットワーク上のホストに割り当てられた IP アドレス（多くの場合 NIC やサービス プロバイダーにより割り当てられた合法的アドレスではない）。
- 外部ホストが内部ネットワークに出現するときの IP アドレス（多くの場合 NIC やサービス プロバイダーにより割り当てられた合法的アドレスではない）。
- 外部ネットワーク上のホストに、所有者が割り当てた IP アドレス。
- エントリが作成されてからの経過時間（「時間：分：秒」形式）。
- エントリが最後に使用されてからの経過時間（「時間：分：秒」形式）。
- 変換タイプを示すフラグ。次のようなフラグがあります。
  - extended：拡張変換。
  - static：スタティック変換。
  - destination：循環式変換。
  - outside：外部変換。
  - timing out：TCP finish（FIN）または reset（RST）フラグにより、以後変換を使用しない。

スタティック情報

スタティック情報には次のような内容が含まれます。

- システム内でアクティブな変換の総数。この数値は、変換が作成されるたびに増加し、変換がクリアまたはタイムアウトになるたびに減少します。
- **ip nat outside** コマンドで outside とマークされたインターフェイスのリスト。
- **ip nat inside** コマンドで inside とマークされたインターフェイスのリスト。
- ソフトウェアが変換テーブル参照を行ってエントリを発見した回数。
- ソフトウェアが変換テーブル参照を行ったが、エントリが見つからず、エントリ作成を試行する必要があった回数。
- ルータが起動されてから、期限切れになった変換の累積数。
- ダイナミック マッピングについての情報。
- 内部送信元変換についての情報。
- 変換に使用されているアクセス リスト番号。
- プールの名称。
- そのプールを使用している変換の数。
- プールで使用されている IP ネットワーク マスク。
- プール範囲の開始 IP アドレス。
- プール範囲の終了 IP アドレス。
- プールのタイプ。汎用タイプまたは循環タイプです。
- 変換に使用可能なプール内のアドレスの数。
- 使用されているアドレスの数。
- プールからの割り当てに失敗した数。

NAT はログ オプション付き ACL をサポートしていません。同様の機能は、次のオプションのいずれかを使用して実現できます。

- ロギング オプションを持つ物理インターフェイスまたは VLAN。
- NetFlow の使用。
- syslog 機能の使用。

Syslog の使用方法

Syslog 分析により、システム エラー メッセージ、例外、他の情報（デバイス コンフィギュレーションの変更など）の集約的なログ作成とトラッキングが行えます。記録されたエラー メッセージ データを使用して、ルータとネットワーク パフォーマンスの分析が行えます。業務に重要な情報とメッセージをまとめたレポートを作成するよう、Syslog 分析をカスタマイズすることが可能です。

詳しくは、『*Resource Manager Essentials and Syslog Analysis: How-To* document』*を参照してください。*

http://www.cisco.com/warp/public/477/RME/rme_syslog.html

NAT のモニタリング方法とメンテナンス方法

ここでは、次の手順について説明します。

NAT 変換情報の表示

変換データと統計情報を表示するには、次の作業を実行します。

手順の概要

1. **enable**
2. **show ip nat translations** [**verbose**]
3. **show ip nat statistics**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**show ip nat translations** [**verbose**] **例：** `Router# show ip nat translations`	（任意）アクティブな NAT 変換を表示します。
ステップ 3	**show ip nat statistics** **例：** `Router# show ip nat statistics`	（任意）アクティブな NAT 変換の統計を表示します。

NAT 変換情報の表示：例

ここでは、次の例について説明します。

NAT 変換の表示

次に、**show ip nat translations** コマンドの出力例を示します。オーバーロードなしで、内部ホスト 2 台がパケットをいくつかの外部ホストと交換しています。

```
Router# show ip nat translations

Pro Inside global      Inside local       Outside local      Outside global

--- 192.168.2.1     192.168.2.12              ---                ---

--- 192.168.2.21    192.168.2.89              ---                --
```

オーバーロードが発生し、Domain Name Server（DNS; ドメイン ネーム サーバ）トランザクションは依然アクティブです。また、2 つの Telnet セッション（2 つの異なるホストからのもの）もアクティブです。2 台の異なる内部ホストが、外部では単一の IP アドレスになることに注意してください。

```
Router# show ip nat translations

Pro Inside global        Inside local       Outside local      Outside global

udp 192.168.2.20:1220  192.168.2.95:1220 192.168.2.22:53 192.168.2.20:53

tcp 192.168.2.20:11012 192.168.2.209:11012 192.168.1.220:23 192.168.2.20:23

tcp 192.168.2.20:1067 192.168.2.20:1067 192.168.2.20:23 192.168.2.20:23
```

次に、**verbose** キーワードを含めた出力例を示します。

```
Router# show ip nat translations verbose


Pro Inside global        Inside local       Outside local      Outside global

udp 192.168.2.20:1220 192.168.2.23:1220 192.168.2.24:53 192.168.2.25:53

        create 00:00:02, use 00:00:00, flags: extended

tcp 192.168.2.23:11012 192.168.2.30:11012 192.168.2.20:23 192.168.2.28:23

        create 00:01:13, use 00:00:50, flags: extended

tcp 192.168.2.24:1067 192.168.2.29:1067 192.168.2.20:23 192.168.2.50:23

        create 00:00:02, use 00:00:00, flags: extended
```

NAT 統計情報の表示

次に、**show ip nat statistic** コマンドの出力例を示します。

```
Router# show ip nat statistics

Total translations: 2 (0 static, 2 dynamic; 0 extended)
Outside interfaces: Serial0
Inside interfaces: Ethernet1
Hits: 135  Misses: 5
Expired translations: 2
Dynamic mappings:
-- Inside Source
access-list 1 pool net-208 refcount 2
 pool net-208: netmask 255.255.255.240
        start 192.168.0.0 end 192.168.255.255
        type generic, total addresses 14, allocated 2 (14%), misses 0
```

タイムアウト前の NAT エントリのクリア

デフォルトでは、ある時点でダイナミック アドレス変換は NAT 変換テーブルからタイムアウトになります。タイムアウトの前にエントリをクリアするには、次の作業を実行します。

手順の概要

1. **enable**
2. **clear ip nat translation inside** *global-ip local-ip* **outside** *local-ip global-ip*
3. **clear ip nat translation outside** *global-ip local-i*p
4. **clear ip nat translation** *protocol* **inside** *global-ip global-port local-ip local-port* **outside** *local-ip local-port-global-ip global-port*
5. **clear ip nat translation** {* | [**forced**] | [**inside** *global-ip local-ip*] [**outside** *local-ip global-ip*]}
6. **clear ip nat translation inside** *global-ip local-ip* [**forced**]
7. **clear ip nat translation outside** *local-ip global-ip* [**forced**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**clear ip nat translation inside** *global-ip local-ip* **outside** *local-ip global-ip* **例：** `Router# clear ip nat translation inside 192.168.2.209 1220 192.168.2.95 1220 outside 192.168.2.100 53 192.168.2.101 53`	（任意）内部変換を含む単一のダイナミック ハーフエントリ、またはダイナミック設定で作成された内部変換と外部変換の両方をクリアします。 • ダイナミック ハーフエントリがクリアされるのは、子変換を持たない場合だけです。
ステップ 3	**clear ip nat translation outside** *global-ip local-ip* **例：** `Router# clear ip nat translation outside 192.168.2.100 1220 192.168.2.80`	（任意）ダイナミック設定で作成された外部変換を含む単一のダイナミック ハーフエントリをクリアします。 • ダイナミック ハーフエントリがクリアされるのは、子変換を持たない場合だけです。
ステップ 4	**clear ip nat translation** *protocol* **inside** *global-ip global-port local-ip local-port* **outside** *local-ip local-port-global-ip global-port* **例：** `Router# clear ip nat translation udp inside 192.168.2.209 1220 192.168.2.195 1220 outside 192.168.2.13 53 192.168.2.132 53`	（任意）UDP 変換エントリだけをクリアします。

	コマンドまたはアクション	目的
ステップ 5	**clear ip nat translation** {* | [**forced**] | [**inside** *global-ip local-ip*] [**outside** *local-ip global-ip*]} **例：** `Router# clear ip nat translation *`	(任意）ダイナミック変換すべて（***** もしくは **forced** キーワードを使用)、内部変換を含む単一のダイナミック ハーフエントリ、外部変換を含む単一のダイナミック ハーフエントリのいずれかをクリアします。 • 単一のダイナミック ハーフエントリをクリアする場合、子変換を持たない場合にだけクリアが実行されます。
ステップ 6	**clear ip nat translation inside** *global-ip local-ip* [**forced**] **例：** `Router# clear ip nat translation *`	(任意）対応する外部変換の有無にかかわらず、ダイナミック設定で作成された内部変換を含む単一のダイナミック ハーフエントリおよびその子変換を、強制的にクリアします。 • ダイナミック ハーフエントリは、子変換の有無にかかわらず、必ずクリアされます。
ステップ 7	**clear ip nat translation outside** *local-ip global-ip* [**forced**] **例：** `Router# clear ip nat translation *`	(任意）ダイナミック設定で作成された外部変換を含む単一のダイナミック ハーフエントリおよびその子変換を、強制的にクリアします。 • ダイナミック ハーフエントリは、子変換の有無にかかわらず、必ずクリアされます。

Syslog での NAT 変換ロギングのイネーブル化

NAT 変換のロギングは、**syslog** コマンドを使用してイネーブルまたはディセーブルにできます。

Syslog 分析により、システム エラー メッセージ、例外、他の情報（NAT 変換など）の集約的なログ作成とトラッキングが行えます。記録されたエラー メッセージ データを使用して、ルータとネットワーク パフォーマンスの分析が行えます。業務に重要な情報とメッセージをまとめたレポートを作成するよう、Syslog 分析をカスタマイズすることが可能です。

前提条件

この作業の実行前に、ロギングのイネーブル化の確認、サーバの IP アドレスの設定、捕捉するメッセージのレベル確定など、必要な **syslog** コマンドを特定しておく必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip nat log translations syslog**
4. **no logging console**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip nat log translations syslog** **例：** `Router(config)# ip nat log translations syslog`	syslog の NAT 変換のロギングをイネーブルにします。
ステップ 4	**no logging console** **例：** `Router(config)# no logging console`	（任意）ログのコンソールへの表示をディセーブルにします。 • コンソールへのロギングは、デフォルトでイネーブルになっています。

NAT のモニタリングおよびメンテナンスの例

ここでは、次の設定例について説明します。

- 「UDP NAT 変換のクリア：例」（P.8）
- 「Syslog のイネーブル化：例」（P.9）

UDP NAT 変換のクリア：例

次に、User Datagram Protocol（UDP; ユーザ データグラム プロトコル）エントリのクリア前後の NAT エントリの例を示します。

```
Router# show ip nat translation

Pro Inside global         Inside local       Outside local      Outside global

udp 192.168.2.20:1220  192.168.2.95:1220 192.168.2.22:53 192.168.2.20:53

tcp 192.168.2.20:11012 192.168.2.209:11012 171.69.1.220:23 192.168.2.20:23

tcp 192.168.2.20:1067 192.168.2.20:1067 192.168.2.20:23 192.168.2.20:23

Router# clear ip nat translation udp inside 192.168.2.20:1067 192.168.2.20:1067 outside
192.168.2.20:23 192.168.2.20:23

Router# show ip nat translation

Pro Inside global      Inside local       Outside local      Outside global

udp 192.168.2.20:1220  192.168.2.95:1220 192.168.2.22:53 192.168.2.20:53
```

```
tcp 192.168.2.20:11012 192.168.2.209:11012 171.69.1.220:23 192.168.2.20:23
```

Syslog のイネーブル化：例

次の例に、NAT エントリを syslog に記録する方法を示します。

```
Router(config)# logging on
Router(config)# logging 1.1.1.1
Router(config)# logging trap informational
Router(Config)# ip nat log translations syslog
```

NAT 情報の記録フォーマット（ICMP ping には NAT オーバーロード コンフィギュレーションを介するなど）は、次のとおりです。

```
Apr 25 11:51:29 [10.0.19.182.204.28] 1: 00:01:13: NAT:Created icmp
135.135.5.2:7 171 12.106.151.30:7171 54.45.54.45:7171
54.45.54.45:7171
Apr 25 11:52:31 [10.0.19.182.204.28] 8: 00:02:15: NAT:Deleted icmp
135.135.5.2:7 172 12.106.151.30:7172 54.45.54.45:7172
54.45.54.45:7172
```

次の作業

- アプリケーション レベル ゲートウェイで使用するよう NAT を設定するには、「NAT でのアプリケーション レベル ゲートウェイの使用」モジュールを参照してください。
- NAT を MPLS VPN と統合するには、「Integrating NAT with MPLS VPNs」モジュールを参照してください。
- ハイ アベイラビリティに NAT を設定するには、「Configuring NAT for High Availability」モジュールを参照してください。

参考資料

ここでは、NAT のモニタリングとメンテナンスに関する関連資料について説明します。

関連資料

関連項目	参照先
NAT コマンド：コマンド構文、コマンド モード、コマンド履歴、デフォルト、使用に関する注意事項、および例	『*Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services,* Release 12.3 』の「*IP Addressing Commands*」の章

規格

規格	タイトル
なし	

MIB

MIB	MIB リンク
なし	選択したプラットフォーム、Cisco IOS リリース、および機能セットの MIB の場所を検索しダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
なし	

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 • テクニカル サポートを受ける • ソフトウェアをダウンロードする • セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける • ツールおよびリソースへアクセスする – Product Alert の受信登録 – Field Notice の受信登録 – Bug Toolkit を使用した既知の問題の検索 • Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する • トレーニング リソースへアクセスする • TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/en/US/support/index.html

コマンド リファレンス

このモジュールに記載されている 1 つ以上の機能で、次のコマンドが追加または変更されています。これらのコマンドの詳細については、『*Cisco IOS <Technology> Command Reference*』（http://www.cisco.com/en/US/docs/ios/ipaddr/command/reference/iad_cr_book.html）を参照してください。すべての Cisco IOS コマンドの詳細については、http://tools.cisco.com/Support/CLILookup でコマンド検索ツールを使用するか、http://www.cisco.com/en/US/docs/ios/mcl/allreleasemcl/all_book.html で『*Cisco IOS Master Command List, All Releases*』を参照してください。

この機能で使用される新しいコマンドまたは変更されたコマンドはありません。

NAT のモニタリングとメンテナンスの機能情報

表 1 に、このモジュールで説明した機能をリストし、特定の設定情報へのリンクを示します。このテーブルには、Cisco IOS Release 12.2(1)、Cisco IOS Release 12.2(1)、12.0(3) またはそれ以降のリリースで導入または変更された新しい機能だけが記載されています。

ご使用の Cisco IOS ソフトウェア リリースでは、一部のコマンドが使用できない場合があります。特定のコマンドのリリース情報については、コマンド リファレンス マニュアルを参照してください。

プラットフォームのサポートおよびソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator を使用すると、特定のソフトウェア リリース、機能セット、またはプラットフォームをサポートする Cisco IOS と Catalyst OS のソフトウェア イメージを判別できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスしてください。Cisco.com のアカウントは必要ありません。

（注） 表 1 に、特定の Cisco IOS ソフトウェア リリース群で特定の機能をサポートする Cisco IOS ソフトウェア リリースだけを示します。特に明記されていない限り、Cisco IOS ソフトウェア リリース群の後続のリリースでもこの機能をサポートします。

表 1　NAT のモニタリングとメンテナンスの機能情報

機能名	リリース	機能情報
NAT：ダイナミック NAT ハーフエントリの強制的クリア	Cisco IOS 12.2 (33) XND	2 つめの forced キーワードが **clear ip nat translation** コマンドに追加され、子変換の有無にかかわらずハーフエントリを削除できるようになりました。