



Cisco Catalyst IE9300 高耐久性シリーズスイッチ IP アドレッシング サービス コンフィギュレーション ガイド

最終更新：2026 年 4 月 28 日

シスコシステムズ合同会社

〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー

<http://www.cisco.com/jp>

お問い合わせ先：シスコ コンタクトセンター

0120-092-255 (フリーコール、携帯・PHS含む)

電話受付時間：平日 10:00～12:00、13:00～17:00

<http://www.cisco.com/jp/go/contactcenter/>

Full Cisco Trademarks with Software License

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

通信、サービス、およびその他の情報

- シスコからタイムリーな関連情報を受け取るには、[Cisco Profile Manager](#) でサインアップしてください。
- 重要な技術によりビジネスに必要な影響を与えるには、[Cisco Services](#) にアクセスしてください。
- サービス リクエストを送信するには、[Cisco Support](#) にアクセスしてください。
- 安全で検証済みのエンタープライズクラスのアプリケーション、製品、ソリューション、およびサービスを探して参照するには、[Cisco DevNet \[英語\]](#) にアクセスしてください。
- 一般的なネットワーキング、トレーニング、認定関連の出版物を入手するには、[Cisco Press](#) にアクセスしてください。
- 特定の製品または製品ファミリの保証情報を探するには、[Cisco Warranty Finder](#) にアクセスしてください。

Cisco バグ検索ツール

[シスコバグ検索ツール](#) (BST) は、シスコ製品とソフトウェアの障害と脆弱性の包括的なリストを管理するシスコバグ追跡システムへのゲートウェイです。BSTは、製品とソフトウェアに関する詳細な障害情報を提供します。

マニュアルに関するフィードバック

シスコのテクニカルドキュメントに関するフィードバックを提供するには、それぞれのオンラインドキュメントの右側のペインにあるフィードバックフォームを使用してください。

偏向のない言語

この製品のマニュアルセットは、偏向のない言語を使用するように配慮されています。このドキュメントセットでの偏向のない言語とは、年齢、障害、性別、人種的アイデンティティ、民族的アイデンティティ、性的指向、社会経済的地位、およびインターセクショナリティに基づく差別を意味しない言語として定義されています。製品ソフトウェアのユーザインターフェイスにハードコードされている言語、基準ドキュメントに基づいて使用されている言語、または参照されているサードパーティ製品で使用されている言語によりドキュメントに例外が存在する場合があります。



目次

Full Cisco Trademarks with Software License iii

通信、サービス、およびその他の情報 iv

Cisco バグ検索ツール iv

マニュアルに関するフィードバック iv

偏向のない言語 v

第 1 章

レイヤ 2 ネットワークアドレス変換 1

レイヤ 2 ネットワークアドレス変換 1

注意事項と制約事項 5

NAT の性能と拡張性 6

レイヤ 2 NAT の設定 7

ポートチャネルでのレイヤ 2 NAT サポートの設定 8

設定の確認 10

基本的な内部から外部への通信：例 11

基本的な内部から外部への通信：設定 12

重複する IP アドレスの例 14

重複する IP アドレスの設定：スイッチ A 15

重複する IP アドレスの設定：スイッチ B 17

第 2 章

レイヤ 3 ネットワークアドレス変換 19

ネットワーク アドレス変換 19

機能情報の確認	20
NAT を設定する利点	20
NAT の機能	21
NAT の用途	22
NAT の内部アドレスおよび外部アドレス	22
VRF 対応ネットワークアドレス変換	23
ルートマップベースのネットワークアドレス変換	24
ルートマップベースのネットワークアドレス変換の制限事項	25
NAT のタイプ	25
NAT による外部ネットワークへのパケットのルーティング（内部送信元アドレス変換）	26
外部送信元アドレス変換	27
ポートアドレス変換	27
重複ネットワーク	29
ネットワークアドレス変換の制限事項	30
NAT の性能とスケール数	32
アドレスのみの変換	32
アドレスのみの変換の制限事項	33
NAT の設定	33
内部送信元アドレスの静的変換の設定	33
内部送信元アドレスの動的変換の設定	35
PAT の設定	37
外部 IP アドレスのみの NAT の設定	39
重複するネットワークの変換の設定	41
アドレス変換タイムアウトの設定	43
レイヤ 3 ポートチャネルでのネットワークアドレス変換の設定	46
NAT でのアプリケーション レベル ゲートウェイの使用	47
NAT の設定のベスト プラクティス	48
ネットワークアドレス変換の設定例	48
内部送信元アドレスの静的変換の設定	48
内部送信元アドレスの動的変換の設定	49
NAT のトラブルシューティング	49

ネットワークアドレス変換の機能履歴 50

第 3 章

VLAN マッピング 51

VLAN マッピング 51

選択的 QnQ 53

トランクポートでの QnQ 53

VLAN マッピング設定時の注意事項 53

選択的 QnQ の設定ガイドライン 54

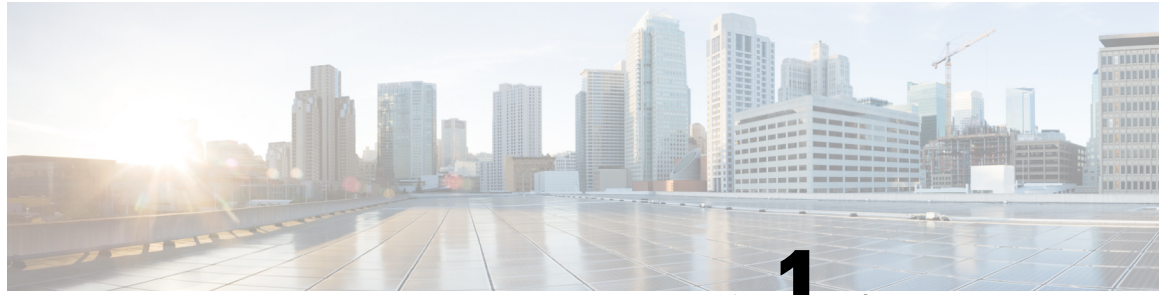
トランクポートでの QnQ の設定ガイドライン 54

VLAN マッピングの設定 54

トランクポートでの選択的 QnQ の設定 54

トランクポートでの QnQ の設定 57

VLAN マッピングの機能履歴 59



第 1 章

レイヤ 2 ネットワークアドレス変換

- [レイヤ 2 ネットワークアドレス変換 \(1 ページ\)](#)
- [注意事項と制約事項 \(5 ページ\)](#)
- [NAT の性能と拡張性 \(6 ページ\)](#)
- [レイヤ 2 NAT の設定 \(7 ページ\)](#)
- [ポートチャネルでのレイヤ 2 NAT サポートの設定 \(8 ページ\)](#)
- [設定の確認 \(10 ページ\)](#)
- [基本的な内部から外部への通信：例 \(11 ページ\)](#)
- [重複する IP アドレスの例 \(14 ページ\)](#)

レイヤ 2 ネットワークアドレス変換

1 対 1 レイヤ 2 NAT (ネットワークアドレス変換) は、固有のパブリック IP アドレスを既存のプライベート IP アドレス (エンドデバイス) に割り当てるサービスです。この割り当てにより、エンドデバイスがプライベートサブネットおよびパブリックサブネット上で通信できます。このサービスは、NAT 対応デバイスで設定され、エンドデバイスに物理的にプログラムされた IP アドレスのパブリックでの「エイリアス」です。これは、通常 NAT デバイスでテーブルとして表されます。

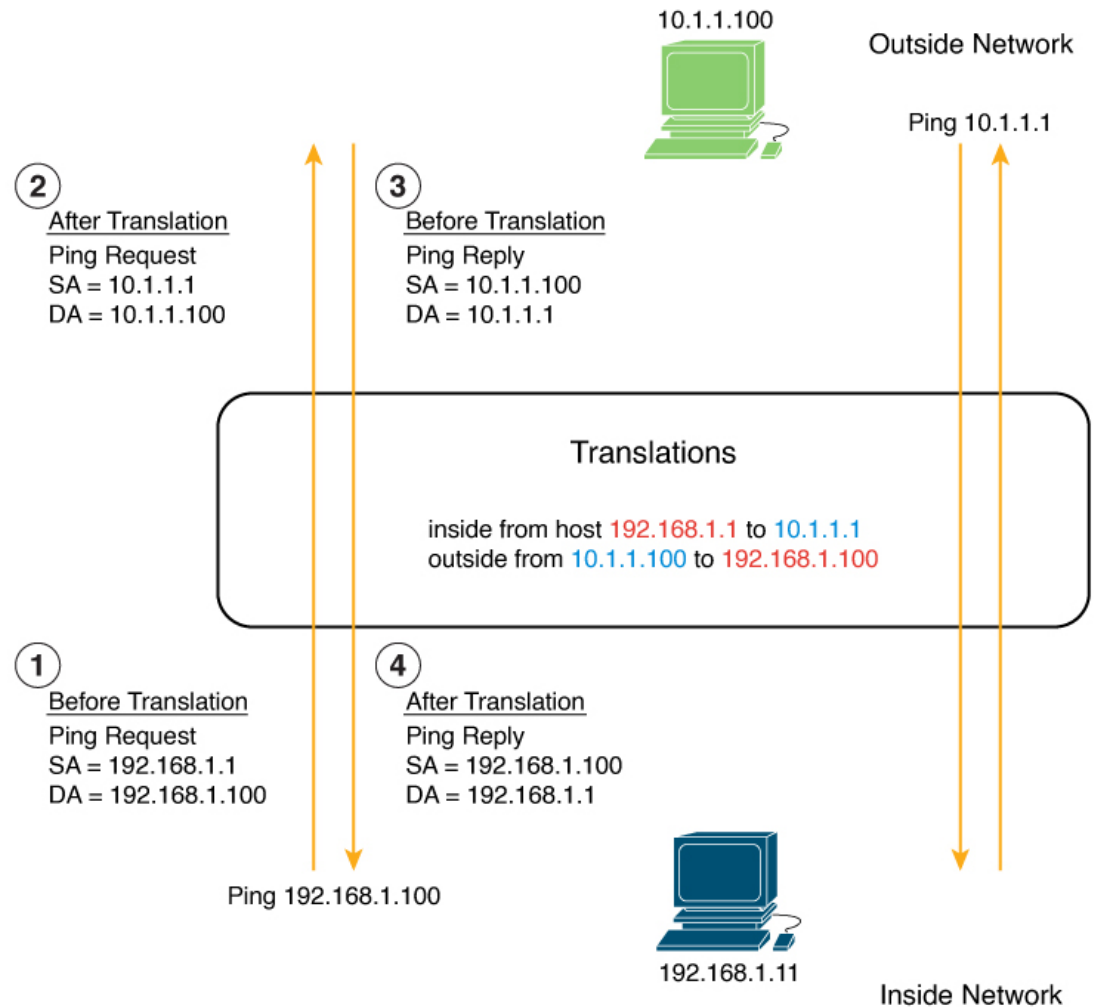
レイヤ 2 NAT はテーブルを使用して、IPv4 アドレスをパブリックからプライベートおよびプライベートからパブリックの両方にラインレートで変換します。レイヤ 2 NAT は、一貫した高レベルの (bump-in-the-wire) ワイヤスピードの性能を提供するハードウェアベースの機能です。またこの機能は、拡張されたネットワーク セグメンテーション用の NAT 境界で複数の VLAN をサポートします。

次に、レイヤ 2 NAT で 192.168.1.x ネットワークのセンサーと 10.1.1.x ネットワークの通信制御装置間のアドレスを変換する例を示します。

1. 192.168.1.x ネットワークは内側/内部 IP アドレス空間、10.1.1.x ネットワークは外側または外部 IP アドレス空間です。
2. 192.168.1.1 のセンサーが、「内部」アドレス 192.168.1.100 を使用して通信制御装置に ping 要求を送信します。

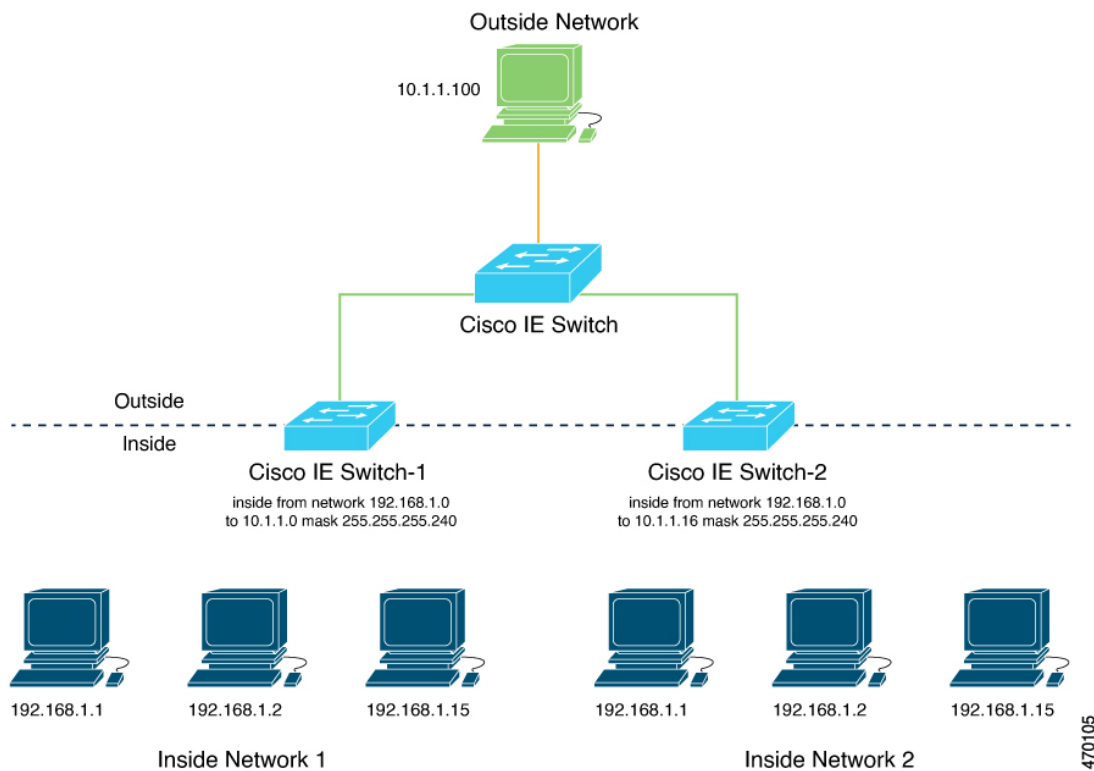
3. パケットが内部ネットワークから送信される前に、レイヤ2 NATは送信元アドレス (SA) を 10.1.1.1 へ、宛先アドレス (DA) を 10.1.1.100 へと変換します。
4. 通信制御装置は 10.1.1.1 へ ping 応答を送信します。
5. パケットが内部ネットワークで受信されると、レイヤ2 NATは送信元アドレスを 192.168.1.100 へ、宛先アドレスを 192.168.1.1 へ変換します。

図 1: ネットワーク間のアドレス変換



多数のノードに対して、サブネット内のすべてのデバイスの変換をまとめて有効にできます。この場合、内部ネットワーク 1 からのアドレスは 10.1.1.0/28 サブネット外部アドレスに変換することができ、内部ネットワーク 2 からのアドレスは 10.1.1.16/28 サブネット外部アドレスに変換することができます。各サブネットのアドレスはすべて 1 つのコマンドを使って変換できます。サブネットベースの変換を使用すると、レイヤ L2 NAT 規則を節約できます。スイッチには、レイヤ 2 NAT 規則の数に制限があります。サブネットを含む規則では、1 つの規則で複数のエンドデバイスを変換できます。

図 2: 内部-外部アドレス変換



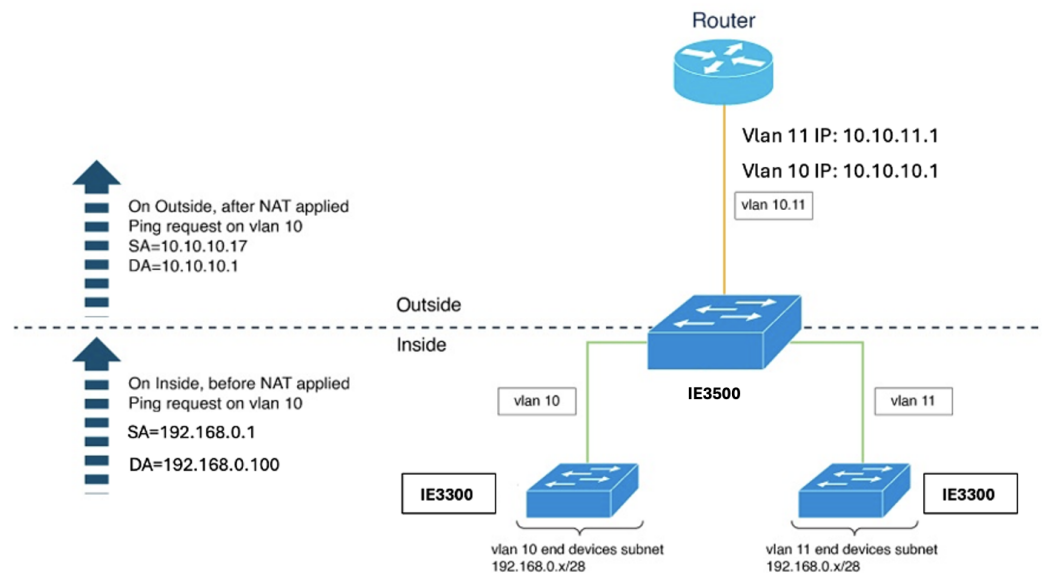
次の図は、レイヤ2 MACアドレスに基づいてイーサネットパケットを転送するアグリゲーションレイヤのスイッチを示しています。この例では、ルータはすべてのサブネットと VLAN のレイヤ 3 ゲートウェイです。

L2NAT インスタンス定義では、**network** コマンドを使用して、同じサブネット内の複数のデバイスの変換行を定義します。この場合、IP アドレスの最後のバイトが 16 で始まり 31 で終わる /28 サブネットです。VLAN のゲートウェイは、IP アドレスの最後のバイトが .1 で終わるルータです。外部ホスト変換は、ルータに提供されます。レイヤ 2 NAT 定義の **network** コマンドは、1 つのコマンドでサブネットに相当するホストを変換し、レイヤ 2 NAT 変換レコードを節約します。

Gi1/1 アップリンク インターフェイスには、VLAN 10 および VLAN 11 サブネット用のレイヤ 2 NAT 変換インスタンスがあります。インターフェイスは、複数のレイヤ 2 NAT インスタンス定義をサポートできます。

下流のスイッチは、レイヤ 2 NAT を実行せず上流のアグリゲーションレイヤスイッチのレイヤ 2 NAT に依存するアクセスレイヤスイッチの例です。

図 3: スイッチの NAT



次の例は、上の図の NAT 設定を示しています。

```

!
l2nat instance Subnet10-NAT
 instance-id 1
 permit all
 fixup all
 outside from host 10.10.10.1 to 192.168.0.100
 inside from network 192.168.0.0 to 10.10.10.16 mask 255.255.255.240
!
l2nat instance Subnet11-NAT
 instance-id 1
 permit all
 fixup all
 outside from host 10.10.11.1 to 192.168.0.100
 inside from network 192.168.0.0 to 10.10.11.16 mask 255.255.255.240
!
interface GigabitEthernet1/1
 switchport mode trunk
 l2nat Subnet10-NAT 10
 l2nat Subnet11-NAT 11
!
Interface vlan 1
 ip address 10.10.1.2

```

注意事項と制約事項

次のリストに、スイッチでレイヤ2 NAT を使用する場合のガイドラインと制限事項を示します。



(注) 規模の詳細については、このガイドの「[NAT の性能と拡張性 \(6 ページ\)](#)」セクションを参照してください。

- レイヤ2 NAT は、スタンドアロンスイッチでサポートされます。
- レイヤ2 NAT はデフォルトでは無効です。設定すると有効になります。このガイドの [レイヤ2 NAT の設定 \(7 ページ\)](#) を参照してください。
- レイヤ2 NAT はユニキャストトラフィックにのみ適用されます。変換されないユニキャストトラフィック、マルチキャストトラフィック、およびIGMPトラフィックは許可されます。
- レイヤ2 NAT は、アップリンクポートでのみサポートされ、Network Essentials ライセンスと Network Advantage ライセンスの両方で使用できます。
- レイヤ2 NAT は、外部 IP アドレスと内部 IP アドレス間の1対1のマッピングをサポートしています。
- レイヤ2 NAT は、アクセスモードまたはトランクモードのアップリンク インターフェイスに適用できます。
- レイヤ2 トラフィックの IPv4 アドレスのみを変換できます。
- 内部ネットワーク変換でサポートされるサブネットマスクは、/24、/25、/26、/27、/28、および/32のみです。
- 外部変換規則は、ホスト変換のみをサポートします。
- ARP はレイヤ2 NAT で透過的に機能しません。ただし、スイッチは、IP パケットのペイロードに埋め込まれている IP アドレスを、プロトコルが機能するように変更します。埋め込まれた IP アドレスは変換されません。
- デバッグの統計情報には、各変換のエントリ、各インスタンスおよび各インターフェイスの変換済み入力と出力の合計が含まれます。また、ARP フィックスアップ統計情報と、ハードウェアに割り当てられた変換エントリの数も含まれます。
- レイヤ2 NAT は、1対多および多対1の IP アドレスのマッピングをサポートしていません。
- パブリックからプライベートへの変換は1対1であるため、レイヤ2 NAT ではパブリック IP アドレスを節約できません。1:N NAT ではありません。

- レイヤ2 NATのホストの変換を設定する場合は、DHCPクライアントとして設定しないでください。
- レイヤ2 NATを使用して内部アドレスを外部アドレスに変換する場合は、変換されたIPアドレスがグローバルネットワークでアクセスできないことを確認します。
- 管理インターフェイスはレイヤ2 NAT機能の背後にあります。そのためこのインターフェイスはプライベートネットワーク VLAN上に置かないようにしてください。プライベートネットワーク VLAN上に存在する場合は、内部アドレスを割り当て、内部の変換を設定します。
- レイヤ2 NATは外部アドレスと内部アドレスを分けるように設計されているため、同じサブネットのアドレスを外部アドレスと内部アドレスの両方に設定しないでください。
- レイヤ2 NATはレイヤ2トラフィック専用です。ルーティング中のパケットには使用しないでください。
- レイヤ2 NATは、CPU宛てのパケットとCPUから送信されるパケットを変換しません。管理トラフィックは、プライベートネットワーク VLANとは異なる VLAN上にある必要があります。
- レイヤ2 NATカウンタはポートに基づいていません。同じレイヤ2 NATインスタンスが複数のインターフェイスに適用されると、対応するレイヤ2 NATカウンタがそれらすべてのインターフェイスに表示されます。

NATの性能と拡張性

レイヤ2 NAT変換および転送は、ハードウェアでラインレートで実行されます。サポートされるレイヤ2 NAT規則の数は、ハードウェアでサポートできるハードウェアエントリの数によって異なります。

拡張性は、内部/外部の組み合わせの数によって異なります。次に、拡張性の例を示します。

- 内部規則のみを持つインスタンスには、合計128個の変換規則を設定できます。
- 1つの内部規則を持つ複数のインスタンスでは、合計128個のインスタンスを128個の異なるVLANに適用できます。
- 1つの内部規則と1つの外部規則を持つ複数のインスタンスには、最大64個のインスタンスを含めることができます。
- 1つの外部規則を持つ1つのインスタンスには、最大100個の内部規則を設定できます。サポートできる内部規則の数は、外部規則の数が増えると減少します。



(注) 規則の数を節約するために、ネットワーク変換規則を使用することをお勧めします。

レイヤ2 NAT の設定

アドレス変換を指定するレイヤ2 NAT インスタンスを設定する必要があります。レイヤ2 NAT インスタンスを物理イーサネットインターフェイスに接続し、インスタンスを適用する VLAN を設定します。レイヤ2 NAT インスタンスは、管理インターフェイス (CLI/SNMP) から設定できます。送受信されたパケットに関する詳細な統計情報を確認できます。このガイドの [設定の確認 \(10 ページ\)](#) セクションを参照してください。

レイヤ2 NAT を設定するには、次の手順を実行します。詳細については、このガイドで「[基本的な内部から外部への通信：例 \(11 ページ\)](#)」と「[重複する IP アドレスの例 \(14 ページ\)](#)」の例を参照してください。

手順

ステップ 1 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。

configure terminal

ステップ 2 新しいレイヤ2 NAT インスタンスを作成します。

l2nat instance *instance_name* インスタンスを作成した後、そのインスタンスのサブモードを開始する場合もこのコマンドを使用します。

ステップ 3 内部アドレスを外部アドレスへ変換します。

inside from [host | range | network] original ip to translated ip [mask] number | mask

単一のホストアドレス、ホストアドレスの範囲、またはサブネット内のすべてのアドレスを変換できます。発信トラフィックの送信元アドレスと着信トラフィックの宛先アドレスを変換します。

ステップ 4 外部アドレスを内部アドレスへ変換します。

outside from [host | range | network] original ip to translated ip [mask] number | mask

単一のホストアドレス、ホストアドレスの範囲、またはサブネット内のアドレスを変換できます。発信トラフィックの宛先アドレスと着信トラフィックの送信元アドレスを変換します。

ステップ 5 config-l2nat モードを終了します。

exit

ステップ 6 指定したインターフェイス (IE 3400 のアップリンクポートのみ) のインターフェイス コンフィギュレーションモードにアクセスします。

interface *interface-id*

ステップ 7 VLAN または VLAN 範囲に指定されたレイヤ2 NAT のインスタンスを適用します。このパラメータが欠落している場合、レイヤ2 NAT インスタンスはネイティブ VLAN に適用されます。

l2nat *instance_name* [vlan | vlan_range]

ステップ8 インターフェイス コンフィギュレーション モードを終了します。

end

ポートチャネルでのレイヤ2 NAT サポートの設定



(注) レイヤ2 NATは、ポートチャネルの論理インターフェイスではサポートされますが、メンバーインターフェイスではサポートされません。

LACPはIEEE 802.3adで定義されており、シスコデバイスがIEEE 802.3adプロトコルに適合したデバイス間のポートチャネルを管理できるようにします。LACPを使用すると、イーサネットポート間でLACPパケットを交換することにより、ポートチャネルを自動的に作成できます。

スイッチまたはスイッチスタックはLACPを使用することによって、LACPをサポートできるパートナーの識別情報、および各ポートの機能を学習します。次に、設定が類似しているポートを単一の論理リンク（チャネルまたは集約ポート）に動的にグループ化します。設定が類似しているポートをグループ化する場合の基準は、ハードウェア、管理、およびポートパラメータ制約です。たとえば、LACPは速度、デュプレックスモード、ネイティブVLAN、VLAN範囲、トランキングステータス、およびトランキングタイプが同じポートをグループとしてまとめます。リンクをまとめてポートチャネルを形成した後で、LACPは単一デバイスポートとして、スパンニングツリーにそのグループを追加します。

LACPモードでは、ポートがLACPパケットを送信できるか、LACPパケットの受信のみができるかどうかを指定します。

アクティブモード：ポートをアクティブネゴシエーションステートにします。この場合、ポートはLACPパケットを送信することによって、相手ポートとのネゴシエーションを開始します。

パッシブモード：ポートをパッシブネゴシエーションステートにします。この場合、ポートは受信するLACPパケットに応答しますが、LACPパケットネゴシエーションを開始することはありません。これにより、LACPパケットの送信を最小限に抑えます。

アクティブおよびパッシブLACPモードはともに、相手ポートとネゴシエーションして、ポート速度などの条件に基づいて（レイヤ2 EtherChannelの場合は、トランク状態およびVLAN番号などの基準に基づいて）、ポートでポートチャネルを形成できるようにします。

ポートチャネルで許可されるバンドル化されたLACPポートの最大数を指定すると、ポートチャネル内の残りのポートがホットスタンバイポートとして指定されます。ポートチャネルのLACPポートの最大数を設定するには、特権EXECモードで開始して、次の手順に従います。この手順は任意です。

手順

ステップ1 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。

device configure

ステップ2 A-LC という新しいレイヤ2 NAT インスタンスを作成します。

device # l2nat instance A-LC

ステップ3 A1 の内部アドレスを外部アドレスへ変換します。

Device(config-l2nat)# inside from host 192.168.1.1 to 10.1.1.1

ステップ4 A2 の内部アドレスを外部アドレスへ変換します。

Device(config-l2nat)# inside from host 192.168.1.2 to 10.1.1.2

ステップ5 A3 の内部アドレスを外部アドレスへ変換します。

Device(config-l2nat)# inside from host 192.168.1.3 to 10.1.1.3

ステップ6 LC の外部アドレスを内部アドレスへ変換します。

Device(config-l2nat)# outside from host 10.1.1.200 to 192.168.1.250

ステップ7 config-l2nat モードを終了します。

Device(config-l2nat)# exit

ステップ8 ポートチャネルのインターフェイス設定モードにアクセスします。

Device(config)# interface port-channel

ステップ9 このインターフェイスのネイティブ VLAN に、先ほどのレイヤ2 NAT インスタンスを適用します。

Device(config-if)#l2nat A-LC

(注)

トランク上のタグ付き通信の場合は、インターフェイスへインスタンスを適用するときに、次のように VLAN 番号を追加します。l2nat instance vlan

ステップ10 特権 EXEC モードに戻ります。

Device# end

設定の確認

手順

レイヤ2 NAT 設定を確認するには、次のコマンドを実行します。

コマンド	目的
<code>show l2nat instance</code>	指定されたレイヤ2 NAT インスタンスの設定の詳細を表示します。
<code>show l2nat interface</code>	1つまたは複数のインターフェイスでのレイヤ2 NAT インスタンスの設定の詳細を表示します。
<code>show l2nat statistics</code>	すべてのインターフェイスのレイヤ2 NAT 統計情報を表示します。
<code>show l2nat statistics interface</code>	指定したインターフェイスのレイヤ2 NAT 統計情報を表示します。
<code>debug l2nat</code>	設定が適用されたときにリアルタイムでのレイヤ2 NAT 設定の詳細の表示を有効にします。
<code>show platform hardware fed switch 1 fwd-asic resource tcam table pbr record 0 format 0 -</code>	ハードウェアエントリを表示します。
<code>-show platform hardware fed switch active fwd-asic resource tcam utilization in PBR</code>	ハードウェアリソース使用率を表示します。

次に、`show l2nat instance` および `show l2nat statistics` コマンドの出力例を示します。

```
switch#show l2nat instance
l2nat instance test
fixup : all
outside from host    10.10.10.200 to 192.168.1.200
inside  from host    192.168.1.1 to 10.10.10.1
l2nat instance test2
fixup : all
inside  from host    1.1.1.1 to 2.2.2.2
outside from host    2.2.2.200 to 1.1.1.200

Switch#show l2nat interface
FOLLOWING INSTANCE(S) AND VLAN(S) ATTACHED TO ALL INTERFACES
=====
l2nat Gi1/1 test
=====

Switch#show l2nat statistics
```

```
STATS FOR INSTANCE: test (IN PACKETS)

TRANSLATED STATS (IN PACKETS)
=====
INTERFACE DIRECTION VLAN   TRANSLATED
Gi1/1     EGRESS    50    0
Gi1/1     INGRESS   50    0
-----

PROTOCOL FIXUP STATS (IN PACKETS)
=====
INTERFACE DIRECTION VLAN   ARP
Gi1/1     REPLY    50    0
Gi1/1     REQUEST  50    0
-----

PER TRANSLATION STATS (IN PACKETS)
=====
TYPE      DIRECTION SA/DA ORIGINAL IP    TRANSLATED IP  COUNT
OUTSIDE  INGRESS  SA   10.10.10.200  192.168.1.200  0
OUTSIDE  EGRESS  DA   192.168.1.200  10.10.10.200  0
INSIDE   EGRESS  SA   192.168.1.1   10.10.10.1    0
INSIDE   INGRESS DA   10.10.10.1    192.168.1.1   0
-----
=====

TOTAL TRANSLATIONS ENTRIES IN HARDWARE: 4
TOTAL INSTANCES ATTACHED : 1
=====

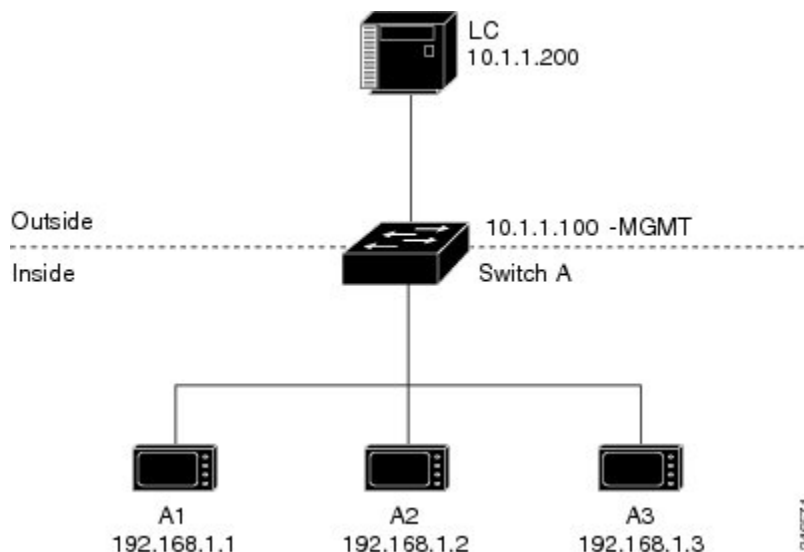
GLOBAL NAT STATISTICS
=====
Total Number of TRANSLATED NAT Packets = 0
Total Number of ARP      FIX UP Packets = 0
=====

ad
```

基本的な内部から外部への通信：例

この例では、A1はアップリンクポートに直接接続されたロジックコントローラ（LC）と通信する必要があります。レイヤ2 NAT インスタンスは、外部ネットワーク（10.1.1.1）上でのA1のアドレスと内部ネットワーク（192.168.1.250）上でのLCのアドレスを提供するように設定されています。

図 4: 基本的な内部から外部への通信



ここで次の通信が発生します。

1. A1 が「SA: 192.168.1.1DA: 192.168.1.250」という ARP 要求を送信します。
2. Cisco スイッチ A は「SA:10.1.1.1DA: 10.1.1.200」という ARP 要求をフィックスアップします。
3. LC は要求を受信し、10.1.1.1 の MAC アドレスを学習します。
4. LC が「SA: 10.1.1.200DA: 10.1.1.1」という応答を送信します。
5. Cisco スイッチ A は「SA: 192.168.1.250DA: 192.168.1.1」という ARP 応答をフィックスアップします。
6. A1 は 192.168.1.250 の MAC アドレスを学習し、通信を開始します。



- (注)
- スイッチの管理インターフェイスは内部ネットワーク 192.168.1.x. とは別の VLAN に属している必要があります。
 - このセクションの例を設定するタスクについては、「[基本的な内部から外部への通信：設定 \(12 ページ\)](#)」セクションを参照してください。

基本的な内部から外部への通信：設定

このセクションでは、前のセクションで説明した内部から外部への通信を設定する手順について説明します。レイヤ2 NAT インスタンスを作成し、変換エントリを2つ追加して、このインスタンスをインターフェイスに適用します。ARP フィックスアップはデフォルトで有効です。

始める前に

「[基本的な内部から外部への通信：例（11 ページ）](#)」セクションの内容を読んで理解してください。

手順

-
- ステップ 1** コンフィギュレーション モードを入力します。
- 例：
- ```
switch# configure
```
- ステップ 2** A-LC という新しいレイヤ 2 NAT インスタンスを作成します。
- 例：
- ```
switch(config)# l2nat instance A-LC
```
- ステップ 3** A1 の内部アドレスを外部アドレスへ変換します。
- 例：
- ```
switch(config-l2nat)# inside from host 192.168.1.1 to 10.1.1.1
```
- ステップ 4** A2 の内部アドレスを外部アドレスへ変換します。
- 例：
- ```
switch(config-l2nat)# inside from host 192.168.1.2 to 10.1.1.2
```
- ステップ 5** A3 の内部アドレスを外部アドレスへ変換します。
- 例：
- ```
switch(config-l2nat)# inside from host 192.168.1.3 to 10.1.1.3
```
- ステップ 6** LC 外部アドレスを内部アドレスへ変換します。
- 例：
- ```
switch(config-l2nat)# outside from host 10.1.1.200 to 192.168.1.250
```
- ステップ 7** config-l2nat モードを終了します。
- 例：
- ```
switch(config-l2nat)# exit
```
- ステップ 8** アップリンクポートのインターフェイス コンフィギュレーション モードにアクセスします。
- 例：
- ```
witch(config)# interface Gi1/1
```
- ステップ 9** このインターフェイスのネイティブ VLAN に、先ほどのレイヤ 2 NAT インスタンスを適用します。
- 例：
- ```
switch(config-if)# l2nat A-LC
```

(注)

トランク上のタグ付きトラフィックの場合は、インターフェイスヘインスタンスを適用するときに、次のように VLAN 番号を追加します。

```
l2nat instance vlan
```

ステップ 10 特権 EXEC モードに戻ります。

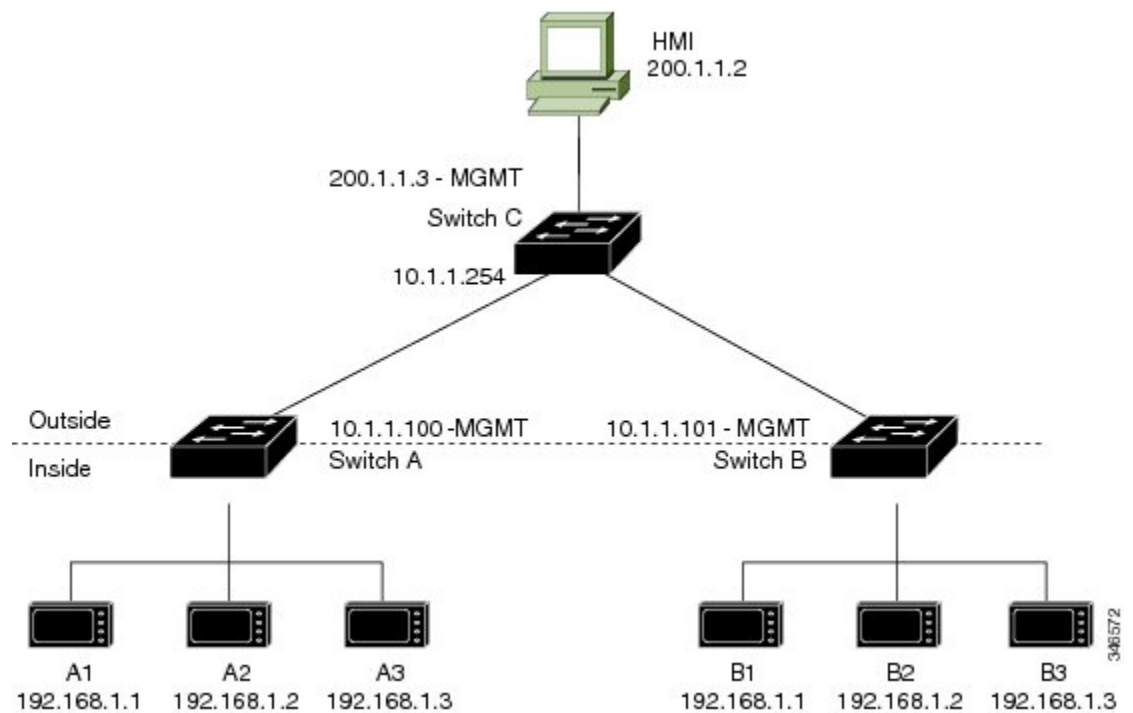
例：

```
switch# end
```

## 重複する IP アドレスの例

ここでは、2台のマシンノードで 192.168.1.x 領域のアドレスが事前設定されています。レイヤ 2 NAT により、これらのアドレスが外部ネットワークの別のサブネット上で一意のアドレスに変換されます。また、マシン間の通信では、ノード A のマシンはノード B の領域で一意のアドレスを必要とし、ノード B のマシンはノード A の領域で一意のアドレスが必要です。

図 5: IP アドレスの重複



- スイッチ C は 192.168.1.x 領域でのアドレスが必要です。パケットがノード A またはノード B で受信されると、スイッチ C の 10.1.1.254 というアドレスが 192.168.1.254 に変換されます。パケットがノード A またはノード B から送信されると、スイッチ C の 192.168.1.254 というアドレスは 10.1.1.254 に変換されます。

- ノード A とノード B のマシンは 10.1.1.x 領域で一意的なアドレスが必要です。設定の容易さと使いやすさを実現するために、10.1.1.x 領域は 10.1.1.0、10.1.1.16、10.1.1.32 などのサブネットに分割されます。各サブネットは異なるノードに使用できます。この例では、10.1.1.16 はノード A に使用され、10.1.1.32 はノード B に使用されます。
- ノード A とノード B のマシンはデータを交換するための一意的なアドレスが必要です。使用可能なアドレスはサブネットに分割されます。便宜上、ノード A のマシンの 10.1.1.16 サブネットアドレスは、ノード B の 192.168.1.16 サブネットアドレスに変換され、ノード B のマシンの 10.1.1.32 サブネットアドレスはノード A の 192.168.1.32 アドレスに変換されます。
- マシンは各ネットワークで一意的なアドレスを持ちます。

表 1: IP アドレスの変換

| ノード                      | ノード A のアドレス   | 外部ネットワークのアドレス | ノード B のアドレス   |
|--------------------------|---------------|---------------|---------------|
| スイッチ A のネットワークアドレス       | 192.168.1.0   | 10.1.1.16     | 192.168.1.16  |
| A1                       | 192.168.1.1   | 10.1.1.17     | 192.168.1.17  |
| A2                       | 192.168.1.2   | 10.1.1.18     | 192.168.1.18  |
| A3                       | 192.168.1.3   | 10.1.1.19     | 192.168.1.19  |
| Cisco スイッチ B のネットワークアドレス | 192.168.1.32  | 10.1.1.32     | 192.168.1.0   |
| B1                       | 192.168.1.33  | 10.1.1.33     | 192.168.1.1   |
| B2                       | 192.168.1.34  | 10.1.1.34     | 192.168.1.2   |
| B3                       | 192.168.1.35  | 10.1.1.35     | 192.168.1.3   |
| スイッチ C                   | 192.168.1.254 | 10.1.1.254    | 192.168.1.254 |

## 重複する IP アドレスの設定 : スイッチ A

このセクションでは、内部ネットワーク内の1つのマシンノードの重複IPアドレスを外部ネットワークのサブネット上の一意的なアドレスに変換するようにレイヤ2 NAT を設定する手順について説明します。この手順は、「[重複する IP アドレスの例 \(14 ページ\)](#)」セクションのスイッチ A を対象としています。

### 始める前に

「[重複する IP アドレスの例 \(14 ページ\)](#)」セクションの内容を読んで理解してください。

## 手順

ステップ1 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。

例 :

```
switch# configure
```

ステップ2 A-Subnet という新しいレイヤ 2 NAT インスタンスを作成します。

例 :

```
switch(config)# l2nat instance A-Subnet
```

ステップ3 ノード A マシンの内部アドレスを 10.1.1.16 255.255.255.240 サブネットのアドレスへ変換します。

例 :

```
switch(config-l2nat)# inside from network 192.168.1.0 to 10.1.1.16 mask 255.255.255.240
```

ステップ4 スイッチ C の外部アドレスを内部アドレスへ変換します。

例 :

```
switch(config-l2nat)# outside from host 10.1.1.254 to 192.168.1.254
```

ステップ5 ノード B マシンの外部アドレスを内部アドレスへ変換します。

例 :

```
switch(config-l2nat)# outside from host 10.1.1.32 to 192.168.1.32
outside from host 10.1.1.33 to 192.168.1.33
outside from host 10.1.1.34 to 192.168.1.34
outside from host 10.1.1.35 to 192.168.1.35
```

ステップ6 config-l2nat モードを終了します。

例 :

```
switch(config-l2nat)# exit
```

ステップ7 アップリンクポートのインターフェイス コンフィギュレーション モードにアクセスします。

例 :

```
switch(config)# interface Gi1/1
```

ステップ8 このインターフェイスのネイティブ VLAN に、先ほどのレイヤ 2 NAT インスタンスを適用します。

例 :

```
switch(config-if)# l2nat A-Subnet
```

(注)

トランク上のタグ付きトラフィックの場合は、インターフェイスへインスタンスを適用するときに、次のように VLAN 番号を追加します。

```
l2nat instance vlan
```

ステップ9 特権 EXEC モードに戻ります。

例 :

```
switch# end
```

---

#### 次のタスク

「[重複する IP アドレスの例 \(14 ページ\)](#)」セクションのスイッチ B の重複 IP アドレスを変換するようにレイヤ 2 NAT を設定します。[重複する IP アドレスの設定 : スイッチ B \(17 ページ\)](#) を参照してください。

## 重複する IP アドレスの設定 : スイッチ B

このセクションでは、内部ネットワーク内の1つのマシンノードの重複 IP アドレスを外部ネットワークのサブネット上の一意のアドレスに変換するようにレイヤ 2 NAT を設定する手順について説明します。この手順は、「[重複する IP アドレスの例 \(14 ページ\)](#)」セクションのスイッチ B を対象としています。

#### 始める前に

「[重複する IP アドレスの例 \(14 ページ\)](#)」セクションの内容を読んで理解してください。

#### 手順

---

ステップ1 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。

例 :

```
switch# configure
```

ステップ2 B-Subnet という新しいレイヤ 2 NAT インスタンスを作成します。

例 :

```
switch(config)# l2nat instance B-Subnet
```

ステップ3 ノード B マシンの内部アドレスを 10.1.1.32 255.255.255.240 サブネットのアドレスへ変換します。

例 :

```
switch(config-l2nat)# inside from network 192.168.1.0 to 10.1.1.32 255.255.255.240
```

ステップ4 スイッチ C の外部アドレスを内部アドレスへ変換します。

例 :

```
switch(config-l2nat)# outside from host 10.1.1.254 to
```

ステップ5 ノード A マシンの外部アドレスを内部アドレスへ変換します。

例 :

```
switch(config-l2nat)# outside from host 10.1.1.16 to 192.168.1.16
outside from host 10.1.1.17 to 192.168.1.17
outside from host 10.1.1.18 to 192.168.1.18
outside from host 10.1.1.19 to 192.168.1.19
```

**ステップ 6** config-l2nat モードを終了します。

例 :

```
switch(config-l2nat)# exit
```

**ステップ 7** アップリンクポートのインターフェイス コンフィギュレーションモードにアクセスします。

例 :

```
switch(config)# interface Gi1/1
```

**ステップ 8** このインターフェイスのネイティブ VLAN に、先ほどのレイヤ 2 NAT インスタンスを適用します。

例 :

```
switch(config-if)# l2nat name1
```

(注)

トランク上のタグ付きトラフィックの場合は、インターフェイスへインスタンスを適用するときに、次のように VLAN 番号を追加します。

```
l2nat instance vlan
```

**ステップ 9** 指定されたレイヤ 2 NAT インスタンスの設定の詳細を表示します。

例 :

```
switch# show l2nat instance name1
```

**ステップ 10** レイヤ 2 NAT の統計情報を表示します。

例 :

```
switch# show l2nat statistics
```

**ステップ 11** 特権 EXEC モードに戻ります。

例 :

```
switch# end
```

---



## 第 2 章

# レイヤ 3 ネットワークアドレス変換

- ネットワーク アドレス変換 (19 ページ)
- NAT を設定する利点 (20 ページ)
- NAT の機能 (21 ページ)
- NAT の用途 (22 ページ)
- NAT の内部アドレスおよび外部アドレス (22 ページ)
- VRF 対応ネットワークアドレス変換 (23 ページ)
- ルートマップベースのネットワークアドレス変換 (24 ページ)
- ルートマップベースのネットワークアドレス変換の制限事項 (25 ページ)
- NAT のタイプ (25 ページ)
- NAT による外部ネットワークへのパケットのルーティング (内部送信元アドレス変換) (26 ページ)
- 外部送信元アドレス変換 (27 ページ)
- ポートアドレス変換 (27 ページ)
- 重複ネットワーク (29 ページ)
- ネットワークアドレス変換の制限事項 (30 ページ)
- NAT の性能とスケール数 (32 ページ)
- アドレスのみの変換 (32 ページ)
- NAT の設定 (33 ページ)
- レイヤ 3 ポートチャネルでのネットワークアドレス変換の設定 (46 ページ)
- NAT でのアプリケーション レベル ゲートウェイの使用 (47 ページ)
- NAT の設定のベストプラクティス (48 ページ)
- ネットワークアドレス変換の設定例 (48 ページ)
- NAT のトラブルシューティング (49 ページ)
- ネットワークアドレス変換の機能履歴 (50 ページ)

## ネットワーク アドレス変換

ネットワーク アドレス変換 (NAT) は、IP アドレスの節約を目的として設計されています。NAT によって、未登録 IP アドレスを使用するプライベート IP ネットワークをインターネット

に接続できます。NATはデバイス（通常、2つのネットワークを接続するもの）上で動作し、内部ネットワークのプライベート（グローバルに一意ではない）アドレスをグローバルにルーティング可能なアドレスに変換します。これは、パケットが別のネットワークに転送される前に行われます。

NATは、ネットワーク全体に対して1つのアドレスだけを外部にアドバタイズするように設定できます。この機能により、そのアドレスの後ろにある内部ネットワーク全体を効果的に隠すことができ、セキュリティが強化されます。NATには、セキュリティおよびアドレス節約の二重の機能性があり、一般的にリモートアクセス環境で実装されます。

NATは、エンタープライズエッジでも使用され、内部ユーザーのインターネットへのアクセスを許可し、メールサーバーなど内部デバイスへのインターネットアクセスを許可します。

## 機能情報の確認

ご使用のソフトウェアリリースでは、このドキュメントで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、「[Bug Search Tool](#)」および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。機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、この章の最後にある機能情報の表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シスコ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にアクセスするには、<https://cfng.cisco.com/>に進みます。Cisco.comのアカウントは必要ありません。

## NATを設定する利点

NATを設定すると、次の利点があります。

- NATはIPが枯渇する問題を解決します。

組織がNATを使用すると、既存のネットワークを持っていてインターネットにアクセスする必要がある場合に、IPアドレスが枯渇する問題を解決できます。ネットワークインフォメーションセンター（NIC）登録IPアドレスをまだ所有していないサイトは、IPアドレスを取得する必要があります。このような場合、254を超えるクライアントが存在するか、または計画されている場合、クラスBアドレスの不足が深刻な問題になります。NATはこのような問題に対応するために、隠された数千の内部アドレスを、取得の容易なClass Cアドレスの範囲にマップします。

- NATはクライアントIPアドレスを外部ネットワークから隠すことで、セキュリティレイヤも提供します。

内部ネットワークのクライアントのIPアドレスをすでに登録しているサイトでも、ハッカーがクライアントを直接攻撃できないように、これらのアドレスをインターネットから隠すことができます。クライアントアドレスを隠すことにより、セキュリティがさらに強化されます。NATによりLAN管理者は、インターネット割り当て番号局の予備プールを利用して、Class Aアドレスを自由に拡張することができます。Class Aアドレスの拡張は

組織内で行われ、LAN またはインターネット インターフェイスでアドレッシングの変更に配慮する必要はありません。

- Cisco ソフトウェアは、選択的、または動的に NAT を実行できます。この柔軟性により、ネットワーク管理者は RFC 1918 アドレスまたは登録したアドレスを使用することができます。
- NAT は、IP アドレスの簡略化や節約のためにさまざまなデバイス上で使用できるように設計されています。また、NAT により、変換に使用できる内部ホストを選択することもできます。
- NAT は、NAT を設定する若干のデバイス以外には、何ら変更を加えずに設定できるという大きな利点があります。

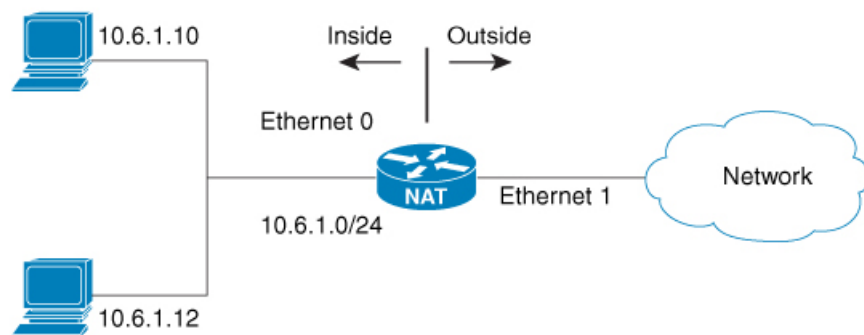
## NAT の機能

NAT が設定されたデバイスには、少なくとも内部ネットワークに対して1つ、外部ネットワークに対して1つのインターフェイスがあります。標準的な環境では、NAT はスタブ ドメインとバックボーン間の出口デバイスに設定されます。パケットがドメインから出て行くとき、NAT はローカルで意味のある送信元 アドレスをグローバルで一意のアドレスに変換します。パケットがドメインに入ってくる際は、NAT はグローバルに一意な宛先アドレスをローカルアドレスに変換します。

複数の内部ネットワークをデバイスに接続でき、同様にデバイスから外部ネットワークへと複数の出口となる点が存在する場合があります。アドレスが足りなくなると、パケットにアドレスを割り当てられなくなった場合、NAT はそのパケットを破棄し、Internet Control Message Protocol (ICMP) ホスト到達不能パケットをその接続先に送信します。

変換および転送は、ハードウェアのスイッチングプレーンで実行されるため、全体的なスループットの性能が改善されます。性能の詳細については、「[NAT の性能とスケール数 \(32 ページ\)](#)」セクションを参照してください。

図 6: NAT



354983

## NAT の用途

NAT は次のシナリオで使用できます。

- ホストのごく少数しかグローバルな一意のIPアドレスを持っていない状況でインターネットに接続する場合。

NAT はスタブドメイン（内部ネットワーク）と、インターネットなどのパブリックネットワーク（外部ネットワーク）との境界にあるデバイス上に設定されます。NATはパケットを外部ネットワークに送信する前に、内部のローカルアドレスをグローバルに一意のIPアドレスに変換します。

接続性の問題への解決策として NAT が役立つのは、スタブドメイン内の比較的少数のホストが同時にドメインの外部と通信する場合のみです。この場合、外部との通信が必要になるときに、グローバルに一意な IP アドレスに変換する必要があるのはこのドメインにある IP アドレスのごく一部のみです。また、これらのアドレスは再利用できます。

- 番号の付け直しを行う場合：

内部アドレスの変更には相当の工数がかかるため、変更する代わりに NAT を使用して変換することができます。

## NAT の内部アドレスおよび外部アドレス

NATにおいて、内部という用語は、組織が所有し変換が必要なネットワークを表します。NATが設定されている場合、このネットワーク内のホストは、ある空間（ローカルアドレス空間として知られている）内にアドレスを持ち、それが別の空間（グローバルアドレス空間として知られている）にあるものとしてネットワークの外側に現れることになります。

同様に、外部という用語は、スタブネットワークの接続先で、通常、その組織の制御下にはないネットワークを表します。外部ネットワーク内のホストを変換の対象にすることもできるため、これらのホストはローカルアドレスとグローバルアドレスを持つことができます。

NAT では、次の定義が使用されます。

- 内部ローカルアドレス：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。このアドレスは、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ルート可能な IP アドレスではありません。
- 内部グローバルアドレス：外部に向けて、1つまたは複数の内部ローカルIPアドレスを表すグローバルなルート可能な IP アドレス（NIC またはサービスプロバイダーにより割り当てられたもの）。
- 外部ローカルアドレス：内部ネットワークから見た外部ホストの IP アドレス。必ずしもルート可能な IP アドレスではありません。内部でルート可能なアドレス空間から割り当てられたものです。

- 外部グローバルアドレス：外部ネットワークに存在するホストに対して、ホストの所有者により割り当てられた IP アドレス。このアドレスは、グローバルにルート可能なアドレス、またはネットワーク空間から割り当てられます。
- 内部送信元アドレス変換：内部ローカルアドレスを内部グローバルアドレスに変換します。
- 外部送信元アドレス変換：外部グローバルアドレスを外部ローカルアドレスに変換します。
- 静的ポート変換：内部/外部ローカルアドレスの IP アドレスとポート番号を、対応する内部/外部グローバルアドレスの IP アドレスとポート番号に変換します。
- 特定のサブネットの静的変換：内部/外部ローカルアドレスの指定された範囲のサブネットを対応する内部/外部グローバルアドレスに変換します。
- ハーフエントリ：ローカルおよびグローバルのアドレス/ポート間のマッピングを表し、NAT モジュールの変換データベースで維持されます。ハーフ エントリは、設定されている NAT 規則に基づいて、静的または動的に作成され得ます。
- フルエントリ/フローエントリ：特定のセッションに対応する一意のフローを表します。ローカルからグローバルへのマッピングに加えて、指定したフローを完全修飾する接続先情報も維持されます。フル エントリは常に動的に作成されて NAT モジュールの変換データベースで維持されます。

## VRF 対応ネットワークアドレス変換

NAT は通常、デフォルトまたはグローバルルーティング ドメインで動作するように設定されます。この機能により、内部および外部の NAT ドメインはデフォルトの VRF スペースに関連付けられ、適宜変換が行われます。ただし、NAT が VRF 設定で実行される必要がある特定のシナリオがあります。一般的なシナリオの1つには、重複するアドレス空間を持つプライベートネットワークの共有サービスアクセスを有効にすることが含まれます。こうしたシナリオでは、特定のプライベートネットワークを異なる VRF に配置し、重複するプライベートアドレスを一意的グローバルアドレスにマッピングする VRF 対応 NAT ルールを設定することで、グローバルサービスアクセスを実現できます。VRF が認識されることにより、プライベートネットワークの VRF が考慮に含められ、結果として NAT がアドレスおよびポートの変換を実行できるようになります。

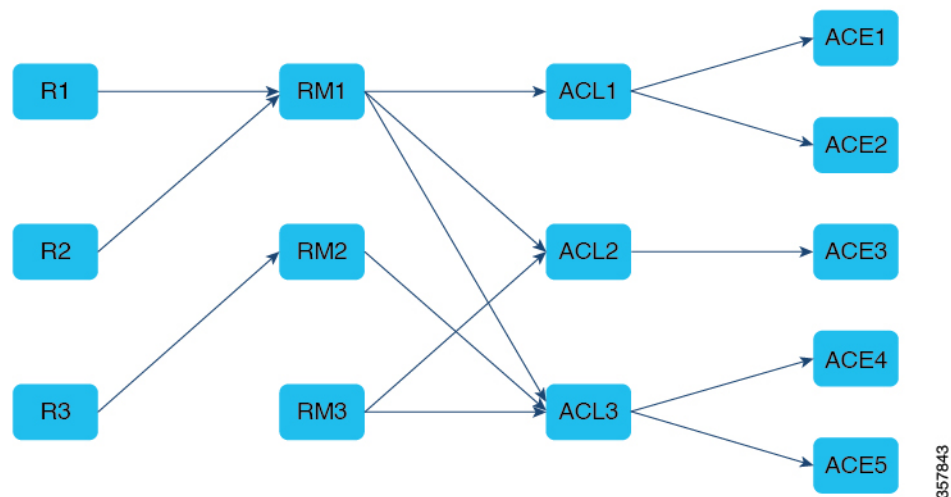
VRF 対応 NAT は、IP アドレスの VRF からグローバルへの変換のみをサポートします。VRF からグローバルへの変換は、特定の VRF に関連付けられている NAT 内部インターフェイスと、グローバル VRF に関連付けられている NAT 外部インターフェイス間で行われます。VRF 内 NAT 変換（特定の同じ VRF 内の NAT 内部インターフェイスと NAT 外部インターフェイスの間）と VRF 間 NAT 変換（異なる VRF に関連付けられている NAT 内部インターフェイスと NAT 外部インターフェイスの間）はサポートされていません。サポートされていないこのようなシナリオでは、NAT の動作は定義されません。VRF からグローバルへの NAT 変換のみをネットワークに展開することを推奨します。

## ルートマップベースのネットワークアドレス変換

ルートマップはアクセス制御リスト（ACL）に似ており、ユーザーは関連するアクションを含む一連の一致基準を定義できます。ルートマップはACLよりも柔軟性があり、ACLでは処理できないユースケースに対応できる機能が追加されています。ルートマップは、ポリシーベースルーティング（PBR）やルート再配布など、さまざまなアプリケーションに広く使用されています。ルートマップの詳細については、『Cisco IOS XE IP ルーティング コンフィギュレーションガイド』の「ルーティング情報を再配布するためのルートマップ」セクションを参照してください。

NATにおいては、ルートマップは宛先に基づく変換に使用されます。この変換では、フローの宛先に基づいて同じローカルアドレスが異なるグローバルアドレスに変換されます。ルートマップベースの静的および動的変換がサポートされており、次の図に示すように、同じルートマップを複数のルールに関連付けることができます。

図 7: NAT ルートマップ



ルートマップには複数の `permit-deny` 句が含まれる場合があります、該当するアドレスの一致基準はACLにより指定されます。ルートマップの評価により、決定された変換に基づいて、`permit` または `deny` が判定されます。

ACLベースのNATとは異なり、ルートマップベースのNATでは、アドレスのみの変換（AOT）が有効になっている場合でも完全なフローエントリが作成されます。この場合、フローごとの順方向および逆方向エントリのプログラミングにより、TCAMリソースの使用量が相対的に多くなります。

# ルートマップベースのネットワークアドレス変換の制限事項

ルートマップベースの NAT には次の制限事項があります。

- ルートマップのサポートは内部変換に限定されます。静的 NAT/PAT と動的 NAT/PAT のみ設定できます。外部変換、静的ネットワーク変換、およびインターフェイスベースの静的変換はサポートされていません。
- ルートマップベースの NAT では、アドレスベースの一致基準のみサポートされます。ネクストホップおよびインターフェイスベースの一致基準はサポートされていません。
- ルートマップに重複する ACE があると、TCAM 使用率が増加します。
- 静的 NAT の場合、特定の packets を許可する同じルートマップ内に後続の permit 句がある場合、deny 句に一致する packets にはソフトウェアスイッチが行われます。
- 動的 NAT の場合、permit 句に関連付けられた deny ACL に一致する packets は、該当する packets を許可する後続の permit 句があった場合でも、変換されずにハードウェア転送されます。
- 非オーバーロードの動的 NAT の場合、外部ドメインから内部グローバルアドレス宛ての packets が変換されます。

## NAT のタイプ

ネットワーク全体を表す 1 つのアドレスのみを外部にアドバタイズするように NAT を設定できます。この設定で、内部ネットワークを外部から効果的に隠すことができるため、セキュリティがさらに強化されます。

NAT には次のタイプがあります。

- 静的アドレス変換（静的 NAT）：ローカルアドレスとグローバルアドレスを 1 対 1 でマッピングします。
- 動的アドレス変換（動的 NAT）：未登録の IP アドレスを、登録済み IP アドレスのプールから取得した登録済み IP アドレスにマップします。
- オーバーロード/PAT：複数の未登録 IP アドレスを、複数の異なるレイヤ 4 ポートを使用して、1 つの登録済み IP アドレスにマップ（多対 1）します。この方法は、ポートアドレス変換（PAT）とも呼ばれます。オーバーロードを使用することにより、使用できる正規のグローバル IP アドレスが 1 つのみでも、数千のユーザーをインターネットに接続することができます。

## NATによる外部ネットワークへのパケットのルーティング（内部送信元アドレス変換）

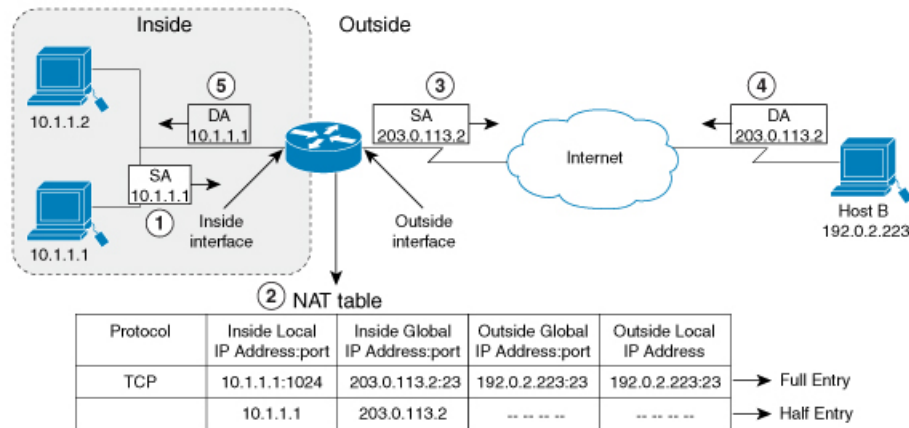
自分が属するネットワークの外部と通信するときに、未登録のIPアドレスをグローバルで一意なIPアドレスに変換できます。

静的または動的内部送信元アドレス変換は、次のようにして設定できます。

- 静的変換は、内部ローカルアドレスと内部グローバルアドレスの間に1対1のマッピングを設定します。外部から固定アドレスを使って内部のホストにアクセスする必要がある場合には、静的変換が便利です。静的変換は、xセクションで説明されているように、静的NAT規則を設定して有効にできます。
- 動的変換は、内部ローカルアドレスとグローバルアドレスのプールの間マッピングを動的に設定します。動的変換は、動的NAT規則を設定することで有効にできます。マッピングは、設定されている規則を実行時に評価した結果に基づいて設定されます。内部ローカルアドレスの指定には、標準と拡張の両方のアクセス制御リスト（ACL）を使用できます。内部グローバルアドレスはアドレスプールまたはインターフェイスから指定できます。動的変換は、「[内部送信元アドレスの動的変換の設定（35ページ）](#)」セクションで説明されているように動的規則を設定して有効にできます。

次の図には、ネットワーク内の送信元アドレスを、ネットワーク外へ送信元アドレスに変換するデバイスが示されています。

図 8: NAT 内部送信元変換



次のプロセスは、上の図の内部送信元アドレス変換を示しています。

- ホスト 10.1.1.1 のユーザーは、外部ネットワークのホスト B との接続を開きます。
- NAT モジュールは、対応するパケットを横取りし、パケットを変換しようとします。一致する NAT 規則の有無に基づいて、次のシナリオが考えられます。

- 一致する静的変換規則が存在する場合、パケットは対応する内部グローバルアドレスに変換されます。存在しない場合、パケットは動変換規則に対して照合され、一致した場合は対応する内部グローバルアドレスに変換されます。NATモジュールは、変換したパケットに対応する完全修飾フロー エントリを変換データベースに挿入します。これにより、このフローに対応するパケットの高速変換および転送が双方向で促進されます。
- 一致する規則がない場合、パケットはアドレス変換を行わずに転送されます。
- 有効な内部グローバルアドレスを取得できない場合は、たとえ一致する規則があってもパケットは破棄されます。



(注) 動変換に ACL が使用される場合、NAT は ACL を評価し、特定の ACL で許可されているパケットのみが変換の対象になります。

3. デバイスはホスト 10.1.1.1 の内部ローカル送信元アドレスを、この変換の内部グローバルアドレス 203.0.113.2 で置き換え、パケットを転送します。
4. ホスト B はこのパケットを受信し、内部グローバル IP 宛先アドレス (DA) 203.0.113.2 を使用して、ホスト 10.1.1.1 に応答します。
5. ホスト B からの応答パケットは、内部グローバルアドレスに送信されます。NAT モジュールはこのパケットを横取りし、変換データベースにセットアップされているフロー エントリを使って対応する内部ローカルアドレスに変換し直します。

ホスト 10.1.1.1 はパケットを受信し、会話を続けます。デバイスは、受信する各パケットについて手順 2 ~ 5 を実行します。

## 外部送信元アドレス変換

ネットワークの外部から内部に移動する IP パケットの送信元アドレスを変換できます。通常、このタイプの変換は、重複しているネットワークを相互接続するために、内部送信元アドレスの変換と組み合わせて使用されます。

このプロセスについては、「[重複するネットワークの変換の設定 \(41 ページ\)](#)」セクションで説明します。

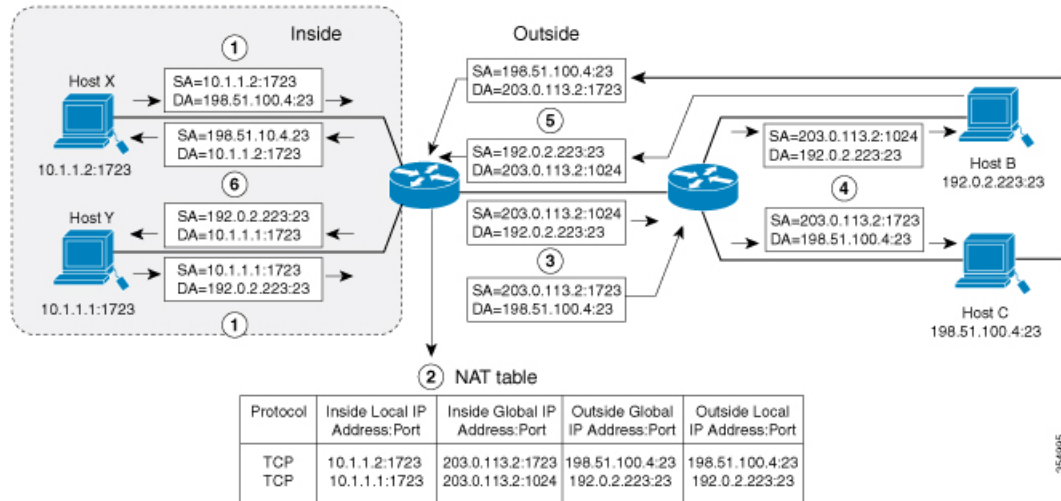
## ポートアドレス変換

デバイスで、多くのローカルアドレスに1つのグローバルアドレスを使用できるようにすることで、内部グローバルアドレスプールのアドレスを節約できます。このタイプの NAT 設定は、オーバーロードまたはポートアドレス変換 (PAT) と呼ばれます。

オーバーロードが設定されている場合、デバイスは、より高いレベルのプロトコルから十分な情報（たとえば、TCP または UDP ポート番号）を保持して、グローバルアドレスを正しいローカルアドレスに戻します。複数のローカルアドレスが1つのグローバルアドレスにマッピングされる場合、各内部ホストの TCP または UDP ポート番号によりローカルアドレスが区別されます。

次の図は、1つの内部グローバルアドレスが複数の内部ローカルアドレスを表すときの NAT の動作を示しています。区別は、TCP ポート番号により行われます。

図 9: 内部グローバルアドレスをオーバーロードする PAT/NAT



このデバイスは、上の図に示すように、内部グローバルアドレスのオーバーロードで次の処理を行います。ホスト B およびホスト C はいずれも、アドレス 203.0.113.2 にある 1つのホストと通信していると信じています。ただし、実際には、異なるホストと通信しています。区別にはポート番号が使用されます。つまり、多数の内部ホストは、複数のポート番号を使用して、内部グローバル IP アドレスを共有することができます。

1. ホスト 10.1.1.1:1723 のユーザはホスト B への接続を開き、ホスト 10.1.1.2:1723 のユーザはホスト C への接続を開きます。
2. NAT モジュールは、対応するパケットを横取りし、パケットの変換を試みます。

一致する NAT 規則の有無に基づいて、次のシナリオが考えられます。

- 一致する静的変換規則が存在する場合はその規則が優先され、パケットは対応するグローバルアドレスに変換されます。存在しない場合、パケットは動的変換規則に対して照合され、一致した場合は対応するグローバルアドレスに変換されます。NAT モジュールは、変換したパケットに対応する完全修飾フローエントリを変換データベースに挿入し、このフローに対応するパケットの高速変換および転送を双方向で促進します。
- 一致する規則がない場合、パケットはアドレス変換を行わずに転送されます。
- 有効な内部グローバルアドレスを取得できない場合は、一致する規則があってもパケットは破棄されます。

- これは PAT 設定であるため、トランスポートのポートにより複数のフローを1つのグローバルアドレスに変換できます。（送信元アドレスに加えて送信元ポートも変換されるため、関連付けられているフローエントリは対応する変換マッピングを維持します。）
3. デバイスは、内部ローカル送信元アドレス/ポート 10.1.1.1/1723 および 10.1.1.2/1723 を対応する選択されたグローバルアドレス/ポート 203.0.113.2/1024 および 203.0.113.2/1723 にそれぞれ置き換えてパケットを転送します。
  4. ホスト B はこのパケットを受信し、ポート 1024 で内部グローバル IP アドレス 203.0.113.2 を使用してホスト 10.1.1.1 に応答します。ホスト C はこのパケットを受信し、ポート 1723 で内部グローバル IP アドレス 203.0.113.2 を使用してホスト 10.1.1.2 に応答します。
  5. デバイスは、内部グローバル IP アドレスを持つパケットを受信すると、内部グローバルアドレスとポート、および外部アドレスとポートをキーとして NAT テーブル検索を実行します。次に、アドレスを内部ローカルアドレス 10.1.1.1:1723/10.1.1.2:1723 に変換し、パケットをホスト 10.1.1.1 および 10.1.1.2 にそれぞれ転送します。

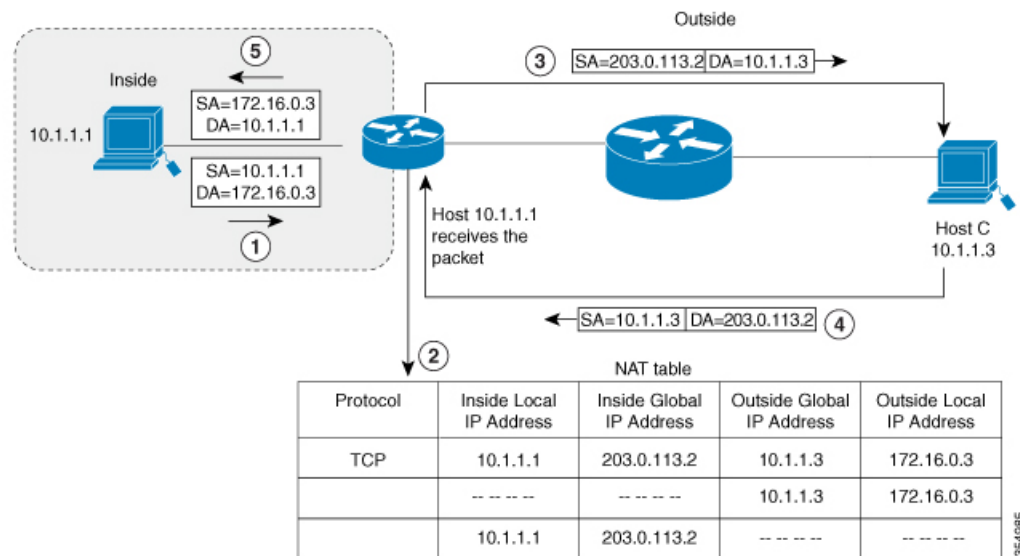
ホスト 10.1.1.1 および 10.1.1.2 はパケットを受信し、通信を続行します。デバイスは、受信する各パケットについて手順 2～5 を実行します。

## 重複ネットワーク

使用する IP アドレスが正当でない、または正式に割り当てられていない場合、IP アドレスを変換するには NAT を使用します。すでに合法的に所有されインターネットまたは外部ネットワーク上のデバイスに割り当てられている IP アドレスを、独自のネットワーク上の別のデバイスに割り当てると、ネットワークの重複が発生します。

次の図は重複したネットワークを示しています。内部ネットワークと外部ネットワークの両方のローカル IP アドレスが同じです (10.1.1.x)。そのように重複しているアドレス空間の間のネットワーク接続を確立するには NAT デバイスを使用して遠隔にある対向のアドレス (10.1.1.3) を内部から見た別のアドレスに変換する必要があります。

図 10: NATによる重複するアドレスの変換



内部ローカルアドレス（10.1.1.1）および外部グローバルアドレス（10.1.1.3）が同じサブネットにあることに注意してください。重複するアドレスを変換するために、まず、内部送信元アドレスの変換によって内部ローカルアドレスが 203.0.113.2 に変換され、NAT テーブルにハーフエントリが作成されます。受信側では、外部送信元アドレスが 172.16.0.3 に変換され、ハーフエントリがもう 1 つ作成されます。すべての変換を完了し、NAT テーブルがフルエントリで更新されます。

次の手順は、重複するアドレスをデバイスが変換する方法を示します。

1. ホスト 10.1.1.1 は 172.16.0.3 への接続を開きます。
2. NAT モジュールは、内部ローカルアドレスと内部グローバルアドレスを相互に、また外部グローバルアドレスと外部ローカルアドレスを相互にマップする変換マッピングをセットアップします。
3. 送信元アドレス（SA）は、内部グローバルアドレスで置き換えられ、宛先アドレス（DA）は外部グローバルアドレスで置き換えられます。
4. ホスト C はパケットを受信し、会話を続けます。
5. デバイスは NAT テーブルの検索を行い、DA を内部ローカルアドレスで、SA を外部ローカルアドレスで置き換えます。
6. この変換プロセスを使用して、パケットがホスト 10.1.1.1 により受信され、会話が続けられます。

## ネットワークアドレス変換の制限事項

以下は NAT の制限事項です。

- NAT の動作によっては、ハードウェアデータプレーンで現在サポートされていません。比較的遅いソフトウェアデータプレーンで実行される動作は次のとおりです。
  - Internet Control Message Protocol (ICMP) パケットの変換。
  - アプリケーションレイヤゲートウェイ (ALG) 処理を必要とするパケットの変換。
  - 内側と外側の両方で変換が必要なパケット。
- ハードウェアで変換および転送できるセッションの最大数は、理想的な設定では240に制限されています。変換が必要なその他のフローは、スループットを下げてソフトウェアデータプレーンで処理されます。



(注) 変換ごとに TCAM の 2 つのエントリが使用されます。

- 設定されている NAT 規則は、リソースの制約のためにハードウェアにプログラムできない場合があります。これにより、特定の規則に該当するパケットが変換されずに転送されることがあります。
- ALG のサポートは、FTP、TFTP、および ICMP プロトコルに現在制限されています。また、TCP SYN、TCP FIN、および TCP RST は ALG トラフィックの一部ではありませんが、ALG トラフィックの一部として処理されます。
- 動的に作成された NAT フローは、非アクティブな状態が一定期間続くとエージアウトします。
- ポリシーベースルーティング (PBR) と NAT は、同じインターフェイスではサポートされていません。PBR と NAT は、異なるインターフェイス上に設定されている場合にのみ連携します。
- NAT は、断片化されたパケットの変換をサポートしていません。
- Bidirectional Forwarding Detection (BFD) セッションが動的 NAT に使用されるものと同じアドレスを使用して動作するように設定されている場合、これらのセッションは失敗する可能性があります。デバイスで BFD と動的 NAT の両方が設定されている場合に発生する競合を回避するには、NAT と重複しないアドレスを使用します。BFD と動的 NAT のオーバーロードを同じインターフェイスに設定する必要がある場合は、プールベースの動的 NAT オーバーロード設定を展開します。このシナリオでも、選択した NAT プールアドレスを BFD に使用しないでください。
- NAT は、ステートフル スイッチオーバー (SSO) をサポートしていません。動的に作成された NAT の状態は、アクティブデバイスとスタンバイデバイスの間で同期されません。
- 等コスト マルチパスルーティング (ECMP) は、NAT でサポートされていません。
- インターフェイスに Flexible NetFlow とネットワークアドレス変換 (NAT) が設定されている場合には、以下のようになります。

- Flexible NetFlow は、変換前のフローの詳細を表示およびエクスポートします。変換後のフローの詳細は表示もエクスポートもしません。アプリケーションレベルゲートウェイ（ALG）フローの詳細は、エクスポートされる変換前のフローの詳細には含まれません。
- ALG トラフィックが CPU を介して変換されると、Flexible NetFlow は、ALG トラフィックの変換後のフローの詳細を表示およびエクスポートします。
- NAT ACL の明示的な拒否アクセス制御エントリ（ACE）はサポートされていません。明示的な許可 ACE のみがサポートされます。
- インターフェイス オーバーロードを使用する NAT の設定に使用されたものと同じ IP アドレスで動作するように NETCONF が設定されると、NETCONF 設定は失敗します。
- NAT は GRE トンネルではサポートされていません。
- 入力および出力 NAT インターフェイスの両方が同じスイッチ上にある場合、ステートフルスイッチオーバー（SSO）後にリモートまたはスタンバイスイッチで TCAM のハードウェア NAT エントリが非同期になることがあります。これは、AOT が有効になっている場合に NAT のタイムアウトが発生すると、リモートスイッチで発生する可能性があります。
- NAT はマルチキャストパケットをサポートしません。
- VRF 間 NAT および VRF 内 NAT はサポートされていません。

## NAT の性能とスケール数

ハードウェアでサポートされる双方向 NAT フローの最大数は 240 に制限されています。

## アドレスのみの変換



(注) アドレスのみの変換を使用すると、フローの処理が最適化され、NAT 機能のスケールが拡張されます。

アドレスのみの変換（AOT）機能は、トランスポートのポートではなくアドレスフィールドのみを変換する必要がある状況で使用できます。そのような状況で AOT 機能を有効にすると、ハードウェアにおいてラインレートで変換および転送できるフローの数が大幅に増加します。この改善は、変換および転送に関連したさまざまなハードウェアリソースの使用を最適化することによって実現されます。

一般的な NAT 集中型リソース割り当て方式では、ハードウェア変換を実行するために 512 個の TCAM エントリが確保されます。その結果、ラインレートで変換および転送できるフローの数が厳密な上限が設定されます。AOT スキームでは、TCAM リソースの使用が高度に最適

化されるため、TCAMテーブルでより多くのフローに対応できるようになり、ハードウェア変換および転送の規模が大幅に拡大します。

AOT は、フローの大部分が単一または少数の宛先に送信される場合に非常に効果的です。そのような良好な条件下では、AOT により、特定の 1 つまたは複数のエンドポイントから発信されるすべてのフローのラインレート変換および転送が有効になる可能性があります。AOT 機能は、デフォルトでは無効になっています。 **no ip nat create flow-entries** コマンドを使用して有効にできます。既存の動的フローは、 **clear ip nat translation** コマンドを使用してクリアできます。AOT 機能は、 **ip nat create flow-entries** コマンドを使用して無効にできます。

## アドレスのみの変換の制限事項

- AOT 機能は、単純な内部静的規則および内部動的規則に対応する変換シナリオでのみ正しく機能すると想定されています。単純な静的規則のタイプは **ip nat inside source static local-ip global-ip** で、動的規則のタイプは **ip nat inside source list access-list pool name** である必要があります。
- AOT が有効になっている場合、 **show ip nat translation** コマンドを使用しても、変換および転送されるすべての NAT フローの可視性が実現することはありません。

## NAT の設定

このセクションで説明するタスクを使用して、NAT を効果的に設定できます。設定によっては、複数の作業を実行する必要があります。

### 内部送信元アドレスの静的変換の設定

内部ローカルアドレスと内部グローバルアドレス間の 1 対 1 マッピングを可能にするには、内部送信元アドレスの静的変換を設定します。外部から固定アドレスを使って内部のホストにアクセスする必要がある場合には、静的変換が便利です。

#### 手順の概要

1. **enable**
2. **configure terminal**
3. 要件に応じて次の 3 つのコマンドのいずれかを使用します。
  - **ip nat inside source static local-ip global-ip**  

```
Switch(config)# ip nat inside source static 10.10.10.1 172.16.131.1
```
  - **ip nat inside source static protocol local-ip port global-ip port**  

```
Switch(config)# ip nat inside source static tcp 10.10.10.1 1234 172.16.131.1 5467
```
  - **ip nat inside source static network local-ip global-ip { prefix\_len len | subnet subnet-mask}**

```
Switch(config)# ip nat inside source static network 10.10.10.1 172.16.131.1
prefix_len 24
```

4. **interface** *type number*
5. **ip address** *ip-address mask [secondary]*
6. **ip nat inside**
7. **exit**
8. **interface** *type number*
9. **ip address** *ip-address mask [secondary]*
10. **ip nat outside**
11. **end**

## 手順の詳細

## 手順

|        | コマンドまたはアクション                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | 目的                                                                                                                                                                                              |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ステップ 1 | <b>enable</b><br>例：<br>Switch> enable                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | 特権 EXEC モードを有効にします。<br>パスワードを入力します（要求された場合）。                                                                                                                                                    |
| ステップ 2 | <b>configure terminal</b><br>例：<br>Switch# 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 | 要件に応じて次の 3 つのコマンドのいずれかを使用します。 <ul style="list-style-type: none"> <li>• <b>ip nat inside source static</b> <i>local-ip global-ip</i><br/>               Switch(config)# ip nat inside source static<br/>               10.10.10.1 172.16.131.1</li> <li>• <b>ip nat inside source static</b> <i>protocol local-ip port global-ip port</i><br/>               Switch(config)# ip nat inside source static<br/>               tcp 10.10.10.1 1234 172.16.131.1 5467</li> <li>• <b>ip nat inside source static network</b> <i>local-ip global-ip { prefix_len len   subnet subnet-mask }</i><br/>               Switch(config)# ip nat inside source static<br/>               network 10.10.10.1 172.16.131.1 prefix_len<br/>               24</li> </ul> | 内部ローカルアドレスと内部グローバルアドレス間の静的変換を設定します。<br>内部ローカルアドレスと内部グローバルアドレス間の静的ポート変換を設定します。<br>内部ローカルアドレスと内部グローバルアドレス間の静的変換を設定します。内部グローバルアドレスに変換するサブネットの範囲を指定できます。IP アドレスのホスト部分は変換されますが、IP のネットワーク部分は変換されません。 |
| ステップ 4 | <b>interface</b> <i>type number</i><br>例：<br>Switch(config)# interface GigabitEthernet 1/0/1                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。                                                                                                                                                    |

|         | コマンドまたはアクション                                                                                                           | 目的                                              |
|---------|------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------|
| ステップ 5  | <b>ip address ip-address mask [secondary]</b><br>例：<br>Switch(config-if)# ip address 10.114.11.39<br>255.255.255.0     | インターフェイスのプライマリ IP アドレスを設定します。                   |
| ステップ 6  | <b>ip nat inside</b><br>例：<br>Switch(config-if)# ip nat inside                                                         | NATの対象である内部ネットワークにインターフェイスを接続します。               |
| ステップ 7  | <b>exit</b><br>例：<br>Switch(config-if)# exit                                                                           | インターフェイス コンフィギュレーション モードを終了し、グローバル設定モードに戻ります。   |
| ステップ 8  | <b>interface type number</b><br>例：<br>Switch(config)# interface GigabitEthernet 1/0/2                                  | 異なるインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。 |
| ステップ 9  | <b>ip address ip-address mask [secondary]</b><br>例：<br>Switch(config-if)# ip address 172.31.232.182<br>255.255.255.240 | インターフェイスのプライマリ IP アドレスを設定します。                   |
| ステップ 10 | <b>ip nat outside</b><br>例：<br>Switch(config-if)# ip nat outside                                                       | 外部ネットワークにインターフェイスを接続します。                        |
| ステップ 11 | <b>end</b><br>例：<br>Switch(config-if)# end                                                                             | インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。  |

## 内部送信元アドレスの動的変換の設定

動的変換は、内部ローカルアドレスとグローバルアドレスのプール間にマッピングを動的に設定します。動的変換は、動的NAT規則を設定することで有効にできます。マッピングは、設定されている規則を実行時に評価した結果に基づいて設定されます。内部ローカルアドレスの指定にはACLを使用できます。また、内部グローバルアドレスは、アドレスプール、またはインターフェイスから指定できます。

プライベートネットワークに存在する複数のユーザーがインターネットへのアクセスを必要としている場合には、動的変換が便利です。動的に設定されたプールIPアドレスは必要に応じて使用でき、インターネットへのアクセスがなくなるときは別のユーザーが使用できるように解放できます。

## 手順の概要

1. **enable**
2. **configure terminal**
3. **ip nat pool name start-ip end-ip netmask netmask | prefix-length prefix-length**
4. **access-list access-list-number permit source [source-wildcard]**
5. **ip nat inside source list access-list-number pool name**
6. **interface type number**
7. **ip address ip-address mask**
8. **ip nat inside**
9. **exit**
10. **interface type number**
11. **ip address ip-address mask**
12. **ip nat outside**
13. **end**

## 手順の詳細

## 手順

|        | コマンドまたはアクション                                                                                                                                                                         | 目的                                           |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------|
| ステップ 1 | <b>enable</b><br>例：<br>Switch> enable                                                                                                                                                | 特権 EXEC モードを有効にします。<br>パスワードを入力します（要求された場合）。 |
| ステップ 2 | <b>configure terminal</b><br>例：<br>Switch# 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 | <b>ip nat pool name start-ip end-ip netmask netmask   prefix-length prefix-length</b><br>例：<br>Switch(config)# ip nat pool net-208<br>172.16.233.208 172.16.233.223 prefix-length 28 | 必要に応じて割り当てられるグローバルアドレスのプールを定義します。            |
| ステップ 4 | <b>access-list access-list-number permit source [source-wildcard]</b><br>例：<br>Switch(config)# access-list 1 permit 192.168.34.0<br>0.0.0.255                                        | 変換されるアドレスを許可する標準アクセス リストを定義します。              |
| ステップ 5 | <b>ip nat inside source list access-list-number pool name</b><br>例：<br>Switch(config)# ip nat inside source list 1 pool<br>net-208                                                   | ステップ 4 で定義したアクセス リストを指定して、動的送信元変換を設定します。     |

|         | コマンドまたはアクション                                                                                                      | 目的                                                    |
|---------|-------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------|
| ステップ 6  | <b>interface</b> <i>type number</i><br>例：<br>Switch(config)# interface GigabitEthernet 1/0/1                      | インターフェイスを指定し、インターフェイス コンフィギュレーションモードを開始します。           |
| ステップ 7  | <b>ip address</b> <i>ip-address mask</i><br>例：<br>Switch(config-if)# ip address 10.114.11.39<br>255.255.255.0     | インターフェイスのプライマリ IP アドレスを設定します。                         |
| ステップ 8  | <b>ip nat inside</b><br>例：<br>Switch(config-if)# ip nat inside                                                    | NATの対象である内部ネットワークにインターフェイスを接続します。                     |
| ステップ 9  | <b>exit</b><br>例：<br>Switch(config-if)#exit                                                                       | インターフェイス コンフィギュレーションモードを終了し、グローバルコンフィギュレーションモードに戻ります。 |
| ステップ 10 | <b>interface</b> <i>type number</i><br>例：<br>Switch(config)# interface GigabitEthernet 1/0/2                      | インターフェイスを指定し、インターフェイス コンフィギュレーションモードを開始します。           |
| ステップ 11 | <b>ip address</b> <i>ip-address mask</i><br>例：<br>Switch(config-if)# ip address 172.16.232.182<br>255.255.255.240 | インターフェイスのプライマリ IP アドレスを設定します。                         |
| ステップ 12 | <b>ip nat outside</b><br>例：<br>Switch(config-if)# ip nat outside                                                  | 外部ネットワークにインターフェイスを接続します。                              |
| ステップ 13 | <b>end</b><br>例：<br>Switch(config-if)# end                                                                        | インターフェイス コンフィギュレーションモードを終了し、特権 EXEC モードに戻ります。         |

## PAT の設定

グローバルアドレスのオーバーロードを使用して、内部ユーザにインターネットへのアクセスを許可し、内部グローバルアドレス プールのアドレスを節約するには、この作業を実行します。

### 手順の概要

#### 1. enable

2. **configure terminal**
3. **ip nat pool name start-ip end-ip netmask netmask | prefix-length prefix-length**
4. **access-list access-list-number permit source [source-wildcard]**
5. **ip nat inside source list access-list-number pool name overload**
6. **interface type number**
7. **ip address ip-address mask [secondary]**
8. **ip nat inside**
9. **exit**
10. **interface type number**
11. **ip address ip-address mask [secondary]**
12. **ip nat outside**
13. **end**

## 手順の詳細

## 手順

|        | コマンドまたはアクション                                                                                                                                                                                     | 目的                                                                                                                                                                   |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ステップ 1 | <b>enable</b><br>例：<br>Switch> enable                                                                                                                                                            | 特権 EXEC モードを有効にします。<br>パスワードを入力します（要求された場合）。                                                                                                                         |
| ステップ 2 | <b>configure terminal</b><br>例：<br>Switch# 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 | <b>ip nat pool name start-ip end-ip netmask netmask   prefix-length prefix-length</b><br>例：<br>Switch(config)# ip nat pool net-208<br>192.168.202.129 192.168.202.158 netmask<br>255.255.255.224 | 必要に応じて割り当てられるグローバルアドレスのプールを定義します。                                                                                                                                    |
| ステップ 4 | <b>access-list access-list-number permit source [source-wildcard]</b><br>例：<br>Switch(config)# access-list 1 permit<br>192.168.201.30 0.0.0.255                                                  | 変換されるアドレスを許可する標準アクセス リストを定義します。<br>アクセス リストは、変換されるアドレスだけを許可する必要があります（各アクセス リストの最後に暗黙の「deny all」ステートメントが存在することに注意してください）。許可する範囲が広すぎるアクセス リストを使用すると、予測困難な結果を招くことがあります。 |
| ステップ 5 | <b>ip nat inside source list access-list-number pool name overload</b><br>例：                                                                                                                     | 手順 4 で定義されたアクセス リストを指定して、動的送信元変換を設定します。                                                                                                                              |

|         | コマンドまたはアクション                                                                                                               | 目的                                              |
|---------|----------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------|
|         | Switch(config)# ip nat inside source list 1 pool net-208 overload                                                          |                                                 |
| ステップ 6  | <b>interface</b> <i>type number</i><br>例：<br>Switch(config)# interface GigabitEthernet 1/0/1                               | インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。    |
| ステップ 7  | <b>ip address</b> <i>ip-address mask [secondary]</i><br>例：<br>Switch(config-if)# ip address 192.168.201.1 255.255.255.240  | インターフェイスのプライマリ IP アドレスを設定します。                   |
| ステップ 8  | <b>ip nat inside</b><br>例：<br>Switch(config-if)# ip nat inside                                                             | NATの対象である内部ネットワークにインターフェイスを接続します。               |
| ステップ 9  | <b>exit</b><br>例：<br>Switch(config-if)# exit                                                                               | インターフェイス コンフィギュレーション モードを終了し、グローバル設定モードに戻ります。   |
| ステップ 10 | <b>interface</b> <i>type number</i><br>例：<br>Switch(config)# interface GigabitEthernet 1/0/2                               | 異なるインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。 |
| ステップ 11 | <b>ip address</b> <i>ip-address mask [secondary]</i><br>例：<br>Switch(config-if)# ip address 192.168.201.29 255.255.255.240 | インターフェイスのプライマリ IP アドレスを設定します。                   |
| ステップ 12 | <b>ip nat outside</b><br>例：<br>Switch(config-if)# ip nat outside                                                           | 外部ネットワークにインターフェイスを接続します。                        |
| ステップ 13 | <b>end</b><br>例：<br>Switch(config-if)# end                                                                                 | インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。  |

## 外部 IP アドレスのみの NAT の設定

デフォルトで NAT は、「[NAT でのアプリケーション レベル ゲートウェイの使用 \(47 ページ\)](#)」セクションで説明されているように、パケットのペイロードに埋め込まれているアドレスを変換します。埋め込みアドレスを変換することが望ましくない場合は、外部の IP アドレスのみを変換するように NAT を設定できます。

## 手順の概要

1. **enable**
2. **configure terminal**
3. **ip nat inside source {list {access-list-number | access-list-name} pool pool-name [overload] | static network local-ip global-ip [no-payload]}**
4. **ip nat inside source {list {access-list-number | access-list-name} pool pool-name [overload] | static {tcp | udp} local-ip local-port global-ip global-port [no-payload]}**
5. **ip nat inside source {list {access-list-number | access-list-name} pool pool-name [overload] | static [network] local-network-mask global-network-mask [no-payload]}**
6. **ip nat outside source {list {access-list-number | access-list-name} pool pool-name | static local-ip global-ip [no-payload]}**
7. **ip nat outside source {list {access-list-number | access-list-name} pool pool-name | static {tcp | udp} local-ip local-port global-ip global-port [no-payload]}**
8. **ip nat outside source {list {access-list-number | access-list-name} pool pool-name | static [network] local-network-mask global-network-mask [no-payload]}**
9. **exit**
10. **show ip nat translations [verbose]**

## 手順の詳細

## 手順

|        | コマンドまたはアクション                                                                                                                                                                                                                                                                        | 目的                                                 |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------|
| ステップ 1 | <b>enable</b><br>例：<br>Device> enable                                                                                                                                                                                                                                               | 特権 EXEC モードを有効にします。<br><br>• パスワードを入力します（要求された場合）。 |
| ステップ 2 | <b>configure terminal</b><br>例：<br>Device# 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 | <b>ip nat inside source {list {access-list-number   access-list-name} pool pool-name [overload]   static network local-ip global-ip [no-payload]}</b><br>例：<br>Device(config)# ip nat inside source static network 10.1.1.1 192.168.251.0/24 no-payload                             | 内部ホスト デバイスでのネットワーク パケット変換を無効化します。                  |
| ステップ 4 | <b>ip nat inside source {list {access-list-number   access-list-name} pool pool-name [overload]   static {tcp   udp} local-ip local-port global-ip global-port [no-payload]}</b><br>例：<br>Device(config)# ip nat inside source static tcp 10.1.1.1 2000 192.168.1.1 2000 no-payload | 内部ホスト デバイスでのポート パケット変換を無効化します。                     |

|         | コマンドまたはアクション                                                                                                                                                                                                                                                                                     | 目的                                          |
|---------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------|
| ステップ 5  | <p><b>ip nat inside source</b> {list {access-list-number   access-list-name} pool pool-name [overload]   static [network] local-network-mask global-network-mask [no-payload]}</p> <p>例 :</p> <pre>Device(config)# ip nat inside source static 10.1.1.1 192.168.1.1 no-payload</pre>             | 内部ホスト ルータでのパケット変換を無効化します。                   |
| ステップ 6  | <p><b>ip nat outside source</b> {list {access-list-number   access-list-name} pool pool-name   static local-ip global-ip [no-payload]}</p> <p>例 :</p> <pre>Device(config)# ip nat outside source static 10.1.1.1 192.168.1.1 no-payload</pre>                                                    | 外部ホスト ルータでのパケット変換を無効化します。                   |
| ステップ 7  | <p><b>ip nat outside source</b> {list {access-list-number   access-list-name} pool pool-name   static {tcp   udp} local-ip local-port global-ip global-port [no-payload]}</p> <p>例 :</p> <pre>Device(config)# ip nat outside source static tcp 10.1.1.1 20000 192.168.1.1 20000 no-payload</pre> | 外部ホスト デバイスでのポート パケット変換を無効化します。              |
| ステップ 8  | <p><b>ip nat outside source</b> {list {access-list-number   access-list-name} pool pool-name   static [network] local-network-mask global-network-mask [no-payload]}</p> <p>例 :</p> <pre>Device(config)# ip nat outside source static network 10.1.1.1 192.168.251.0/24 no-payload</pre>         | 外部ホスト デバイスでのネットワーク パケット変換を無効化します。           |
| ステップ 9  | <p><b>exit</b></p> <p>例 :</p> <pre>Device(config)# exit</pre>                                                                                                                                                                                                                                    | グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。 |
| ステップ 10 | <p><b>show ip nat translations</b> [verbose]</p> <p>例 :</p> <pre>Device# show ip nat translations</pre>                                                                                                                                                                                          | アクティブな NAT を表示します。                          |

## 重複するネットワークの変換の設定

スタブ ネットワーク内の IP アドレスが別のネットワークに属する正式な IP アドレスであるときに、静的変換を使用して、これらのホストやルータと通信する必要がある場合は、重複するネットワークの静的変換を設定します。



(注) NAT 外部変換を成功させるためには、デバイスに外部ローカルアドレスのルートを設定する必要があります。ルートは手動で、または **ip nat outside source {static | list}** コマンドと関連付けられた **add-route** オプションを使用して設定できます。ルートの自動作成を有効にする **add-route** オプションを使用することを推奨します。

## 手順の概要

1. **enable**
2. **configure terminal**
3. **ip nat inside source static** *local-ip global-ip*
4. **ip nat outside source static** *local-ip global-ip*
5. **interface** *type number*
6. **ip address** *ip-address mask*
7. **ip nat inside**
8. **exit**
9. **interface** *type number*
10. **ip address** *ip-address mask*
11. **ip nat outside**
12. **end**

## 手順の詳細

### 手順

|        | コマンドまたはアクション                                                                                                                               | 目的                                           |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------|
| ステップ 1 | <b>enable</b><br>例：<br>Switch> enable                                                                                                      | 特権 EXEC モードを有効にします。<br>パスワードを入力します（要求された場合）。 |
| ステップ 2 | <b>configure terminal</b><br>例：<br>Switch# configure terminal                                                                              |                                              |
| ステップ 3 | <b>ip nat inside source static</b> <i>local-ip global-ip</i><br>例：<br>Switch(config)# ip nat inside source static<br>10.1.1.1 203.0.113.2  | 内部ローカルアドレスと内部グローバルアドレス間の静的変換を設定します。          |
| ステップ 4 | <b>ip nat outside source static</b> <i>local-ip global-ip</i><br>例：<br>Switch(config)# ip nat outside source static<br>172.16.0.3 10.1.1.3 | 外部ローカルアドレスと外部グローバルアドレス間の静的変換を設定します。          |

|         | コマンドまたはアクション                                                                                                      | 目的                                             |
|---------|-------------------------------------------------------------------------------------------------------------------|------------------------------------------------|
| ステップ 5  | <b>interface</b> <i>type number</i><br>例：<br>Switch(config)# interface GigabitEthernet 1/0/1                      | インターフェイスを指定し、インターフェイス コンフィギュレーションモードを開始します。    |
| ステップ 6  | <b>ip address</b> <i>ip-address mask</i><br>例：<br>Switch(config-if)# ip address 10.114.11.39<br>255.255.255.0     | インターフェイスのプライマリ IP アドレスを設定します。                  |
| ステップ 7  | <b>ip nat inside</b><br>例：<br>Switch(config-if)# ip nat inside                                                    | 内部と接続されることを示すマークをインターフェイスに付けます。                |
| ステップ 8  | <b>exit</b><br>例：<br>Switch(config-if)# exit                                                                      | インターフェイス コンフィギュレーションモードを終了し、グローバル設定モードに戻ります。   |
| ステップ 9  | <b>interface</b> <i>type number</i><br>例：<br>Switch(config)# interface GigabitEthernet 1/0/2                      | 異なるインターフェイスを指定し、インターフェイス コンフィギュレーションモードを開始します。 |
| ステップ 10 | <b>ip address</b> <i>ip-address mask</i><br>例：<br>Switch(config-if)# ip address 172.16.232.182<br>255.255.255.240 | インターフェイスのプライマリ IP アドレスを設定します。                  |
| ステップ 11 | <b>ip nat outside</b><br>例：<br>Switch(config-if)# ip nat outside                                                  | 外部と接続されることを示すマークをインターフェイスに付けます。                |
| ステップ 12 | <b>end</b><br>例：<br>Switch(config-if)# end                                                                        | インターフェイス コンフィギュレーションモードを終了し、特権 EXEC モードに戻ります。  |

## アドレス変換タイムアウトの設定

NAT の設定に基づき、アドレス変換のタイムアウトを設定できます。

デフォルトでは、動的に作成された変換エントリは、さまざまなリソースを効率的に利用できるようにするために、アクティブでない状態が一定時間続くとタイムアウトします。必要に応じて、タイムアウトのデフォルト値を変更できます。主な変換タイプに関連付けられているデフォルトのタイムアウト設定は、次のとおりです。

- 確立された TCP セッション : 24 時間

- UDP フロー : 5 分
- ICMP フロー : 1 分

デフォルトのタイムアウト値は、ほとんどの展開シナリオでタイムアウト要件を満たすことができます。ただし、これらの値は必要に応じて調整/微調整できます。短いタイムアウト値を設定すると（60 秒未満）、CPU の使用率が高くなるため推奨されません。詳細については、x セクションを参照してください。

この項で説明するタイムアウトは、設定に応じて変更できます。

- 動的設定のためにグローバル IP アドレスを迅速に解放する必要がある場合は、**ip nat translation timeout** コマンドを使用して、デフォルトのタイムアウトよりもタイムアウトを短く設定してください。ただし、次の手順で指定するコマンドで設定した他のタイムアウトよりも長い時間にしてください。
- TCP セッションが両側から受け取る終了 (FIN) パケットで正しく終了していない場合、またはリセット時に正しく終了しない場合は、**ip nat translation tcp-timeout** コマンドを使用してデフォルトの TCP タイムアウトを変更してください。

## 手順の概要

1. **enable**
2. **configure terminal**
3. **ip nat translation seconds**
4. **ip nat translation udp-timeout seconds**
5. **ip nat translation tcp-timeout seconds**
6. **ip nat translation finrst-timeout seconds**
7. **ip nat translation icmp-timeout seconds**
8. **ip nat translation syn-timeout seconds**
9. **end**

## 手順の詳細

### 手順

|        | コマンドまたはアクション                                                   | 目的                                           |
|--------|----------------------------------------------------------------|----------------------------------------------|
| ステップ 1 | <b>enable</b><br>例 :<br>Switch> enable                         | 特権 EXEC モードを有効にします。<br>パスワードを入力します（要求された場合）。 |
| ステップ 2 | <b>configure terminal</b><br>例 :<br>Switch# 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。                 |

|        | コマンドまたはアクション                                                                                                              | 目的                                                                                                                                                                    |
|--------|---------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ステップ 3 | <b>ip nat translation seconds</b><br>例：<br><pre>Switch(config)# ip nat translation 300</pre>                              | (任意) NAT 変換がタイムアウトになるまでの時間を変更します。<br><br>デフォルト タイムアウトは 24 時間です。これは、ハーフエントリのエージング タイムに適用されません。                                                                         |
| ステップ 4 | <b>ip nat translation udp-timeout seconds</b><br>例：<br><pre>Switch(config)# ip nat translation udp-timeout 300</pre>      | (任意) UDP タイムアウト値を変更します。                                                                                                                                               |
| ステップ 5 | <b>ip nat translation tcp-timeout seconds</b><br>例：<br><pre>Switch(config)# ip nat translation tcp-timeout 2500</pre>     | (任意) TCP タイムアウト値を変更します。<br><br>デフォルトは 24 時間です。                                                                                                                        |
| ステップ 6 | <b>ip nat translation finrst-timeout seconds</b><br>例：<br><pre>Switch(config)# ip nat translation finrst-timeout 45</pre> | (任意) Finish and Reset タイムアウト値を変更します。<br><br><b>finrst-timeout</b> : TCP セッションが finish-in (FIN-IN) 要求と finish-out (FIN-OUT) 要求の両方を受信した後の、または TCP セッションリセット後のエージング タイム。 |
| ステップ 7 | <b>ip nat translation icmp-timeout seconds</b><br>例：<br><pre>Switch(config)# ip nat translation icmp-timeout 45</pre>     | (任意) ICMP タイムアウト値を変更します。                                                                                                                                              |
| ステップ 8 | <b>ip nat translation syn-timeout seconds</b><br>例：<br><pre>Switch(config)# ip nat translation syn-timeout 45</pre>       | (任意) 同期 (SYN) タイムアウト値を変更します。<br><br>同期タイムアウトまたはエージングタイムは、TCP セッションで SYN 要求が受信された場合にのみ使用されます。同期確認応答 (SYNACK) 要求が受信されると、タイムアウトが TCP タイムアウトに変更されます。                      |
| ステップ 9 | <b>end</b><br>例：<br><pre>Switch(config-if)# end</pre>                                                                     | インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。                                                                                                                        |

# レイヤ3 ポートチャネルでのネットワークアドレス変換の設定

## 手順

---

### ステップ1 enable

例：

```
Switch> enable
```

特権 EXEC モードを有効にします。

- パスワードを入力します（要求された場合）。

### ステップ2 configure terminal

例：

```
Switch# 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 interface port-channel *port-channel-number*

例：

```
Switch(config)# interface port-channel 10
```

ポートチャネル インターフェイス モードを開始します。

### ステップ4 ip address *ip-address mask [secondary]*

例：

```
Switch(config)# ip address 10.114.11.39 255.255.255.0
```

インターフェイスのプライマリ IP アドレスを設定します。

### ステップ5 ip nat inside

例：

```
Switch(config)# ip nat inside
```

NAT の対象である内部ネットワークにインターフェイスを接続します。

### ステップ6 interface port channel *port-channel-number*

例：

```
Switch(config)# interface port-channel 11
```

ポートチャネル インターフェイス モードを開始します。

### ステップ7 ip address *ip-address mask [secondary]*

例：

```
Switch(config)# ip address 172.31.232.182 255.255.255.240
```

インターフェイスのプライマリ IP アドレスを設定します。

#### ステップ8 ip nat outside

例：

```
Switch(config)# ip nat outside
```

外部ネットワークにインターフェイスを接続します。

#### ステップ9 end

例：

```
Switch(config)# end
```

インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

## NATでのアプリケーションレベルゲートウェイの使用

NAT は、アプリケーション データ ストリームで送信元および宛先 IP アドレスを伝送しない TCP/UDP トラフィックにおいて変換サービスを実行します。送信元および宛先 IP アドレスを伝送しないプロトコルには、次のものがあります。

- HTTP
- TFTP
- Telnet
- Archie
- Finger
- ネットワーク タイム プロトコル (NTP)
- ネットワーク ファイル システム (NFS)
- リモートログイン (rlogin)
- リモートシェル (rsh)
- リモートコピー (rcp)

アドレス/ポート情報をペイロードで搬送するアプリケーションは、NAT アプリケーション レベル ゲートウェイ (ALG) により、NAT ドメイン全体で正しく機能できます。パケット ヘッダ内のアドレス/ポートの通常の変換に加えて、ALG はペイロードに存在するアドレス/ポートの変換も処理し、一時マッピングを設定します。

## NAT の設定のベストプラクティス

- 静的規則と動的規則の両方が設定されている場合は、規則に指定されているローカルアドレスが重複していないことを確認してください。このような重複の可能性がある場合は、静的規則が使用するアドレスを動的規則に関連付けられている ACL で除外してください。同様に、グローバルアドレス間の重複もなくする必要があります。重複していると、望ましくない動作が生じることがあります。
- NAT 規則に関連付けられている ACL では、**permit ip any any** などの範囲の広いフィルタリングを使用しないでください。このようなフィルタリングは、必要のないパケットを変換することがあります。
- 複数の NAT 規則でアドレス プールを共有しないでください。
- 静的 NAT と動的プールで同じ内部グローバル アドレスを定義しないでください。これを行うと、望ましくない結果を招くことがあります。
- NAT に関連付けられているデフォルトのタイムアウト値を変更する場合は、慎重に行ってください。タイムアウト値を短くすると、CPU の使用率が高くなる可能性があります。
- 変換エントリを手動でクリアする場合は、アプリケーションセッションが中断されることがあるため、慎重に行ってください。
- NAT 対応インターフェイスを通過する ALG パケットは、パケットが変換されるかどうかに関係なく、CPU にパントされます。そのため、NAT トラフィック専用のインターフェイスを使用することをお勧めします。NAT 変換する必要がない他のタイプのトラフィックにはすべて、別のインターフェイスを使用します。

## ネットワークアドレス変換の設定例

### 内部送信元アドレスの静的変換の設定

次の例では、10.114.11.0 ネットワークからアドレス指定される内部ホストがグローバルに一意的な 172.31.233.208/28 ネットワークにどのように変換されるかを示しています。その後、10.114.11.0 ネットワーク（本物の 10.114.11.0 ネットワーク）の外部ホストから送信されたパケットは、10.0.1.0/24 ネットワーク由来に見えるように変換されます。

```
ip nat pool net-208 172.31.233.208 172.31.233.223 prefix-length 28
ip nat pool net-10 10.0.1.0 10.0.1.255 prefix-length 24
ip nat inside source list 1 pool net-208
ip nat outside source list 1 pool net-10
!
interface gigabitethernet 1/0/1
 ip address 172.31.232.182 255.255.255.240
 ip nat outside
!
interface gigabitethernet 1/0/2
 ip address 10.114.11.39 255.255.255.0
```

```
ip nat inside
!
```

```
access-list 1 permit 10.114.11.0 0.0.0.255
```

次に、重複するローカルアドレスを変換する静的 VRF 対応 NAT 設定の例を示します。

```
ip nat inside source static 192.168.121.33 10.2.2.1 vrf vrf1
ip nat inside source static 192.168.121.33.10.2.2.2 vrf vrf2
```

## 内部送信元アドレスの動的変換の設定

次の例では、192.168.1.0 または 192.168.2.0 ネットワークのいずれかのネットワークからアドレス指定される内部ホストがグローバルに一意的な 172.31.233.208/28 ネットワークにどのように変換されるかを示しています。

```
ip nat pool net-208 172.31.233.208 172.31.233.223 prefix-length 9
ip nat inside source list 1 pool net-208
!
```

```
interface gigabitethernet 1/0/1
ip address 172.31.232.182 255.255.255.240
ip nat outside
```

```
!
```

```
interface gigabitethernet 1/0/2
ip address 192.168.1.94 255.255.255.0
ip nat inside
```

```
!
```

```
access-list 1 permit 192.168.1.0 0.0.0.255
```

```
access-list 1 permit 192.168.2.0 0.0.0.255
```

```
!
```

次に、重複するローカルアドレスを変換する動的 VRF 対応 NAT 設定の例を示します。

```
ip nat inside source list 1 interface gigabitethernet 1/0/1 vrf vrf1 overload
!
```

```
ip route vrf vrf1 0.0.0.0 0.0.0.0 192.168.1.1
```

```
!
```

```
access-list 1 permit 10.1.1.1.0 0.0.0.255
```

```
!
```

```
ip nat inside source list 1 interface gigabitethernet 1/0/2 vrf vrf1 overload
```

```
!
```

```
ip route vrf vrf1 0.0.0.0 0.0.0.0 172.16.1.1 global
```

```
access-list 1 permit 10.1.1.0 0.0.0.255
```

```
!
```

## NAT のトラブルシューティング

ここでは、NAT のトラブルシューティングと確認のための基本的な手順について説明します

- NAT で実現できることを明確に定義する。
- **show ip nat translation** コマンドで、正しい変換テーブルが存在していることを確認する。
- **show ip nat translation verbose** コマンドで、タイマーの値が正しく設定されていることを確認する。
- **show ip access-list** コマンドで、NAT の ACL 値をチェックする。
- **show ip nat statistics** コマンドで、NAT の全体的な設定をチェックする。

- **clear ip nat translation** コマンドで、タイマーの期限が切れるより早く NAT 変換テーブルのエントリをクリアする。
- **debug nat ip** と **debug nat ip detailed** コマンドを使用して、NAT 設定をデバッグする。

NAT のトラブルシューティングの詳細については、Cisco.com の「[Verifying NAT Operation and Basic NAT Troubleshooting](#)」を参照してください。

## ネットワークアドレス変換の機能履歴

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

| リリース                          | 機能                                                             | 機能説明                                                                                                                                                                                                                                                                                                  |
|-------------------------------|----------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Cisco IOS XE Cupertino 17.7.1 | レイヤ3 ネットワークアドレス変換 (Cisco Catalyst IE9300 Rugged Series Switch) | <p>NATによって、未登録IPアドレスを使用するプライベートIPネットワークをインターネットに接続できます。NATはデバイス上で動作し、通常は2つのネットワークを同時に接続して、パケットが一方のネットワークに転送される前に、内部ネットワークのプライベートアドレスをグローバルルーティング可能アドレスに変換します。</p> <p>この機能のサポートは、次のスイッチモデルで導入されました。</p> <ul style="list-style-type: none"> <li>• IE-9310-26S2C-A</li> <li>• IE-9320-26S2C-A</li> </ul> |



## 第 3 章

# VLAN マッピング

- [VLAN マッピング \(51 ページ\)](#)
- [VLAN マッピング設定時の注意事項 \(53 ページ\)](#)
- [VLAN マッピングの設定 \(54 ページ\)](#)
- [VLAN マッピングの機能履歴 \(59 ページ\)](#)

## VLAN マッピング

VLAN マッピングの典型的な展開においては、サービスプロバイダーは、遠隔拠点にある顧客のスイッチをあたかもローカル拠点の一部のように見せることを含む透過的なスイッチングインフラを提供することを求められます。これにより、顧客は、同じ VLAN ID 空間を使用し、プロバイダーネットワークを介してレイヤ2制御プロトコルを一貫して実行できます。このようなシナリオでは、サービスプロバイダーは自身の割り当てた VLAN ID を顧客に強制しないことが推奨されます。

変換済み VLAN ID (S-VLAN) を確立する方法のひとつは、顧客のネットワークに接続されたトランクポートで、顧客 VLAN をサービスプロバイダー VLAN にマッピングすることです (VLAN ID マッピングと呼ばれます)。ポートに入るパケットは、ポート番号とパケットの元の顧客 VLAN-ID (C-VLAN) に基づいて、サービスプロバイダー VLAN (S-VLAN) にマッピングされます。

サービスプロバイダーの内部割り当ては、顧客 VLAN と競合する場合があります。顧客のトラフィックを分離するために、サービスプロバイダーは、トラフィックがクラウドにある間、特定の VLAN を別の VLAN にマッピングできます。

### サポート対象スイッチ

VLAN マッピングは、Cisco Catalyst IE9300 Rugged Series Switches のすべてのモデルでサポートされています。この機能は、Network Essentials または Network Advantage ライセンスで使用できます。

## 展開例

スイッチのすべての転送処理は、C-VLAN 情報ではなく、S-VLAN 情報を使用して実行されます。これは、VLAN ID が、入力時に S-VLAN にマッピングされるためです。



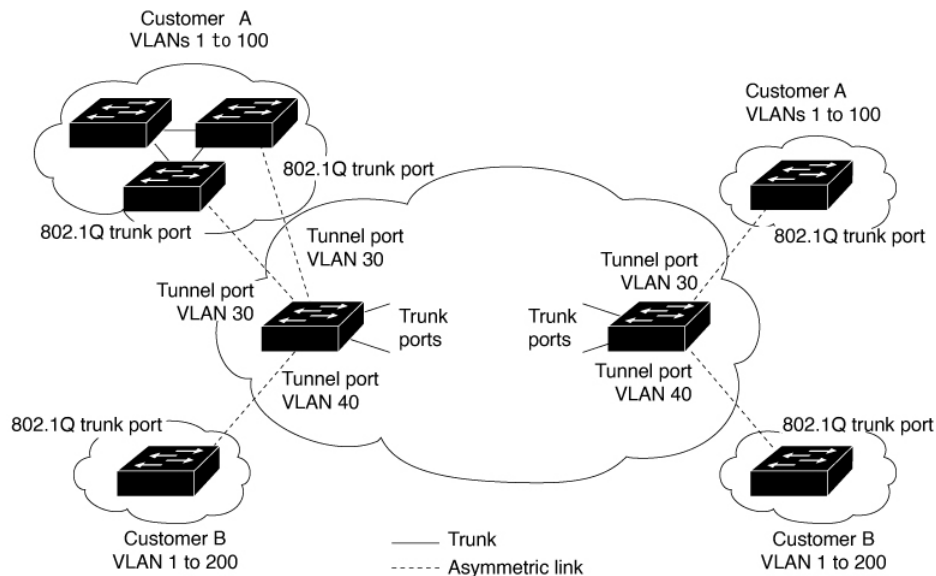
- (注) VLAN マッピングが設定されているポートで機能を設定する場合は、顧客 VLAN-ID (C-VLAN) ではなく S-VLAN を常に使用します。現時点では、1 対 1 の VLAN マッピングはサポートされていません。

VLAN マッピングが設定されているインターフェイスでは、指定された C-VLAN パケットはポートに入るとき、指定された S-VLAN にマッピングされます。パケットがポートから出る場合も同様に、顧客 C-VLAN にマッピングが行われます。

スイッチはトランクポートにおける次の種類の VLAN マッピングをサポートします。

## 顧客 VLAN からサービスプロバイダー VLAN へのマッピング

図 11: QnQ トポロジ



図は、顧客 A と顧客 B がサービスプロバイダーネットワークの別サイドにおいて複数サイトで同じ VLAN を使用するトポロジを示しています。サービスプロバイダーバックボーン経由でパケットを伝送できるように、顧客 VLAN ID をサービスプロバイダー VLAN ID にマッピングします。サービスプロバイダーバックボーンの反対側で、そちら側の顧客拠点で使用するために元の顧客 VLAN ID に戻されます。サービスプロバイダーネットワークのそれぞれの側の顧客接続ポートで同じ VLAN マッピングセットを設定します。

## 選択的 QnQ

選択的 QnQ は、UNI に入ろうとする指定の顧客 VLAN を指定の S-VLAN ID にマッピングします。S-VLAN ID は入り口で未変更の C-VLAN に追加され、パケットはサービス プロバイダー ネットワーク内を二重タグ付きで伝送されます。出口では、S-VLAN ID が削除され、顧客 VLAN-ID がパケットに保持されます。デフォルトでは、指定した顧客 VLAN に一致しないパケットは破棄されます。

## トランクポートでの QnQ

トランクポートの QnQ は、UNI に入る顧客 VLAN すべてを指定の S-VLAN ID にマッピングします。選択的 QnQ と同様に、パケットには二重タグが付けられ、出口では S-VLAN ID が削除されます。

## VLAN マッピング設定時の注意事項



(注) デフォルトで、VLAN マッピングは設定されていません。

ガイドラインは次のとおりです。

- VLAN マッピングが EtherChannel で有効になっている場合、設定は EtherChannel バンドルのすべてのメンバーポートには適用されず、EtherChannel インターフェイスにのみ適用されます。
- VLAN マッピングが EtherChannel で有効であり、競合するマッピングがメンバーポートで有効になっている場合、ポートは EtherChannel から削除されます。
- ポートのモードが「トランク」モード以外に変更されると、EtherChannel のメンバーポートは EtherChannel バンドルから削除されます。
- 一貫して制御トラフィックを処理するには、次のようにレイヤ2プロトコルトネリングを有効にするか（推奨）、

```
!
Device(config)# interface Gig 1/0/1
Device(config-if)# switchport mode access
Device(config-if)# l2protocol-tunnel stp
Device(config-if)# end
```

または、次のようにスパニングツリーの BPDU フィルタを挿入します。

```
Current configuration : 153 bytes
!
Device(config)# interface Gig 1/0/1
Device(config-if)# switchport mode trunk
Device(config-if)# switchport vlan mapping 10 20
Device(config-if)# spanning-tree bpdufilter enable
Device(config-if)# end
```

- デフォルトのネイティブ VLAN、ユーザ設定のネイティブ VLAN、および予約済みの VLAN（範囲 1002 - 1005）は、VLAN マッピングに使用できません。
- PVLAN サポートは、VLAN マッピングが設定されている場合は使用できません。

## 選択的 QnQ の設定ガイドライン

- S-VLAN は、作成済み、かつ、選択的 QnQ が設定されているトランクポートの許可 VLAN リストに存在する必要があります。
- 選択的 QnQ が設定されている場合、デバイスは CDP、STP、LLDP、および VTP のレイヤ 2 プロトコルトネリングをサポートします。
- IP ルーティングは、選択的 QnQ 対応ポートではサポートされません。
- IPSG は、選択的 QnQ 対応ポートではサポートされません。

## トランクポートでの QnQ の設定ガイドライン

- S-VLAN は、作成済み、かつ、トランクポートでの QnQ が設定されているトランクポートの許可 VLAN リストに存在する必要があります。
- トランクポートでの QnQ が設定されている場合、デバイスは CDP、STP、LLDP、および VTP のレイヤ 2 プロトコルトネリングをサポートします。
- 入力および出力 SPAN、および RSPAN は、QnQ が有効になっているトランクポートでサポートされます。
- QnQ を有効にすると、SPAN フィルタリングを有効にして、マッピングされた VLAN（S-VLAN）上のトラフィックのみを監視できます。
- IGMP スヌーピングは C-VLAN ではサポートされません。

## VLAN マッピングの設定

ここでは、VLAN マッピングの設定方法について説明します。

## トランクポートでの選択的 QnQ の設定

トランクポートで選択的 QnQ の VLAN マッピングを設定するには、次の手順を実行します。



---

(注) 同じインターフェイスでは、1対1のマッピングと選択的 QnQ を設定できません。

---

## 手順の概要

1. **enable**
2. **configure terminal**
3. **interface *interface-id***
4. **switchport mode trunk**
5. **switchport vlan mapping *vlan-id* dot1q-tunnel *outer vlan-id***
6. **switchport vlan mapping default dot1q-tunnel *vlan-id***
7. **exit**
8. **spanning-tree bpdudfilter enable**
9. **end**
10. **show interfaces *interface-id* vlan mapping**
11. **copy running-config startup-config**

## 手順の詳細

## 手順

|        | コマンドまたはアクション                                                                                                                                                  | 目的                                                                                                                                  |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------|
| ステップ 1 | <b>enable</b><br>例：<br>Device> <b>enable</b>                                                                                                                  | 特権 EXEC モードを有効にします。<br>パスワードを入力します（要求された場合）。                                                                                        |
| ステップ 2 | <b>configure terminal</b><br>例：<br>Device# <b>configure terminal</b>                                                                                          | 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 | <b>interface <i>interface-id</i></b><br>例：<br>Device(config)# <b>interface gigabitethernet1/0/1</b>                                                           | サービス プロバイダー ネットワークに接続されるインターフェイスのインターフェイス コンフィギュレーション モードを開始します。物理インターフェイスまたは EtherChannel ポート チャンネルを入力できます。                        |
| ステップ 4 | <b>switchport mode trunk</b><br>例：<br>Device(config-if)# <b>switchport mode trunk</b>                                                                         | 指定したインターフェイスをトランク ポートとして設定します。                                                                                                      |
| ステップ 5 | <b>switchport vlan mapping <i>vlan-id</i> dot1q-tunnel <i>outer vlan-id</i></b><br>例：<br>Device(config-if)# <b>switchport vlan mapping 16 dot1q-tunnel 64</b> | マッピングする VLAN ID を入力します。<br><br>• <i>vlan-id</i> : 顧客のネットワークからスイッチに入る顧客 VLAN ID (C-VLAN)。指定できる範囲は 1 ~ 4094 です。VLAN-ID のストリングを入力できます。 |

|         | コマンドまたはアクション                                                                                                                                    | 目的                                                                                                                                                                                                                                                  |
|---------|-------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|         |                                                                                                                                                 | <ul style="list-style-type: none"> <li>outer-vlan-id : サービス プロバイダー ネットワークの外部 VLAN ID (S-VLAN)。指定できる範囲は 1 ~ 4094 です。</li> </ul> <p>VLAN マッピング設定を削除するには、このコマンドの no 形式を使用します。 <b>no switchport vlan mapping all</b> コマンドを入力すると、すべてのマッピング設定が削除されます。</p> |
| ステップ 6  | <b>switchport vlan mapping default dot1q-tunnel vlan-id</b><br>例 :<br>Device(config-if)# <b>switchport vlan mapping default dot1q-tunnel 22</b> | <p>ポート上のすべてのマッピングされていないパケットが、指定された S-VLAN で転送されるように指定します。</p> <p>デフォルトでは、マッピングされた VLAN に一致しないパケットは破棄されます。</p> <p>タグなしトラフィックは破棄されずに転送されます。</p>                                                                                                       |
| ステップ 7  | <b>exit</b><br>例 :<br>Device(config-if)# <b>exit</b>                                                                                            | グローバル コンフィギュレーション モードに戻ります。                                                                                                                                                                                                                         |
| ステップ 8  | <b>spanning-tree bpdupfilter enable</b><br>例 :<br>Device(config)# <b>spanning-tree bpdupfilter enable</b>                                       | <p>スパニングツリーの BPDU フィルタを挿入します。</p> <p>(注)<br/>           一貫して制御トラフィックを処理するには、レイヤ 2 プロトコルトンネリングを有効にするか (推奨)、またはスパニングツリーの BPDU フィルタを挿入します。</p>                                                                                                         |
| ステップ 9  | <b>end</b><br>例 :<br>Device(config)# <b>end</b>                                                                                                 | 特権 EXEC モードに戻ります。                                                                                                                                                                                                                                   |
| ステップ 10 | <b>show interfaces interface-idvlan mapping</b><br>例 :<br>Device# <b>show interfaces gigabitethernet1/0/1 vlan mapping</b>                      | 設定を確認します。                                                                                                                                                                                                                                           |
| ステップ 11 | <b>copy running-config startup-config</b><br>例 :<br>Device# <b>copy running-config startup-config</b>                                           | (任意) コンフィギュレーション ファイルに設定を保存します。                                                                                                                                                                                                                     |

## 例

次の例では、ポートに選択的 QnQ マッピングを設定して、C-VLAN ID が 2～5 のトラフィックが、S-VLAN ID が 100 であるスイッチに入るようにする方法を示します。デフォルトでは、その他の VLAN ID のトラフィックは破棄されます。

```
Device(config)# interface GigabitEthernet1/0/1
Device(config-if)# switchport vlan mapping 2-5 dot1q-tunnel 100
Device(config-if)# exit
```

次の例では、ポートに選択的 QnQ マッピングを設定して、C-VLAN ID が 2～5 のトラフィックが、S-VLAN ID が 100 であるスイッチに入るようにする方法を示します。他の VLAN ID のトラフィックは、S-VLAN ID 200 で転送されます。

```
Device(config)# interface GigabitEthernet1/0/1
Device(config-if)# switchport vlan mapping 2-5 dot1q-tunnel 100
Device(config-if)# switchport vlan mapping default dot1q-tunnel 200
Device(config-if)# exit
```

```
Device# show vlan mapping
Total no of vlan mappings configured: 5
Interface Hu1/0/50:
VLANs on wire Translated VLAN Operation

2-5 100 selective QinQ
* 200 default Q
```

## トランクポートでの QnQ の設定

トランクポートで QnQ の VLAN マッピングを設定するには、次の作業を行います。

### 手順の概要

1. **enable**
2. **configure terminal**
3. **interface interface-id**
4. **switchport mode trunk**
5. **switchport vlan mapping default dot1q-tunnel vlan-id**
6. **exit**
7. **spanning-tree bpdupfilter enable**
8. **end**
9. **show interfaces interface-idvlan mapping**
10. **copy running-config startup-config**

## 手順の詳細

## 手順

|        | コマンドまたはアクション                                                                                                                                   | 目的                                                                                                                         |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------|
| ステップ 1 | <b>enable</b><br>例：<br>Device> <b>enable</b>                                                                                                   | 特権 EXEC モードを有効にします。<br>パスワードを入力します（要求された場合）。                                                                               |
| ステップ 2 | <b>configure terminal</b><br>例：<br>Device# <b>configure terminal</b>                                                                           | 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 | <b>interface interface-id</b><br>例：<br>Device(config)# <b>interface gigabitethernet1/0/1</b>                                                   | サービス プロバイダー ネットワークに接続される インターフェイスのインターフェイス コンフィギュレーション モードを開始します。物理 インターフェイス または EtherChannel ポート チャンネルを入力できます。            |
| ステップ 4 | <b>switchport mode trunk</b><br>例：<br>Device(config-if)# <b>switchport mode trunk</b>                                                          | 指定した インターフェイス を トランク ポート として 設定 します。                                                                                       |
| ステップ 5 | <b>switchport vlan mapping default dot1q-tunnel vlan-id</b><br>例：<br>Device(config-if)# <b>switchport vlan mapping default dot1q-tunnel 16</b> | ポート上のすべてのマッピングされていない C-VLAN パケットが、指定された S-VLAN で転送されるように指定します。                                                             |
| ステップ 6 | <b>exit</b><br>例：<br>Device(config-if)# <b>exit</b>                                                                                            | グローバル コンフィギュレーション モードに戻ります。                                                                                                |
| ステップ 7 | <b>spanning-tree bpdupfilter enable</b><br>例：<br>Device(config)# <b>spanning-tree bpdupfilter enable</b>                                       | スパニングツリーの BPDU フィルタを挿入します。<br><br>(注)<br>一貫して制御トラフィックを処理するには、レイヤ 2 プロトコル トンネリング を有効にするか (推奨)、またはスパニングツリーの BPDU フィルタを挿入します。 |
| ステップ 8 | <b>end</b><br>例：<br>Device(config)# <b>end</b>                                                                                                 | 特権 EXEC モードに戻ります。                                                                                                          |

|         | コマンドまたはアクション                                                                                                                       | 目的                              |
|---------|------------------------------------------------------------------------------------------------------------------------------------|---------------------------------|
| ステップ 9  | <b>show interfaces <i>interface-id</i> vlan mapping</b><br>例 :<br>Device# <b>show interfaces gigabitethernet1/0/1 vlan mapping</b> | 設定を確認します。                       |
| ステップ 10 | <b>copy running-config startup-config</b><br>例 :<br>Device# <b>copy running-config startup-config</b>                              | (任意) コンフィギュレーション ファイルに設定を保存します。 |

### 例

次の例では、ポートで QnQ マッピングを設定して、任意の VLAN ID のトラフィックが、S-VLAN ID 200 で転送されるようにする方法を示します。

```
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# switchport vlan mapping default dot1q-tunnel 200
Device(config-if)# exit
```

## VLAN マッピングの機能履歴

次の表に、この章で説明する機能のリリースおよび関連情報を示します。これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

| リリース                 | 機能            | 機能情報             |
|----------------------|---------------|------------------|
| Cisco IOS XE 17.13.1 | 選択的 QnQ       | 機能のサポートが追加されました。 |
|                      | トランクポートでの QnQ |                  |



## 翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。