レイヤ 2 NAT ソフトウェア設定ガイド（IE 2000/IE 4000/IE 4010/IE 5000 スイッチ用）

改訂：2021 年 9 月 28 日

レイヤ 2 NAT の設定

このドキュメントでは、Cisco Industrial Ethernet 2000 シリーズ、Cisco Industrial Ethernet 4000 シリーズ、Cisco Industrial Ethernet 4010 シリーズ、および Cisco Industrial Ethernet 5000 シリーズ スイッチでのレイヤ 2 ネットワークアドレス変換（NAT）の設定について詳しく説明します。

L2 ネットワークアドレス変換（NAT）について

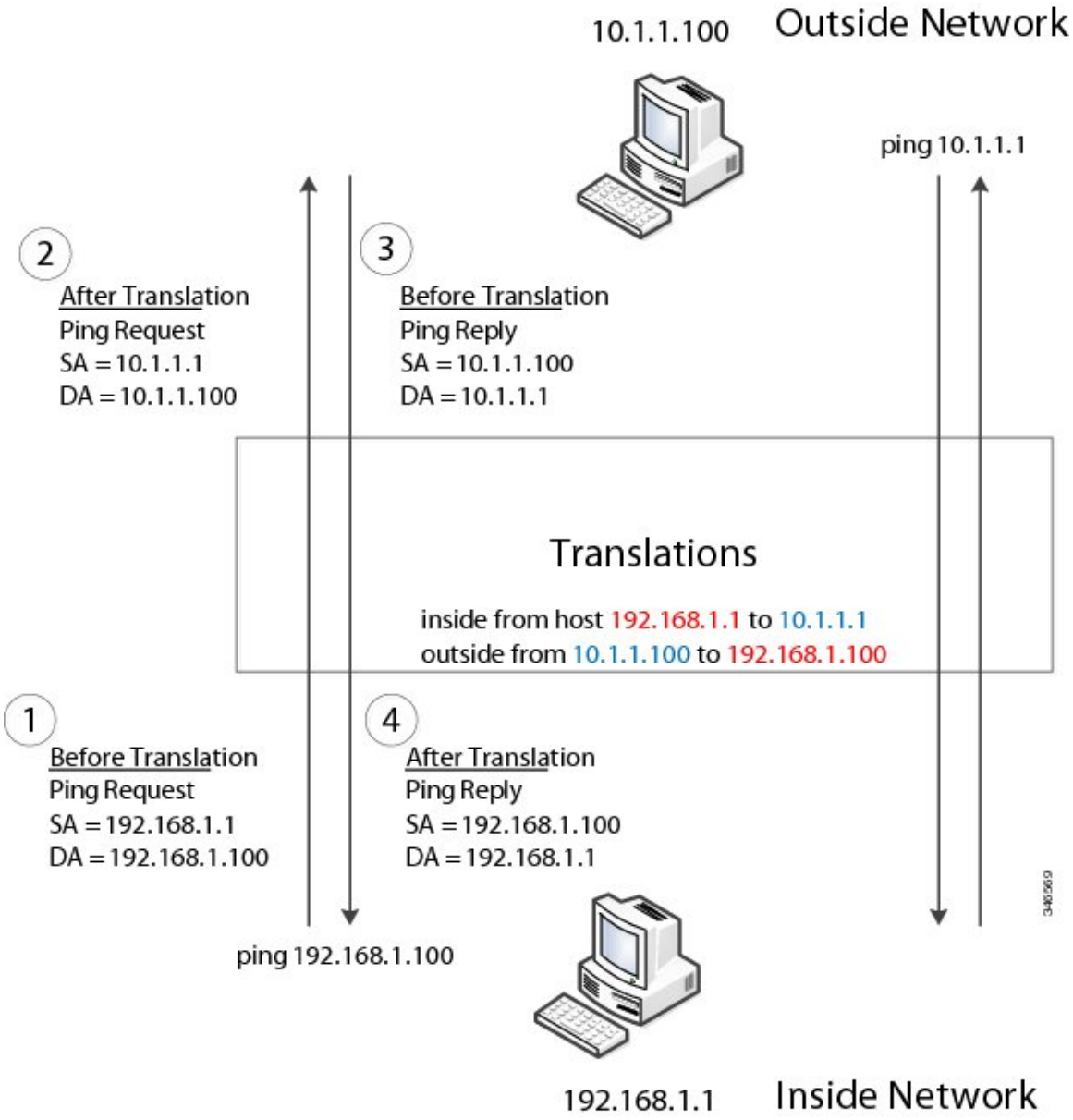
1 対 1（1：1）レイヤ 2 NAT は、固有のパブリック IP アドレスを既存のプライベート IP アドレス（エンド デバイス）に割り当てるサービスであり、エンド デバイスがプライベートとパブリック サブネット上で通信できるようになります。このサービスは、NAT 対応デバイスで設定され、エンドデバイスに物理的にプログラムされた IP アドレスのパブリックでの「エイリアス」です。これは、通常 NAT デバイスでテーブルとして表されます。

レイヤ 2 NAT には、プライベートからパブリックおよびパブリックからプライベートへサブネットの変換を定義できる 2 種類の変換テーブルがあります。レイヤ 2 NAT は、一貫した高レベルの（bump-in-the-wire）ワイヤスピードのパフォーマンス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。

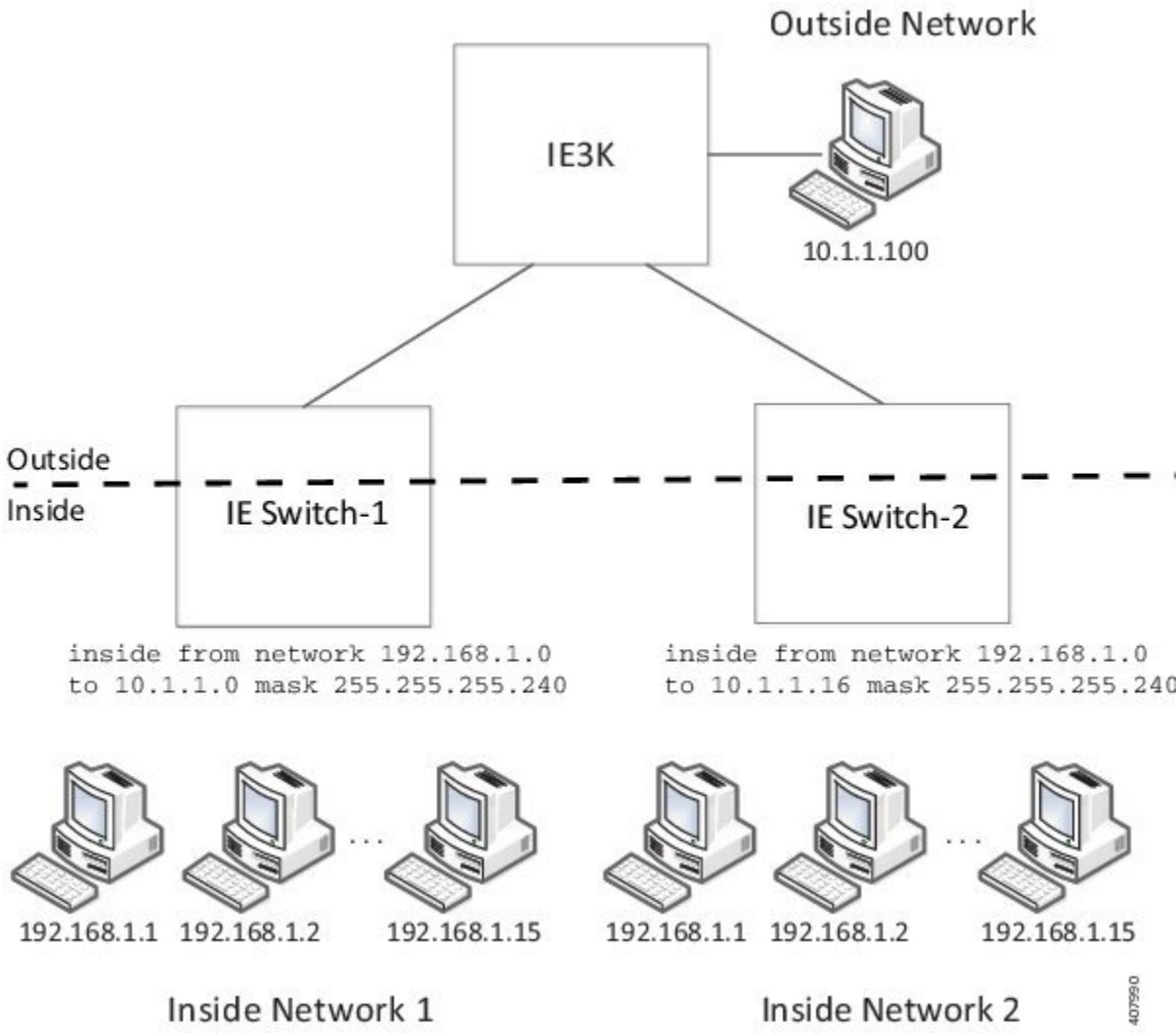
次に、レイヤ 2 NAT で 192.168.1.x ネットワークのセンサーと 10.1.1.x ネットワークの通信制御装置間のアドレスを変換する例を示します。

1. 192.168.1.x ネットワークは内部/内部 IP アドレス空間、10.1.1.x ネットワークは外部/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

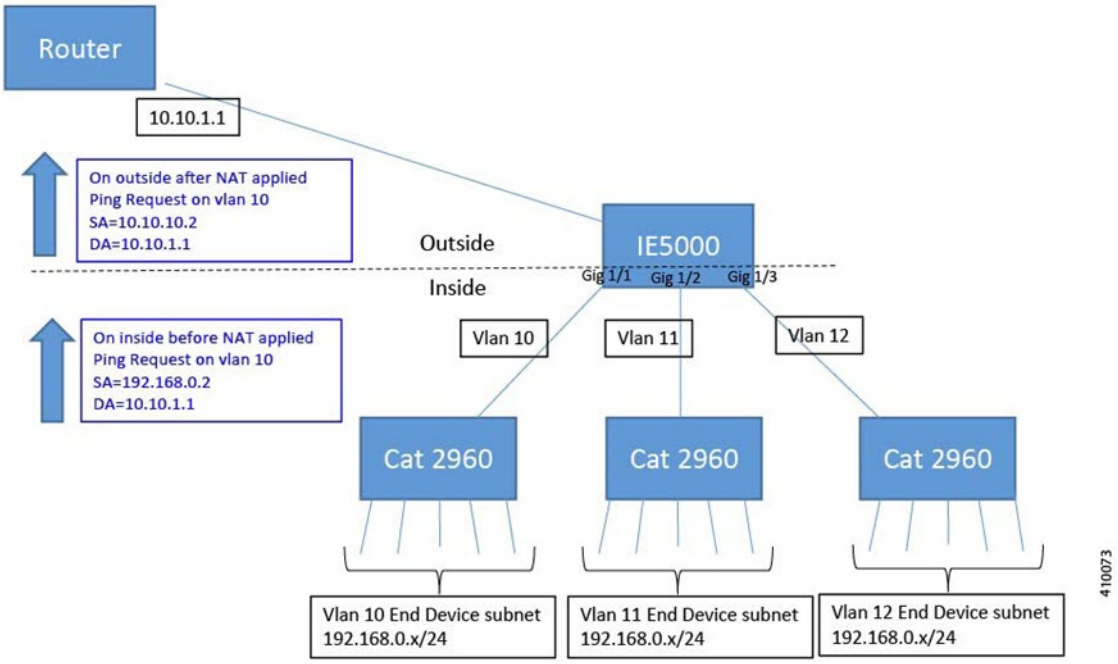


大規模なノードでは、サブネット内のすべてのデバイスに対してまとめて変換をイネーブルにできます。この場合、内部ネットワーク 1 からのアドレスは 10.1.1.0/28 サブネットで外部アドレスに変換することができ、内部ネットワーク 2 からのアドレスは 10.1.1.16/28 サブネットで外部アドレスに変換することができます。各サブネットのアドレスはすべて 1 つのコマンドを使って変換できます。



次の図に、配布レベルでの IE 5000 NAT の設定を示します。この例では、IE 5000 は Catalyst 2960 スイッチを介してプライベートネットワーク内のデバイスに接続します。Catalyst スイッチは、アクセスレイヤで NAT を実行していません。IE5000 では、3 つの異なるアクセススイッチ用の 3 つのインターフェイスで L2 NAT を実行しています。IE スイッチでは、128 個の L2 NAT インスタンスをサポートできます。この例では、128 個のうち 3 個のみ表示されています。サブネット全体を 1 つの L2 NAT インスタンスで設定できます。

図 *2 : IE 5000* での *NAT*



上の図に表示されている IE 5000 NAT の設定は次のとおりです。

```
Instance10:
 inside from network 192.168.0.0 to 10.10.10.0 mask 255.255.255.0
 outside from host 10.10.10.254 to 192.168.9.254 gateway
Instance11:
 inside from network 192.168.0.0 to 10.10.11.0 mask 255.255.255.0
 outside from host 10.10.11.254 to 192.168.9.254 gateway
Instance12:
 inside from network 192.168.0.0 to 10.10.12.0 mask 255.255.255.0
 outside from host 10.10.12.254 to 192.168.9.254 gateway
.
.
.
Interface vlan 10
 ip address 10.10.10.254 mask 255.255.255.0
Interface vlan 11
 ip address 10.10.11.254 mask 255.255.255.0
Interface vlan 12
Ip address 10.10.12.254 mask 255.255.255.0
Interface gig 1/1
 switchport access vlan 10
 l2nat instance10
Interface gig 1/2
 switchport access vlan 11
 l2nat instance11
Interface gig 1/3
 switchport access vlan 12
 l2nat instance12
```

前提条件

- IE 2000：レイヤ 2 NAT は Cisco IOS 15.0(2)EB 以降で使用可能な拡張 LAN Base フィーチャセットに含まれています。
- IE 4000：レイヤ 2 NAT は Cisco IOS 15.2.(2)EA 以降で使用可能な LAN Base フィーチャセットに含まれています。
- IE 4010：レイヤ 2 NAT は Cisco IOS 15.2(4)EC1 以降で使用可能な LAN Base フィーチャセットに含まれています。
- IE 5000：レイヤ 2 NAT は Cisco IOS 15.2(2)EB 以降で使用可能な LAN Base フィーチャセットに含まれています。

注意事項と制約事項

- IPv4 アドレスのみ変換できます。
- 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。未変換の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 トラフィックを許可することができます。
- 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。
- 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 ではパブリック IP アドレスを節約できません。
- 埋め込まれた IP アドレスが変換されないため、FTP トラフィックは機能しません。
- 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。
- ARP、ICMP などの特定のプロトコルは、レイヤ 2 NAT 越しに透過的に機能しませんが、これはデフォルトで「フィックスアップ」されます。「フィックスアップ」とは、プロトコルが機能するように IP パケットのペイロードに組み込まれた IP アドレスが変更されることを意味します。
- NAT インスタンスの設定をサポートするインターフェイスは次のとおりです。
  - IE2000：Gig 1/1 および Gig 1/2（アップリンク）
  - IE4000：Gig 1/1 ー Gig 1/4（アップリンク）
  - IE4010：すべてのインターフェイスで L2NAT をサポートできます。IE4010 には、インターフェイスグループの制限があります。Gig 1/1 ー 6 および Gig 1/13 ー 1/18 のインターフェイス（左端の 12 個のインターフェイス）のうち、NAT インスタンスを同時にサポートできるインターフェイスは 4 つのみです。また、右端のインターフェイス、Gig 1/7 ～ 1/12、Gig 1/19 ～ 1/24、および Gig 1/25 ～ 1/28 のうち、NAT インスタンスを同時にサポートできるインターフェイスは 4 つのみです。
  - IE5000：すべてのインターフェイスで L2NAT をサポートできます。IE5000 には、インターフェイスグループの制限があります。Gig 1/1 ー 1/6 および Gig 1/13 ー 1/18 のインターフェイス（左端の 12 個のインターフェイス）のうち、NAT インスタンスを同時にサポートできるインターフェイスは 4 つのみです。また、右端のインターフェイス、Gig 1/7 ～ 12、Gig 1/19 ～ 1/24、および TenGig 1/1 ～ 1/4 のうち、NAT インスタンスを同時にサポートできるインターフェイスは 4 つのみです。

（注） IE4010 プラットフォームおよび IE5000 プラットフォームのダウンリンクポート（Gig 1/1 ー Gig 1/24）で L2NAT インスタンスを設定する場合は、対応する変換マップの「内部」および「外部」IP アドレスを、アップリンクポート（Gig 1/25、28 または TenGig 1/1 ー 1/4）の変換マップと比較して逆の順序で設定する必要があります。

- ダウンリンクポートには、VLAN、トランク、レイヤ 2 チャネルなどがあります。
- スイッチには、128 のレイヤ 2 NAT インスタンスを設定できます。
- レイヤ 2 NAT 設定では最大 128 の VLAN が利用できます。
- 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 上にはありません。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。
- L2NAT 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ことを推奨します。

デフォルト設定

機能	デフォルト設定
一致しないトラフィックまたは変換するように設定されていないトラフィック タイプのパケットの許可またはドロップ	すべての一致しない、マルチキャストの IGMP パケットをドロップする。
プロトコル フィックスアップ	フィックスアップは、ARP および ICMP に対してイネーブルになっています。

レイヤ 2 NAT の設定

アドレスの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。その後、インターフェイスおよび VLAN にこれらのインスタンスを接続します。一致しないトラフィックと変換するよう設定されていないトラフィック タイプでは、トラフィックの許可またはドロップを選択できます。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（設定の確認 （9 ページ）を参照）。

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、基本的な内部から外部への通信の例 （9 ページ）および重複する IP アドレスの例 （11 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* [**gateway**]

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。**gateway** キーワードはオプションであり、デバイスマネージャの利用時にのみ使用されます。

ステップ 5　NAT 変換によって ICMP および IGMP の変換が修正されます。デフォルトでは、ARP と ICMP の両方のフィックスアップが有効になっているため、通常はデフォルトを変更しない限りこのコマンドは必要ありません。

fixup arp | icmp | all

（注）　ICMP では、ICMP エラーメッセージに対するフィックスアップのみがサポートされます。

ステップ 6　（オプション）未変換のユニキャストトラフィックを許可します（デフォルトではドロップされます）。

permit { **multicast** | **igmp** | **all** }

ステップ 7　config-l2nat モードを終了します。

exit

ステップ 8　指定したインターフェイス（IE2000 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 9　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 10　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

設定の確認

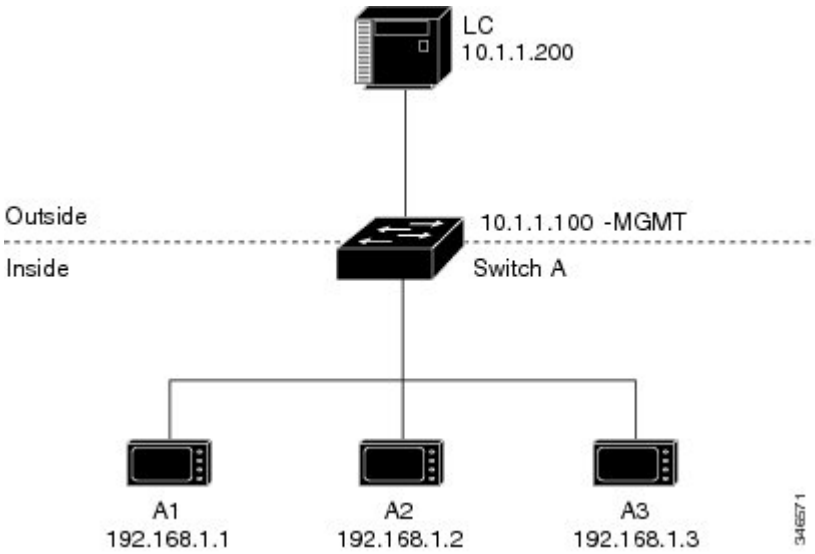
レイヤ 2 NAT が正常に動作し、接続されていることを確認するには、エンドデバイスに設定されている実際の IP アドレスではなく、レイヤ 2 NAT 変換マップで設定されている変換済み IP アドレスを ping します。レイヤ 2 NAT 設定を表示するには、以下に示す **show** コマンドを使用します。

コマンド	目的
show l2nat instance	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。
show l2nat interface	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。
show l2nat statistics	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。
show l2nat statistics interface	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。
debug l2nat	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イネーブルにします。

基本的な内部から外部への通信の例

ここでは、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 *3*：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。

次の表は、このシナリオの設定作業を示しています。レイヤ 2 NAT インスタンスが作成され、2 つの変換エントリを追加し、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イネーブルです。

（注） この例は、IE 2000 スイッチに基づいています。IE 4000 および IE 5000 スイッチでは、インターフェイスの番号が異なる場合があります。

表 *1*：基本的な内部から外部への *Cisco* スイッチ *A* の設定例

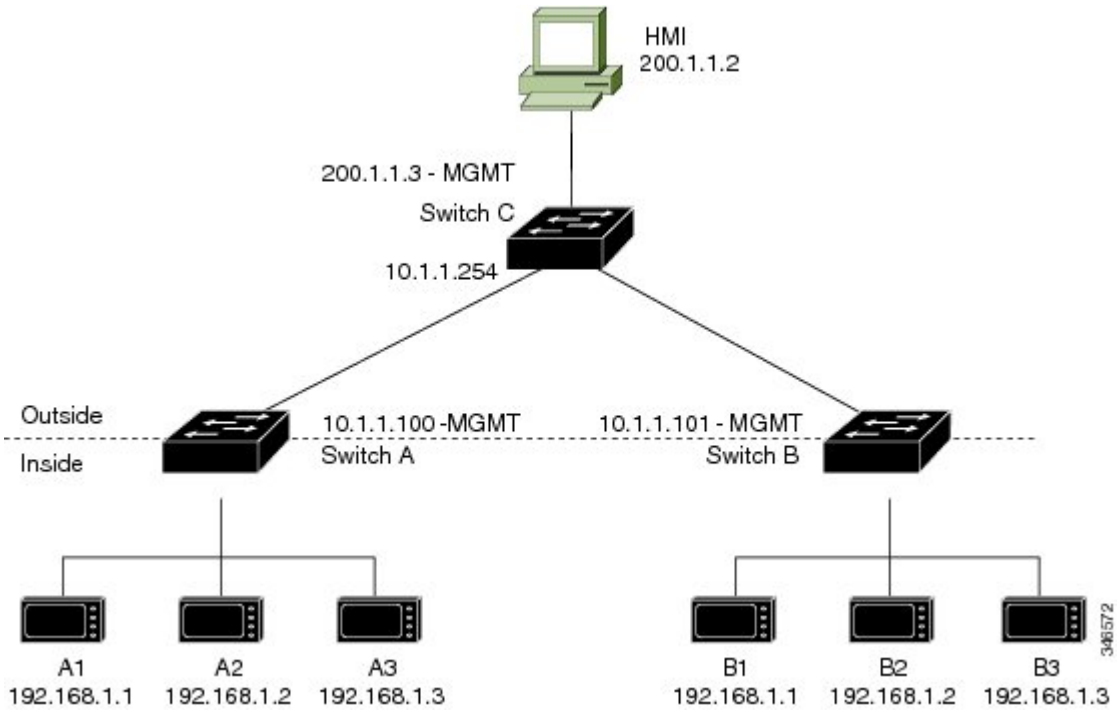
	コマンド	目的
1.	Switch# **configure**	グローバル コンフィギュレーション モードを開始します。
2.	Switch(config)# **l2nat instance A-LC**	A-LC という新しいレイヤ 2 NAT インスタンスを作成します。
3.	Switch(config-l2nat)# **inside from host 192.168.1.1 to 10.1.1.1**	A1 の内部アドレスを外部アドレスへ変換します。
4.	Switch(config-l2nat)# **inside from host 192.168.1.2 to 10.1.1.2**	A2 の内部アドレスを外部アドレスへ変換します。
5.	Switch(config-l2nat)# **inside from host 192.168.1.3 to 10.1.1.3**	A3 の内部アドレスを外部アドレスへ変換します。
6.	Switch(config-l2nat)# **outside from host 10.1.1.200 to 192.168.1.250**	LC の外部アドレスを内部アドレスへ変換します。
7.	Switch(config-l2nat)# **exit**	config-l2nat モードを終了します。
8.	Switch(config)# **interface Gi1/1**	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。

	コマンド	目的
9.	Switch(config-if)# **l2nat A-LC**	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。 （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*
10.	Switch# **end**	特権 EXEC モードに戻ります。

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 *4 : 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 領域で一意の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の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のアドレスを持ちます。

表 *2: 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

表 3 : アドレスが重複するスイッチ A の設定例 （12 ページ）に、スイッチ A の設定作業を示します。スイッチ B の設定作業については、表 4 : サブネットのスイッチ B の設定例 （13 ページ）に示します。

（注） この例は、IE 2000 スイッチに基づいています。IE 4000 および IE 5000 スイッチでは、インターフェイスの番号が異なる場合があります。

表 *3:* アドレスが重複するスイッチ *A* の設定例

	コマンド	目的
1	Switch# **configure**	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。
2	Switch(config)# **l2nat instance A-Subnet**	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。

	コマンド	目的
3	Switch(config-l2nat)# **inside from network 192.168.1.0 to 10.1.1.16 mask 255.255.255.240**	ノード A の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。
4	Switch(config-l2nat)# **outside from host 10.1.1.254 to 192.168.1.254**	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。
5	Switch(config-l2nat)# **outside from network 10.1.1.32 to 192.168.1.32 255.255.255.240**	ノード B のマシンの外部アドレスを内部アドレスへ変換します。
6	Switch(config-l2nat)# **exit**	config-l2nat モードを終了します。
7	Switch(config)# **interface Gi1/1**	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。
8	Switch(config-if)# **l2nat A-Subnet**	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。 （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*
9	Switch# **end**	特権 EXEC モードに戻ります。

表 *4*:サブネットのスイッチ *B* の設定例

	コマンド	目的
1.	Switch# **configure**	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。
2.	Switch(config)# **l2nat instance B-Subnet**	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。
3.	Switch(config-l2nat)# **inside from network 192.168.1.0 to 10.1.1.32 255.255.255.240**	ノード B の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。
4.	Switch(config-l2nat)# **outside from host 10.1.1.254 to 192.168.1.254**	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。
5.	Switch(config-l2nat)# **outside from network 10.1.1.16 to 192.168.1.16 255.255.255.240**	ノード A のマシンの外部アドレスを内部アドレスへ変換します。
6.	Switch(config-l2nat)# **exit**	config-l2nat モードを終了します。
7.	Switch(config)# **interface Gi1/1**	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。

	コマンド	目的
8.	Switch(config-if)# **l2nat name1**	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。 （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*
9.	Switch# **show l2nat instance name1**	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。
10	Switch# **show l2nat statistics**	レイヤ 2 NAT の統計情報を表示します。
11	Switch# **end**	特権 EXEC モードに戻ります。

関連資料

- Cisco Industrial Ethernet 2000 Series Switches Configuration Guides
- Cisco Industrial Ethernet 4000 Series Switches Configuration Guides
- Cisco Industrial Ethernet 4010 Series Switches Configuration Guides
- Cisco Industrial Ethernet 5000 Series Switches Configuration Guides

機能の履歴

機能名	プラットフォーム	リリース	機能情報
レイヤ 2 NAT	IE 5000	Cisco IOS リリース 15.2(2)EB	初期サポート
	IE 4010	Cisco IOS リリース 15.2(4)EC1	
	IE 4000	Cisco IOS リリース 15.2.(2)EA	
	IE 2000	Cisco IOS リリース 15.0(2)EB	

【注意】シスコ製品をご使用になる前に、安全上の注意（**www.cisco.com/jp/go/safety_warning/**）をご確認ください。本書は、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。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

この資料の記載内容は2008年10月現在のものです。
この資料に記載された仕様は予告なく変更する場合があります。

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/