



CHAPTER 46

レイヤ 2 NAT の設定

この章では、Cisco IOS Release 15.0(2)EB で導入されたレイヤ 2 NAT 機能を設定する際に役立つ情報を提供します。

- [機能情報の確認](#)
- [レイヤ 2 NAT の前提条件](#)
- [レイヤ 2 NAT 設定の制約事項](#)
- [ガイドライン](#)
- [レイヤ 2 NAT 設定に関する情報](#)
- [管理インターフェイスの使用](#)
- [レイヤ 2 NAT の設定方法](#)
- [レイヤ 2 NAT 設定のモニタリング](#)
- [レイヤ 2 NAT 設定のトラブルシューティング](#)
- [設定例](#)
- [その他の関連資料](#)



(注) Cisco Industrial Ethernet 2000 シリーズ スイッチの詳細については、www.cisco.com/en/US/products/ps12451/tsd_products_support_series_home.html にあるリリース ノート、コマンドリファレンス、およびコンフィギュレーションガイドを参照してください。

機能情報の確認

ご使用のソフトウェア リリースでは、このマニュアル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。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノート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 には、<http://www.cisco.com/go/cfn> からアクセスします。Cisco.com のアカウントは必要ありません。

レイヤ 2 NAT の前提条件

レイヤ 2 NAT は Cisco IOS 15.0(2)EB 以降で使用可能な拡張 LAN ベース フィーチャ セットに含まれています。モデルによってライセンスのアップグレードおよびソフトウェアのアップグレードを必要とする可能性があります。詳細については、www.cisco.com/en/US/docs/switches/lan/cisco_ie2000/software/release/15_0_2_eb/upgrade/guide/ie2000_ug.html を参照してください。

レイヤ 2 NAT 設定の制約事項

- レイヤ 2 NAT は Cisco IOS 15.0(2)EB 以降で使用可能な拡張 LAN ベース フィーチャ セットに含まれています。
- 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 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。

ガイドライン

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。

- このスイッチの 2 個のアップリンクポートに関してレイヤ 2 NAT を設定できます。
- ダウンリンクポートは、VLAN、トランク、レイヤ 2 チャン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。
- 設定できる変換エントリは 128 個です。
- レイヤ 2 NAT 設定では最大 128 の VLAN が利用できます。
- ARP、ICMP などの特定のプロトコルは、レイヤ 2 NAT で透過しませんが、これはデフォルトで「固定」されています。

レイヤ 2 NAT 設定に関する情報

概念について

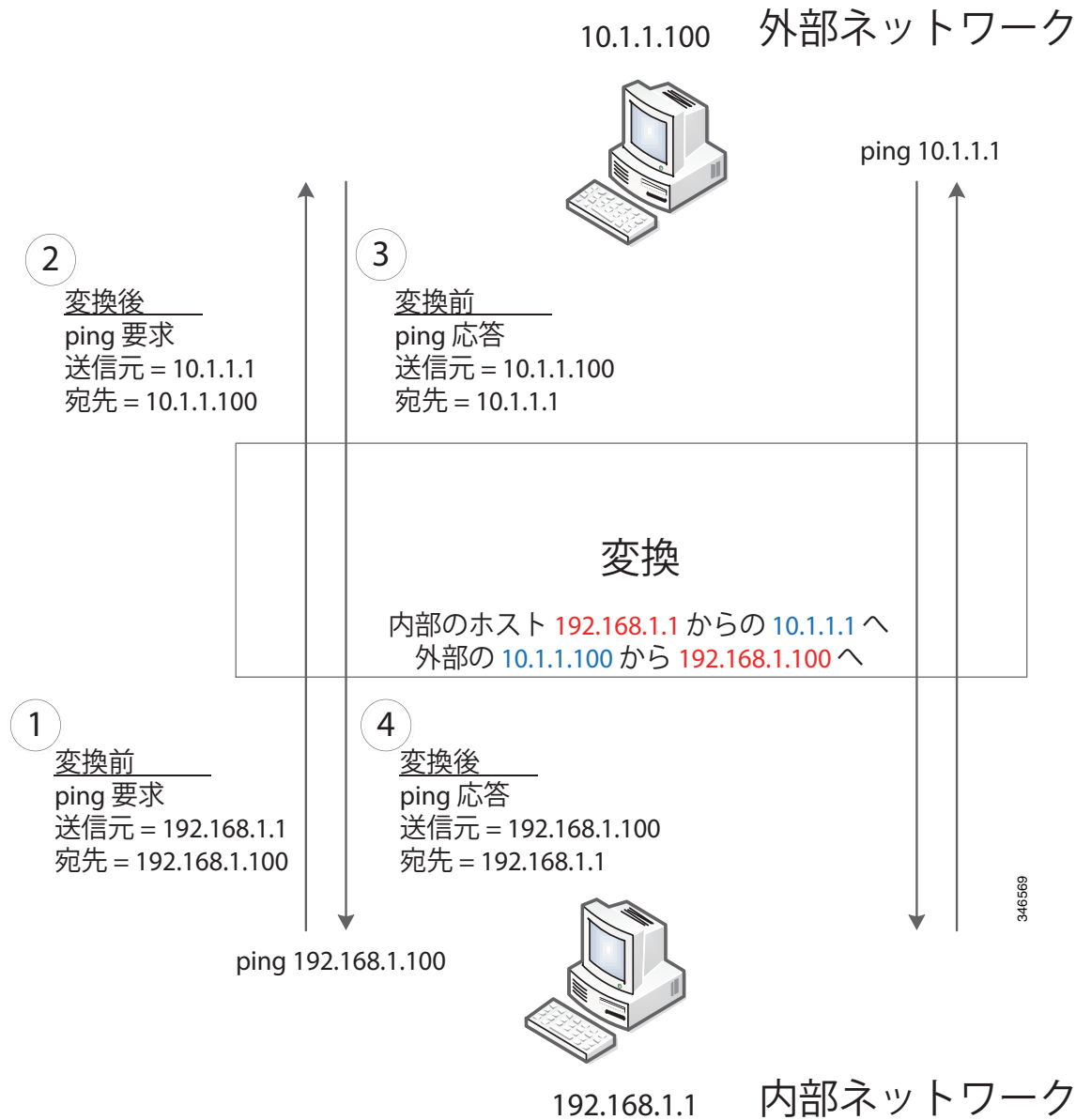
1 対 1 (1 : 1) レイヤ 2 NAT は、固有のパブリック IP アドレスを既存のプライベート IP アドレス (エンドデバイス) に割り当てるサービスであり、エンドデバイスがプライベートとパブリックサブネット上で通信できるようになります。このサービスは、NAT 対応デバイスで設定され、エンドデバイスに物理的にプログラムされた IP アドレスのパブリックでの「エイリアス」です。これは、通常 NAT デバイスでテーブルとして表されます。

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 はスイッチの負荷全体で、一貫した高レベルの (bump-in-the-wire) 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。リングアーキテクチャのサポートは NAT 境界で冗長が可能なレイヤ 2 NAT に組み込まれています。

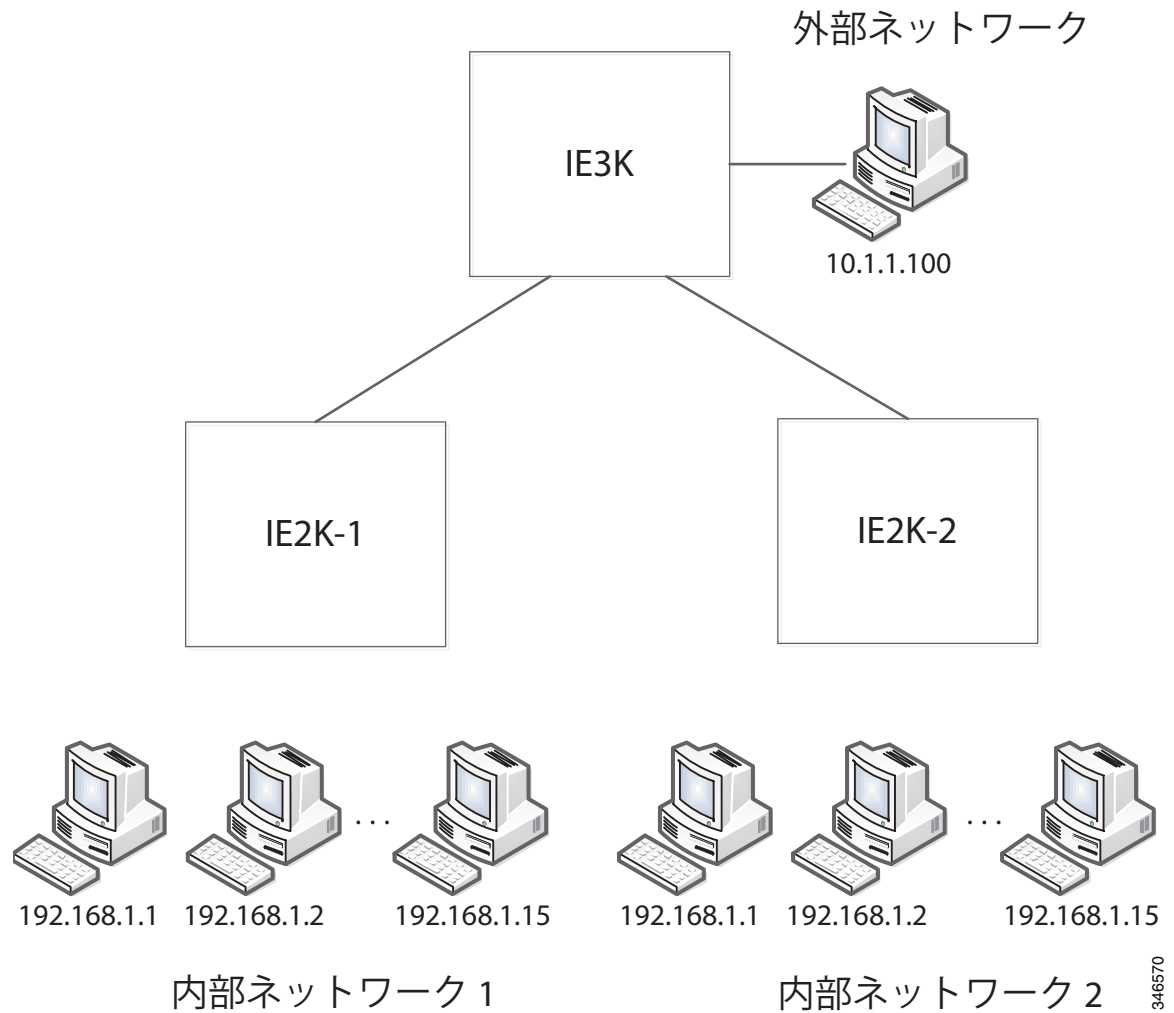
図 46-1 レイヤ 2 NAT では、192.168.1.x ネットワークのセンサーと 10.1.1.x ネットワークの通信制御装置間でアドレスを変換します。

1. 192.168.1.1 のセンサーが通信制御装置に「内部」アドレス 192.168.1.100 を使用して ping 要求を送信します。
2. 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 は送信元アドレスを 10.1.1.1 へ、宛先アドレスを 10.1.1.100 へと変換します。
3. 通信制御装置は 10.1.1.1 へ ping 応答を送信します。
4. 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 へと変換します。

図 46-1 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ただちに交換をイネーブルにできません。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 サブネットに外部アドレスに変換することができ、ネットワーク 2 からのアドレスは 10.1.1.16/28 サブネットに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。



管理インターフェイスの使用

管理インターフェイスはレイヤ 2 NAT 機能の先にあります。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。

レイヤ 2 NAT の設定方法

レイヤ 2 NAT のデフォルト設定

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	ARP のフィックスアップ

レイヤ 2 NAT のセットアップ

レイヤ 2 NAT を設定するには、次の手順を実行します。この章の詳細については、例を参照してください。

	コマンド	目的
ステップ 1	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。
ステップ 2	l2nat instance instance_name	新しいレイヤ 2 NAT インスタンスを作成します。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	inside from [host range network] original ip to translated ip[mask] number mask	内部アドレスを外部アドレスへ変換します。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	outside from [host range network] original ip to translated ip[mask] number mask	外部アドレスを内部アドレスへ変換します。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および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	exit	config-l2nat モードを終了します。
ステップ 6	interface interface-id	指定したインターフェイス（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。
ステップ 7	l2nat instance_name [vlan vlan_range]	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。
ステップ 8	end	インターフェイス コンフィギュレーション モードを終了します。
ステップ 9	show l2nat instance instance_name	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。
ステップ 10	show l2nat statistics	両方のアップリンク ポートについてレイヤ 2 NAT の統計情報を表示します。
ステップ 11	end	特権 EXEC モードに戻ります。

レイヤ 2 NAT 設定のモニタリング

表 46-1 レイヤ 2 NAT 設定の表示

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。

レイヤ 2 NAT 設定のトラブルシューティング

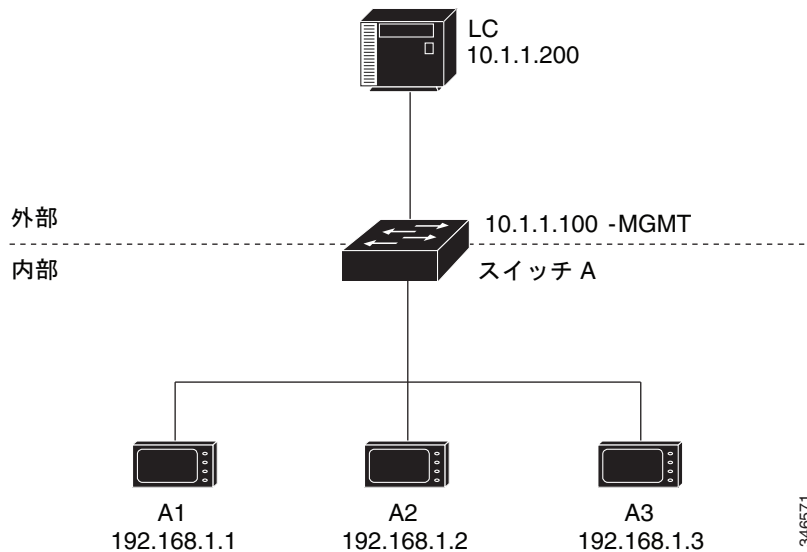
表 46-2 レイヤ 2 NAT 設定のトラブルシューティング

コマンド	目的
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。

設定例

基本的な内部から外部への通信の例

図 46-2 基本的な内部から外部への通信



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。

ここで次の通信が発生します。

1. A1 が ARP 要求を送信します。
SA: 192.168.1.1
DA: 192.168.1.250
2. Cisco スイッチ A は ARP 要求をフィックスアップします。
SA: 10.1.1.1
DA: 10.1.1.200
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 が応答を送信します。
SA: 10.1.1.200
DA: 10.1.1.1
5. Cisco スイッチ A は ARP 応答をフィックスアップします。
SA: 192.168.1.250
DA: 192.168.1.1
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。

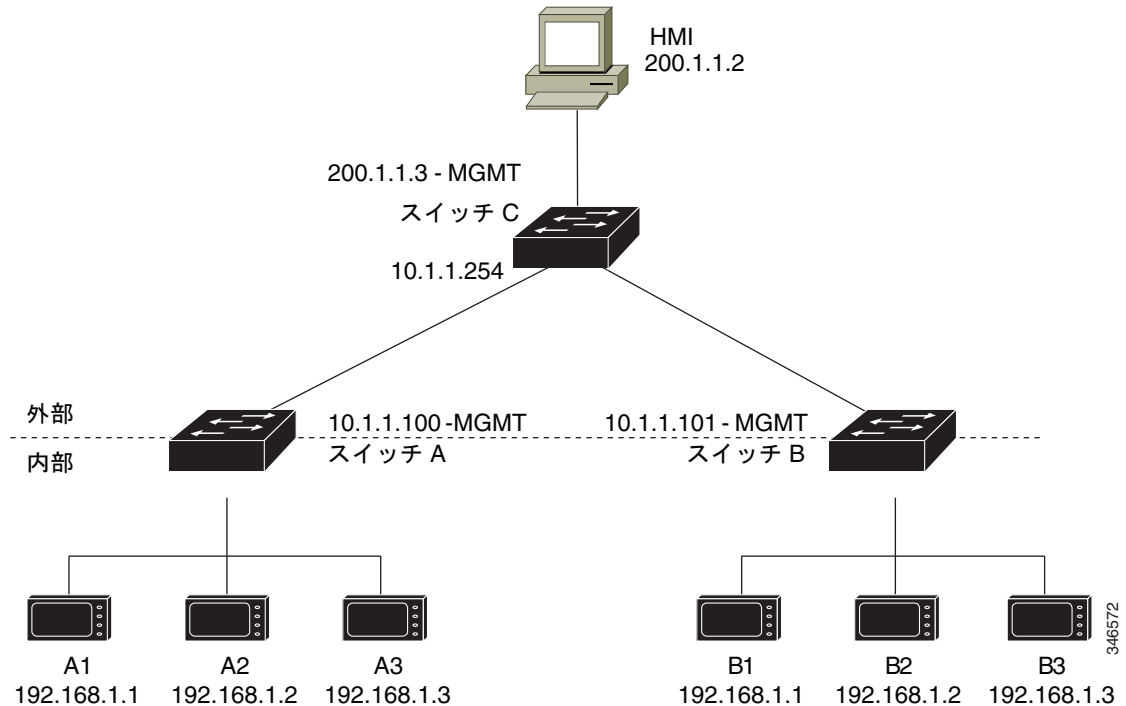
表 46-2 に、ここでの設定作業を示します。レイヤ 2 NAT インスタンスが作成され、2 つの変換エントリーを追加し、インスタンスをインターフェイスに適用します。ARP フィックスアップはデフォルトでイネーブルです。

表 46-3 基本的な内部から外部への例での Cisco スイッチ A の設定

	コマンド	目的
ステップ 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。
ステップ 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。
ステップ 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。
ステップ 4	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。
ステップ 5	Switch(config-l2nat)# exit	config-l2nat モードを終了します。
ステップ 6	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。
ステップ 7	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。
ステップ 8	Switch# end	特権 EXEC モードに戻ります。

重複する IP アドレスの例

図 46-3 IP アドレスの重複



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 は、これらのアドレスを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するために使用されます。また、マシン間の通信で、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。

- 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 10.1.254 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 のマシン用の 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へ変換されます。ノード B マシン用の 10.1.1.32 サブネットアドレスは、ノード A の 192.168.1.32 サブネット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。

	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 46-4 に、スイッチ A の設定作業を示します。表 46-5 に、Cisco スイッチ B の設定作業を示します。

表 46-4 アドレス重複の場合のスイッチ A の設定

	コマンド	目的
ステップ 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。
ステップ 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。
ステップ 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。
ステップ 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。
ステップ 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ノード B の内部アドレスに変換します。
ステップ 6	Switch(config-l2nat)# exit	config-l2nat モードを終了します。
ステップ 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。
ステップ 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。
ステップ 9	Switch# end	特権 EXEC モードに戻ります。

表 46-5 サブネットの場合のスイッチ B の設定

	コマンド	目的
ステップ 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。
ステップ 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。
ステップ 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。
ステップ 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。
ステップ 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ノード A の内部アドレスに変換します。
ステップ 6	Switch(config-l2nat)# outside from network 10.1.1.32 to 192.168.1.0 255.255.255.240	ノード B のマシンの外部アドレスをノード B の内部アドレスに変換します。
ステップ 7	Switch(config-l2nat)# exit	config-l2nat モードを終了します。
ステップ 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。
ステップ 9	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。
ステップ 10	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。
ステップ 11	Switch# show l2nat statistics	レイヤ 2 NAT の統計情報を表示します。
ステップ 12	Switch# end	特権 EXEC モードに戻ります。

その他の関連資料

ここでは、スイッチ管理に関する参考資料について説明します。

関連資料

関連項目	マニュアル タイトル
このスイッチの Cisco IOS コマンド	『Cisco IE2000 Switch Series Command Reference』
Cisco IOS 基本コマンド	『Cisco IOS Configuration Fundamentals Command Reference』
ライセンス アップグレードの手順	『Software Activation Licensing Upgrade Instructions for the Cisco IE2000 Switch Series』

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	—

MIB

MIB	MIB のリンク
—	Cisco IOS XR ソフトウェアを使用して MIB を検索およびダウンロードするには、 http://cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml にある Cisco MIB Locator を使用し、[Cisco Access Products] メニューからプラットフォームを選択します。

RFC

RFC	タイトル
この機能によりサポートされた新規 RFC または改訂 RFC はありません。またこの機能による既存 RFC のサポートに変更はありません。	—

シスコのテクニカル サポート

説明	リンク
シスコのテクニカル サポート Web サイトでは、製品、テクノロジー、ソリューション、技術的なヒント、およびツールへのリンクなどの、数千ページに及ぶ技術情報が検索可能です。Cisco.com に登録済みのユーザは、このページから詳細情報にアクセスできます。	http://www.cisco.com/en/US/support/index.html

