

ip nat outside source list コマンドを使用した設定例

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[表記法](#)

[設定](#)

[ネットワーク図](#)

[設定](#)

[確認](#)

[トラブルシューティング](#)

[要約](#)

[関連情報](#)

概要

このドキュメントでは、ip nat outside source list コマンドを使用した設定例を示し、NAT プロセスで IP パケットがどのように処理されるかについて簡単に説明します。このコマンドを使用して、ネットワークの外部からネットワークの内部に送信される IP パケットの送信元アドレスを変換できます。このアクションは、ネットワークの内部から外部に向かって反対方向に移動する IP パケットの宛先アドレスを変換します。このコマンドは、ネットワークの重複（内部のネットワークアドレスがネットワークの外部アドレスに重複する）などの状況で役に立ちます。次のネットワーク構成図を例に説明します。

前提条件

要件

このドキュメントに特有の要件はありません。

使用するコンポーネント

このドキュメントの内容は、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。ただし、このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco 2500 シリーズ ルータ
- すべてのルータで動作する Cisco IOS® ソフトウェア リリース 12.2(24a)

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

表記法

ドキュメントの表記法の詳細は、「[シスコテクニカルティップスの表記法](#)」を参照してください。

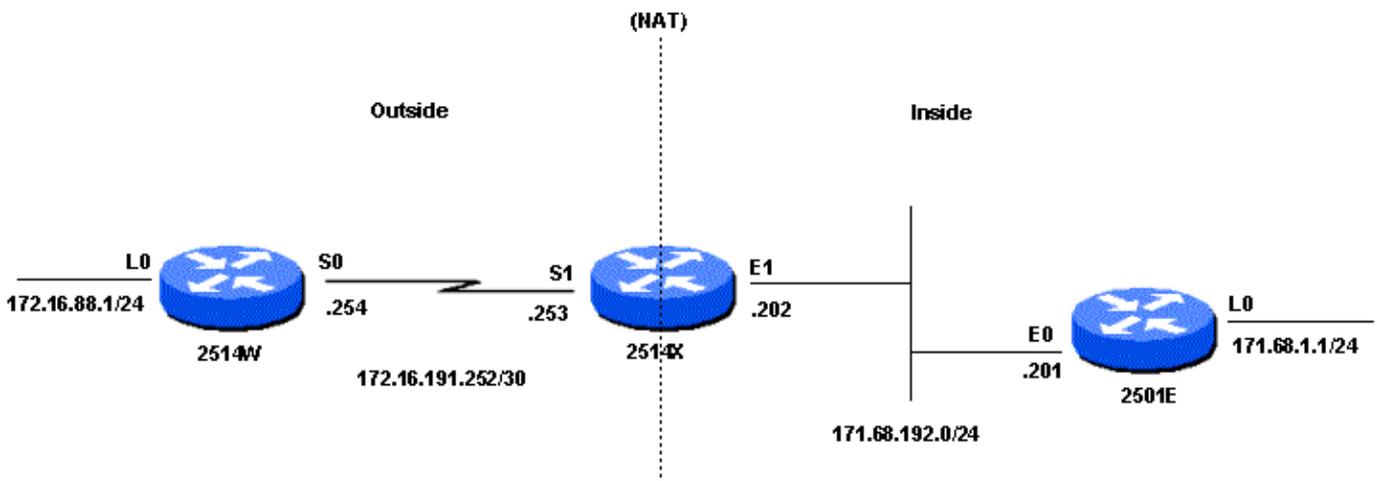
設定

このセクションでは、このドキュメントで説明する機能を設定するために必要な情報を提供しています。

注：この文書で使用されているコマンドの詳細を調べるには、「[Command Lookup ツール](#)」を使用してください（登録ユーザのみ）。

ネットワーク図

このドキュメントでは、次のネットワーク セットアップを使用します。



ルータ 2514W の Loopback0 インターフェイス (172.16.88.1) からルータ 2501E の Loopback0 インターフェイス (171.68.1.1) への ping を実行すると、次の事象が発生します。

デフォルト ルートを使用して設定されているため、ルータ 2514W によりパケットがルータ 2514X に転送されます。ルータ2514Xの外部インターフェイスでは、パケットの送信元アドレス (SA)は172.16.88.1で、宛先アドレス(DA)は171.68.1.1です。SAはアクセスリスト1で許可され、`ip nat outside source list`コマンドで使用されるため、NATプールNet171通知から1アドレスに交換されます。`ip nat outside source list`コマンドがNATプール「[Net171](#)」を参照している。この場合、アドレスは、この NAT プールで最初に使用できるアドレスの 171.68.16.10 に変換されます。変換後、ルータ2514Xはルーティングテーブルで宛先を検索し、パケットをルーティングします。ルータ2501Eは、着信インターフェイス上のパケットをSA 171.68.16.10とDAが171.68.1.1で確認し、Internet Control Message Protocol(ICMP)エコー応答を171.68.16.10に送信して応答します。ルートがない場合、パケットをドロップします。この場合、ルータには (デフォルト) ルートがあるため、SAが171.68.1.1、DAが171.68.16.10を使用してルータ2514Xにパケットを送信し

まず。ルータ2514Xは、内部インターフェイス上のパケットを確認し、171.68.16.10アドレスへのルートを確認します。経路がない場合、ICMP 到達不能応答で応答します。この例では、[171.68.16.10](#) へのルートが存在するため、外部グローバル アドレスと外部ローカル アドレス間の変換に基づいてホスト ルートを追加する ip nat outside source コマンドの add-route オプションによって、パケットのアドレスが 172.16.88.1 に逆変換され、外部インターフェイスからパケットがルーティングされます。

設定

ルータ2514W

```
hostname 2514W
!  
!--- Output suppressed. interface Loopback0 ip address  
172.16.88.1 255.255.255.0 ! -- Output suppressed.  
interface Serial0 ip address 172.16.191.254  
255.255.255.252 no ip mroute-cache ! -- Output  
suppressed. ip classless ip route 0.0.0.0 0.0.0.0  
172.16.191.253 ! -- Default route to forward packets to  
2514X. ! -- Output suppressed.
```

ルータ2514X

```
hostname 2514X  
!  
!--- Output suppressed. ! interface Ethernet1 ip address  
171.68.192.202 255.255.255.0 ip nat inside no ip mroute-  
cache no ip route-cache ! -- Output suppressed.  
interface Serial11 ip address 172.16.191.253  
255.255.255.252 ip nat outside no ip mroute-cache no ip  
route-cache clockrate 2000000 ! ip nat pool Net171  
171.68.16.10 171.68.16.254 netmask 255.255.255.0 ! --  
NAT pool defining Outside Local addresses to be used for  
translation. ! ip nat outside source list 1 pool Net171  
add-route ! -- Configures translation for Outside Global  
addresses ! -- with the NAT pool. ip classless ip route  
172.16.88.0 255.255.255.0 172.16.191.254 ip route  
171.68.1.0 255.255.255.0 171.68.192.201 ! -- Static  
routes for reaching the loopback interfaces ! -- on  
2514W and 2501E. access-list 1 permit 172.16.88.0  
0.0.0.255 ! -- Access-list defining Outside Global  
addresses to be translated. ! -- Output suppressed. !
```

ルータ2501E

```
hostname 2501E  
!  
!--- Output suppressed. interface Loopback0 ip address  
171.68.1.1 255.255.255.0 ! interface Ethernet0 ip  
address 171.68.192.201 255.255.255.0 ! -- Output  
suppressed. ip classless ip route 0.0.0.0 0.0.0.0  
171.68.192.202 ! -- Default route to forward packets to  
2514X. ! -- Output suppressed.
```

確認

このセクションでは、設定が正常に動作しているかどうかを確認する際に役立つ情報を示しています。

一部の show コマンドは [アウトプット インタープリタ ツールによってサポートされています \(登録ユーザ専用 \)](#)。このツールを使用することによって、show コマンド出力の分析結果を表示できます。

次の出力で示されているように、変換エントリを確認するために show ip nat translations コマンドを使用できます。

```
2514X# show ip nat translations
Pro Inside global      Inside local      Outside local      Outside global
--- 171.68.1.1         171.68.1.1       171.68.16.10      172.16.88.1
--- ---                ---              171.68.16.10      172.16.88.1
```

2514X#

上記の出力には、ルータ 2514W の Loopback0 インターフェイス上のアドレスである外部グローバルアドレス 172.16.88.1 が外部ローカル アドレス 171.68.16.10 に変換されることが示されています。

次に示されているように、ルーティング テーブル エントリを確認するために show ip route コマンドを使用できます。

```
2514X# show ip route
```

```
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default, U - per-user static route
        o - ODR, P - periodic downloaded static route
```

```
Gateway of last resort is not set
```

```
    171.68.0.0/16 is variably subnetted, 3 subnets, 2 masks
C       171.68.192.0/24 is directly connected, Ethernet1
S       171.68.1.0/24 [1/0] via 171.68.192.201
S       171.68.16.10/32 [1/0] via 172.16.88.1
    172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
S       172.16.88.0/24 [1/0] via 172.16.191.254
C       172.16.191.252/30 is directly connected, Serial1
```

2514X#

上記の出力には、ip nat outside source コマンドの add-route オプションに従って作成される、外部ローカル アドレス 171.68.16.10 の /32 ルートが示されています。このルートは、ネットワークの内部から外部へ送信されるパケットのルーティングと変換に使用されます。

[トラブルシューティング](#)

ここでは、設定のトラブルシューティングに使用できる情報を示します。

次の出力は、ルータ2514Wのloopback0インターフェイスアドレス(172.16.88.1)からルータ2501Eのloopback0インターフェイスアドレス(171.68.1.1)にpingしながら、ルータ2514Xでdebug ip packetおよびdebug ip natコマンドを実行した結果です。

```
*Mar  1 00:02:48.079: NAT*: s=172.16.88.1->171.68.16.10, d=171.68.1.1 [95]
!--- The source address in the first packet arriving on !--- the outside interface is first
```

```

translated. *Mar 1 00:02:48.119: IP: tableid=0, s=171.68.16.10 (Serial1), d=171.68.1.1
(Ethernet1), routed via
RIB
*Mar 1 00:02:48.087: IP: s=171.68.16.10 (Serial1), d=171.68.1.1 (Ethernet1), g=171.68.192.201,
len
100, forward
!--- The ICMP echo request packet with the translated source address !--- is routed and
forwarded on the inside interface. *Mar 1 00:02:48.095: IP: tableid=0, s=171.68.1.1 (Ethernet1),
d=171.68.16.10 (Serial1), routed via
RIB
!--- The ICMP echo reply packet arriving on the inside interface !--- is first routed based on
the destination address. *Mar 1 00:02:48.099: NAT: s=171.68.1.1, d=171.68.16.10->172.16.88.1
[95]
!--- The destination address in the packet is then translated. *Mar 1 00:02:48.103: IP:
s=171.68.1.1 (Ethernet1), d=172.16.88.1 (Serial1), g=172.16.191.254, len 1
00, forward
!--- The ICMP echo reply packet with the translated destination !--- address is forwarded on the
outside interface.

```

上述の手順は、外部インターフェイス上で受信される各パケットで繰り返されます。

要約

ip nat outside source static コマンド (スタティック NAT) の代わりに ip nat outside source list コマンド (ダイナミック NAT) を使用した場合の大きな違いは、(NAT が設定された) ルータによってパケットの変換基準が確認されるまで、変換テーブルにエントリがない点にあります。上記の例では、SA 172.16.88.1 を持つパケット (ルータ 2514X の外部インターフェイスに到達したパケット) は、ip nat outside source list コマンドで使用される基準、access-list 1 に適合しています。このため、内部ネットワークから送信されるパケットがルータ 2514W の loopback0 インターフェイスと通信するためには、まず外部ネットワークからパケットが発信される必要があります。

この例には、重要事項が 2 点含まれています。

第 1 に、外部から内部へパケットが送られるときは、最初に変換が行われてから、ルーティングテーブル内で宛先がチェックされます。内部から外部へパケットが送られるときは、最初にルーティングテーブル内で宛先がチェックされてから、変換が行われます。

第 2 に、上記の各コマンドを使用したときに、IP パケットのどの部分が変換されるかを確認することが重要です。次の表に、ガイドラインを示します。

コマンド	アクション
ip nat outside source list	<ul style="list-style-type: none"> 外部から内部へ送られる IP パケットの送信元が変換される。 内部から外部へ送られる IP パケットの宛先が変換される。
ip nat inside source list	<ul style="list-style-type: none"> 内部から外部へ送られる IP パケットの送信元が変換される。 外部から内部へ送られる IP パケットの宛先が変換される。

上記のガイドラインが示しているのは、パケットの変換方法が 1 通りではないということです。固有のニーズに従って、NAT インターフェイスの定義方法 (内部または外部) と、変換前後にルーティングテーブルに含まれる経路を決定する必要があります。パケットの変換される部分は、

パケットが送られる方向と、NAT の設定方法によって異なる点に留意してください。

関連情報

- [スティック上のネットワーク アドレス変換](#)
- [NAT テクノロジーに関するサポート ページ](#)
- [テクニカルサポート - Cisco Systems](#)