重複ネットワーク間の通信を有効にするための NAT の設定

目次

概要

このドキュメントでは、ネットワーク アドレス変換（NAT）を設定し、それぞれ異なるネットワーク セグメント（IP スペースは重複）に属するサーバとクライアントとの間で通信を可能にする方法について説明します。

前提条件

要件

このドキュメントに関しては個別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。

本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 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。 稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

注: この資料は Cisco IOS を実行するスイッチおよびすべての Ciscoルータに適用します。

背景説明

目的

重複する IP スペースを持つ 2 つの個別のネットワーク セグメント上で、サーバとクライアントとの間の通信を可能にします。重複は通常、ネットワークがマージされるときに発生します。

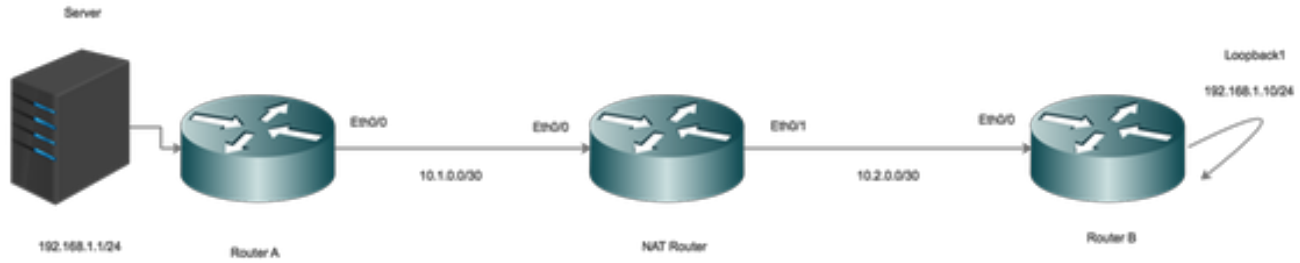
説明

同じ IP スペースを持つ 2 つのネットワークがルータ A とルータ B を介して接続されています（ここではループバックを使用してネットワークをシミュレート）。

ルータ A とルータ B の間の NAT ルータは、重複する IP ネットワーク スペース間の通信を可能にします。

設定

ネットワーク図



トラフィック フロー

- クライアントがサーバのグローバル IP へのトラフィックを開始すると、トラフィックは NAT ルータに到達し、サーバに転送されますが、トラフィックが NAT ルータに戻されると、内部インターフェイスではサーバ 192.168.1.1 が接続/認識されているためにルータがトラフィックを転送できません。
- これを修正するには、外部ソース トラフィックが NAT ルータを通過するときに、そのトラ

フィックをマスク（NAT）します。
- 内部インターフェイスと外部インターフェイスで NAT を有効にします。

```
interface Ethernet0/0
description Connection to Server
ip address 10.1.0.2 255.255.255.252
ip nat inside
end

!

interface Ethernet0/1
description Connection to Clients
ip address 10.2.0.2 255.255.255.252
ip nat outside
end

!
```

内部ローカル アドレスを内部グローバル アドレスに変換するように NAT を設定します。

```
ip nat inside source static 192.168.1.1 10.100.1.1 extendable
```

ここで、クライアントの送信元トラフィックが NAT 外部インターフェイスに到達したときにトラフィックを変換するように NAT ステートメントを設定します。

```
ip nat outside source static network 192.168.1.0 10.100.2.0 /24
```

ルーティング設定

サーバのルート： サーバの特定のルートが LAN（イーサネット 0/0）を指すように設定されていることに注意してください。

```
ip route 192.168.1.1 255.255.255.255 Ethernet0/0 10.1.0.1
```

クライアント ネットワークのルート：

```
ip route 192.168.1.0 255.255.255.0 Ethernet0/1 10.2.0.1
```

確認

このセクションでは、設定が正常に機能していることを確認します。

```
*Aug 12 11:34:59.963: NAT*: o: icmp (192.168.1.10, 10) -> (10.100.1.1, 10) [42]
*Aug 12 11:34:59.963: NAT*: o: icmp (192.168.1.10, 10) -> (10.100.1.1, 10) [42]
*Aug 12 11:34:59.963: NAT*: s=192.168.1.10->10.100.2.10, d=10.100.1.1 [42]
*Aug 12 11:34:59.963: NAT*: s=10.100.2.10, d=10.100.1.1->192.168.1.1 [42]
*Aug 12 11:34:59.963: NAT*: i: icmp (192.168.1.1, 10) -> (10.100.2.10, 10) [42]
*Aug 12 11:34:59.963: NAT*: s=192.168.1.1->10.100.1.1, d=10.100.2.10 [42]
*Aug 12 11:34:59.963: NAT*: s=10.100.1.1, d=10.100.2.10->192.168.1.10 [42]
NAT-Router#
*Aug 12 11:34:59.964: NAT*: o: icmp (192.168.1.10, 10) -> (10.100.1.1, 10) [43]
*Aug 12 11:34:59.964: NAT*: s=192.168.1.10->10.100.2.10, d=10.100.1.1 [43]
*Aug 12 11:34:59.964: NAT*: s=10.100.2.10, d=10.100.1.1->192.168.1.1 [43]
*Aug 12 11:34:59.964: NAT*: i: icmp (192.168.1.1, 10) -> (10.100.2.10, 10) [43]
*Aug 12 11:34:59.964: NAT*: s=192.168.1.1->10.100.1.1, d=10.100.2.10 [43]
```

```
*Aug 12 11:34:59.964: NAT*: s=10.100.1.1, d=10.100.2.10->192.168.1.10 [43]
NAT-Router#
```

このように、クライアントがトラフィック（192.168.1.10）を開始すると、外部 NAT インターフェイスは外部グローバル アドレスを外部ローカル アドレス（10.100.2.10）に変換してから、トラフィックを NAT 内部インターフェイスにルーティングします。

ここで、NAT 内部インターフェイスが宛先（10.100.1.1）を内部ローカル アドレス（192.168.1.1）に変換し、トラフィックはサーバに向かって移動します。

サーバは、送信元アドレス 10.100.2.10 のトラフィックを受信しました。

トラブルシューティング

現在のところ、この設定に関する特定のトラブルシューティング情報はありません。

制限

この設定では、クライアントだけが接続を開始でき、接続は成功します。

外部ローカルからグローバルへの変換テーブルには NAT エントリがないため、トラフィックは内部から（サーバから）発信できません（NAT は失敗する）。