

NAT の ICMP フラグメントの処理方法

目次

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[表記法](#)

[ケース 1](#)

[ケース 2](#)

[ケース 3](#)

[要約](#)

[関連情報](#)

概要

ここでは、ネットワーク アドレス変換 (NAT) オーバーロードが設定されている場合に、NAT が Internet Control Message Protocol (ICMP) フラグメントをどのように処理するかについて説明します。NAT オーバーロードの詳細については、『[NAT FAQ](#)』を参照してください。

ICMP フラグメントの処理方法は、NAT 変換テーブルの状態と、NAT ルータが ICMP フラグメントを受け取った順番によって異なります。ここでは、3 通りの異なるケースについて調べます。その場合も、それぞれ 3600 バイト長のフラグメント (3 つの IP フラグメント) を使って、172.16.0.1 から 172.17.1.2 へ 2 回ずつ ping を送信しています。

前提条件

要件

このドキュメントに関する固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。

表記法

ドキュメント表記の詳細は、『[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。

ケース 1

このシナリオでは、NAT が変換テーブル内に完全拡張変換エントリを作成する様子を確認します。一旦それが実行されると、NAT プールには他の使用可能なアドレスは存在せず、NAT はパケットの第 1 フラグメント (フラグメント 0) よりも前に受けとったすべてのフラグメントをドロップします。

開始時点では、プールの 1 つのアドレスのみが過負荷の処理を行います。NAT 変換テーブルは空です。NAT 設定は次のように表示されます。

```
ip nat pool POOL1 10.10.10.3 10.10.10.3 prefix-length 24
ip nat inside source list 5 pool POOL1 overload
access-list 5 permit 172.16.0.0 0.0.0.31
```

パケットが NAT のルータに到着し始めたときに、何が起きるのかを確認しましょう。

1. パケット 1 フラグメント 0 が到着すると、NAT は完全拡張変換エントリを作成します。その後、NAT はパケット 1 フラグメント 0 を変換し転送します。これで、変換テーブルは次のように表示されます。

Pro	Inside global	Inside local	Outside local	Outside global
icmp	10.10.10.3:24320	172.16.0.1:24320	172.17.1.2:24320	172.17.1.2:24320

上記の変換テーブル内の番号 24320 に着目してください。それは、IP データグラムの ICMP ヘッダーに含まれる ICMP ID 値です。IP データグラムのフラグメント 0 だけにこの ICMP ヘッダーが含まれています。複数のフラグメントが同一のパケットに属しているかどうかを判断するため、NAT はオリジナルの IP データグラムのすべてのフラグメントで IP ヘッダー内を検索し、IP ID 値を追跡する必要があります。複数のフラグメントが、すでに拡張変換エントリが作成されているフラグメント 0 と同一の IP ID 値を持つ場合は、NAT は同じ拡張変換エントリを使ってこれらのフラグメントを変換します。IP 識別フィールドに関する詳細については [RFC 791](#) を参照して下さい。ICMP 識別フィールドに関する詳細については [RFC 792](#) を参照して下さい。
2. パケット 1 フラグメント 2 とパケット 1 フラグメント 1 が到着します。これらのフラグメントは、フラグメント 0 を含むパケットと同一のパケット (すでに変換が作成されている) に属しているため、NAT は上記の変換エントリを使って、これらのフラグメントを変換して転送します。宛先デバイスは、パケット 1 のすべてのフラグメントを受け取ると、応答を送信します。
3. パケット 2 フラグメント 1 が到着します。これは新しいパケットであるため、IP ID 値は NAT によってこれまでに記録された値と一致しません。そのため、NAT では既存の変換を使用できません。また、それはすでに完全拡張変換エントリを持っており、別のエントリを作成するための ICMP ID を持っていないため、新たな変換エントリを作成することもできません。NAT はパケット 2 フラグメント 1 をドロップします。
4. パケット 2 フラグメント 0 が到着します。ICMP ID が一致するため、NAT は上記の変換エントリを使います。(ping の 1 つのセットに含まれるすべての ping が同じ ICMP ID 番号を使用)。この時点で、NAT はこのパケットの IP ID 値を記録します。NAT はパケット 2 フラグメント 0 を変換し転送します。
5. パケット 2 フラグメント 2 が到着します。今度は、IP ID 値が以前のステップで NAT が記録した値と一致するため、NAT は上記の変換エントリを使用することができます。NAT はパケット 2 フラグメント 2 を変換し転送します。宛先デバイスは、フラグメント 0 と 2 だけを受け取るため (フラグメント 1 は損失)、応答は送りません。

ケース 2

このシナリオでは、第 1 フラグメント (フラグメント 0) 以外のフラグメントが最初に到着した

ときに、完全拡張変換でまだ使用されていないアドレスが NAT プール内にある限り、NAT は単純変換を作成することを確認します。

開始時には、NAT プール内にはアドレスが 1 つしか存在せず、NAT 変換テーブルは空で、設定は次のようになっています。

```
ip nat pool POOL1 10.10.10.3 10.10.10.3 prefix-length 24
ip nat inside source list 5 pool POOL1 overload
access-list 5 permit 172.16.0.0 0.0.0.31
```

1. パケット 1 フラグメント 1 が到着します。フラグメント内に ICMP ID 情報がないため、NAT では変換テーブルに完全拡張変換エントリを作成できません。ただし、完全拡張変換はまだ実行されていないため、NAT は単純変換エントリを入力します。その後、NAT はパケット 1 フラグメント 1 を変換し転送します。変換エントリは次のように表示されます。

Pro	Inside global	Inside local	Outside local	Outside global
---	10.10.10.3	172.16.0.1	---	---

2. パケット 1 フラグメント 0 が到着します。ICMP ID 情報がこのフラグメントに含まれているため、NAT は完全拡張変換エントリを入力します。Pro

local	Outside local	Outside global	Pro	Inside global	Inside
---	10.10.10.3	172.16.0.1	---	---	---

icmp 10.10.10.3:24321 172.16.0.1:24321 172.17.1.2:24321 172.17.1.2:24321その後、NAT は IP ID 情報を記録し、パケット 1 フラグメント 0 を変換し転送します。

3. パケット 1 フラグメント 2 が到着します。このフラグメントは、NAT がステップ 2 で記録した情報と同じ IP ID 情報を持っているため、NAT は完全拡張変換を使用して、パケット 1 フラグメント 2 を変換し転送します。宛先デバイスは、すべてのフラグメントを受け取り、応答を返します。この時点では、NAT 変換テーブルがクリアされるか、タイムアウトになるまで、すべての ping が成功します。

ケース 3

このシナリオでは、第 1 フラグメント (フラグメント 0) 以外のフラグメントが最初に到着したときに、完全拡張変換でまだ使用されていないアドレスが NAT プール内にある限り、NAT は単純変換を作成することを確認します。NAT テーブル内の拡張変換がすでにアドレスを使用している場合は、各フラグメントの発信元アドレスを別のアドレスへ NAT 変換するという危険を冒すこととなります。

開始時に、NAT プール内の複数のアドレスがオーバーロードを実施するため、変換テーブルにはすでに拡張変換が登録されており、設定は次のようになります。

```
ip nat pool POOL1 10.10.10.3 10.10.10.5 prefix-length 24
ip nat inside source list 5 pool POOL1 overload
access-list 5 permit 172.16.0.0 0.0.0.31
```

変換テーブルは次のように表示されます。

Pro	Inside global	Inside local	Outside local	Outside global
icmp	10.10.10.3:24322	172.16.0.1:24322	172.17.1.2:24322	172.17.1.2:24322

1. パケット 1 フラグメント 1 が到着します。このフラグメントには ICMP ID 情報がないため、NAT は完全拡張変換テーブル エントリを作成できません。また、IP アドレス 10.10.10.3 に対応する既存の拡張エントリが存在するため、この IP アドレスの単純変換エントリは作成できません。NAT は解放されている次の IP アドレス (10.10.10.4) を使って、単純変換エントリを作成します。その後、NAT はパケット 1 フラグメント 1 を変換し転送します。

これで、変換テーブルは次のように表示されます。Pro

local	Inside global	Inside
local	Outside local	Outside global

---	10.10.10.4	172.16.0.1	---	---
icmp	10.10.10.3:24322	172.16.0.1:24322	172.17.1.2:24322	172.17.1.2:24322

2. パケット 1 フラグメント 0 が到着します。このフラグメントには ICMP ID 情報が含まれているため、NAT はアドレス 10.10.10.3 に対応する完全拡張変換エントリを入力し、このパケットの IP ID 情報を記録します。その後、NAT はパケット 1 フラグメント 0 を変換し転送します。これで、変換テーブルは次のように表示されます。Pro Inside global

Inside local	Outside local	Outside global	Pro	Inside global
---	10.10.10.4	172.16.0.1	---	---
icmp	10.10.10.3:24322	172.16.0.1:24322	172.17.1.2:24322	172.17.1.2:24322
icmp	10.10.10.3:24323	172.16.0.1:24323	172.17.1.2:24323	172.17.1.2:24323

3. パケット 1 フラグメント 2 が到着します。その IP ID 情報は NAT がステップ 2 で記録した情報と一致するため、NAT はステップ 2 で作成した完全拡張変換エントリを使って、パケット 1 フラグメント 2 を変換し転送します。この時点で、宛先デバイスはパケット 1 のすべてのフラグメントを受け取りますが、フラグメント 0 と 2 の発信元アドレスは 10.10.10.3 に変換されており、フラグメント 1 は 10.10.10.4 に変換されています。そのため、宛先デバイスは、パケットを再組立てできず、応答も返信しません。
4. パケット 2 フラグメント 0 が到着します。NAT は、フラグメントの ICMP ID フィールドの値に応じて、上記の完全拡張変換を使うか、新たな完全拡張変換を作成します。どちらも場合も、NAT は IP ID 情報を記録します。その後、NAT はパケット 2 フラグメント 0 を変換し転送します。
5. パケット 2 フラグメント 2 が到着します。その IP ID 情報は、ステップ 4 で NAT が記録した情報と一致するため、NAT はステップ 4 で作成した 2 番目の完全拡張変換を使用します。NAT は、パケット 2 フラグメント 2 を変換し転送します。
6. パケット 2 フラグメント 1 が到着します。その IP ID 情報は、ステップ 4 で NAT が記録した情報と一致するため、NAT はステップ 4 で作成した 2 番目の完全拡張変換エントリを使用します。NAT は、パケット 2 フラグメント 1 を変換し転送します。宛先デバイスは、パケット 2 のこれらのフラグメントをすべて、同一の送信元 (10.10.10.3) から受け取ったため、パケットを再組立てし、応答を返します。

要約

NAT は、NAT ルータがフラグメントを受け取った順番、そのときの変換テーブルの状態など多数の要因に応じて、ICMP フラグメントをドロップするか転送します。一部の状況では、NAT によるフラグメントの変換が異なるため、宛先デバイスによるパケットの再構成が不可能になります。

関連情報

- [NAT に関するサポートページ](#)
- [IP ルーティングに関するサポート ページ](#)
- [テクニカルサポート - Cisco Systems](#)