

HPE

GreenLake

無計画なハイブリッドクラウドから
計画的なハイブリッドクラウドへ。
かしこい選択。

概要解説をダウンロード

@IT > クラウド > Windows Server Insider > 第12回 TCP/IPプロトコルを支えるICMPメッセージ：...

第12回 TCP/IPプロトコルを支えるICMPメッセージ

(3/3 ページ)

2003年06月13日 00時00分 公開

[デジタルアドバンテージ, 著]

印刷

通知

見る

Share

18

前のページへ

1

2

3

タイプ3—あて先不達

これは何らかの理由で、あて先となるサービスへパケットを送ることができない場合に、送信元に対して送り返されるエラー・メッセージである。例えば特定のTCPやUDPポートに向けて送られた通信要求に対して、そのポートをリッスン（待ち受け）しているサービスがない場合とか、IPフラグメンテーションが必要にもかかわらず、IPパケット中の「フラグメント禁止bit（DF bit）」がセットされていて、その先へパケットをルーティング（フォワード）することができない、といったエラーを伝えるために利用される。

前ページ最後のPPPoE環境におけるpingの実行例では、大きなパケットを送信しようとした場合に、最終的なあて先ホストではなく、経路途中にあるルータから、これ以上送信できないというエラーが戻ってきていたが、そこで使われているのがこのICMPの「あて先不達」というメッセージである。このメッセージは、ルーティングの途中のマシン（ルータ）から返信されることもあるし、最終的なあて先となるマシン（ターゲット・ホスト）自身から返信されることもある。

ICMPのヘッダ中にある「コード」部分には、エラーの要因を表す数値がセットされ、送信される。具体的には、次のようなエラー要因がある。

コード	意味
0	ネットワークが到達できない：ルータが定義されていない
1	ホストに到達できない：ターゲットとなるマシンが見つからない
2	プロトコルに到達できない：指定されたプロトコルが利用できない
3	ポートに到達できない：指定されたポートで待ち受け（リッスン）状態になっていない
4	DFフラグがセットされていてフラグメントできない：IPフラグメンテーションが必要だが、DFフラグがセットされているので、IPパケットをフラグメントすることができない。なおRFC1191（PMTU discovery）では、このメッセージを返す場合に、正しいMTU値をICMPヘッダ中に格納することを求めている
5	ソース・ルートの失敗：IPパケット中にソース・ルート（経由するルートの指定）が含まれているが、そのルートへルーティングすることができない
7～	そのほかのさまざまな理由（優先度指定やサービス・タイプの指定などが正しくないなど）によってIPパケットをあて先まで届けることができない。7以上のコードは、オリジナルのRFC（RFC792）では定義されておらず、その後の拡張によって定義されている

ICMPあて先不達の要因コード

タイプ5—ICMPリダイレクト

これは、ルーティングに関する情報を伝えるためのICMPメッセージである。IPパケットの送信先が適切でない場合に、ルータによって送信元に返信されることがある（ルータでしかサポートされていないメッセージである）。

以下の図をみて欲しい。いまPC1が、インターネットへ向けてIPパケットを送信しようとしている。だがPC1が属しているネットワークには、2台のルータ（ゲートウェイ）が存在し、片方のルータ1は社内ネットワークへ、そしてもう1つのルータ2はインターネットへそれぞれ接続されているものとする。通常、1台のマシンでは、デフォルト・ゲ

検索

ホワイトペーパー



セキュアSD-WANを見据えてルーティング処理を刷新、トヨタシステムの選択は？



検知してからどうするか!? 標的型サイバー攻撃における内部対策の提案



ネットワーク製品の導入に関する読者調査レポート(2014年12月)



もう「Wi-Fi 7」時代? 無線LANの気になる進化

HPE

GreenLake

無計画なハイブリッドクラウドから
計画的なハイブリッドクラウドへ。
かしこい選択。

スポンサーからのお知らせ


- PR -

重要なのは発展性 なぜ今、“ストレージ”に注目が集まっているのか


中堅中小企業の“ネットワーク課題”はこれで解決！

Special

- PR -



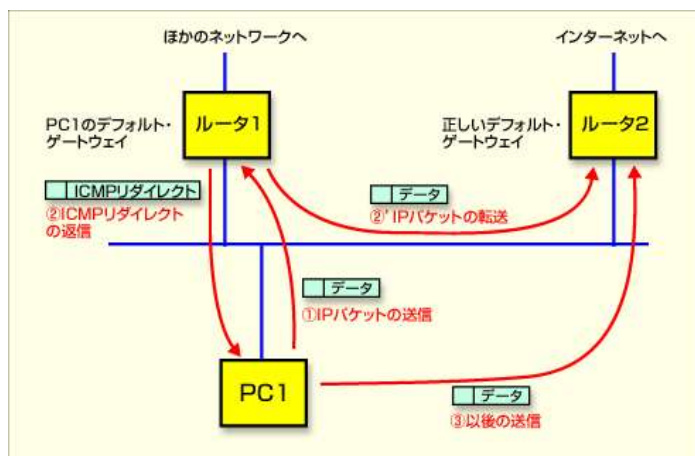
複数ベンダーの「継ぎはぎSASE」で生じる課題、どうすれば解決できるのか？



「ほとんど誰も見ていない」社内ポータル、どう変えるべき？
New!

データは「守りながら活用する時代」に

ートウェイ（明示的なルーティング経路が指定されていない場合に利用されるルータ）は1つしか定義することができない。この環境では、社内のほかのホストと通信することが多いので、デフォルト・ゲートウェイは「ルータ1」に設定されている。つまり、あて先がローカルのLANではないIPパケットは（社内ネットワークかインターネットかにかかわらず）、すべてルータ1に送られるということである。



ICMPリダイレクト・メッセージの送信

LAN上のマシンが適切でないルータに対してパケットを送信すると、IPパケットを別のルータへフォワードすると同時に、より適切なルータの存在をICMPリダイレクト・メッセージによってIPパケットの送信元へ通知する。

このような環境において、PC1がインターネットと直接通信を行おうとすると何が起るだろうか。



Special

- PR -

オンプレのハードウェアも「サブスク」の時代へ コストや契約はどう変わる？

PC1が例えばインターネット上のwww.mycompanysite.comへアクセスする場合、図中の (1) のように、最初のIPパケットはデフォルト・ゲートウェイであるルータ1に送られることになる（PC1におけるデフォルト・ゲートウェイはルータ1だから）。ローカルのLAN上に存在しないマシンと通信する場合、すべてのパケットはデフォルト・ゲートウェイに送られることになっているから、この動作は正常な動作である。

だが、ルータ1は直接インターネットに接続されているわけではない。ルータ1がインターネットにアクセスするためには、ルータ2にパケットを送り（ルーティングし）、そこからさらにインターネットへパケットをルーティングしてもらう必要がある（図中の (2) '）。ルータ1はインターネットに対する経路を知っているので、このような動作ができるのである。

以上の動作により、PC1からのパケットはインターネットへ送信されることになるが、ルータ1がいちいちパケットを中継することは明らかにムダな動作である。ルータ1の負荷が増えるだけでなく、時間的にもロスするからだ。そこで登場するのがこのICMPのリダイレクト・メッセージである。

ルータ1がパケットをルータ2にフォワードするとき、同時に、パケットの送信元であるPC1に対して、ICMPリダイレクトのメッセージを返信しておく（図中の (2) ）。このパケット中には、「指定されたあて先（この場合は、インターネット上の特定のホスト）に到達するためには、ルータ2を使う方がよい」というメッセージが含まれている。

このICMPリダイレクトを受け取ったPC1は、自身のルーティング・テーブルに対して、「www.mycompanysite.com（のIPアドレス）に到達するためには、ルータ2を使う」というルーティング・テーブルのエントリを追加する。これにより、以後の通信はすべ



「守る」だけでは不十分 今どきのストレージには何が必要？



社内ルールだけでは限界 有名無実化した「ローカル保存禁止」にどう対応？



オンプレのハードウェアも「サブスク」の時代へ コストや契約はどう変わる？



「ネットワークが分からない」状態からでも丸ごとサポート New!



自分が作ったアプリがスマホで動くさまを見ると、学生の目が輝くんです New!



NTTデータと日本IBMがタッグ！ AIは仕事をどう変える？

@IT Special へ

Windows Server Insider 記事ランキング

本日

月間

Excel（エクセル）で日付から自動的に曜日を入力する

【Excel】重複データを色付けして瞬時にダブりをチェックする

【Excel】パスワードロックを強制的に解除する方法

TCP/IP通信の状態を調べる「netstat」コマンドを使いこなす【Windows OS】

Windows OSのdirコマンドでファイル名の一覧を取得する

システム要件を満たさないPCをWindows 11 2023 Update（23H2）にアップデートする方法

【Windows 10/11】えっ、UTF-8じゃなくてShift-JISで？ お手軽文字コード変換方法まとめ

PDFファイルにキーボードから直接文字入力する方法【本家Acrobat Reader編】

Excelの落とし穴「先頭のゼロ（0）」問題の対処法

【Windows 10/11】PCが数分で勝手にスリープするのを防ぐ

ランキングをもっと見る

あなたにおすすめの記事

- PR -



中堅中小企業の“ネットワーク課題”はこれで解決！ New!

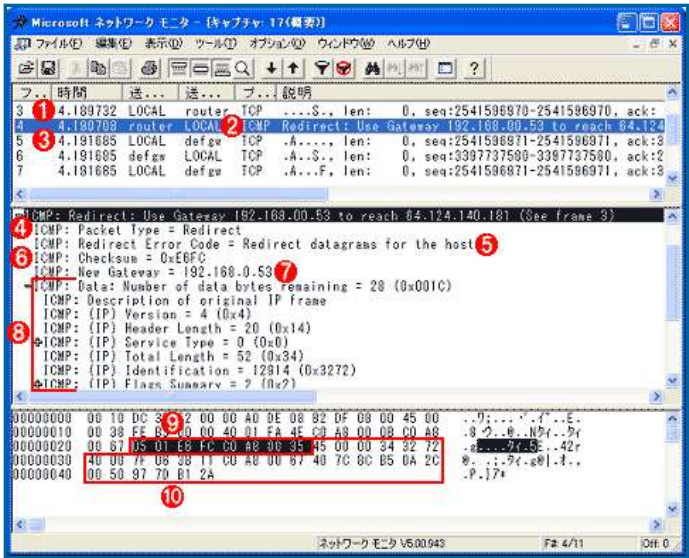


オンプレのハードウェアも「サブスク」の時代へ コストや契約はどう変わる？

て直接ルータ2と行われることになり（図中の **(3)**）、無駄なトラフィックが抑えられることになる。

以上のような仕組みにより、取りあえず正しいルートへのルーティングが行われるようになる。ただしこのようにして追加されたルーティング・テーブルのエントリは動的なものであり、時間が経つと自動的に削除されてしまう（ルーティング・テーブルの増大の抑制や、ルータ・アドレスの動的な変更などに対処するため）。また、1ホストIPアドレスごとに1エントリずつ作られるので、ルーティング・テーブルのサイズも大きくなってしまいうという問題点がある。可能ならネットワークの設計を変更して、このようなICMPに頼らなくても済むようにするのが望ましいだろう。

以下にICMPリダイレクトによってルートが変更されている例をあげておく。



ICMPリダイレクトの例

ICMPリダイレクト・メッセージの解析例。その直前にあるpingコマンドは、デフォルト・ルータに送られたが、それは適切なルートではないので、ICMPリダイレクトが返されている。以後のパケットは、別のルータへ送られている。

- (1) 最初のTCP要求パケットはルータ「router」へ送っている。
- (2) routerからICMPのリダイレクト・メッセージが送り返されてきた。
- (3) 以後のパケットは、(2) で指示された別のルータ「defgw」へ向けて送信されている。
- (4) ICMPのリダイレクト・メッセージ。
- (5) コードは0x01。特定のホストに対するリダイレクトの要請。
- (6) チェックサム。1の補数演算。
- (7) より適切な、新しいゲートウェイのIPアドレス。
- (8) オリジナルのIPパケットの先頭部分の情報のコピー。リダイレクトの原因などを調査する場合に利用できる。
- (9) ICMPリダイレクト・メッセージのヘッダ部分。
- (10) オリジナルのIPパケットの先頭部分の情報のコピー。

タイプ11—ICMP時間超過

これは、ルーティングの途中で、時間（回数）が超過してしまった場合に、IPパケットの送信元に対して返信されるICMPメッセージである。

このメッセージが生成される要因は2つある。1つは、IPヘッダ中のTTLが0になってしまった場合である。IPヘッダ中には、TTLというフィールドがあり、ルータによってパケットがフォワードされるたびに1ずつ減算される。このTTL値が0になると、そのIPパケットは破棄され、IPパケットが無限にルーティングされるのを防いでいる。そのとき、同時に元の送信元に対してICMPの時間超過メッセージが送られ、送信元では、パケットが経路の途中で破棄されたことを知ることができる。もしこのメッセージが返されないとなると、パケットが相手まで届いたかどうかを知ることが困難になるだろう（ルータによって破棄されたか、それとも相手からの応答が遅れているのかを区別するのが難しくなる）。ちなみにWindowsのtracertコマンドは、このメッセージを受信することによって、パケットがどこまで届いたかを調べている。



自分が作ったアプリがスマホで動くさまを見ると、学生の目が輝くんです **New!**

@IT Special

ミドルの転職・AMBIの人気コンテンツ - PR -



若手7割がスタートアップ転職に意欲 | AMBI (アンビ)



あなたの職務適性が15分でわかる | AMBI (アンビ)

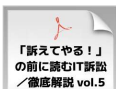


官公庁関連の厳選求人、多数掲載中！「ミドルの転職」

@IT eBook



解決！Python CSVファイル編



誰か、要件追加を止めてくれ！——「旭川医大の惨劇」徹底解説



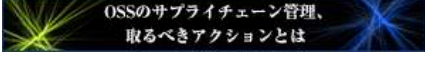
目指せ、共有フォルダ管理の達人！ Windowsファイル共有を“極める”ためのPowerShellコマンドレット基本集



IT人材ゼロでDX!? お悩み中小企業のためのDX推進が分かる無料の電子書籍とは

一覧ページへ

注目のテーマ



システム開発ノウハウ【発注ナビ】 - PR -



受注ゼロから一転、開発会社が2000万円の案件を獲得できた理由



「React.js」を使った開発で実績豊富な15社



「AI開発」でおすすめの25社【2023年版】

次の例は、TTLを5にしてwww.microsoft.comというホストへpingを実行してみた場合の例である。TTLが5しかないようだと、たいていの場合は、プロバイダのネットワークの中でパケットが破棄されることになるだろう。

```
C:\>ping -n 1 -i 5 www.microsoft.com ...TTLを5にしてpingしてみる
```

```
Pinging www.microsoft.akadns.net [207.46.249.190] with 32 bytes of data:
```

```
Reply from 210.153.XXX.XXX: TTL expired in transit.
```

```
...TTLが尽きて破棄された。このIPアドレスはプロバイダのネットワークの中。
```

```
Ping statistics for 207.46.XXX.XXX:
```

```
Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
```

```
Approximate round trip times in milli-seconds:
```

```
Minimum = 0ms, Maximum = 0ms, Average = 0ms
```



このICMPメッセージが生成されるもう1つの要因としては、IPフラグメントの再構成の失敗がある。ルーティングの途中でIPパケットのフラグメンテーションが行われた場合、最終的にIPパケット全体を再構成するためには、すべてのフラグメントがそろうまでである一定時間待つ必要がある。だが、あらかじめ決められた時間（例えば30秒など）待っても全体がそろわない場合は、再構成をあきらめ、同時にこのICMPメッセージを送り返すことになっている。

その他のICMPメッセージ

以上のほかにもいくつかのICMPメッセージがあるが、あまり使われることがない、もしくは専門的すぎるので、ここではいくつかを簡単に解説するととどめておく。

■ソース・クエンチ（送信元抑制）

このメッセージは、ネットワークが高負荷／過負荷状態であることを示すために使われるメッセージである。パケットをルーティングしようとしたけれども、ネットワークが過負荷状態になっていて送信が困難な場合、このメッセージをIPパケットの送信元に送り返して、送信を一時的に抑制してもらうために利用されることになっている。だが実際には、そのようなメッセージを送信することすら困難であったりするので、現実的には利用されていない。

■アドレス・マスク要求／応答

アドレス・マスクの情報を取得するために利用される。IPネットワークにおけるルーティングでは、ネットワーク・アドレスとホスト・アドレスをきちんと区別することが重要であるが、このICMPメッセージは、ネットマスクの情報をルータから動的に取得するために用意されている。

パスMTU検出（path MTU discovery）

これは特定のICMPメッセージではないが、ICMPを使った機能の1つなのでここで紹介しておく。

経路途中にMTUサイズの小さなネットワークが存在する場合、ルータによってIPパケットのフラグメンテーションが行われる。だが、フラグメント化と再構成は、ルータにとっても、通信相手のコンピュータにとっても負荷のかかる処理であり、可能ならば避けることが望ましい。そこであらかじめ通信ルートのMTUが分かっているならば、最初からそのMTUサイズに合わせて、フラグメンテーションの不要な、適切なサイズのIPパケットを送信することができる。このような経路途中のMTUサイズを調査する方法を「PMTU検出（Path MTU discovery）」といい、[RFC1191](#)で標準化されている。

PMTUの原理は簡単である。DFフラグ（フラグメント禁止フラグ）を有効にして、サイズをいろいろに変更したIPパケットを送信してみる。先のpingコマンドの例で示したように、MTUサイズを超える大きなパケットをDFフラグ付きで送信すると、その直前のルータから「ICMPあて先不達」のメッセージが戻ってくる（このとき、ICMPヘッダ中に正しいMTU値をセットしてから返すように求められている）。これにより、特定のネットワークにおけるMTUサイズを知ることができる。ただし、フラグメント化されたパケットのルーティングや、（セキュリティ上の理由などによって）それに対するICMPあ

て先不達メッセージの送信を禁止しているようなルータがあれば（このようなルータは「ブラックホール・ルータ」と呼ばれることがある。外部に対しては何もメッセージを返さないからである）、このPMTU機能は正しく働かない。そのため、Windows OSなどでも、この機能を使うかどうかをレジストリで制御することができるようにしている（参考情報：「Microsoft Windows 2000 TCP/IP 実装詳細」）。

次の回へ >>

インデックス ●● 「連載 基礎から学ぶWindowsネットワーク — Windowsネットワーク管理者への道 — 」

前のページへ

1

2

3

Copyright© Digital Advantage Corp. All Rights Reserved.



基礎から学ぶWindowsネットワーク 連載一覧

全 23 回

新しい連載記事が 9 件あります	
第14回	信頼性のある通信を実現するTCPプロトコル（その1）
第13回	データグラム通信を実現するUDPプロトコル
第12回	TCP/IPプロトコルを支えるICMPメッセージ
第11回	MACアドレスを解決するARPプロトコル
第10回	IPパケットの構造とIPフラグメンテーション
過去の連載記事が 9 件あります	

Special

データは「守りながら活用する時代」に

NTTデータと日本IBMがタッグ！ AIは仕事をどう変える？

「守る」だけでは不十分 今どきのストレージには何が必要？

ローコードツールの現在地。AI、機械学習とのシナジーで新たな価値を生み出す **New!**

オンプレのハードウェアも「サブスク」の時代へ コストや契約はどう変わる？

社内ルールだけでは限界 有名無実化した「ローカル保存禁止」にどう対応？

「ほとんど誰も見ていない」社内ポータル、どう変えるべき？ **New!**

中堅中小企業の“ネットワーク課題”はこれで解決！ **New!**

@IT Special >

この記事に関連する製品／サービスを比較（キーマンズネット）

まずネットワークの性質を十分に見極めよう！『ネットワーク管理』製品比較

構築したいネットワーク要件で大きく変わる『ルーター』の選び方

L4負荷分散とL7負荷分散どちらを重視？『ADC／ロードバランサ』製品一覧

既存のネットワーク構成とマッチする？『WAN高速化』製品の選び方

信頼性や可用性に対する取り組みは？『ネットワークスイッチ』製品比較

印刷

通知

見る

Share

18

@ITについて

[お問い合わせ](#)

[広告について](#)

[採用広告について](#)

[利用規約](#)

[著作権・リンク・免責事項](#)

[サイトマップ](#)

RSSについて

[@ITのRSS一覧](#)

アイティメディアIDについて

[アイティメディアIDとは](#)

メールマガジン登録

@ITのメールマガジンは、もちろん、すべて無料です。ぜひメールマガジンをご購読ください。

申し込みページへ