BackOffice 原稿(１回目)
「入門・ビギナーのためのネットワークトラブル対策」

奥川博司

この連載では、青葉マークをつけたようなWindows NT 管理者の方を対象として想定し、主にネットワークのトラブルシューティング力を向上させるお手伝いができればと思います。まず、最初はトラブルシューティングに役に立つネットワーク系のコマンドラインユーティリティの説明をおこなってゆきます。

コマンドラインユーティリティを使う前に

コマンドラインユーティリティを良く使う場合は、\Winnt\System32\Cmd.exe のショートカットをデスクトップに置いておくと便利です。また、[コンソール]コントロールパネルにて、使いやすいように設定しておくことをお勧めします、[レイアウト]ページにて 画面バッファのサイズの高さを 200 ぐらいに、ウィンドウのサイズでも高さを 40 程度にしておくと良いと思います。

Windows NT の場合は、カーソルキーの上下で そのコマンドプロンプトを開いてから入力されたコマンドを記憶しているので同じコマンドを入力する際の手間を省いてください。ちょっとしたことですが、知っていると知らないとでは随分 効率が違います。

ヘルプファイルは結構 便利

たいていの コマンドラインユーティリティでは -? あるいは /? を付けて起動することで 使い方や実行時引数の説明が表示されますが、英語で表示されるものがほとんどです。そこで頼りになるのが ヘルプファイルです。

Windows NT の場合は、[スタート]メニューから [ヘルプ]を選択し 目次 の 「Windows NT コマンド」「Windows NT コマンドリファレンス」を選択すると コマンドラインユーティリティの説明を参照することができます。Windows 95の場合は残念ながらヘルプファイルでこれらのコマンドラインユーティリティについて説明されているページを見つけることができなかったのですが、今回 紹介したコマンドに関するリファレンスは最後に付けておきますのでご参照ください。

表1 に、ネットワーク関係のコマンドを示します。

ipxroute とnet 系のコマンド以外は、TCP/IP プロトコルがインストールされていないと無効となりますが、ほとんどの方は TCP/IP を利用されていると思いますので ここでは、TCP/IP プロトコルがインストールされていることを前提として話を進めてゆきます。

これらのコマンドのなかから今回は、ping, arp, tracert, nbtstat などについて説明していきたいと思います。

表1.ネットワーク関係のコマンド一覧

コマンド名	
arp	finger
ftp	hostname
ipconfig	ipxroute
lpq	lpr
nbtstat	netstat
net (コマンド オプション)	nslookup
ping	rcp
rexec	route
rsh	tftp
tracert	

Pingコマンド

最近ではPing という言葉はかなり一般的になってきているように思えますのでご存知の方も多いとおもうのですが、一応 基本ということでご説明しておきます。

トラブルシューティングには欠かせないのがこのPing コマンドです。簡単に言うと このコマンドは指定した相手に「返事をください」というパケットを送信して、その返事が返ってくるかどうか またどのぐらい時間がかかったかを調べるためのものです。ping [IP アドレス] や、 ping [ホスト名] と入力することで実行します。実行画面を 図１ に示します。

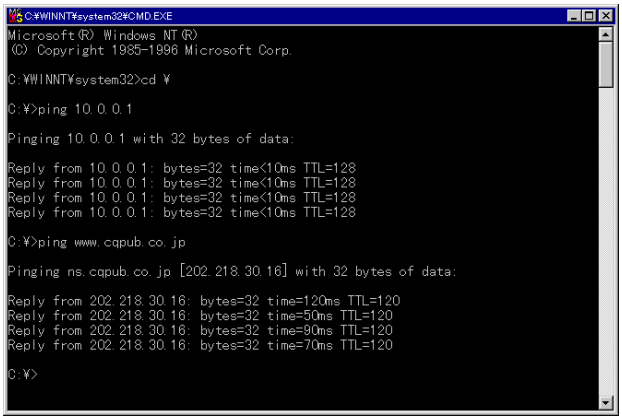

図１. pingの実行画面

最初のLAN 上にある端末(この例では、10.0.0.1)へのPing 結果からは 32bytes のデータ部分を持つパケットを送信したら 応答時間は 10ms 以下でTTL(Time to Live)というそのパケットの寿命をあらわしている値は 255だったということがわかります。次のCQ 出版のWeb サーバへPing をした結果では、応答時間が約80ms 程度でTTL が120となっています。

使い時は、やはり相手のマシンが生きているのか死んでいるのかを調べたいときでLAN においてはPing を実行しても応答が無い場合は相手マシンが死んでいるか あるいは 途中経路が遮断されていないかどうかを確認すべきです。このとき 例えばルータを介している場合には、ルータに対してもPing 行ったり、対象マシンの近くにあるマシンに対してもPing を行っておくことで 対象マシンだけが通信できないのか それともその辺り一帯にある端末全てに対して通信できないのかを調べておくことで トラブル箇所の特定をスムーズに進めることが可能です。*1

Ping コマンドの少し変わった利用法としては、Ping -t -l 65500 [宛先] というオプションを指定すると、65500bytes のデータ*2をCtrl+Cなどして割込みを発生させない限り応答確認パケットを送受信することになりますので ネットワークへ若干の負荷をかけることができたり(とはいえ パケットの発生間隔は結構 長いのでLAN においては、それ程の負荷にはなりません)、Ping -a [IP アドレス] とすることでIP アドレスからホスト名への変換を行わせることもできます。

ARPコマンド

アドレス・リゾリューション・プロトコル(ARP)と同一の名前を持つコマンドです。ARP とは、IP アドレスからMAC アドレス*3を検索するためのプロトコルです。MAC アドレスは規約的には、全世界において一意であることが保証されているため イーサネットでは、宛先や送り元を特定するためにMAC アドレスが利用されます。
さて、ARP コマンドですが その役割は、ARP によって解決されたIP アドレスとMAC アドレスの対比を示すARP テーブルの参照や、ARP テーブルからのエントリの削除、ARP テーブルへのエントリの手動登録などができます。このARP テーブルのエントリは一度解決したアドレスを永久に保持しているわけではなく、最近通信を行った機器のアドレスを一定期間だけの保持しています。
このコマンドを実行するときに一番利用頻度が高いオプションは、「arp -a」でのARP テーブルを表示だと思います。実行した画面を 図2 に示します。

"No ARP Entries Found" は、ARP テーブルが空であるということなので、最近 通信が行われていないことが見て取れます。ここで属しているネットワークに対してping のブロードキャストを実行してみましょう。(この例では、端末が属しているのが 10.* というネットワークですので 10.255.255.255 というアドレスに対してPing を行っています)
Ping が終了した後、おなじく 「arp -a」コマンドを実行すると

*1 Internet上に存在するマシンに対しては 意図的に Pingに応答しないように設定されているものもありますので、Pingの応答が無くても単純に死んでいると判断することはできません
*2 NT 4.0のヘルプでは データサイズの最大値は 8192となっているのですが、実際には 65500まで指定できるようです
*3 インターフェースアドレス、物理アドレスなどとも呼ばれます。ちなみに、MACは Media Access Controlの略です

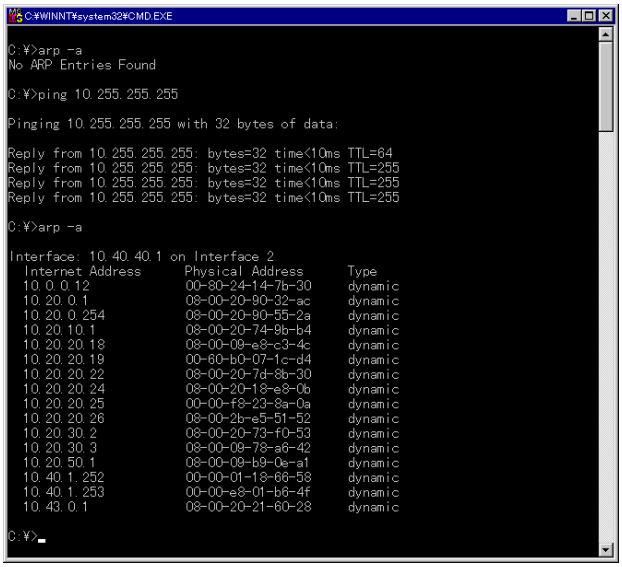

図2. arpの実行画面

ARP テーブルに 反応があった機器のエントリが追加されていることがお分かりいただけると思います。
アプリケーションによっては、エラー時のログメッセージなどでIP アドレスではなくMAC アドレスを表示するものもありますので、ARP コマンドを実行されることで 表示されるARP テーブルをExcel などで管理されるといざというときに役に立つこともあるかと思います。また、MAC アドレスの先頭6文字には、ベンダ ID 呼ばれる各ベンダ固有の値が使用されているため 機器種別が大まかに類推可能であったりします。代表的な ベンダ ID を 表2に示します。*4

Tracerouteコマンド

Traceroute コマンドは、その名の通りRoute(経路)をTrace(追跡)するコマンドです。UNIX では、tracerotueとフルスペルなのですが、Windows のコマンドではtracert.exeと短縮された名前になっています。
Tracert コマンドも内部的にはPing コマンドを実行したときと同じようなことを行っているのですが、違うのは目的とした機器に到達するまでの 道のりを示すために一つルータを越える度に、その機器のホスト名、IP アドレスと応答時間を表示するところです。
ホスト名を見れば大体の場所は想像できますので、国内の回線が遅くなっているとか、目的の機器まであと少しなのだが そこがすごくボトルネックとなっているなどといったことを類推することができます。
Tracert を使うのは、何処が混んでいるのかを知るときぐらいで 社内ネットワークでのトラブルの解決にはあまり使わないかもしれませんが、外部へアクセスする際にレスポンスが悪い場合は、試しにTracert を実行してみることで どこが原因かを調べてみるのも良いと思います。

*4 更に詳しく知りたい場合は http://standards.ieee.org/regauth/oui/index.html などを参照してください

表2.代表的なベンダーコード

ベンダーコード	ベンダー名
00000C	CISCO
00000E	Fujitsu
00001B	Novell
00004C	NEC
000087	Hitachi
0000E2	Acer
0000E8	Accton
0000F4	Allied
0000F8	DEC
002035	IBM
004026	MELCO
00805F	Compaq
008098	TDK
00A024	3COM
00A0C9	Intel
00A0DE	YAMAHA
00C04F	DELL
080020	Sun
080007	Apple
00A0B0	I-O DATA

また、Tracert はデフォルトでIP アドレスから ホスト名の変換を行いますので、Web サーバのアクセスログなどを見る際に、2つ3つIP アドレスからホスト名を知りたい時などTracert コマンドは手軽に利用することができます。
Tracert には、あまりオプションは無くtracert [宛先] という使い方さえ覚えておけば良いと思います。実行画面を 図3 に示します。

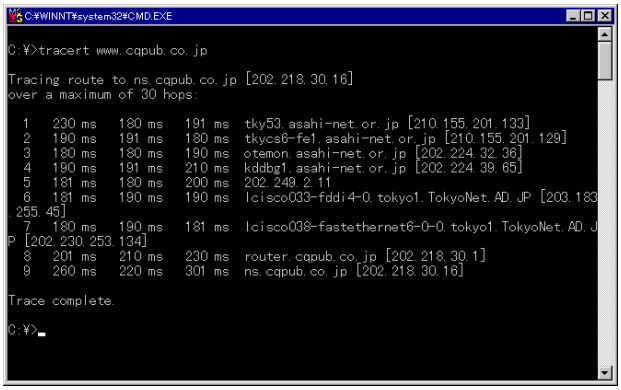

図3. tracertの実行画面

Nbtstatコマンド

Nbtstat コマンドでは、NetBIOS over TCP/IP というTCP/IP プロトコルの上層で動くNetBIOS に関係する情報を表示することができます。
リモートの端末に関する情報を取得するために役にたつのが -A オプションです。NetBIOS 名がわかっている場合はnbtstat -a [名前]、IP アドレスがわかっている場合はnbtstat -A [IP アドレス]などとして実行します。前述のPing のブロードキャストで、ネットワークに接続されているIP アドレスのリストを得た後にnbtstat -Aを利用してさらに詳しい情報を取得できれば 図4 のように、現在 その端末にログインしているユーザ名なども得ることができるためその端末の利用者などを推測するための有力な手がかりを得ることができます。この例では、COCKTAIL というドメインのJINRO という端末の情報を表示した結果です。ここで表示されている <03>などといった表記は 表3、表4に示すような意味を持っています。
またNbtstat コマンドでは、現在 そのような自分の端末に対して現在どのような接続が行われているか、どの程度の入出力があったかをnbtstat -sあるいは、 nbtstat -Sとして実行することで表示することもできます。小文字の場合は、リモートホスト名がNetBIOS 名で、大文字の場合は、IP アドレスにて表示されます。ほかにもnbtstat -cとすることで、キャッシュテーブルに残っているリモート端末の名前を表示することができます。

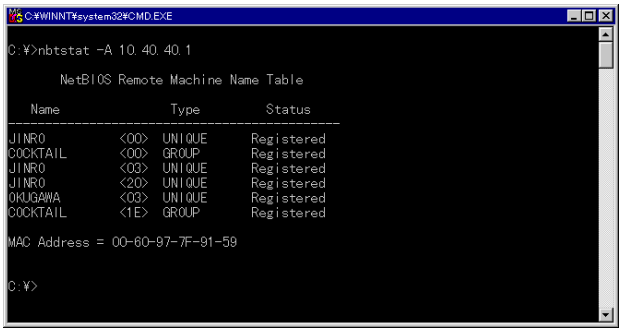

図4. nbtstatの実行画面

表3. NetBIOSのサービス名

<00>	ワークステーションサービス名。一般にはNetBIOSコンピュータ名と呼ばれる
<03>	メッセンジャーサービス名。コンピュータ名と現在ログオンしているユーザ名に付与される
<1B>	ドメインマスタブラウザ名
<06>	RAS サーバサービス
<1F>	NetDDE サービス
<20>	ファイル共有のためのサーバサービス名
<21>	RAS クライアント
<BE>	ネットワークモニタエージェント
<BF>	ネットワークモニタユーティリティ

(一意なNetBIOSコンピュータ名に付与されるもの)

表4. NetBIOSのサービス名

<1C>	ドメイングループ名
<1D>	マスタブラウザ名
<1E>	グループ名
<20>	管理グループを識別するための特殊グループ名
MSBROWSE,	別のマスタブラウザにドメイン名を知らせるためにローカルサブネット上でブロードキャストすることを示す

(NetBIOSグループ名に付与されるもの)

◇ Ping

リモート コンピュータ、またはコンピュータへの接続を検査します。このコマンドはTCP/IPプロトコルがインストールされている場合のみ有効です。

ping [-t] [-a] [-n count] [-l length] [-f] [-i ttl] [-v tos] [-r count] [-s count] [[-j computer-list] | [-k computer-list]] [-w timeout] destination-list

● パラメータ

-t

割り込みが発生するまで、指定したコンピュータを検査します。

-a

アドレスを解決してコンピュータ名に変えます。

-n count

countで指定した数のECHOパケットを送信します。既定値は 4 です。

-l length

lengthで指定した量のデータが入っているECHOパケットを送信します。既定値は 32 バイトです。最大値は 8192 です。

-f

Do Not Fragmentフラグをパケットに入れて送信します。パケットは、ルート上のゲートウェイによってフラグメント化されることはありません。

-i ttl

Time To Liveフィールドをttlで指定した値に設定します。

-v tos

Type Of Serviceフィールドをtosで指定した値に設定します。

-r count

発信パケットと返信パケットのルートをRecord Routeフィールドに記録します。countには、最小で 1 つ、最大で 9 つのコンピュータを指定することができます。

-s count

countで指定した数のホップに対してタイムスタンプを指定します。

-j computer-list

computer-listで指定したコンピュータ一覧を経由してパケットをルーティングします。連続したコンピュータは、中間ゲートウェイで区切られる可能性があります (loose source routed)。IPで許される最大数は 9 です。

NetBIOS over TCP/IP

NetBIOS は、ネットワーク上の端末間でやりとりを行うために定められたアプリケーションインターフェースのことで、通信プロトコルは定義していなかったのですが、後にNetBIOS インターフェースに基づくNetBEUI プロトコルが登場し しばらくの間はNetBIOS NetBEUIと認識されていたような時期がありました。しかしNetBEUI は 比較的規模の小さなネットワークしか考慮しておらずルータを越えることができないプロトコルだったために出てきたのが、TCP/IP 上のNetBIOS インターフェースNetBTや、IPX/SPX 上のNetBIOS インターフェースNWLink NetBIOS です。

NetBT では、NetBIOS の名前解決の仕組みを拡張してDNSへの問い合わせを利用可能にしているなど利便性を向上させているのですが、仕組みを細かく知ろうとする方にとっては この辺りが話しを複雑にしてしまっているようです。

以下では、NetBT を使用するときTCP/IP のどのポート番号が利用されているのかを利用されているかを説明します。通常 外部へ接続するルータなどでは以下のポートは通過しないように遮断しておくのが一般的です。

■ UDP ポート 137 (ネームサービス)

NetBIOS の名前解決のためには、NetBT ネームサービスとして定義されているUDP ポート137でブロードキャストが送信されます。

通常 ルータはブロードキャストパケットは全て遮断するのですが、LAN においてNetBT によるブラウジングを可能にするために、この ポート番号のパケットを転送するように設定することもあります。

■ UDP ポート 138 (データグラムサービス)

NetBIOS にはデータグラムというコネクションレス型の通信手段が用意されており、受信確認が必要ないデータをネットワーク上のひとつ、あるいは複数に対して送信することができます。例えば同じグループに属している端末すべてにメッセージを伝えるために、そのグループの宛先 ID に対してひとつのデータグラムを送ることで目的が達せられたりします。

データグラムには、UDP ポート 138が利用されます。

■ TCP ポート 139 (セッションサービス)

NetBIOS には信頼性の高い通信を行うために、セッションと呼ばれるコネクション型の通信手段があります。これは、ネットワーク上の２つの名前同士(ここで言う名前とは、NetBIOS ネームサービスで使用される 一意な名前の事です)でデータ転送を行うためのもので、通常 サーバからファイルをコピーする場合などは、セッションによって通信が行われます。

セッションによる通信には、TCP ポート 139が利用されます。

-k computer-list

computer-listで指定したコンピュータ一覧を経由してパケットをルーティングします。連続したコンピュータは、中間ゲートウェイで区切られません (strict source routed)。IPで許される最大数は 9 です。
-w timeout
タイムアウトの間隔をミリ秒単位で指定します。
destination-list 検査するリモート コンピュータを指定します。

◇ Arp
アドレス解決プロトコル (ARP) で使われるIPとイーサネットまたはトークン リングとの物理アドレス変換テーブルを表示、および修正します。このコマンドはTCP/IPプロトコルがインストールされている場合のみ有効です。
arp -a [IP アドレス] [-N [インターフェイスアドレス]]
arp -d IP アドレス [インターフェイスアドレス]
arp -s IP アドレス イーサネットアドレス [インターフェイスアドレス]
● パラメータ
-a
TCP/IPに照会を行い、現在のARPエントリを表示します。IPアドレスを指定すると、指定したコンピュータのIPおよび物理アドレスのみを表示します。
-g
-aと同じ。
IPアドレス
IPアドレスをドット区切り 10 進表記で指定します。
-N
インターフェイスアドレスで指定したネットワーク インターフェイスのARPエントリを表示します。
インターフェイスアドレス
アドレス変換テーブルを修正しなければならないインターフェイスのIPアドレスがあれば、指定します。ない場合は、最初の適切なインターフェイスが使用されます。

-d
IPアドレスで指定したエントリが削除されます。
-s
ARPキャッシュにエントリを追加し、IPアドレスを物理アドレス (イーサネット アドレス) に関連付けます。物理アドレスは、ハイフンで区切った 6 個の 16 進バイトとして入力します。IPアドレスは、ドット区切り 10 進表記で指定されます。このエントリは永続的です。つまり、タイムアウトの時間が終了した後でも、キャッシュから自動的に削除されることはありません。
イーサネットアドレス
物理アドレスを指定します。

◇ Tracert
tracert [-d] [-h最大ポップ数] [-jコンピュータ一覧] [-wタイムアウト] ターゲット名
この診断ユーティリティは、ICMP (Internet Control Message Protocol; インターネット制御メッセージ プロトコル) エコー パケットにさまざまなTTL (Time-To-Live; 有効期限) の値を載せて宛て先に送信することで、宛て先へのルートを突き止めます。パス上の各ルーターでは、パケットを送信する前に、パケット上のTTLを少なくとも 1 だけ減少させる必要があります。こうすることで、TTLは実際のホップ カウントになります。パケット上のTTLが 0 になったら、ルーターは、送信元システムにICMP Time Exceeded メッセージを送り返すことになっています。tracertは、まず、エコー パケットにTTL値 1 を載せて送信し、次のルーターにエコー パケットが送信されるたびにTTLを 1 だけ増分していきます。ターゲットが応答するか、最大TTLに達するまでこれを継続します。tracertは、中間のルーターから送り返されたICMP Time Exceeded メッセージを調べてルーターを突き止めます。ルーターの中には、有効期限の切れたパケットを何の通知も出さずに送出しないものがあることに注意してください。この場合、tracert
ではこの種のルーターは見えません。
● パラメータ
-d
アドレスからコンピュータ名への解決を実行しません。
-h最大ホップ数
ターゲット検索用の最大ホップ数を指定します。
-jコンピュータ一覧
コンピュータ一覧の記述に沿って緩やかな送信元ルート (loose source route) を指定します。
-wタイムアウト
タイムアウトで指定したミリ秒だけ、応答するのを毎回待ちます。
ターゲット名
ターゲット コンピュータの名前です。

◇ Nbtstat
この診断コマンドはプロトコルの統計情報と、NBT (TCP/IP上のNetBIOS) を使う現在のTCP/IP接続を表示します。このコマンドはTCP/IPプロトコルがインストールされている場合のみ有効です。
nbtstat [-aリモート名] [-A IP アドレス] [-c] [-n] [-R] [-r] [-S] [
-s] [間隔]
● パラメータ
-aリモート名
指定したリモート名を使ってリモート コンピュータの名前テーブルの一覧を表示します。
-A IPアドレス
指定したIPアドレスを使って、リモート コンピュータの名前テーブルの一覧を表示します。
-c

各名前のIPアドレスを提供するNetBIOS名キャッシュの内容を一覧表示します。
-n
ローカルNetBIOS名の一覧を表示します。"Registered" は、ブロードキャスト (Bnode) またはWINS (別のノード型) によりその名前は登録されていることを表します。
-R

NetBIOS名キャッシュからすべての名前を取り除いた後で、LMHOSTSファイルを再読み取りします。
-r
Windows ネットワークの名前解決統計情報の一覧を表示します。WINSを使用するように構成されたWindows NT コンピュータでは、このオプションは、ブロードキャストまたはWINSを介して解決した名前および登録した名前の数を返します。
-S
IPアドレスのみによるリモート コンピュータを一覧表示して、クライアントおよびサーバー セッションの両方を表示します。
-s
クライアントおよびサーバー セッションの両方を表示します。リモート コンピュータのIPアドレスをHOSTSファイルを使って名前に変換しようとします。

間隔
指定した秒間隔で、選択した統計情報を再表示します。統計情報の再表示を停止するには、Ctrl + Cキーを押します。このパラメータが省略されると、nbtstatは、現在の構成情報を一度だけ印刷します。

◇ 参考文献

Microsoft Windows NT 4.0 Server ネットワーキングガイド　アスキー出版局
Windows 3.1 プログラミングバイブル2 Best of Microsoft Systems Journal Vol.3　株式会社アスキー
Windows NT ヘルプファイル