ネットワーク診断ツール

1V−1

川副 博
日本アイ・ビー・エム株式会社
東京基礎研究所

1 はじめに

事業所規模でのネットワークの事故を3回経験した。各回とも、最初に全てのサーバマシンを調べ、これらが不調が理由ではないことを確認した。その後、市販のネットワーク観測装置を使ってネットワーク（とつながっているマシンと）を調べて、原因を発見した。この経験を体系づけ、診断支援ツールを作成したので報告する。

ネットワーク　使用中のネットワークはトークンリングを主としたものである。基幹トークンリングにブリッジを介してサブリングが継っている。サブリング上にはゲートウェイがいくつかあり、トークンリング、イーサネットと継っている。別のゲートウェイを介して他事業所とも継っている。ネットワーク上にはTCP/IP, NETBIOS, SNA のプロトコルのフレームが流れている。

ネットワーク観測装置はトークンリング上で接続された点を通るフレームを表示、ファイルに記録できる。ファイル容量の制限から1回に記録できる時間は2分程度である。特殊なトークンリングカードを持つパソコンとプログラムから成っている。

事故の例　半日以上ネットワークが使えなくなった事故として, TCF Cluster（IP でのプロトコル番号87を使う[1]）によるネットワーク混雑を発端とするものがある。例としてこれを使うので概略を述べる。

サブネット上で TCF Cluster を組んでいたグループがサブネットと基幹トークンリングとの間に新たなゲートウェイを追加された。Cluster 間でのデータグラムが基幹トークンリングを経由するようになり、基幹トークンリングが飽和した。他の事業所で当事業所のネットワークの不調に気付き、当事業のサーバーマシンに向けて大量に ping した。パソコンの LAN サーバが暴走しリクエスタに対してデータグラムを大量発行した。

2 体系

上の事故での回復作業の経験をもとにして、当事業所のネットワーク用に次の体系を帰納した。

- 正常時のトークンリングの特徴と異常時の特徴とを比較して異常を発見する。

ここで特徴というのは、次の3点である。

1. リングでの1秒当たりのフレーム数
2. LLC の一つ上のレベルでのプロトコルのフレーム数の比 (TCP/IP,NETBIOS,SNA)
3. TCP/IP のプロトコルのフレーム数の比

上の特徴を正常時と異常時とを比較すると、異常時にはそれぞれフレーム数が多い、あるプロトコルが多いという形で異常が現れるので、原因究明中は上の特徴を抽出することを省き、フレームを多く発行しているマシンから点検するという方法もある。

3 有効性

正常時と実際の事故の時とでのこれらの特徴の違いを示す。図1から図3まではネットワーク観測装置の記録を診断支援ツールで解析し、(表計算ソフトで) グラフ化したものである。各グラフとも横軸は1つの記録（10秒から2分程度）に対応している。1から13までが事故時、15から28が正常時である。表1に事故の内容を示す。

3.1 リングでの1秒当たりのフレーム数（図1）

正常時は秒当たり 100 フレーム以下である。3, 6, 8 は異常だとわかる。事故時の他の記録で、ネットワークが異常なのにこの特徴が正常時と変わらない理由は、ネットワークが使えなかったのでユーザの多くがマシンを使っていなかった。このため、普段なら発生するトラフィックが発生しなかった。このマイナス分に異常に発生したトラフィックが隠れたためである。このことは次の2つの特徴で裏付けられる。

3.2 LLC の一つ上のレベルでのプロトコルのフレーム数の比（図2）

正常時は TCP/IP が 60 ～ 90%を、NETBIOS が 5 ～ 30%をそれぞれ占めている。NETBIOS の比率が 70%以上なので、6, 7, 8, 10, 12 での事故の原因は NETBIOS を使うマシンだと推測できる。

Network Diagnostic Tool
Hiroshi KAWAZOE
Tokyo Research Laboratory, IBM Japan, Ltd.

表 1: 異常の内容

番号	内容
1	TCF Cluster の大量データグラム
2	TCF Cluster の大量データグラム
3	ping の嵐
4	ping の嵐
5	ping の嵐
6	NETBIOS の暴走
7	NETBIOS の暴走
8	NETBIOS の暴走
9	NETBIOS の暴走（サーバを調整中）
10	NETBIOS の暴走（サーバを調整中）
11	NETBIOS の暴走（サーバを調整中）
12	NETBIOS の暴走（サーバを調整中）
13	正常復帰

3.3 TCP/IP のプロトコルのフレーム数の比（図 3）

正常時は TCP, UDP がほとんどである。Unknown プロトコル（TCP, UDP, ICMP 以外）は無い。基幹トークンリング上に NFS Server/Client と CPU サーバ（ここから X Window の TCP コネクションを張る）とがあるので、TCP と UDP との比は一定とならない。Unknown プロトコルがあるので、1,2 での事故の原因は Unknown Protocol を発信しているマシンだと推測できる。ICMP が 70%以上を占めているので、3, 4, 5 の異常の原因は ICMP を発信していマシンと推測できる。

4 診断支援ツール

診断支援ツールは原因究明中に使うために表を作る。この表には MAC Address（とあれば IP address と）を送信したフレームの数で並べてある。送信フレーム数の多いマシンから検査していくの役立つ。

5 おわりに

異常時、正常時それぞれのネットワークを流れるフレームの特徴を比べてネットワークの異常の原因を求める体系を紹介した。比べる特徴は 1. リングでの 1 秒当たりのフレーム数, 2. LLC の一つ上のレベルでのプロトコルのフレーム数の比, 3. TCP/IP のプロトコルのフレーム数の比, である。異常時にはこれらは" 他より多い" という形で異常が現れるので原因究明中はフレームを多く発信しているマシンから点検していくという手順を示した。

参考文献

[1] Reynolds, J. K. and Postel, J. B., *Assigned numbers*, RFC-1060, ISI, Mar., 1990

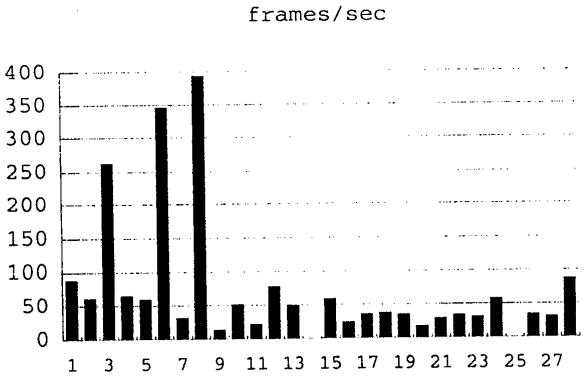

図 1: 1 秒当たりのフレーム数

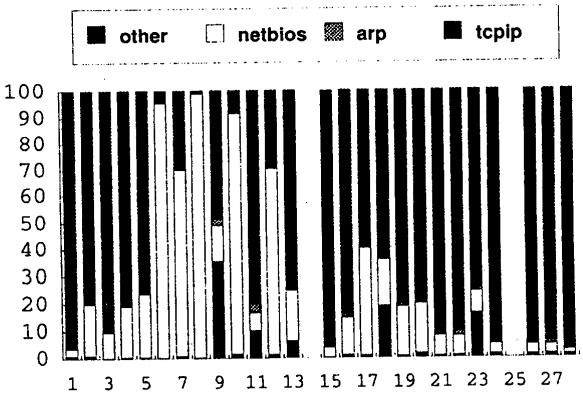

図 2: LLC の一つ上のプロトコルのフレーム数の比

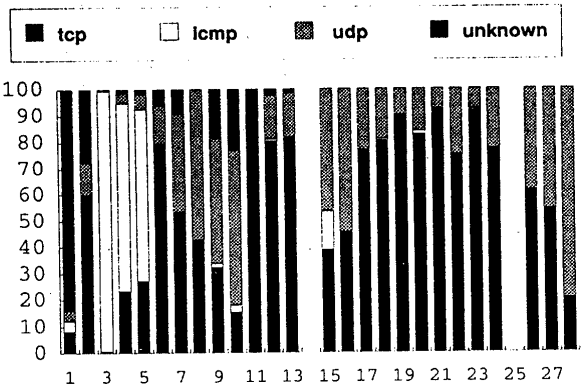

図 3: TCP/IP のプロトコルのフレーム数の比