プロトコルモニタリングによるネットワーク障害監視システム

3U－5

大岸　智彦　井戸上　彰　加藤　聰彦　鈴木　健二

KDD研究所

1．はじめに

近年、インターネットが急速に普及し、IPをベースとしたネットワークの構築がさかんに行われている。IPネットワークでは、端末の所有者やサーバの管理者が個々にネットワークの設定や管理を行うため、ネットワークに接続できないといった障害が発生した場合に、その原因の追求が困難となり、復旧に時間を要することが多い。

これまで、障害監視装置としてRMON[1]ベースのシステムなどが提案されているが、端末が稼働しているか否かなどの物理的なレベルの情報の収集にとどまっている。しかしながら、実際には、端末におけるDNSサーバのアドレス設定の誤りや、ルーティングテーブルの不具合、ネットワークの構成変更などによるサーバ情報の不一致など、さまざまな原因で障害が発生する。そこで筆者等は、ネットワーク上を流れるパケットを監視し、端末毎、プロトコル毎の動作を解析することにより、上位層に起因する障害までを監視する機能を持つネットワーク障害監視システムを検討してきた[2]。本稿では、本システムの実装と実際の適用例について述べる。

2．実装

2．1．概要

本システムは図1に示すように、オンライン／オフライン機能からなる。オンラインでは、抽出したパケットを、端末毎のイベントシーケンスに並び替え、それらを連続的に解析することにより、重複IPアドレスの検出などの障害や、ルータのIPアドレス変更などの構成変更を、リアルタイムに表示するとともに、DNSサーバのIPアドレスやARPキャッシュなど、個々の端末の構成情報、イベント毎にパラメータの解析結果を行ったエミュレーション結果、及び、障害の一覧を解析ログに蓄積する。この際、実際のイベント順序がモニタした順序と異なる可能性があるため、一定時間経過してから解析を行う[2]。また、これらの情報を出力するため、検出された端末やルータなどのリストからなるサブネット情報、ルーティングテーブルやTCPコネクション毎の状態など、個々の端末における、プロトコル別の管理情報を推定した端末情報などを推定する。オフラインでは、出力ずみの解析ログをもとに、特定の端末／

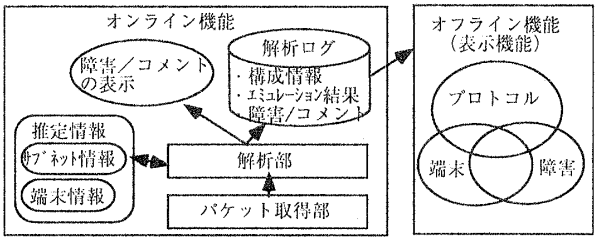
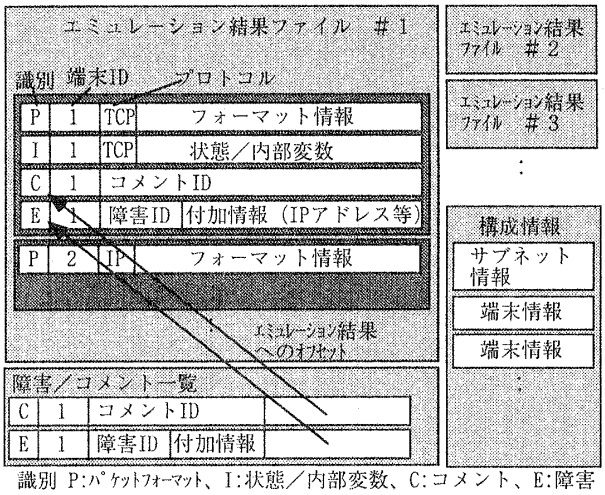


図1　システム構成

プロトコルに着目した解析結果、障害が発生した時点付近での各端末の振舞いなどを表示する。

2．2．解析ログの構成

オンラインで蓄積する解析ログの構成を図2に示す。長時間モニタできるようにエミュレーション結果は、一定サイズ毎のファイルに分割する。個々のイベントに対し、パケットフォーマット、イベント解析後の状態／内部変数、構成変更などのコメント、及び、障害の項目を作成する。



識別 P:パケットフォーマット、I:状態／内部変数、C:コメント、E:障害

図2　解析ログの構成

2．3．構成情報／障害の種別

本システムが推定する構成情報、障害の種別を表1に示す。サブネット情報としては、端末情報へのリンクを含む端末IDリスト、及び、各種サーバIDなど、サブネット毎の情報を管理する。端末情報としては、各プロトコル毎に、ARPキャッシュなどのテーブルや、request/responseの対応づけなどの状態遷移のためのパラメータを管理する。これらには、ドメイン管理テーブルなどのように、サーバのみが管理する情報と、DHCP使用の有無のようにクライアントのみが管理する情報が存在する。障害としては、サブネット内のサーバにつながらないといったサブ

Network Surveillance System by Monitoring Protocol Behaviors

Tomohiko Ogishi, Akira Idoue, Toshihiko Kato and Kenji Suzuki　KDD R&D Laboratories

ネット内の端末やサーバにおける誤った設定、サーバの非稼動、スループット低下などの障害を扱う。

表1　構成情報、及び、障害の種別

構成情報（サブネット情報）	
端末IDリスト（端末情報へのリンク含む）、ルータIDリスト、DNS/DHCP/FTP/HTTP/SMTPサーバIDリスト	
構成情報（端末情報）	
ARP	ARPキャッシュ、request/responseの対応づけ
IP	ルーティングテーブル、外部端末へのアクセス履歴、IPフォワーディングの有無
DNS	DNSサーバのIPアドレス、ドメイン管理テーブル、question/answerの対応づけ
DHCP	DHCPの使用の有無、IPアドレス割当テーブル、状態遷移
TCP	コネクション管理テーブル（状態遷移、内部変数）
障害の種別	
サーバの非稼動	ルータ、DNS/DHCP/FTP/HTTP/SMTPサーバ
端末の設定誤り	サブネットID、ネットマスク、デフォルトルータ、ルーティングテーブル、DNS/SMTPサーバのIPアドレス、IPアドレスの重複
サーバ構成変更よる端末の情報の不一致	ARPキャッシュ
サーバの設定誤り	ドメイン管理テーブル、IPアドレス割当テーブル
特定端末からのスループットの低下	TCPでの過剰な再送、ウインドウサイズの設定値の誤り

3．障害検出例

本システムをサブネット内に設置し、端末及びサーバで意図的に誤った設定を行うことにより、以下の障害を観測した。オンラインでは、障害（E）及びコメント（C）のみを表示するため、図3～4はオフラインでの観測結果を示している。

3．1．ルーティングの障害

サブネット内に2台のルータが存在する場合、端末の設定に不具合があると、冗長な転送パケットが発生する場合が考えられる。図3は、端末でルータTR2をスタティックルーティングとして設定したため、ルータTR1経由のネットワークへの送信するIPパケットに対し、ICMP Redirectが連続して返送された例である。本システムは、モニタしたパケットシーケンスを以下のように推定している。

・着IPアドレスixがサブネット外のアドレスであるため、着物理アドレスar2は、端末Txへのパケットをルーティングするために、端末T1に設定されたルータの物理アドレスと判断する。－①

・Txへのパケットは、ルータTR1経由の方がホップ数が少ないことをルータTR2が通知している。－②

・ICMP Redirectの発物理／発IPアドレス、または、サブネット外端末からのパケットの発物理アドレスがこれまでに検出されたものと異なれば、新しいルータを検出したものと判断している。－③

・①と同じパケットがTR2からTR1に転送されており、冗長なパケットと判断できる。－④

・ICMP Redirectを受信したにもかかわらず、⑤でTR2経由でTxにパケットを送信しているため、⑥で、TR2へのスタティックなルーティング設定が原因で、ICMP Redirectが無視されたものと判断している。

```
①P T1 TCP SYN  SHA:a1 DHA:ar2 SIP:i1 DIP:ix
②P TR2 ICMP Redirect  SHA:ar2 DHA:a1 SIP:ir2 DIP:i1 redirected_IP:ir1
③C New router detected. HA:ar2 IP:ir2
④P TR2 T2 TCP SYN  SHA:ar2 DHA:ar1 SIP:i1 DIP:ix
  P TR1 TCP SYN+ACK  SHA:ar1 DHA:a1 SIP:ix DIP:i1
③C New router detected. HA:ar1
⑤P T1 TCP DT  SHA:a1 DHA:ar2 SIP:i1 DIP:ix
⑥E Redirection not working.  static_router_IP:ir2
    redirected_router_IP:ir1
  P T1 TCP DT  SHA:ar2 DHA:ar1 SIP:i1 DIP:ix
  P TR2 ICMP Redirect  SHA:ar2 DHA:a1 SIP:ir2 DIP:i1 redirected_IP:ir1
```

T1, TR1, TR2: 設定に不具合のある端末、及び、ルータ1、2の識別
a1, ar1, ar2: それぞれ端末T1, ルータTR1, TR2の物理アドレス
i1, ir1, ir2, ix: それぞれ端末T1, ルータTR1, TR2, 相手先のサブネット外の端末TxのIPアドレス
SHA, DHA: Source/Destination Hardware Address
SIP, DIP: Source/Destination IP Address

図3　ルーティングの障害

3．2．DHCPサーバの設定誤りによる障害

図4は、サブネット内に2つのDHCPサーバが存在し、それらが同じIPアドレスを割り当て可能な設定になっている場合に発生する障害例を示している。

・T1からのアドレス割当て要求（①）に対し、2つのDHCP Offerが返信されているため、サブネット内にDHCPサーバが2つ存在すると判断する。－②

・TD1がIPアドレスを割り当てている。－③

・T2からのアドレス割当て要求(④)に対し、2つのDHCPサーバが応答しているが、TD2はTD1がi1を割り当てたことをプロトコル上認識しないため、i1を割り当てようとしている。－⑤

・TD1, TD2が、T1, T2に同じIPアドレスを割り当てたため、T1, T2からの通信の観測により、IPアドレス重複の障害と判断した。－⑥

```
①  P T1 DHCP Discover  SHA:a1 DHA:br SIP:00 DIP:br
②  P TD1 DHCP Offer  SHA:ad1 DHA:br SIP:id1 DIP:br yourIP:i1
   P TD2 DHCP Offer  SHA:ad2 DHA:br SIP:id2 DIP:br yourIP:i1
   P T1 DHCP Request  SHA:a1 DHA:br SIP:00 DIP:br serverIP:id1
③  P TD1 DHCP Ack  SHA:ad1 DHA:br SIP:id1 DIP:br
   P TD1 DHCP Offer  SHA:ad2 DHA:br SIP:id2 DIP:br yourIP:i1
   P T1 IP  SHA:a1 DHA:ar SIP:i1 DIP:ix
④  P T2 DHCP Discover  SHA:a2 DHA:br SIP:00 DIP:br
⑤  P TD1 DHCP Offer  SHA:ad1 DHA:br SIP:id1 DIP:br yourIP:i2
   P TD2 DHCP Offer  SHA:ad2 DHA:br SIP:id2 DIP:br yourIP:i1
   P T1 DHCP Request  SHA:a1 DHA:br SIP:00 DIP:br serverIP:id2
   P TD2 DHCP Ack  SHA:ad2 DHA:br SIP:id2 DIP:br
   P T2 IP  SHA:a2 DHA:ar SIP:i1 DIP:ix
⑥  P T1 IP  SHA:a1 DHA:ar SIP:i1 DIP:ix
   E Duplicate IP address. IP:i1 HA1:a1 HA2:a2
```

T1, T2, TD1, TD2: それぞれ2台の端末、2台のDHCPサーバの識別
a1, a2, ad1, ad2: T1,T2,TD1,TD2の物理アドレス
id1, id2, ix: TD1,TD2,サブネット外端末TxのIPアドレス
i1, i2: 動的に割り当て可能なIPアドレス
br, 00: ブロードキャストの物理／IPアドレス、オール0のIPアドレス
yourIP, serverIP: サーバが割り当てた／端末が要求したIPアドレス

図4　DHCPサーバの設定誤りによる障害

4．まとめ

本稿では、プロトコルモニタリングによるネットワーク障害監視システムの実装と具体的な障害例について述べた。本システムは、サブネット上での端末やサーバの設定誤りなどに基づく障害を検出するのに有効であると考えられる。最後に日頃ご指導頂くKDD研究所村谷所長に感謝する。

参考文献

[1] S. Waldbusser, "Remote Network Monitoring Management Information Base," RFC1757, Feb. 1995.

[2] 大岸、井戸上、加藤、鈴木、「複数プロトコルの振舞いとその関連を解析する汎用インターネットプロトコルアナライザの設計」、第58回情処大会、Mar. 1999.