ＯＳＩによるＬＡＮ統合管理のための実装規約

1G－9

（３）管理機能

吉江　信夫[1]、小松　文子[2]、中川路　哲男[3]、渡辺　修[4]、勅使河原　可海[2]
住友電気工業[1]、ＮＥＣ[2]、三菱電機[3]、エヌケーエクサ[4]

１．はじめに

ＬＡＮは、ダウンサイジングの潮流と相まって急速に普及、大規模化している。ＬＡＮ機器ではＳＮＭＰエージェントの実装が当たり前となり、ベンダＭＩＢのオープン化が進み、一方でＲＭＯＮといったより実質的なＬＡＮ管理への仕組みが実現されつつある。しかし、ＳＮＭＰによる管理ではＬＡＮの大規模化に対応できなくなってきている。ＳＮＭＰバージョン２ではマネージャ間通信の機能が盛り込まれているが、トラップ情報の集約といった限られた範囲のものでしかない。我々は、大規模ＬＡＮを統合管理するためにＯＳＩ管理によるＬＡＮ管理実装規約を開発中である。本稿では、ＬＡＮ機器における管理の側面を明確にし障害管理に対する要件を検討したので、その結果について報告する。

２．管理対象の範囲（管理機器）

大規模なＬＡＮではＦＤＤＩを代表とするバックボーンＬＡＮに、Ethernetといった支線ＬＡＮがブリッジ、ルータといった中継装置で接続される形態を取る。また、末端機器（エンドステーション）はEthernetにハブを介して接続される傾向にある。本規約では、ネットワーク層以下において末端機器間で正常にデータの受け渡しができることを管理目的としている。即ち、中継装置とこれにより接続されるメディア（本稿ではＭＡＣ副層以下により構成されるネットワークを指す）の管理、特に障害管理を実現するための規約である。表１に本規約が対象とする機器の一覧を示す。これらのＲＦＣで規定されているＭＩＢはＧＤＭＯのＭＩＢを参考にしておりほぼ一対一のマッピングが可能である。但し、ＲＭＯＮ（RFC1271）についてはＧＤＭＯには対応するＭＩＢは存在しない。

表１．管理対象機器

	ＲＦＣ	ＧＤＭＯ
ＦＤＤＩ	RFC1285	SMT(X3T9)
８０２．３	RFC1284	IEEE802.3
（ＲＭＯＮ）	RFC1271	－
末端機器	RFC1213	(IIMC[1])
ルータ（IP）	RFC1213	(IIMC)
ブリッジ	RFC1286	IEEE802.1d
ハブ	RFC1368	IEEE802.3K

３．管理機能

ネットワーク管理で最も重要なのは障害管理である。末端機器間の通信障害は、メディア障害かルーティング障害に起因することが多いが、ネットワークの構成の把握なくしては、障害管理は実現できない。以下、本実装規約で規定する構成管理と障害管理について機器毎に述べる。

３－１　メディア（セグメント）管理

（１）ＦＤＤＩ

ＦＤＤＩはＳＭＴという最も進化した層管理プロトコルを有しており、これを利用することでＦＤＤＩの管理情報はくまなく収集することができる。しかし、ＳＭＴはメディアに閉じたプロトコルでありマネージャからの直接的な利用は現実的でない。Proxy AgentにおいてＳＭＴとマッピングする方法と、RFC1285（ＳＮＭＰ）を利用する方法が考えられが、後者ではトラップの規定がなくProxyでポーリングを行いその結果を通知することになる。ＦＤＤＩ管理ではリングの構成管理（機器の接続関係）と、リングの状態監視が重要となる。２次リングを使用するラップ状態、ビーコンと呼ばれるリング異常、２重アドレス等が特徴的な障害となる。

（２）Ethernet

FDDIと異なり層管理プロトコルはなく、ネットワーク構成は獲得しにくく、一般には機器に閉じた情

Implementation Specification of LAN Integrated Management Based on OSI (3)Functions
Nobuo YOSHIE[1], Ayako KOMATSU[2], Tetsuo NAKAKAWAJI[3], Osamu WATANABE[4], Yoshimi TESHIGAWARA[2]
Sumitomo Electric Industries[1], NEC[2], Mitsubishi Electric Corp.[3], NK-Exa[4]

報（Ethernet I/Fの情報）しか得られない。本規約ではEthernetのメディアとしての管理を実現すべくＲＭＯＮを想定し、Ethernetに接続され通信を行っている機器の構成情報（ＭＡＣアドレス）とメディアとしての障害統計情報を利用する。また、ＲＭＯＮはアラームを発行できるメカニズムがあり実用的かつ効率的な管理が実現可能である。Ethernetの特徴的な障害としてはコリジョンの多発による送信不能、送信遅延等がある。

３－２　中継装置の管理

（１）ルータ

ＦＤＤＩ、Ethernetといった物理的なネットワークの上にルーティング層（ネットワーク層）で分離できる論理的なネットワークがある。ルーティングの失敗は、主にルーティングテーブルの異常か、もしくはルータのインタフェース（ｉｆ）ダウンにより発生する。本規約ではＭＩＢ－ＩＩで得られるＩＰルーティング情報とｉｆ状態を障害管理の対象とする。ｉｆは、ＭＡＣアドレスを識別子とする機器とメディアを接続する論理的接点であり、ルーティングの入出力先としてポイントされる[1]。ルータの最も重要な障害はｉｆのダウンにある。

（２）ブリッジ

メディア間を接続するブリッジは、インタネットの中では捕らえにくい機器である。ブリッジはメディアを分割するが、ＩＰネットワークと異なりＭＡＣアドレスは一般にネットワークに依存せず、末端機器がどちらのメディアに接続されているのか判別が難しい。異種のメディアを接続している場合にはＭＩＢ－ＩＩのｉｆタイプ（ifType）により判断が可能である。しかし、Ethernet同士である場合には、Bridge MIBのフィルタリング情報かＲＭＯＮに頼ることになる。ブリッジには、ポートと呼ばれるＭＡＣ層へのサービスインタフェースが定義されているが、これはｉｆと一対一に対応付けられる。ブリッジの場合もｉｆ（ポート）の障害が重要となるがこれ以外に以下のような障害がある。

・輻輳によるフレームの廃棄

・フィルタリングＤＢの障害：無効なＭＡＣアドレスの利用（保存時間内）や静的エントリの登録誤り

３－３　ハブの管理

ハブは、IEEE 802.3リピータとして規定されている。ハブは、メディアとしては１つのEthernet上に存在し、ブリッジのようにメディアを分割するものではない。しかし、物理的には（物理層として）、分断しており、ハブのポートに接続された機器はハブの障害の影響を受ける。ハブは、ソースアドレス機能によりポートに接続された機器のＭＡＣアドレス（LastSourceAddress）を保存しておりこれによりハブの接続機器を知ることができる。ハブの特徴的な障害としてはポート状態（PortAdminStatus, AutoPartitions）の異常がある。この他に標準的なEthernetのエラーカウンタにより障害を判断する。なお、ハブのポートはｉｆとは対応していない。

４．トラップのマッピング

代表的なＳＮＭＰのトラップをＯＳＩ管理にマッピングするモデルを以下に示す。

（１）初期化（coldStart、warmStart）トラップ

状態管理機能（ISO 10164-2）の状態変更通知にマッピングし、操作状態をDisabledからEnabledに変更する。また、このトラップをオブジェクト生成通知へマッピングし新たな機器の発見に利用する。

（２）ｉｆダウン（linkDown, linkUp）トラップ

警報報告機能（ISO 10164-4）を利用し、通信警報通知にマッピングする。アラーム原因はローカル伝送誤りとする。なお、本トラップについてはｉｆの操作状態に対する状態変更通知にマッピングする案も検討中である。

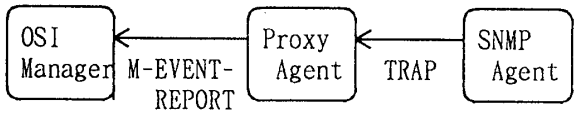

図１．トラップのマッピング

５．おわりに

本稿ではＬＡＮ統合管理のための管理機能について報告した。今後はこの検討結果を基に更に検討を重ね、ＬＡＮの実用的な管理を目指した実装規約を完成させる予定である。

最後に本実装規約に関する検討に参加頂いているＩＮＴＡＰ　ＮＭ専門委員会の皆様に感謝します。

参考文献

[1]中川路他：OSIによるLAN統合管理のための実装規約(2)情報ﾓﾃﾞﾙ, 情処学会第47回全国大会, 1993