

(19) 世界知的所有権機関
国際事務局



(43) 国際公開日
2004年8月19日 (19.08.2004)

PCT

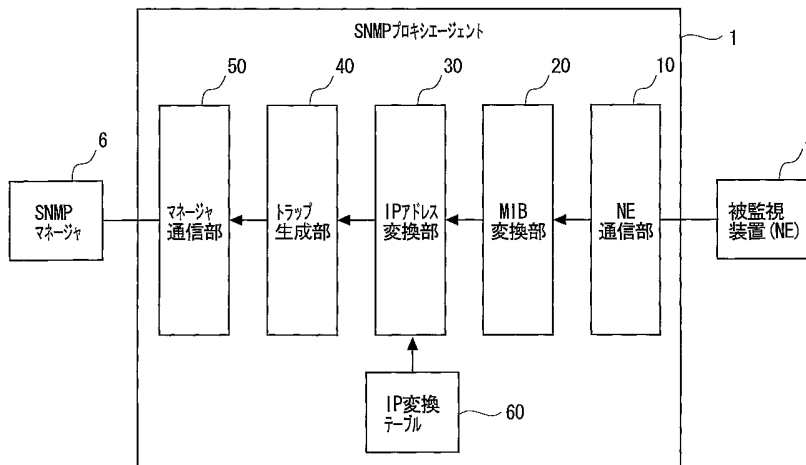
(10) 国際公開番号
WO 2004/071014 A1

- (51) 国際特許分類7: H04L 12/24, G06F 13/00
- (21) 国際出願番号: PCT/JP2003/001230
- (22) 国際出願日: 2003年2月6日 (06.02.2003)
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語
- (71) 出願人 (米国を除く全ての指定国について): 富士通株式会社 (FUJITSU LIMITED) [JP/JP]; 〒211-8588 神奈川県川崎市中原区上小田中4丁目1番1号 Kanagawa (JP).
- (72) 発明者; および
- (75) 発明者/出願人 (米国についてのみ): 前田 秀樹 (MAEDA,Hideki) [JP/JP]; 〒211-8588 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内 Kanagawa (JP). 木幡 誠 (KOBATA,Makoto) [JP/JP]; 〒211-8588 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内 Kanagawa (JP). 熊野 聡 (KUMANO,Satoshi) [JP/JP]; 〒211-8588 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内 Kanagawa (JP). 原 清史 (HARA,Kiyofumi) [JP/JP]; 〒211-8588 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内 Kanagawa (JP).
- (74) 代理人: 遠山 勉, 外 (TOYAMA,Tsutomu et al.); 〒103-0004 東京都中央区東日本橋3丁目4番10号 アクロポリス2 1ビル6階 Tokyo (JP).
- (81) 指定国 (国内): JP, US.
- 添付公開書類:
— 国際調査報告書
- 2文字コード及び他の略語については、定期発行される各PCTガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

(54) Title: SNMP PROXY AGENT AND MANAGEMENT INFORMATION RELAY METHOD

(54) 発明の名称: SNMP プロキシエージェント、及び管理情報中継方法

A SNMPプロキシエージェントのシステム構成図



- A...SNMP PROXY AGENT SYSTEM CONFIGURATION DIAGRAM
 6...SNMP MANAGER
 50...MANAGER COMMUNICATION UNIT
 40...TRAP GENERATION UNIT
 30...IP ADDRESS CONVERSION UNIT
 20...MIB CONVERSION UNIT
 10...NE COMMUNICATION UNIT
 5...MONITORED DEVICE (NE)
 60...IP CONVERSION TABLE
 1...SNMP PROXY AGENT

(57) Abstract: An SNMP proxy agent includes a format conversion unit for converting management information received from a monitored device not using the SNMP as a management protocol, into a format corresponding to the SNMP, an IP address conversion unit for converting the

[続葉有]

WO 2004/071014 A1



particular information on the monitored device included in the management information into a virtual IP address indicating the monitored device, a trap generation unit for generating an SNMP trap having the aforementioned virtual IP address set as a transmission origin and containing the management information after the conversion, and a transmission unit for transmitting the generated SNMP trap to an SNMP manager.

(57) 要約: SNMPプロキシエージェントは、SNMPを管理プロトコルとしない被監視装置から受信される管理情報をSNMPに対応する形式に変換する形式変換部と、上記管理情報に含まれる上記被監視装置の特定情報をこの被監視装置を示す仮想IPアドレスに変換するIPアドレス変換部と、上記仮想IPアドレスが送信元に設定され変換後の管理情報を含むSNMPトラップを生成するトラップ生成部と、上記生成されたSNMPトラップをSNMPマネージャに送信する送信部とを備える。

明 細 書

SNMPプロキシエージェント、及び管理情報中継方法

技術分野

本発明はSNMP (Simple Network Management Protocol : 簡易ネットワーク管理プロトコル) などのマネージャ・エージェント構造を持つマネージャ・エージェントモデルシステムに関する。更に詳細には、本発明はSNMPを管理プロトコルとしない被監視装置をSNMPマネージャで監視するために、被監視装置の監視プロトコルをSNMPに変換するSNMPプロキシエージェントに関する。

背景技術

従来、複数のネットワーク構成装置 (伝送装置などの被監視装置) とこれらのネットワーク構成装置を接続する伝送路とを含むネットワーク (管理対象システム) と、このネットワークを監視して管理情報を収集する監視装置 (管理ステーション) とから構成されるネットワーク管理システムが種々存在する。

例えば、SNMPに則ってIP (Internet Protocol) アドレスを持たない複数の非SNMP対応の伝送装置 (エージェント) を監視するために、SNMPプロキシエージェントをエージェントとマネージャとの間に配置しているネットワーク管理システムとしてのマネージャ・エージェントモデルシステムがある。

従来のSNMPプロキシエージェントでは、SNMPを管理プロトコルとしない被監視装置から送信される障害情報及び装置状態情報などの管理情報に関しては、それら管理情報をMIB (Management Information Base) 形式に変換してSNMPマネージャに通知する際、送信元アドレスとしてSNMPプロキシエージェントのIPアドレスを設定していた。そのため、SNMPマネージャにて管理情報の送信元である被監視装置を識別するために、被監視装置のローカルアドレス (本発明では、IPアドレス以外の装置名、装置番号等を示す) をMIBのインデックス情報として使用することになり、様々な形式で存在するローカルアドレスにより装置を識別していた。これに対し、「特許第3017089号公報：ネットワーク管理装置および方法 (特許文献1)」で示されるように、SNMP

マネージャにおいて被監視装置のローカルアドレスを仮想IPアドレスに変換し、その仮想IPアドレスをSNMPマネージャ内部で送信元アドレスに設定し直すことで統一形式により識別を行うなどの工夫を行っていた。その他に、「特開2000-236348号公報：インターネットプロトコルを用いた遠隔機器の管理システム（特許文献2）」で示されるように、プロキシエージェントに仮想的なIPアドレスを持たせ、そのIPアドレスの仮想的に割り当てられたソケットを送信元として、マネージャと通信を行う構成を採用していた。

上述のように、従来では、被監視装置のローカルアドレスをインデックスとするため、装置を識別するための情報がIPアドレス以外の形式で混在し、SNMPマネージャの管理方法が統一できず、SNMPマネージャの管理や操作が煩雑になるといった問題があった。その問題に対して、「特許第3017089号公報（特許文献1）」に示されるような、SNMPマネージャにおいてローカルアドレスからIPアドレスへの変換を行う方法では、IPアドレスで統一的に管理が可能となるが、SNMPマネージャ内部において被監視装置のローカルアドレスを管理する必要があるため、新たにサポートする非SNMP系装置が追加になった場合には、SNMPプロキシエージェントと共に前記アドレス変換部も改造する必要がある。即ち、システムの管理元であるSNMPマネージャを改造することになるため、改造が複雑になり手間がかかるという問題があった。また、「特開2000-236348号公報（特許文献2）」に示されるような、IPアドレスを仮想的に割り当てたソケットを送信元とする方法では、新たにサポートする非SNMP系装置が追加になった場合には、プロキシエージェント自体のIPアドレス設定の変更（ソケットの増加）を行う必要が生じ、OSレベルのシステム変更が必須になる上、さらに、非SNMP系装置が増加し続けると、システム全体の通信性能が落ち、システムの資源の枯渇に繋がるという問題があった。

[特許文献1]

特許第3017089号公報

[特許文献2]

特開2000-236348号公報

発明の開示

本発明は、上述した問題点を解決するためになされたものである。即ち、本発明の目的の一つは、SNMPマネージャの管理方法が統一でき、管理や操作が容易になるSNMPプロキシエージェントを提供することにある。

また、本発明の目的の一つは、新たにサポートする非SNMP系装置が追加になった場合でもSNMPエージェントのIPアドレス管理に関する改造を必要としないSNMPプロキシエージェントを提供することにある。

本発明は、上記課題を解決するために、以下の手段を採用した。即ち、本発明は、

SNMPを管理プロトコルとしない被監視装置の特定情報をこの被監視装置を示す仮想IPアドレスに変換する手段と、

上記仮想IPアドレスが送信元に設定されたSNMPマネージャ宛のSNMPトラップを生成する手段とを備えるSNMPプロキシエージェントである。

更に詳しくは、本発明は、

SNMPを管理プロトコルとしない被監視装置から受信される管理情報をSNMPに対応する形式に変換する形式変換手段と、

上記管理情報に含まれる上記被監視装置の特定情報をこの被監視装置を示す仮想IPアドレスに変換するIPアドレス変換手段と、

上記仮想IPアドレスが送信元に設定され変換後の管理情報を含むSNMPトラップを生成するトラップ生成手段と、

上記生成されたSNMPトラップをSNMPマネージャに送信する送信手段とを備えるSNMPプロキシエージェントである。

これにより、SNMPを管理プロトコルとしない被監視装置から受信される管理情報とその管理情報の送信元である被監視装置を識別する際に、SNMPマネージャ側で、IPアドレスにより統一的な形式で管理することができる。

好ましくは、上記トラップ生成手段は、SNMPを管理プロトコルとする他の被監視装置からの管理情報が受信された場合には、その被監視装置が保持する実際のIPアドレスが送信元に設定されたトラップを生成すればよい。

これにより、SNMPを管理プロトコルとする被監視装置から受信される管理情報についても、SNMPマネージャ側で、SNMPを管理プロトコルとしない被監視装置と同様に管理することができる。

好ましくは、上記トラップ生成手段は、上記被監視装置に対応するSNMPのバージョンがバージョン1の場合には、上記仮想IPアドレスをSNMPバージョン1のトラップフォーマットのエージェントアドレス部に制御情報として設定すればよい。

好ましくは、上記トラップ生成手段は、上記被監視装置に対応するSNMPのバージョンがバージョン2の場合には、上記仮想IPアドレスをSNMPバージョン2のトラップフォーマットのデータ本体部にオブジェクトとして設定すればよい。

好ましくは、上記トラップ生成手段は、上記被監視装置に対応するSNMPのバージョンがバージョン3の場合には、上記仮想IPアドレスをSNMPバージョン3のトラップフォーマットのデータ本体部にオブジェクトとして設定すればよい。

これにより、SNMPのバージョンに応じたトラップを生成して、SNMPマネージャ側に送信することができる。

本発明は、コンピュータが、以上のいずれかの処理を実行する方法であってもよい。即ち、本発明は、

SNMPプロキシエージェントとして機能するコンピュータがSNMPマネージャの管理対象となる被監視装置からの管理情報を中継する方法であって、

SNMPを管理プロトコルとしない被監視装置から受信される管理情報をSNMPに対応する形式に変換するステップと、

上記管理情報に含まれる上記被監視装置の特定情報をこの被監視装置を示す仮想IPアドレスに変換するステップと、

上記仮想IPアドレスが送信元に設定され変換後の管理情報を含むSNMPトラップを生成するステップと、

上記生成されたSNMPトラップをSNMPマネージャに送信するステップとを含む管理情報中継方法である。

このようにSNMPプロキシエージェントを被監視装置とSNMPマネージャの間に設置して管理情報を中継することにより、SNMPマネージャの管理対象となる被監視装置からの管理情報がSNMPマネージャに送信される場合、SNMPマネージャ側で管理し易いアドレス形式やデータ形式となる管理情報をトラップとしてSNMPマネージャに与えることができる。

本発明によれば、SNMPプロキシエージェントにおいて、送信される管理情報に含まれる被監視装置を特定する情報を仮想なIPアドレス形式に変換するため、SNMPマネージャ側では、被監視情報を特定するための情報をすべてIPアドレス形式で認識でき、管理方法が統一できるため、管理や操作が容易になる。

また、本発明によれば、SNMPマネージャ上で被監視装置のローカルアドレスを管理する必要があるため、新たにサポートする非SNMP系装置が追加になった場合でもSNMPエージェントのIPアドレス管理に関する改造が不要となる。

図面の簡単な説明

FIG. 1は、本発明の一実施の形態のマネージャ・エージェントモデルシステムを示すブロック図であり、

FIG. 2は、FIG. 1に示すプロキシエージェントの構成及び動作について説明するためのブロック図であり、

FIG. 3は、IP変換テーブルのデータ構造を示す図であり、

FIG. 4は、IPフレームのデータ構造を示す図であり、

FIG. 5は、SNMP v1におけるトラップのデータ構造を示す図であり、

FIG. 6は、SNMP v2 (v3)におけるトラップのデータ構造を示す図であり、

FIG. 7は、IPアドレス変換部における処理を示すフローチャートであり、

FIG. 8は、トラップ生成部における処理を示すフローチャートである。

発明を実施するための最良の形態

次に、本発明の実施の形態について図面を参照して説明する。

[マネージャ・エージェントモデルシステムの構成]

FIG. 1は、本発明の一実施の形態のマネージャ・エージェントモデルシステムを示すブロック図である。

本発明の一実施の形態を示すFIG. 1を参照すると、ネットワーク管理プロトコルとしてのSNMPのマネージャ・エージェント構造を持つマネージャ・エージェントモデルシステムは、非SNMP対応エージェントのネットワーク構成装置としての複数の被監視装置（NE # 1, # 2・・・）と、これらの被監視装置を後に詳述するプロキシエージェント1に接続する伝送路及びLAN（Local Area Network）とを含む非SNMPネットワーク2（管理対象システム）を備える。

また、マネージャ・エージェントモデルシステムは、SNMP対応エージェントのネットワーク構成装置としての複数の被監視装置（NE # 11～# 12）と、これらの被監視装置をプロキシエージェント1に接続するIPネットワークとしてのLANとを含むSNMPネットワーク3（管理対象システム）を備える。

このマネージャ・エージェントモデルシステムは、更にIPネットワークとしてのLANを通してプロキシエージェント1に接続され、管理対象システムを監視して障害情報及び装置の状態変化情報などの管理情報を収集する監視装置としてのSNMPマネージャを有するSNMPネットワーク4（管理ステーション）を備えている。

管理対象システムの非SNMPネットワーク2及びSNMPネットワーク3をそれぞれ構成する被監視装置のそれぞれは、具体的には伝送装置などであり、図示省略の複数の端末装置を収容している。ここでは、非SNMPネットワーク2の被監視装置は、伝送路を介して縦続接続形態を採っているが、リング型（ループ状）接続など他の接続形態を採ることも可能である。

管理対象システム2、3における各被監視装置は、プロキシエージェント1を介し、ネットワークの障害や被監視装置の状態等を管理ステーション4におけるSNMPマネージャに知らせるために、コネクションレス型プロトコルUDP（User Datagram Protocol）上で動作するネットワーク管理のための管理情報の交換プロトコルであるSNMPに則ったメッセージのうちのトラップ（TRAP）を

使用する。

このトラップは、管理対象システム2、3における各被監視装置から管理ステーション4におけるマネージャにプロキシエージェント1を介し、自律的にかつ単方向に送信される。

〔プロキシエージェントのシステム構成及び動作の概要〕

次に、FIG. 1に示すプロキシエージェント1の構成及び動作についてFIG. 2を用いて説明する。

FIG. 2は、SNMPプロキシエージェント1のシステムの一例を示すブロック図である。SNMPプロキシエージェント1は、システムの管理対象である被監視装置5 (NE) とシステムの管理元であるSNMPマネージャ6との間に接続される。SNMPプロキシエージェント1は、例えば、サーバマシン等のコンピュータで構成され、図示しないが、CPU等のプロセッサと、主記憶装置と、補助記憶装置と、通信制御装置と、入力装置と、出力装置とを備え、更に、FIG. 2に示すように、NE通信部10と、MIB変換部20と、IPアドレス変換部30と、トラップ生成部40と、マネージャ通信部50と、IP変換テーブル60とを含む装置として機能する。

次に、SNMPプロキシエージェント1内で機能する各構成要素の動作の概要について説明する。NE通信部10は、被監視装置5 (NE) から送信される管理情報 (障害情報、装置の状態変化情報など) を受信し、その受信した内容をMIB変換部20に通知する。MIB変換部20は、NE通信部10から通知される情報を受信し、その内容をMIB形式に変換して、IPアドレス変換部30に通知する。IPアドレス変換部30は、MIB変換部20から通知された情報に含まれる送信元 (発生元) のIPアドレスを条件によって変換し、変換後のIPアドレスを送信元 (発生元) IPアドレスとしてトラップ生成部40に通知する。送信元IPアドレスは、IP変換テーブル60を参照することにより取得する。即ち、被監視装置を特定する情報であるローカルアドレス (NEN_o. ; 装置番号) と各IPアドレスの組を登録したIP変換テーブル60を参照して、被監視装置を特定する情報であるローカルアドレス (NEN_o. ; 装置番号) と仮想IPアドレスとを変換する。

トラップ生成部40は、IPアドレス変換部30から通知された情報を元にトラップを生成して、その内容をマネージャ通信部50に通知する。即ち、通知された仮想IPアドレスと管理情報(障害情報、装置の状態変化情報など)を元に、その仮想IPアドレスを送信元としたトラップを生成する。なお、トラップ生成部40は、IPプロトコルを管理プロトコルの下位レイヤで使用している被監視装置に対しては、被監視装置の実IPアドレスを送信元としたトラップを生成する。マネージャ通信部50は、トラップ生成部40から受信したトラップを含むIPフレームをSNMPマネージャ6に対して送信する。この時、IPフレームのIPヘッダの送信元アドレスには、仮想IPアドレスが設定される。

[データ構成]

次に、各データ60~90のデータ構造について、FIG. 3~FIG. 6を用いて説明する。

《IP変換テーブル》

FIG. 3は、IP変換テーブル60のデータ構造の例を示す。IP変換テーブル60において、NENo. は、被監視装置に対して付けられた被監視装置を識別するための装置番号である。本実施形態では、NENo. (装置番号)をローカルアドレスとして示している。仮想IPアドレスは、各被監視装置(NENo.)に対応する仮想的なIPアドレスである。なお、被監視装置がSNMPに対応している場合には、仮想IPアドレスを示すフィールド部に被監視装置の実IPアドレスが格納される。SNMPVer. は、各被監視装置(NENo.)に対応するSNMPのバージョン情報を示す。

《IPフレーム》

FIG. 4は、IPフレーム70のデータ構造の例を示す。IPフレーム70は、データの識別情報や処理の優先順位等の制御情報を含むIPヘッダ部と送信データ本体を含むIPデータ部とから構成される。IPヘッダ部の構成については、既に知られているため詳細な説明は省略し、本実施形態に関連する要素のみを説明する。IPヘッダ部は、主な要素として、送信元アドレス(Source Address)と、送信先アドレス(Destination Address)とを示す各フィールド部を有する。IPヘッダの送信元アドレス部(Source Address)には、トラップ生成部4

0において、IPアドレス変換部30より得られた被監視装置の仮想IPアドレスが設定される。IPヘッダの送信先アドレス部(Destination Address)には、SNMPマネージャ6のIPアドレスが設定される。IPデータ部は、送信データ本体(障害情報、装置の状態変化情報などの管理情報)にトランスポート層のヘッダ(本実施形態では、UDPヘッダとなる)を付加した構成となる。

《トラップデータ》

次に、本実施形態において、被監視装置から送信される管理情報に対して、SNMPプロキシエージェント1とSNMPマネージャ6間で授受されるPDU(Protocol Data Unit)であるトラップのデータ構造について説明する。トラップは、エージェント側で発生したイベント(障害、装置の状態変化)をマネージャに通知するために使用される。本実施形態において、トラップは、SNMP v1、v2、v3において適用できるため、各トラップについてFIG. 5~FIG. 7を用いて説明する。なお、各トラップのデータ構造については、一般に知られているため詳細な説明は省略し、本発明に関連する主要素のみを説明する。

FIG. 5には、SNMP v1におけるトラップ80のデータ構造の例を示す。トラップ80は、制御情報等を含むヘッダ部と管理情報であるデータ本体を含むデータ部(Variable binding:可変結合部)とから構成される。ヘッダ部は、主要素として、送信元アドレス(Agent Address)を示すフィールド部を有する。送信元アドレス部(Agent Address)には、トラップ生成部40において、IPアドレス変換部30より得られた被監視装置の仮想IPアドレスが設定される。データ部は、MIBオブジェクト識別子とデータの組み合わせを設定する各フィールドを有する。トラップ80は、情報をオブジェクトとして扱い、それぞれのフィールド部にオブジェクト識別子を付けて情報を管理する。

FIG. 6には、SNMP v2(v3)におけるトラップ90のデータ構造の例を示す。このトラップ90は、SNMP v2に対応する。トラップ90は、制御情報等を含むヘッダ部と管理情報であるデータ本体を含むデータ部(Variable binding:可変結合部)とから構成される。ヘッダ部の構成は、本発明に深く関連しないので、詳細な説明については省略する。データ部は、MIBオブジェクト識別子とデータとの組み合わせを含む送信元アドレス(IP Address)を示すフィ

ールド部を有する。送信元アドレス部 (IP Address) には、トラップ生成部 40 において、IP アドレス変換部 30 より得られた被監視装置の仮想 IP アドレスが設定される。トラップ 90 は、トラップ 80 と同様に、情報をオブジェクトとして扱う。

なお、SNMP v 3 のトラップのデータ構造は、FIG. 6 に示す SNMP v 2 のトラップのデータ構造と同じであるため、詳細な説明については省略する。SNMP v 3 のトラップは、各被監視装置 (NENo.) に対応する SNMP のバージョンが v 3 の時に適用される。

[IP アドレス変換部における動作フロー]

次に、SNMP プロキシエージェント 1 内の IP アドレス変換部 30 の具体的な処理について、FIG. 7 を用いて説明する。

FIG. 7 は、IP アドレス変換部 30 における動作フローの例である。IP アドレス変換部 30 は、MIB 変換部 20 から通知された管理情報に対し、その管理情報に含まれる、送信元となる被監視装置を特定するための情報であるローカルアドレスを条件によって変換し、変換後の IP アドレスを送信元の IP アドレスとしてトラップ生成部 40 に通知する。

まず、IP アドレス変換部 30 は、MIB 変換部 20 から情報の通知があるか否かを判断する (S1)。MIB 変換部 20 から情報の通知があった場合には、その情報の送信元である被監視装置が IP アドレスを保持している装置であるか否かを判断する (S2)。MIB 変換部 20 から通知された情報において、該当する被監視装置が IP アドレスを持たない装置であれば、FIG. 3 に示すような予め設定されている IP 変換テーブル 60 を参照し、対応する仮想 IP アドレスを送信元 IP アドレスとして設定する (S3)。また、該当する被監視装置が IP アドレスを持つ装置であれば、IP アドレスを変換せず、その被監視装置の持つ実 IP アドレスをそのまま送信元 IP アドレスとして設定する (S4)。MIB 変換部 20 から通知された管理情報と得られた送信元 IP アドレスとをトラップ生成部 40 に通知する (S5)。このようにして、IP アドレス変換部 30 は、管理情報 (障害情報、装置の状態変化情報など) を送信した送信元となる被監視装置を特定する情報であるローカルアドレス (NENo.; 装置番号) から、

そのローカルアドレスに対応する仮想IPアドレスをIP変換テーブル60より求め、得られた仮想IPアドレスを含む情報をトラップ生成部40に通知する。

これにより、被監視装置がIPアドレスを持たない場合（被監視装置がSNMPに対応しない場合）でも、IPアドレス以外の被監視装置を特定する情報（装置名、装置番号等）を仮想的なIPアドレスに変換でき、アドレスの形式をIPアドレス形式に統一することができる。

〔トラップ生成部における動作フロー〕

次に、SNMPプロキシエージェント1内のトラップ生成部40の具体的な処理について、FIG. 8を用いて説明する。

FIG. 8は、トラップ生成部40における動作フローの例である。

トラップ生成部40は、IPアドレス変換部30から通知された管理情報と送信元IPアドレスとを元にトラップを生成して、その内容をマネージャ通信部50に通知する。

まず、トラップ生成部40は、IPアドレス変換部30からトラップ生成部40に対して、情報の通知があるか否かを判断する(S11)。IPアドレス変換部30から情報の通知があった場合には、トラップを生成する(S12)。そして、IPアドレス変換部30から通知された送信元IPアドレスを、IPヘッダの送信元アドレス部(Source Address)に設定する(S13)。

次に、通知された情報を元に管理情報の送信元である被監視装置におけるSNMPのバージョン情報の判断をする(S14)。このバージョン情報は、IPアドレス変換部30から通知される情報に含まれる。SNMPのバージョン情報の判断において、対応するSNMPのバージョンがv1の場合は、IPアドレス変換部30から通知された送信元IPアドレスをSNMPトラップPDUの送信元アドレス部(agent address)に設定する(S15)。また、対応するSNMPのバージョンがv2、v3の場合は、IPアドレス変換部30から受信した送信元IPアドレスをSNMP v2(v3)トラップPDUの可変結合部(Variable Binding)にオブジェクトとして設定する(S16)。

最終的に完成したトラップ情報をマネージャ通信部50に通知する。なお、非SNMP対応の被監視装置からのアドレスは、各トラップPDUに仮想IPアド

レスとして設定されるので、必ずしも I P ヘッダ部の送信元アドレス部 (Source Address) に送信元 I P アドレスを設定する必要はなく、SNMP マネージャの管理方法に応じて設定すればよい。

これにより、被監視装置が I P アドレスを持たない場合 (被監視装置が SNMP に対応しない場合) でも、その被監視装置からの管理情報の送信元を I P アドレス形式に統一したトラップを生成することができる。

[プロキシエージェントの具体的動作例]

次に、SNMP プロキシエージェント 1 の具体的動作例について、FIG. 1 から FIG. 8 を併せ参照して説明する。

具体的には、非 SNMP 対応のネットワーク上の装置 No. 「# 2」に状態変化が生じた場合を例に説明する。

NE 通信部 10 は、非 SNMP 対応のネットワーク上の装置「# 2」から管理情報として装置 No. 情報を含む状態変化情報を受信し、その内容を MIB 変換部 11 へと通知する。

MIB 変換部 11 は、NE 通信部 10 から通知された管理情報を受信し、その管理情報を MIB 形式に変換して I P アドレス変換部 30 に通知する。即ち、MIB 変換部 11 は、被監視装置からの管理情報を SNMP に対応する形式に変換する。

I P アドレス変換部 30 は、MIB 変換部 11 から MIB 形式に変換された情報を受信すると、その情報の送信元である被監視装置が I P アドレスを保持しているか否かを判別する。この具体例では、装置 No. 「# 2」は I P アドレスを保持しない被監視装置であるので、FIG. 3 に示した、予め設定されている I P 変換テーブル 60 を参照し、対応する仮想 I P アドレス「192.168.1.102」を取得する。この仮想 I P アドレスは、管理情報の送信元 I P アドレスとしてトラップ生成部 40 に通知される。また、SNMP に対応する I P アドレスを保持する被監視装置の場合は、I P アドレスを変換せず、被監視装置の実 I P アドレスを送信元 I P アドレスとしてトラップ生成部 40 に通知する。

トラップ生成部 40 は、I P アドレス変換部 30 から通知された送信元 I P アドレス「192.168.1.102」を、FIG. 4 に示す I P フレームの I P ヘッダにおけ

る送信元アドレス部 (Source Address) に設定する。また、トラップ生成部 40 には、IP アドレス変換部 30 により、FIG. 3 に示した IP 変換テーブル 60 を参照することにより取得された、送信元 IP アドレス「192.168.1.102」に対応する SNMP のバージョン情報が通知される。トラップ生成部 40 では、このバージョン情報を用いてトラップを生成する。この具体例の場合では、送信元 IP アドレス「192.168.1.102」に対応する SNMP のバージョンは「v2」であるため、FIG. 6 に示す SNMP v2 トラップを生成し、トラップ PDU の可変結合部 (Variable binding) にオブジェクトとして送信元 IP アドレス「192.168.1.102」を設定する。こうして生成されたトラップをマネージャ通信部 50 に通知する。

マネージャ通信部 50 は、トラップ生成部 40 から通知された、仮想 IP アドレス「192.168.1.102」が設定された SNMP v2 トラップを SNMP マネージャ 6 に対して送信する。

このように、本発明では、IP アドレスを持たない被監視装置 (SNMP を管理プロトコルとしない被監視装置) と IP アドレスを持つ被監視装置 (SNMP を管理プロトコルとする被監視装置) とから通知される管理情報をすべて IP アドレスという形式により統一的に管理することができる。

以上の実施形態は、一例である。具体的な構成は例の実施形態に限るものではなく、本発明の要旨を逸脱しない限りの設計変更等はこの発明に含まれるものとする。

産業上の利用可能性

本発明は、SNMP を管理プロトコルとしない被監視装置と SNMP を管理プロトコルとする被監視装置とを SNMP マネージャにおいて統一的に管理するシステムに適応可能である。

請求の範囲

1. SNMPを管理プロトコルとしない被監視装置の特定情報をこの被監視装置を示す仮想IPアドレスに変換する手段と、

前記仮想IPアドレスが送信元に設定されたSNMPマネージャ宛のSNMPトラップを生成する手段とを備えるSNMPプロキシエージェント。

2. SNMPを管理プロトコルとしない被監視装置から受信される管理情報をSNMPに対応する形式に変換する形式変換手段と、

前記管理情報に含まれる前記被監視装置の特定情報をこの被監視装置を示す仮想IPアドレスに変換するIPアドレス変換手段と、

前記仮想IPアドレスが送信元に設定され変換後の管理情報を含むSNMPトラップを生成するトラップ生成手段と、

前記生成されたSNMPトラップをSNMPマネージャに送信する送信手段とを備えるSNMPプロキシエージェント。

3. 前記トラップ生成手段は、SNMPを管理プロトコルとする他の被監視装置からの管理情報が受信された場合には、その被監視装置が保持する実際のIPアドレスが送信元に設定されたトラップを生成する

請求の範囲1又は2記載のSNMPプロキシエージェント。

4. 前記トラップ生成手段は、前記被監視装置に対応するSNMPのバージョンがバージョン1の場合には、前記仮想IPアドレスをSNMPバージョン1のトラップフォーマットのエージェントアドレス部に制御情報として設定する

請求の範囲1又は2記載のSNMPプロキシエージェント。

5. 前記トラップ生成手段は、前記被監視装置に対応するSNMPのバージョンがバージョン2の場合には、前記仮想IPアドレスをSNMPバージョン2のトラップフォーマットのデータ本体部にオブジェクトとして設定する

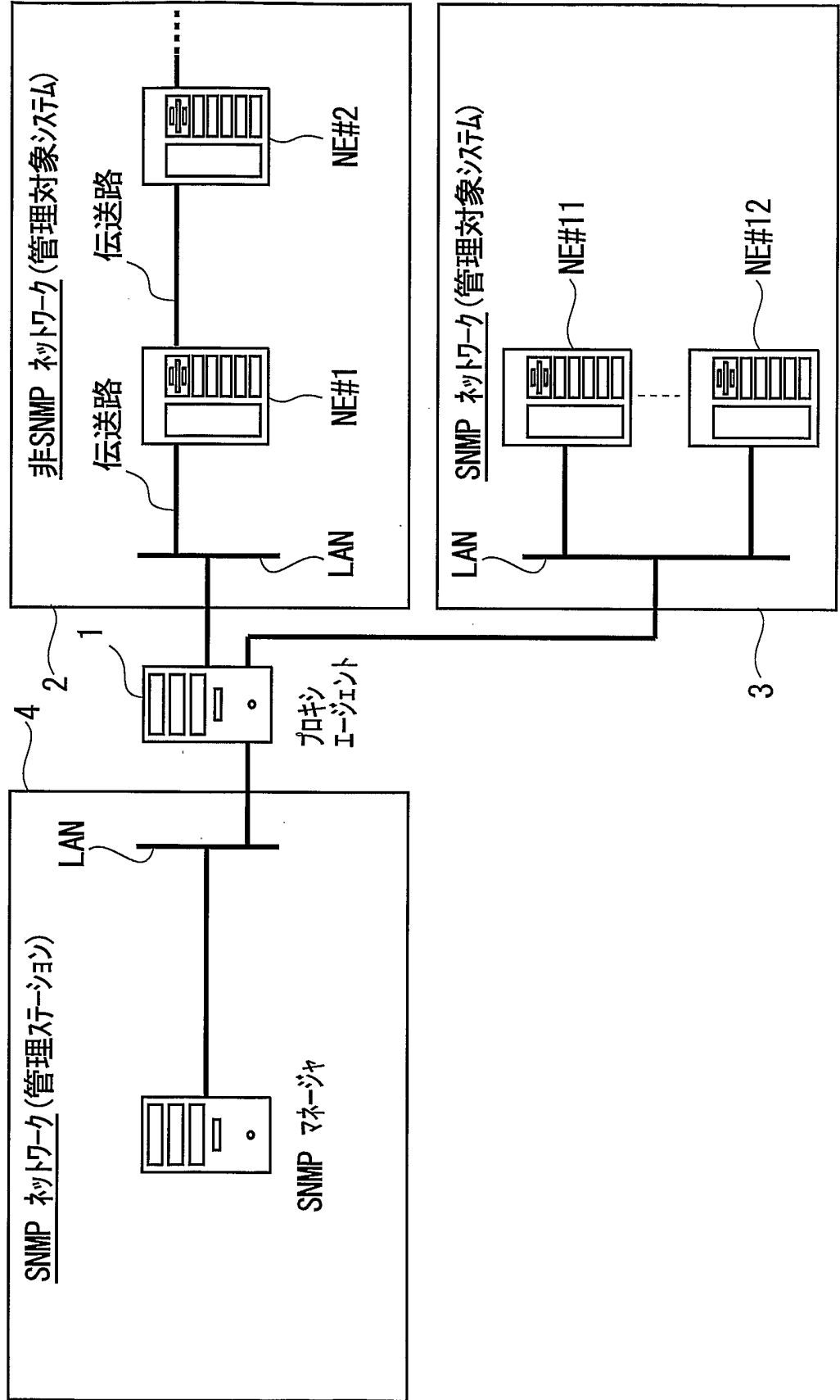
請求の範囲 1 又は 2 記載の SNMP プロキシエージェント。

6. 前記トラップ生成手段は、前記被監視装置に対応する SNMP のバージョンがバージョン 3 の場合には、前記仮想 IP アドレスを SNMP バージョン 3 のトラップフォーマットのデータ本体部にオブジェクトとして設定する請求の範囲 1 又は 2 記載の SNMP プロキシエージェント。

7. SNMP プロキシエージェントとして機能するコンピュータが SNMP マネージャの管理対象となる被監視装置からの管理情報を中継する方法であって、
SNMP を管理プロトコルとしない被監視装置から受信される管理情報を SNMP に対応する形式に変換するステップと、
前記管理情報に含まれる前記被監視装置の特定情報をこの被監視装置を示す仮想 IP アドレスに変換するステップと、
前記仮想 IP アドレスが送信元に設定され変換後の管理情報を含む SNMP トラップを生成するステップと、
前記生成された SNMP トラップを SNMP マネージャに送信するステップとを含む管理情報中継方法。

FIG. 1

マネージャ・エージェントモデルシステム(ネットワーク管理システム)



非SNMP ネットワーク (管理対象システム)

伝送路



NE#1

NE#2

LAN

SNMP ネットワーク (管理ステーション)

LAN



SNMP マネージャ



プロキシ
エージェント

SNMP ネットワーク (管理対象システム)



NE#11

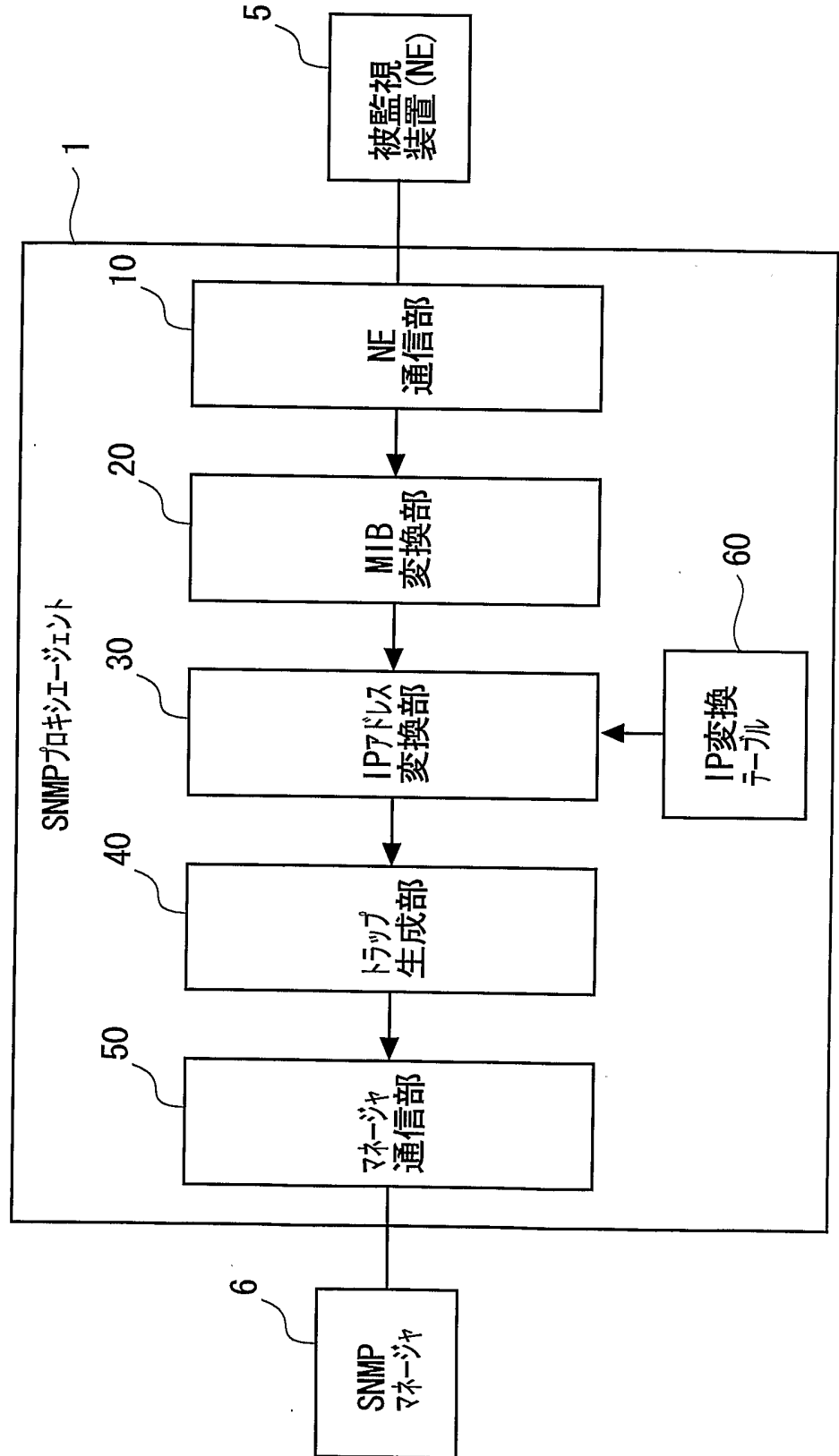
NE#12

LAN

3

FIG. 2

SNMPプロキジェントのシステム構成図



3/8

FIG. 3

IP変換テーブル

60

NE No.	仮想IPアドレス	SNMP Ver
#1	192.168.1.101	v1
#2	192.168.1.102	v2
#3	192.168.1.103	v1
#4	10.34.121.15	v3
⋮	⋮	⋮

FIG. 4

IPフレームのデータフォーマット

70

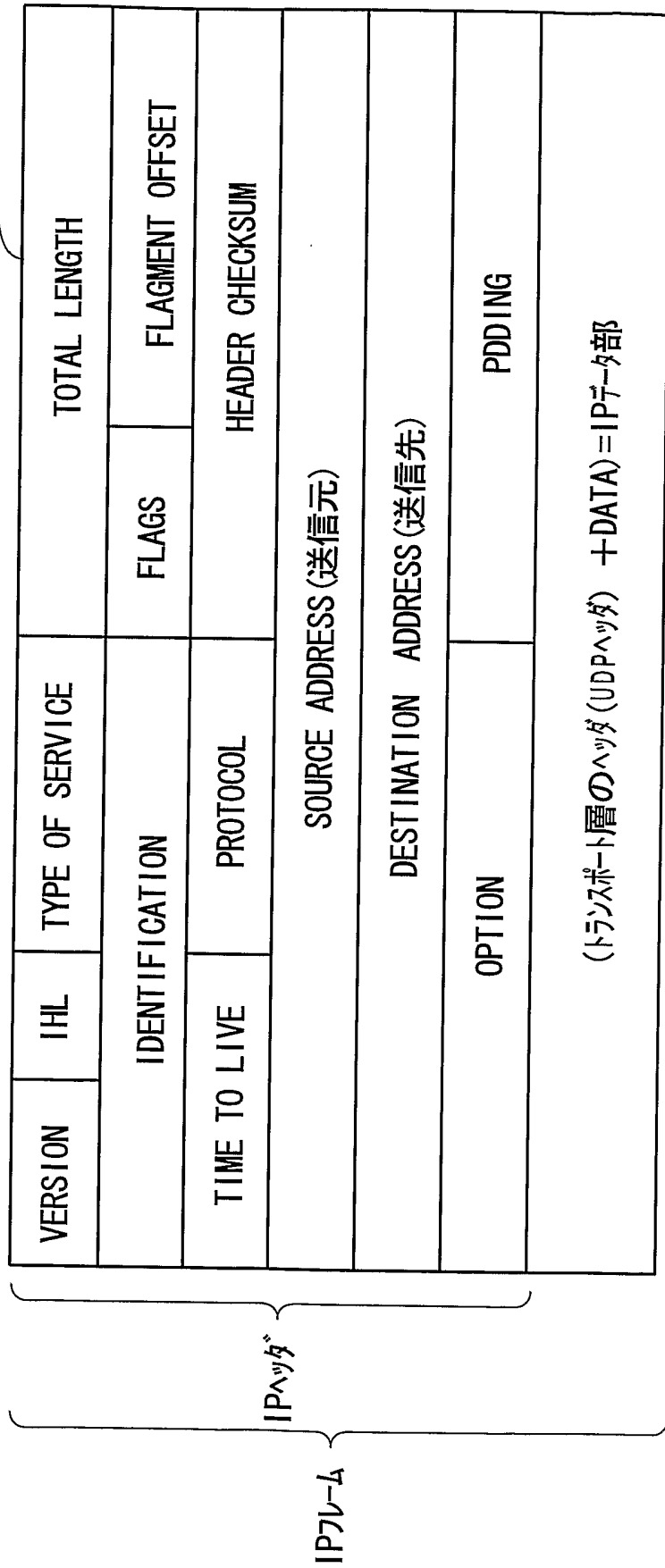


FIG. 5

SNMPトラップのデータフォーマット

5/8

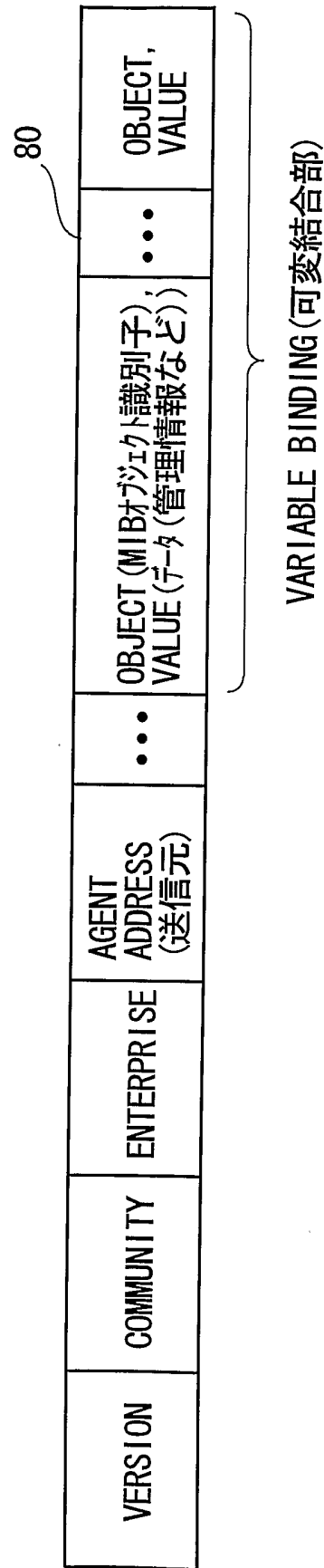
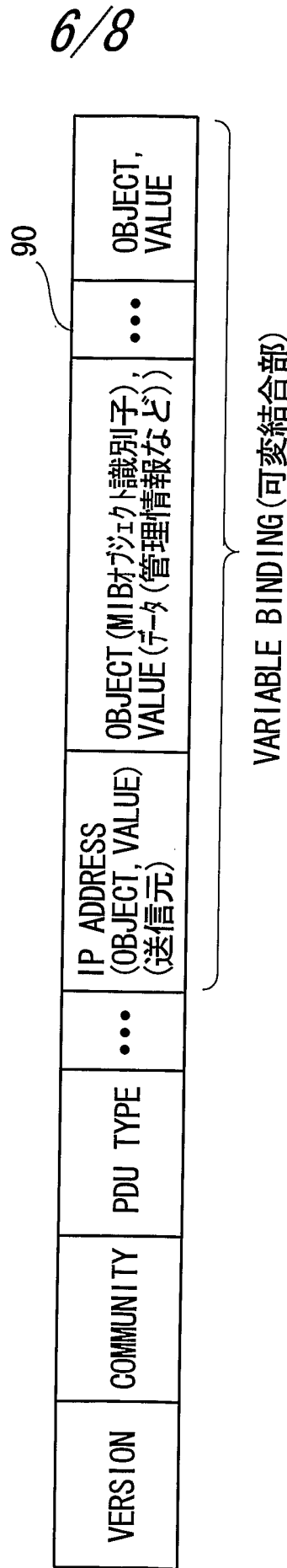


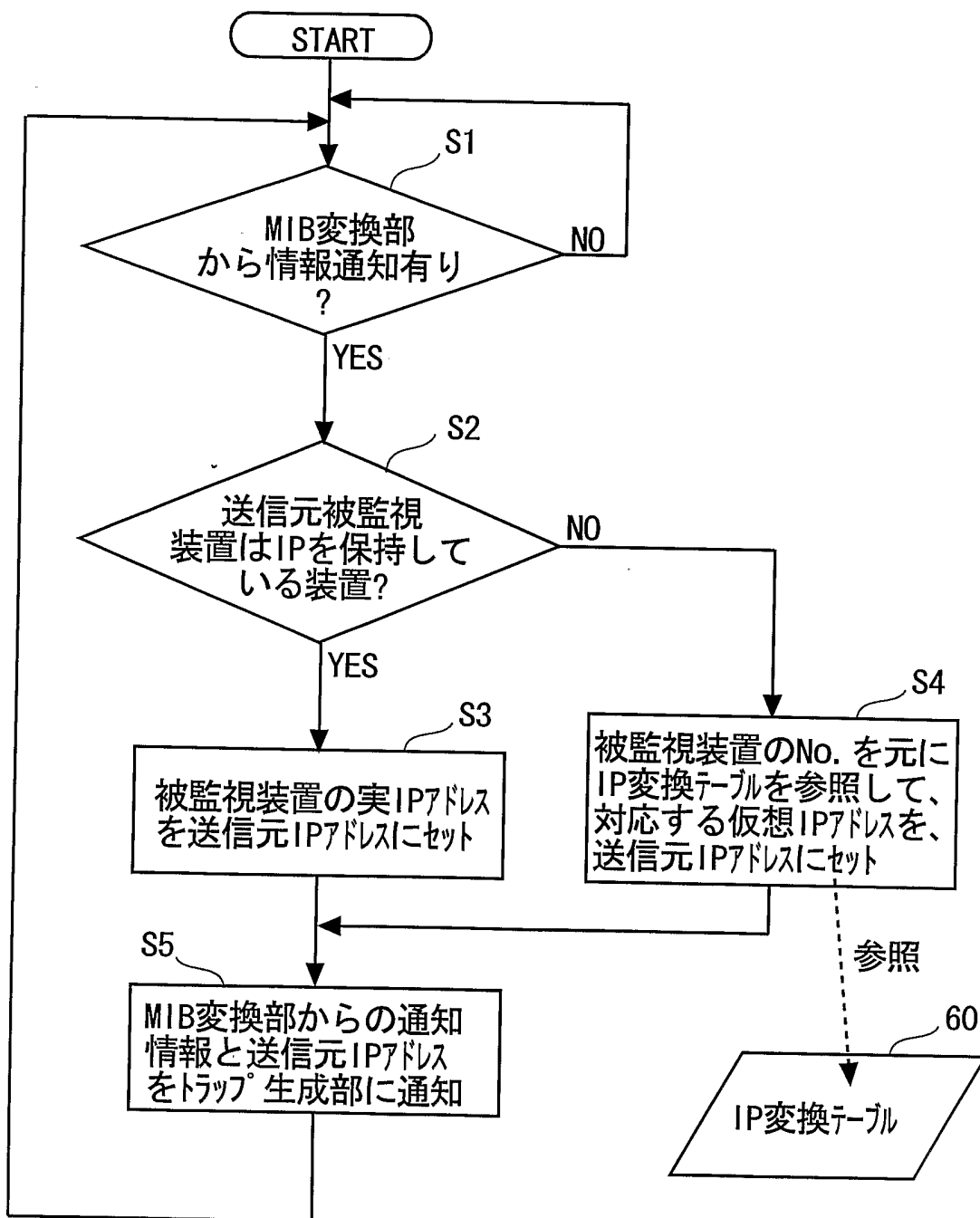
FIG. 6

SNMPv2 (v3) トラップのデータフォーマット



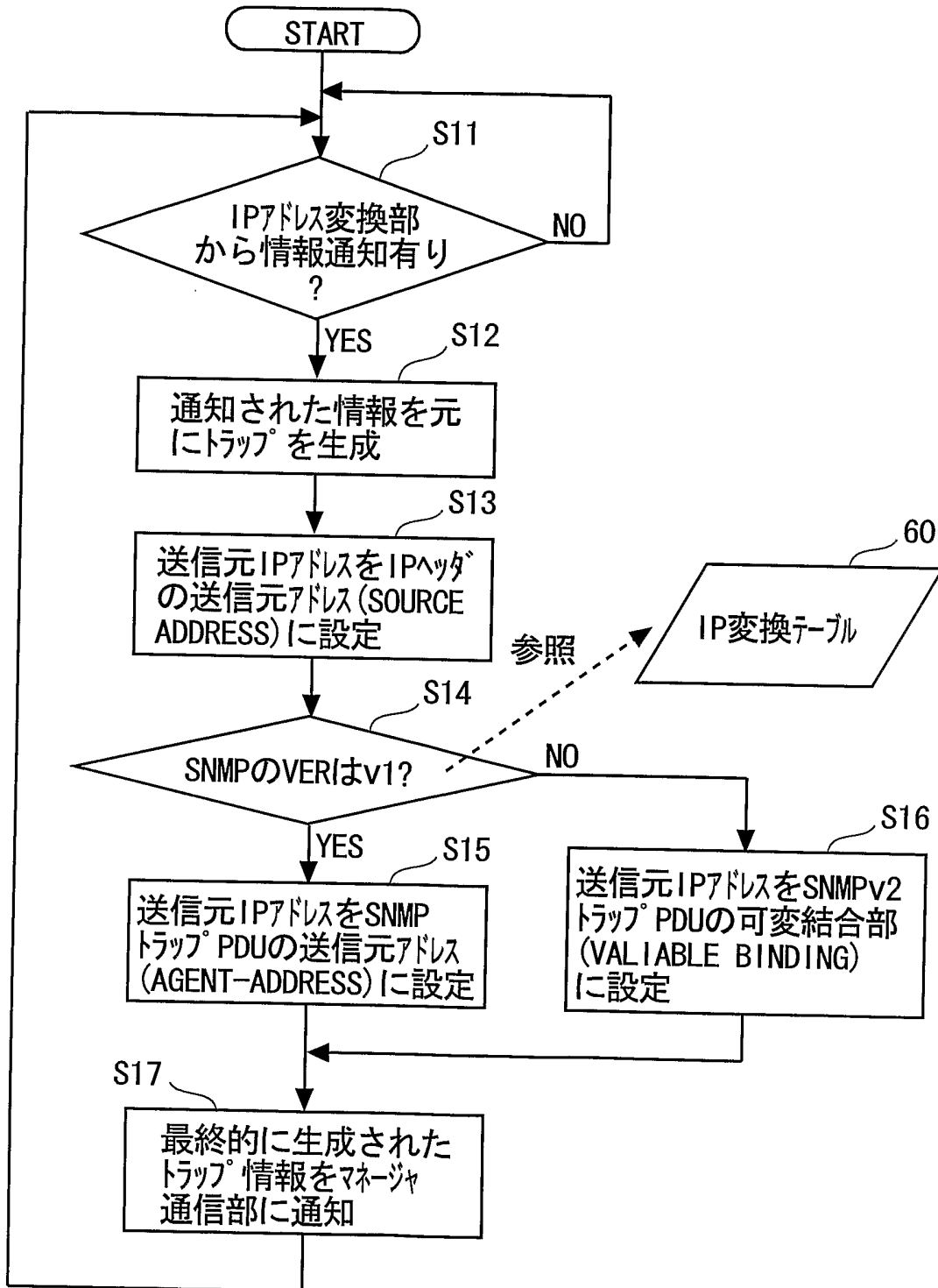
7/8 FIG. 7

IPアドレス変換部のフロー



8/8 FIG. 8

トラップ生成部のフロー



INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP03/01230

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl⁷ H04L12/24, G06F13/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl⁷ H04L12/24, G06F13/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1926-1996 Toroku Jitsuyo Shinan Koho 1994-2000
Kokai Jitsuyo Shinan Koho 1971-2000 Jitsuyo Shinan Toroku Koho 1996-2000

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 10-4407 A (NEC Corp.), 06 January, 1998 (06.01.98), Full text; all drawings (Family: none)	1-7
Y	JP 2000-183875 A (NEC Corp.), 30 June, 2000 (30.06.00), Page 5, right column, line 18 to page 6, left column, line 15; Fig. 1 (Family: none)	1-7
Y	JP 2002-190810 A (Hitachi, Ltd.), 05 July, 2002 (05.07.02), Page 3, right column, line 37 to page 4, right column, line 50; page 6, right column, line 36 to page 7, left column, line 23; Figs. 1, 11 & US 2002/0133582 A1	1-7

Further documents are listed in the continuation of Box C. See patent family annex.

* Special categories of cited documents:	"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A" document defining the general state of the art which is not considered to be of particular relevance	"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E" earlier document but published on or after the international filing date	"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&" document member of the same patent family
"O" document referring to an oral disclosure, use, exhibition or other means	
"P" document published prior to the international filing date but later than the priority date claimed	

Date of the actual completion of the international search
06 May, 2003 (06.05.03)

Date of mailing of the international search report
20 May, 2003 (20.05.03)

Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP03/01230

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 6-252986 A (Mitsubishi Electric Corp.), 09 September, 1994 (09.09.94), Page 2, right column, line 19 to page 3, right column, line 28; Fig. 2 (Family: none)	1-7
A	JP 7-321885 A (Mitsubishi Electric Corp.), 08 December, 1995 (08.12.95), Page 3, left column, line 23 to right column, line 47; Fig. 11 (Family: none)	1-7
A	JP 8-102756 A (Fujitsu Ltd.), 16 April, 1996 (16.04.96), Page 2, right column, line 30 to page 3, right column, line 18; Fig. 38 (Family: none)	1-7

A. 発明の属する分野の分類 (国際特許分類 (IPC))		
Int Cl ⁷ H04L 12/24, G06F 13/00		
B. 調査を行った分野		
調査を行った最小限資料 (国際特許分類 (IPC))		
Int Cl ⁷ H04L 12/24, G06F 13/00		
最小限資料以外の資料で調査を行った分野に含まれるもの		
日本国実用新案公報 1926-1996年 日本国公開実用新案公報 1971-2000年 日本国登録実用新案公報 1994-2000年 日本国実用新案登録公報 1996-2000年		
国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)		
C. 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y	JP 10-4407 A(日本電気株式会社)1998.01.06 全文、全図 (ファミリーなし)	1-7
Y	JP 2000-183875 A(日本電気株式会社)2000.06.30 5頁右欄18行~6頁左欄15行、図1 (ファミリーなし)	1-7
Y	JP 2002-190810 A(株式会社日立製作所)2002.07.05 3頁右欄37行~4頁右欄50行、6頁右欄36行~7頁左欄23行、図1, 11 & US 2002/0133582 A1	1-7
<input checked="" type="checkbox"/> C欄の続きにも文献が列挙されている。 <input type="checkbox"/> パテントファミリーに関する別紙を参照。		
* 引用文献のカテゴリー 「A」 特に関連のある文献ではなく、一般的技術水準を示すもの 「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの 「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す) 「O」 口頭による開示、使用、展示等に言及する文献 「P」 国際出願日前で、かつ優先権の主張の基礎となる出願 の日の後に公表された文献 「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの 「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの 「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの 「&」 同一パテントファミリー文献		
国際調査を完了した日	06.05.03	国際調査報告の発送日
国際調査機関の名称及びあて先 日本国特許庁 (ISA/JP) 郵便番号100-8915 東京都千代田区霞が関三丁目4番3号	特許庁審査官 (権限のある職員) 衣嶋 文彦 印	5 X 9199
		電話番号 03-3581-1101 内線 3556

C (続き) . 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
A	JP 6-252986 A(三菱電機株式会社)1994. 09. 09 2頁右欄19行~3頁右欄28行、図2 (ファミリーなし)	1-7
A	JP 7-321885 A(三菱電機株式会社)1995. 12. 08 3頁左欄23行~右欄47行、図11 (ファミリーなし)	1-7
A	JP 8-102756 A(富士通株式会社)1996. 04. 16 2頁右欄30行~3頁右欄18行、図38 (ファミリーなし)	1-7