IPv4/IPv6 ネットワークにおける不正端末検出システム

才所　秀明　　古舘　丈弘　　堤　俊之
日立ソフトウェアエンジニアリング（株）

1. はじめに

IPv6 の普及に伴い、IPv4 だけのネットワークから IPv6 との並存環境になりつつある。IPv6 のプラグアンドプレイ技術[1]は、DHCP のようにサーバを置かずとも、容易にネットワーク利用環境を構築できるため非常に利便性が高い。しかし、企業内ネットワーク等を考えた場合、DHCP やプラグアンドプレイ技術は、不正な端末を接続し易くしたとも言える。特に、プラグアンドプレイの場合、DHCP では可能だったサーバでの認証が出来ないため、さらに危険である。そのため、ネットワークに接続された端末、特に不正端末を即座に検出し排除することができるネットワーク管理システムが求められている。本稿では、この要求を満たす不正端末検出システムの考察と、試作結果について述べる。

2. 不正端末検出システムの概要

2.1. 不正端末検出システムへの要求事項

不正端末検出システムへの要求事項として以下の事項が挙げられる。
(1) IPv4/IPv6 並存環境でも利用可能
(2) 端末を即時に接続位置を含めて検出可能
(3) 不正な端末を自動的に判断
(4) 管理者が容易に接続端末情報を参照可能
(5) 不正な端末をネットワークから排除可能

ここで(1)及び(2)は、端末の検出方法が問題になる。

2.2. 端末検出方法

2.1 節の要求事項(1)から、IP アドレスを端末の識別子として利用することは適当でない。そこで識別子として MAC アドレスを利用する。この MAC アドレスを利用し LAN 上の端末を発見する方法には、MIB 収集方式とパケット監視方式の 2 種類が考えられる。

MIB 収集方式は LAN を構成するスイッチ等の MIB 情報を収集し利用するアプローチであり、パケット監視方式は、ネットワークを流れるパケットをキャプチャし解析するアプローチである。表 1 に利点と欠点をまとめる。

方式	利点	欠点
MIB 収集	(1) ポート特定可	(1) 検出の即時性無 (2) SNMP 対応が必須
パケット監視	(1) 検出の即時性有	(1) ポート特定不可 (2) 検出の完全性無 (3) 処理負荷高

表 1　MIB 収集方式の比較

要求事項(2)では端末検出の即時性と、端末接続位置の特定が求められている。これを実現するためには、端末検出はパケット監視方式を主体とし、位置特定に MIB 収集方式を利用する必要がある。ただし、パケット監視方式には、検出の完全性や処理負荷の問題がある。そこで、試作及び実験を通して、その実現性を考察した。

2.3. 試作システムの構成

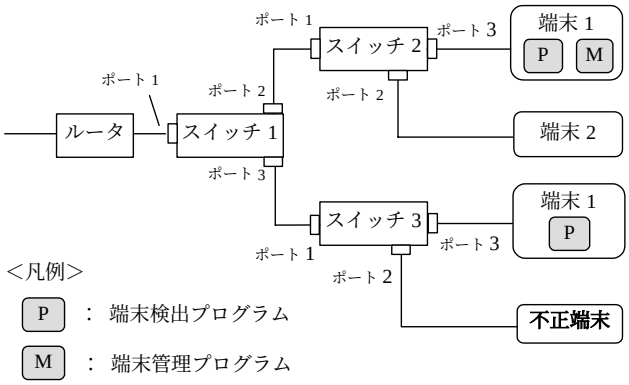

図 1　不正端末検出システムの構成図

試作システムの構成図を図 1 に示す。本システムは、以下の 2 つから構成される。
(1) 端末検出プログラム（Probe）
(2) 端末管理プログラム（Manager）

2.3.1. 端末検出プログラム（Probe）

Probe は、2.2 節のパケット監視方式に基づき端末検出を行うものである。

具体的にはパケットをキャプチャし、送信元 MAC アドレスの一覧をキャッシュに保持する。キャッシュに無いアドレスが発見されたら取り込んだパケットごと Manager に送る。Probe は管理するネットワーク（通常、サブドメインが単位）に一つ以上設置する。

2.3.2. 端末管理プログラム（Manager）

Manager は、次の処理を行うものである。

Non-Approved Terminal Detection System in IPv4/IPv6 Network
Hideaki Saisho, Takehiro Furudate, Toshiyuki Tsutsumi
Hitachi Software Engineering Co.,Ltd

(1) Probe から受けたパケットの処理
Manager は、正当な端末の MAC アドレスを含めた情報を保持する機器情報データベースを持ち、Probe から得られた端末が不正端末かどうかを MAC アドレスで自動的に判断する。また、2.2 節の MIB 収集方式のように SNMP を用いて MIB 情報を収集し、端末の接続位置を特定する。

(2) 管理者へのユーザインタフェースの提供
管理者に対し、検知した端末情報の表示機能、機器情報データベースへの登録機能などを持つ Web ベースのインタフェースを提供する。

(3) 不正端末のネットワークから排除手段の提供
SNMP を用いたスイッチポートの開閉によって、不正端末のネットワークからの排除手段を提供する。

3. 評価実験と結果の検討

3.1. 実験環境と実験項目

以下環境で本システムの実験を行った。

- システム環境

利用マシン : PenIII 800MHz,512Mbyte
利用 OS : FreeBSD4.4
備考 : Probe と Manager を同一のマシンで実行

- ネットワーク環境

PC 及びワークステーション: 40 台
インテリジェントスイッチ : 5 台

以下の 2 つの実験を行った。

(1) 不正端末検出システムの動作中に、端末及び不正端末を接続してネットワークを利用
(2) 不正端末検出システムを起動し、それまでに既に起動していた端末を検出

3.2. 実験結果及び評価検討

3.2.1. 端末検出の完全性

3.1 節の(1)の実験に関しては、端末の接続位置に関係なく端末を即時に検出した。しかし、(2)の実験においては、検出できない端末が見られた。これは、ブロードキャスト通信の有無が関係している。(1)では、ARP リクエストなどブロードキャスト通信が必ず起こるため Probe で検出できる。これに対し(2)では、ブロードキャスト通信が起きない可能性があり、Probe の位置によって検出できないことがある。

ただし、この問題は Probe を複数各所に配置することで解決可能である。

3.2.2. スケーラビリティ

本システムでは、Probe と Manager を分けることで、パケット監視方式の処理負荷の問題を解決している。本実験でもほぼ検出漏れは起こらなかった。しかし、検出の集中度によっては検出洩れが起こる場合があった。

この原因を詳しく調査した結果、試作システムの実装上の問題であることが分かった。試作では Manager が Probe から送られたパケットを逐次処理している。この処理の中で位置特定処理、特に SNMP 通信部が処理時間を長くしている。この位置特定処理を分離し、後回しにすることで検出漏れを防ぐことが可能である。

3.3. 拡張機能の検討

試作及び実験を通じて、改良が必要である点を以下に挙げる。

(1) 不正端末判断の強化
検出した端末が不正か否かを機器情報データベースの MAC アドレスのみで判定しているが、NIC の交換などに対応できない。これは、他のインベントリ情報などの活用で解決可能である。

(2) MAC アドレスフィルタリング機能の利用
不正端末をネットワークから排除する方法として、スイッチポートの開閉を用いている。しかし、無線 LAN-AP をスイッチに接続した場合は、正規の端末をも同時に排除してしまう恐れがある。これは、不正端末を排除する方法として、無線 LAN-AP の MAC アドレスフィルタリング機能を用いることで解決可能である。

(3) 切断と接続先変更の通知
本システムでは、接続の検知は行っているが切断や接続先変更には対応していない。これは、端末を検出後に、定期的に Ping などで接続性をテストし、MIB 情報から接続先を再検知することで解決可能である。

4. おわりに

本稿ではパケット監視方式を主体とした不正端末検出システムを提案した。試作し評価した結果、端末が接続されたら即座に検出できることが確認できた。実装上の問題から検出洩れが発生する場合があることが判明したが、実装の修正により実現可能である見通しを得ることが出来た。今後の課題は、3.3 節で述べた拡張機能の実装及び評価である。

参考文献

[1] S.Thomson and T.Narten, IPv6 Stateless Address Autoconfiguration, RFC2462, 1998.