E-07

物理的原因による通信障害のリモート診断方法提案

Proposal of remote diagnose method of network trouble from physical cause

坂田 渉†　　川橋 裕‡
Sakata Sho　　Yutaka Kawahashi

1. はじめに

従来，組織内ネットワークのボトルネックは管理者が運用しているネットワーク(以下バックボーンネットワーク)の信頼性と回線容量にあった．しかし，通信性能や機器性能の向上により信頼性が向上し，回線容量も増大したため，このボトルネックは解消されつつある．近年はボトルネックがバックボーンネットワーク下に接続されたユーザ端末側へと移行しつつある．したがって，バックボーンネットワークが正常に動作していても，ユーザ側の機器の不具合により障害発生が報告される場合が増えている．

ユーザから報告される障害内容は，ネットワークに繋がらないと体感したことである．この障害内容に対して，管理者はユーザ側に原因があるのか，管理者側のバックボーンネットワークに原因があるのか，障害原因の切り分けをおこなわなければならない．

多くの場合，管理者が得られる情報はユーザが「繋がらない」と体感したことだけである．したがって，管理者はネットワーク機器の確認や聞き取り調査，現地調査など様々な面から調査をおこない，原因の切り分けに必要な情報を可能な限り収集する必要がある．さらに，ネットワーク機器の操作やユーザとの適切な情報交換には多様な能力が求められる．ネットワーク機器の確認にはコマンドなどの知識が必要である．どのコマンドを実行すればどのような結果が出力され，結果から何がわかるかを理解するにはある程度の経験が必要である．聞き取り調査や現地調査も同様に何をおこなえばどのような返事が期待でき，返事から何がわかるかを理解していなければならない．これらをまとめておこなえるのは総合的な技術を持った管理者のみである．しかし，以上の手法では時間がかかるため，ユーザから障害発生の報告があるたびに管理者が他の業務に集中できない問題が発生する．したがって，これらの障害原因を切り分ける負担を軽減するために，障害原因をリモートで診断できる環境が必要である．

和歌山大学では，先行研究の MARS(Monitoring, Analysis and Response System)[1]を運用することでネットワーク接続を監視している．MARS は端末の IP アドレスと MAC アドレス，場所，利用時間を記録し，一定期間保存している．以上の情報により，MARS は IP アドレスの設定ミス，IP アドレスの競合などのユーザの設定ミスによる通信障害をリモートで診断することができる．しかし，MARS を用いても通信障害の原因を切り分けることができない場合が存在する．端末不良および，管理範囲外でのケーブル誤接続による L2 ループなどの，物理的な原因による障害はリモートで診断できない．これらは端末が設置されている現場で調査することでしか切り分けできない．加えて，これらの物理的な障害を予防することは難しい．端末不良を予防するためには安価なケーブル，筐体の持ち込み制限などが考えられる．L2 ループを防止するためにはケーブルを抜き差すたびに通知することや，ハブの持ち込み制限が考えられる．以上のような制限事項を多数設けることで防止することはできるが，ユーザの利便性が損なわれるため実施することは難しい．実施したとしても制限事項に反するユーザがいる可能性があるため，完全に排除することはできない．

本研究は，物理的な原因による障害をリモートで診断するシステムを構築し，管理者の支援を目的とする．本研究では，物理的な原因として端末不良と L2 ループを引き起こすケーブル誤接続箇所の 2 つを扱う．端末不良は，その端末から送信されるパケットのフレーム長が異常であることや，CRC がチェックサムと不一致であるという特徴が見られる．この特徴を利用することで端末不良を検出する．L2 ループを引き起こすケーブルの誤接続箇所には，L2 ループが発生する際に MAC アドレス誤学習が起こる特徴が見られる．この特徴を利用することでケーブル誤接続箇所を特定する．

提案システムは，エッジスイッチの各ポートが受信したエラーパケット数を定期的に収集し，端末接続情報と照らし合わせ発信端末を特定する．加えて，L2 ループが発生した時はスイッチに出力される MAC アドレス誤学習のログを収集する．ログだけでは正確にケーブル誤接続箇所を特定できないが，MARS の端末接続情報を参照することで正しくケーブル誤接続箇所を特定することができる．本研究では，端末不良の検出については本学内ネットワークに提案システムを設置し，L2 ループを引き起こすケーブル誤接続箇所の特定については実験環境において動作実験をおこなった．本論文では，既存技術とそれぞれの問題点について述べた後，実装した提案システムの構成と動作について説明し．最後に実験の結果と評価について述べる．

2. 既存技術

端末不良の検出と L2 ループを引き起こすケーブル誤接続箇所の特定に関する既存技術について述べる．加えて，それぞれの既存技術における問題点を述べる．

2.1 端末不良の検出

2.1.1 統合監視システム

統合監視システムとは，ネットワークに接続された端末の状態を集中監視するシステムである．オープンソースソフトウェアで広く普及しているものとして ZABBIX[2], NAGIOS[3] がある．これらは収集した監視データの履歴やグラフを表示する機能や，収集したデータに閾値を設定し，障害時に管理者へ通知する障害検知と通知機能を備えている．端末に専用エージェントを導入することでより多くの情報を収集できるようになり，端末不良を検出することができる．前提として，監視対象である端末の存在を把握していなければならない．PING の応答確認による死活監視の場合は端末の IP アドレスを把握しておく必要がある．端末不良を検出するためには死活監視だけでは難しいため，

†和歌山大学, Wakayama University

‡ 和歌山大学システム情報学センター, Center for Information Science, Wakayama University

専用エージェントのインストールをおこない端末の詳細な情報を収集しなければならない．

2.1.2 統合監視システムの問題点

統合監視システムを用いてユーザ端末の不良を検出するためには，ユーザが端末を組織内ネットワークに追加する時に管理者へ申請する必要がある．管理者は申請に応じてユーザ端末に IP アドレスを貸し出し，ユーザ端末に専用エージェントのインストールを指示する．以上の申請制度と専用エージェントインストールの義務化を実施することで端末不良を検出することができる．しかし，これらの制限事項はユーザの利便性を損なうため，ユーザにとって好まれない傾向がある．加えて，制限事項を設けた場合でも必ず管理者へ申請をせず持ち込まれた端末が存在するため，ネットワークに接続された全ての端末を監視することはできない．

2.2 L2 ループの検出

L2 ループを事前に防止する STP(Spanning Tree Protocol) と，事後に被害の拡大を防ぐ Storm Control，原因箇所を特定する L2 ループ検出機能について述べる．

2.2.1 STP

STP とはループ状に形成されたネットワーク内で L2 ループを防止するためのプロトコルで，IEEE 802.1D[4] として標準化されている．BPDU(Bridge Protocol Data Unit)と呼ばれる制御情報をやり取りし，ループを形成するポートをブロックすることで L2 ループを防止する．

2.2.2 Storm Control

ユーザがケーブルを誤接続することによりループが形成され，ブロードキャストストームが発生する．ブロードキャストストームとは，ループが形成されたスイッチにおいてブロードキャストパケットが大量に複製される現象で，スイッチの帯域を埋め尽くしてしまう問題である．Storm Control はブロードキャストパケットに閾値を設定し，閾値を超えた場合パケットを破棄もしくはポートをブロックすることができる．以上の方法で Storm Control は L2 ループ発生後に被害範囲を拡大させないことができる．しかし，ブロードキャストは実際にループが形成されたスイッチだけでなく同じサブネット内全域に転送されるため，原因箇所から離れたスイッチで Storm Control が作動してしまうことがある．

2.2.3 L2 ループ検出機能

L2 ループ検出機能とはスイッチに搭載されたベンダー独自の機能で，L2 ループの原因箇所を特定できる．専用の L2 ループ検出用パケットを送信し，送信スイッチにパケットが戻ってきたことで L2 ループを検出できる．通過するパケットをリアルタイムにフィルタリングする技術もあるが，必要な記憶容量が大きいためスイッチの価格が高い傾向にある．

2.2.4 問題点

事前対策としては STP が挙げられるが，STP に対応していないスイッチが存在すると正常に機能しない場合がある．よって，完全な L2 ループ回避の実現は難しい．事後対策としては Storm Control と L2 ループ検出機能が挙げられる．Storm Control は多くのベンダーで導入されており，被害範囲を拡大させないためには有用であるが，必ずしも原因箇所を特定できるとは限らない．L2 ループ検出機能の L2 ループ検出用パケットはベンダー独自の機能であるため，他のベンダーのスイッチによって破棄される場合がある．よって同一ベンダーのスイッチを多数導入する必要があり，既存システムへの適用は現実的でない．加えて，ユーザが持ち込むハブの種類にも制限を設ける必要がでてくる．

3. 先行研究

3.1 MARS

先行研究である MARS の動作と端末接続情報について述べる．MARS は，RADIUS 認証プロトコル[5] を利用してエッジスイッチが通知する端末の接続情報を収集する．エッジスイッチとは，バックボーンネットワークの末端のスイッチのことである．RADIUS 認証プロトコルは RFC2865 で策定されており，ダイアルアップによるリモート接続時のユーザ認証プロトコルである．近年はダイアルアップだけでなく，ブロードバンド接続や VPN，VLAN，無線 LAN への接続する際のユーザ認証にも利用されている．エッジスイッチにネットワーク認証の設定をし，RADIUS サーバと連携させる必要がある．エッジスイッチと MARS 間の動作手順を図 1 と下記に示す．

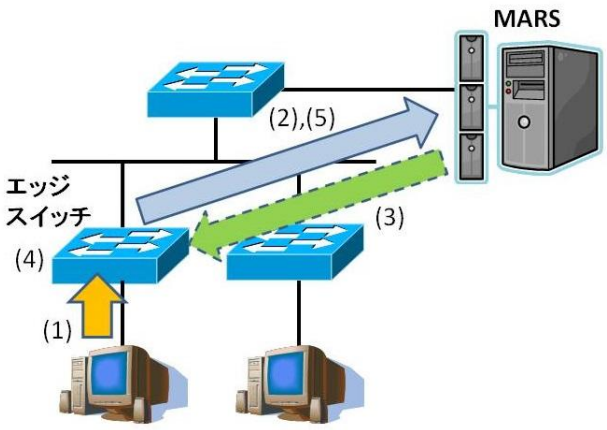


図 1 MARS の動作手順

(1) 端末がエッジスイッチに接続
(2) エッジスイッチは接続要求を MARS(RADIUS サーバ)に送信
(3) MARS は受信した情報を基に認証し，認証結果をエッジスイッチに通知
(4) エッジスイッチは通知された認証結果に基に，端末の接続を許可
(5) エッジスイッチは端末が接続を開始もしくは終了した事実を MARS に通知

上記に加えて，RADIUS サーバが端末の接続に対して全許可という判定および応答をすることで，ユーザに認証を求めない設計としている．これにより，ユーザに認証を求めないという運用ポリシの組織に対して，MARS を導入する際の敷居を低くしている．エッジスイッチが MARS に通知する情報を次に示す．

- セッション ID
- 端末の IP アドレス

- エッジスイッチの IP アドレス
- エッジスイッチのポート番号
- 接続開始および終了状態
- 接続開始および終了時刻

MARS はエッジスイッチから収集した情報からパッチ情報と連携し，端末の居場所である部屋名を特定する．端末が接続を開始してから終了するまでの通信をセッションと定義し，収集される端末の接続情報を各セッションごとに管理している．端末の接続情報として管理される項目を下記に示す．MARS はこれらの情報をデータベースに格納している．

- セッション ID
- 端末の DNS ホスト名
- 端末の IP アドレス
- 端末の MAC アドレス
- エッジスイッチの IP アドレス
- エッジスイッチのポート番号
- 棟名
- 部屋名
- 接続開始時刻
- 接続終了時刻

3.2 障害の切り分けと問題点

MARS は 3.1 節で示した端末の接続情報から障害を切り分けることができる．以下に示す障害を検出し，WEB インタフェースを用いてネットワーク管理者に提示する．

- IP アドレスの設定ミス
- IP アドレスの競合
- L2 ループ

これらの障害は MARS を用いることで原因を切り分けることができる．しかし，物理的な端末不良による通信障害は MARS を用いても原因を切り分けることができない．L2 ループを引き起こすケーブル誤接続箇所については，MARS を用いることで特定できる場合もあるが，全ての L2 ループにおいて原因箇所が特定できるわけではない．MARS によって原因箇所が特定できる場合と特定できない場合を図 2 と下記に示す．

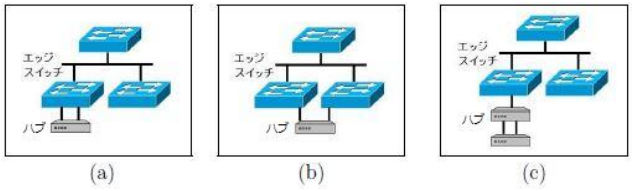


図 2　L2 ループ形成パターン

図 2 の(a)，(b)，(c) はいずれもエッジスイッチの配下にユーザがハブを用いてループを形成した場合を想定している．(a)，(b) のようにエッジスイッチを含むループが形成された場合，収集した端末の接続情報で同じ時刻にエッジスイッチの複数ポートから同一の MAC アドレスが接続を開始する事象が見受けられる．このことから接続が開始された複数ポートのうち，いずれかがケーブル誤接続箇所だと特定できる．さらに，エッジスイッチは管理者側が設置したスイッチであり，高性能なためほとんどの場合 STP が動作している．したがって，このようなループが形成された場合，エッジスイッチのどちらかのポートがブロックされ L2 ループが発生することは少ない．一方で，(c) はエッジスイッチの配下でループが形成されており，エッジスイッチの単一ポートに接続されている．この場合，エッジスイッチで STP が動作していたとしてもポートはブロックされない．MARS が収集した端末の接続情報に特徴的な事象は見受けられないためケーブル誤接続箇所は特定できない．

4. 研究目的

2 章で述べたように，端末不良を検出するためにはユーザに制限事項を設けなければならない．既存システムへの適用は現実的でない．既存のスイッチに搭載された技術を用い，ユーザがどのような機器を導入した場合でも動作する環境が必要である．

本研究では，物理的な障害をリモートで診断するシステムを構築し，管理者を支援することを目的とする．物理的な障害とは端末不良および，管理範囲外でのケーブル誤接続による L2 ループを示す．物理的な障害は起こりうるものであるため，発生を防止する技術ではなく発生原因を迅速に診断できる環境を作る．制限事項を設けることなくユーザに意識させないで導入が可能なシステムを目指す．加えて，既存のスイッチに独自機能を搭載することなく，ユーザがどのような機器を導入した場合でも L2 ループの原因箇所が特定できることを目指す．エッジスイッチの監視と MARS の端末接続情報を関連付けることにより，以上の条件を満たすシステムを構築する．

5. 提案手法

本章では端末不良の検出とケーブル誤接続による L2 ループ原因箇所特定のそれぞれに対する提案手法を述べる．

5.1 端末不良の検出

端末不良を検出するために SNMP(Simple Network Management Protocol)[6] を用いてエッジスイッチを監視し，エッジスイッチの各ポートが受信したエラーパケット数を収集する．エラーパケットを出力している端末は端末不良であると考えられる．以下，エラーパケット数を収集するために用いた SNMP と収集方法について述べる．

5.1.1 エラーパケット数の収集方法

- ifInErrors(OID:1.3.6.1.2.1.2.2.1.14)

ifInErrors は 0 から始まる整数値で，スイッチの各ポートが受信したエラーパケット数を示す．具体的なエラーパケットの種類を表 3 に示す．表 3 に示されたうち runts，giants，no buffer，CRC，frame を受信した場合，端末不良の可能性がある．ifInErrors はこれらのパケットの合計数値を通知する．取得できる数値はスイッチが起動してからの累積エラーパケット数であるため，取得するたびに差分を計算しなければならない．そのため，取得した値を毎回データベースに格納し，前回に取得した値との差分を計算する必要がある．

種類	説明
runts	フレームが最小サイズ未満なため破棄
giants	フレームが最大サイズを超えるため破棄
no buffer	スイッチのバッファスペース不足のため破棄
CRC	CRCがチェックサムと不一致なため破棄
frame	総ビット数が8の整数倍でないため破棄
overrun	受信速度がスイッチの処理能力を超えたため破棄
ignored	スイッチ内部バッファでの動作が低速なため破棄

表 3　エラーパケットの詳細

5.2　L2 ループ原因箇所特定

L2 ループは rsyslog[7] を用いてエッジスイッチの MAC アドレス誤学習ログを収集し，MARS の端末接続情報と関連付けることによってケーブルが誤接続された箇所を特定する．以下，MAC アドレス誤学習の利用とログの収集について述べる．

5.2.1　MAC アドレス誤学習の利用

スイッチは MAC アドレステーブルを保持しており，スイッチに届いたパケットの送信元 MAC アドレスを見て，どのポートの先にどの MAC アドレスが存在しているか学習する．通常は 1 つの MAC アドレスに 1 つのポートが割り当てられており，スイッチは MAC アドレステーブルを参照してパケットを送信するポートを選択している．しかし，MAC アドレス誤学習が発生すると 1 つの MAC アドレスに対して複数のポートが割り当てられ，スイッチはどのポートにパケットを送信するか選択できなくなる．つまり，誤学習された MAC アドレスの端末は通信ができなくなる．L2 ループが発生し，MAC アドレス誤学習が引き起こされる流れを図 4 と下記に示す．

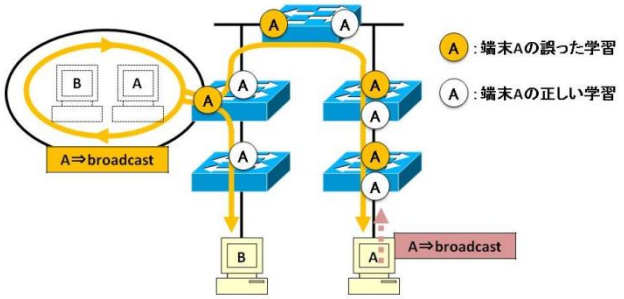


図 4　MAC アドレス誤学習

端末 A からブロードキャストパケットが送信され，ループを形成するスイッチにパケットが到着する．そこでパケットが巡回し，端末 A からのパケットが 2 つのポートで受信される．すると，スイッチはあたかも端末 A が 2 箇所に存在するように学習し，パケットを正しく送信することができなくなる．端末 A が接続されているスイッチとループが形成されているスイッチの間にある全てのスイッチが誤学習する．スイッチは誤学習した発信端末が実際にどのポートに存在していたかを記録していないため，発信端末が存在する 2 ポートのうち，どちらが正しい学習でどちらが誤学習かを判別できない．

MARS の端末接続情報から発信端末が過去にどのポートに存在していたかがわかる．よって，MAC アドレス誤学習のログから正しい学習と誤学習を判別することができる．誤学習を追いかけることでケーブルの誤接続箇所を特定する．本研究ではケーブル誤接続箇所の特定が目的であるため，L2 ループが発生した後に被害範囲の拡大を防止する機能はない．よって，前提としてエッジスイッチでは Storm Control が有効とする．

6. 実装

6.1　ネットワーク環境

本学内のネットワーク環境を参考にし，エッジスイッチとなる機器に Cisco[8] 社製 Catalyst スイッチを用いた．提案システムを実装するためには MARS が動作する環境が必要である．MARS を動作させるためにスイッチがネットワーク認証機能を有している必要があるため，ネットワーク認証機能を有しているスイッチの IOS を使用する．本研究で動作確認した機器は下記の通りである．

Catalyst 3560（Cisco IOS 12.2(50)SE 以降）
Catalyst 2960（Cisco IOS 12.2(50)SE 以降）

6.2　ハードウェア環境

実装したシステムのハードウェア環境を以下に示す．

- OS：CentOS6.3
- CPU： Intel(R) Core(TM) i3-2120 CPU @ 3.30GHz
- Memory：4 [GB]

6.3　ソフトウェア環境

5 章で述べた提案手法をオープンソースソフトウェアの Apache[9]， MySQL[10]， Net-SNMP[11]， rsyslog，highcharts[12] を用いて実装した．いずれも広く利用されており，安定性が高い．提案システムは，これらの環境に bash(Bourne-Again Shell)，Perl および PHP を用いて実現した．以下に Net-SNMP，rsyslog，highcharts の概要について述べる．

Net-SNMP

サーバなどを監視するために SNMP を実装した BSD Lisence を採用するオープンソースのソフトウェアである．Net-SNMP に付属する snmpget コマンドを用いて OID と監視対象の指定により，OID に対応する情報を取得することができる．本システムでは Net-SNMP のライブラリを用い，エッジスイッチの SNMP エージェントからエラーパケット数を取得する．

rsyslog

システムの動作状況やメッセージなどのログを取得するプログラムである．ネットワークを通じて様々なシステムのログデータを集中して管理することができる．あらかじめユーザが指定した形式でログの保存ができ，加工したログを任意のプログラムに引き渡すことができる．本システムでは rsyslog を用いて Catalyst スイッチから MAC アドレス誤学習のログを収集し，Perl プログラムで処理する．

highcharts

Web でグラフを描写するための JavaScript ライブラリである．CSV ファイルから数値を読み取り，リアルタイムでグラフを表示することができる．highcharts は特定データの一時消去，ラベル表示など，対話性に優れたユーザインタフェースである．本システムでは，

highcharts を用いてエラーパケット数と端末接続状況のグラフを管理者に提示する．

6.4　システム構成

提案システムの処理手順と各部について図 5 と下記に示す．

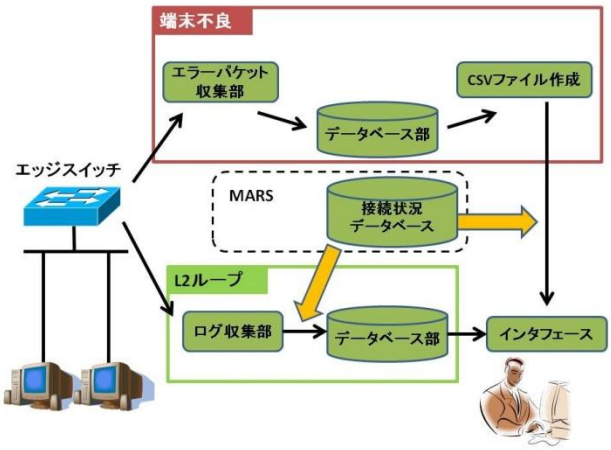


図 5　システムの処理手順

(1)　エラーパケット数を収集
(2)　エラーパケット数をデータベースに格納
(3)　CSV ファイルに形成して管理
(4)　MARS の端末接続情報を関連付けてグラフを管理者に提示
(5)　MAC アドレス誤学習のログを収集
(6)　MARS の端末接続情報を参照し，正しい端末の位置を検索
(7)　L2 ループを引き起こしたケーブル誤接続箇所をネットワーク管理者に提示

次に，提案システムを構成する各部について述べる．

エラーパケット収集部

エラーパケット収集部は，5.1 節で述べた OID を用いて，10 分ごとにエッジスイッチの各ポートが受信したエラーパケット数を取得する．

端末不良データベース部

5.1 節で述べたようにエッジスイッチから取得できる数値はエッジスイッチが起動してからの累積エラーパケット数であるため，取得するたびに差分を計算しなければならない．そのため，端末不良データベース部では取得した値を毎回データベースに格納し，前回に取得した値との差分を計算する．

CSV ファイル作成部

グラフ表示に用いる highcharts を使用するために CSV ファイルに形成する必要がある．よって，エッジスイッチの各ポートが受信したエラーパケット数を CSV ファイルに形成して管理する．

ログ収集部

Cisco 社製 Catalyst スイッチに設定を加え，rsyslog サーバにログを収集する．

L2 ループデータベース部

特定できたケーブル誤接続箇所をデータベースに格納する．

6.4.1　インタフェース

インタフェースを Perl および PHP，highcharts で記述した Web アプリケーションにより実装している．端末不良のインタフェースは図 6 と図 7 で，L2 ループのインタフェースは図 8 である．図 6 の下部は 1 日の間で，エラーパケットを受信したポートに存在している端末情報を表示している．これらはエラーパケットの発信端末である可能性がある．管理者は上部にある検索欄にエッジスイッチの IP アドレス，ポート番号，日付を入力することで図 7 のようなグラフを表示することができる．図 7 のグラフは，あるエッジスイッチのポートについて表示したものである．下部に表示された要素のうち，最初の要素である Gi0/12 はポートが受信したエラーパケット数を表している．続く残りの要素はそのポートに存在する端末の MAC アドレスを表している．端末はリンクアップ状態時にパケット数が 50 の値をとり，リンクダウン状態はパケット数が 0 の値をとる．3 つの端末はいずれも 1 日の間，常にリンクアップ状態にあることが読み取れる．このグラフを用いて管理者は発信端末を特定する．highcharts で出力しているため，WEB 上でグラフにカーソルを合わせると細かな時刻とエラーパケット数が表示される．任意の要素をグラフから除外することもできる．図 8 は L2 ループの原因となったケーブル誤接続箇所を管理者に提示するインタフェースである．エッジスイッチの IP アドレス，ポート番号，L2 ループ発生時刻を管理者に提示する．

図 6　端末不良のインタフェース

図 7　グラフ表示

L2ループ発生箇所

No	SW IPaddr	SW Port	Time
1	192.168.200.252	Fa0/4	2014-01-26 16:49:11

図 8　L2 ループのインタフェース

7. 運用実験

7.1 端末不良の検出

端末不良の検出は，端末不良を意図的に引き起こすことができないため，本学内で実際に使用されている端末を対象にした．提案システムを本学内ネットワークのエッジスイッチ 27 台に適用し，27 台のうち 2 台のエッジスイッチからエラーパケットを受信するポートが見つかった．WEB インタフェースに出力されたグラフを図 9 と図 10 に示す．

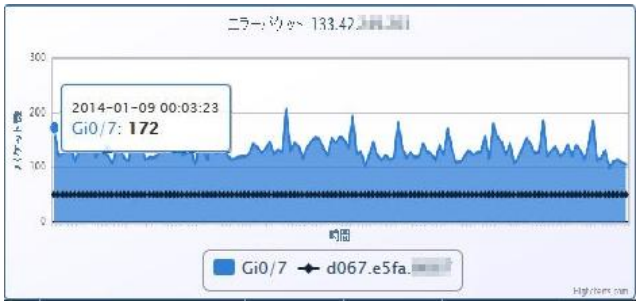


図 9　学内エッジスイッチ A の Gi0/7

図 10　学内エッジスイッチ B の Gi0/12

図 9 は，以前から端末が 1 つだけが接続されているため，MAC アドレスが d067.e5fa の端末がエラーパケットの発信端末であることが判別できた．図 10 は，端末が 2 つ接続されているが図から読み取れるように，MAC アドレスが 0022.cf3b の端末が接続されるとエラーパケット数が増加し，接続が切れるとエラーパケット数が減少している．よってエラーパケットの発信端末は MAC アドレスが 0022.cf3b の端末だと特定できた．以上の d067.e5fa と 0022.cf3b について調査し，実際に物理的な障害が発生しているか確認をおこなった．

d067.e5fa はエッジスイッチから情報コンセントまでの館内ケーブルの老朽化によって，エラーパケットが出力されていることが分かった．館内ケーブルは管理者側の責任でもあるため，d067.e5fa に関してはユーザ側に責任はなかった．0022.cf3b については PING の応答確認を実施したところ不定期に要求がタイムアウトし，23%のパケットが損失していた．実際に確認をおこなったところ，0022.cf3b はイーサネットコンバーターを経由して情報コンセントに接続されていた．イーサネットコンバーターを取り除き，端末を情報コンセントに直接接続したところ正常に PING の応答確認ができた．以上からイーサネットコンバーターに不良があったことが確認できた．

7.2 L2 ループ原因箇所特定

L2 ループを発生させた場合，ストームによって通信障害が発生するため実験環境を構築した．Cisco 社製の Catalyst 3560 スイッチでバックボーンネットワークを構築し，提案システムを導入した．エッジスイッチの配下に Buffalo 社製スイッチングハブを 2 台接続し，意図的にループを形成した．MAC アドレスが誤学習される端末の位置は固定されていないため，2 つのパターンで実験をおこなった．それぞれを図 11 と図 12 を用いて下記に示す．

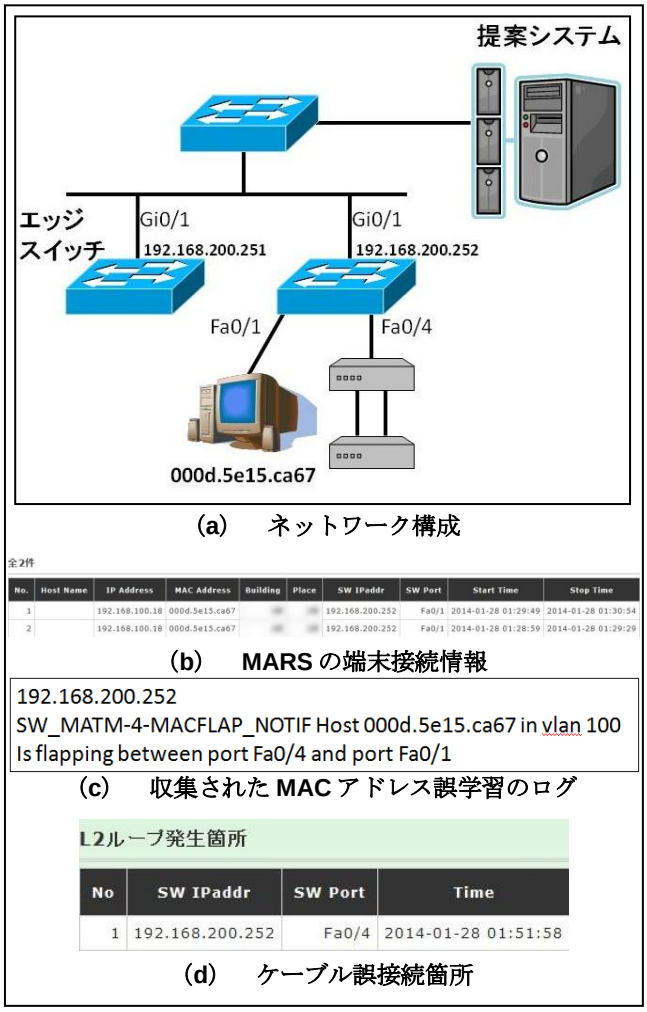
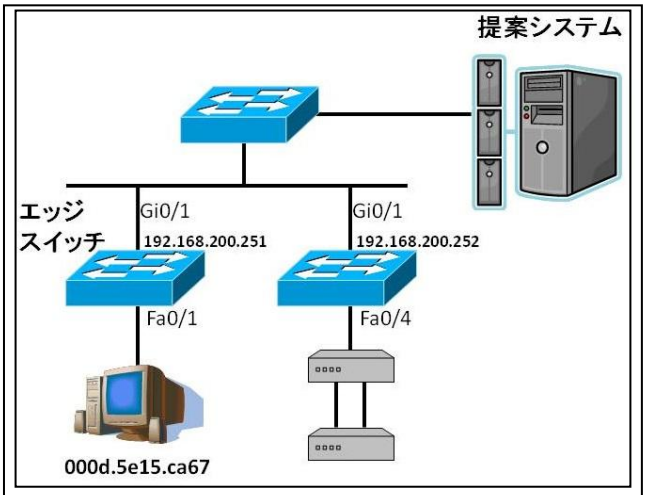


図 11　発信端末とループ形成箇所が同一のエッジスイッチに存在する場合

図 11 はループ形成箇所と発信端末の 000d.5e15.ca67 が同一のエッジスイッチに存在している．この場合，(c) に示すように 1 つのエッジスイッチのみで MAC アドレスの誤学習が発生する．学習されたスイッチの IP アドレスは 192.168.200.252 で，ポートは Fa0/1 と Fa0/4 である．(b) に示された MARS の端末接続情報を参照することで発信端末は 192.168.200.252 の Fa0/1 に存在しているため，Fa0/4 は誤学習だとわかる．(d) は提案システムにより，管理者に提示されたインタフェースである．正しくケーブルの誤接続箇所を特定できていることがわかる．



（a） ネットワーク構成

全4件

No.	Host Name	IP Address	MAC Address	Building	Place	SW IPaddr	SW Port	Start Time	Stop Time
1		192.168.100.17	000d.5e15.c9c4			192.168.200.252	Fa0/4	2014-01-28 01:23:36	
2		192.168.100.18	000d.5e15.ca67			192.168.200.251	Fa0/1	2014-01-28 01:02:18	
3		192.168.100.18	000d.5e15.ca67			192.168.200.251	Fa0/1	2014-01-28 00:41:51	2014-01-28 00:42:14
4		192.168.100.18	000d.5e15.ca67			192.168.200.251	Fa0/1	2014-01-28 00:40:55	2014-01-28 00:41:06

（b） MARS の端末接続情報

192.168.200.251
SW_MATM-4-MACFLAP_NOTIF Host 000d.5e15.ca67 in vlan 100
Is flapping between port Fa0/1 and port Gi0/1

192.168.200.252
SW_MATM-4-MACFLAP_NOTIF Host 000d.5e15.ca67 in vlan 100
Is flapping between port Fa0/4 and port Gi0/1

（c） 収集された MAC アドレス誤学習のログ

L2ループ発生箇所

No	SW IPaddr	SW Port	Time
1	192.168.200.252	Fa0/4	2014-01-28 01:25:19

（d） ケーブル誤接続箇所

図 12 発信端末とループ形成箇所が別のエッジスイッチに存在する場合

図 12 はループ形成箇所と発信端末の 000d.5e15.ca67 が別のエッジスイッチに存在している．この場合，(c) に示すように 2 つのエッジスイッチで MAC アドレス誤学習が発生する．(b) に示された MARS の端末接続情報を参照すると発信端末は 192.168.200.251 の Fa0/1 に存在している．よって，MAC アドレス誤学習したエッジスイッチのうち，発信端末が存在していなかった 192.168.200.252 にケーブル誤接続箇所があると特定できる．192.168.200.252 で学習された 2 ポートはアップリンクとダウンリンクである．アップリンクとはバックボーンネットワークに接続されているポートで，ダウンリンクとはユーザが接続するポートのことである．正しい学習はエッジスイッチのアップリンクで誤学習はダウンリンクであるが，スイッチや MARS はアップリンクとダウンリンクの区別ができない．そこで，MARS の端末接続情報から過去に端末が 1 台でも接続されていればダウンリンクと判断する．今回の実験では Fa0/4 には端末が存在していたため，Fa0/4 はダウンリンクであると判断できる．以上からケーブルの誤接続箇所は 192.168.200.252 の Fa0/4 とわかる．(d) は提案システムにより，管理者に提示されたインタフェースである．正しくケーブルの誤接続箇所を特定できていることがわかる．

8. 評価

8.1 ユーザに制限事項を設けない

2.1 節で述べた統合監視システムはユーザに制限事項を設ける必要がある．組織内ネットワークにおいて，無許可で IP アドレスを使用するユーザや，IP アドレスの変更があっても申告しないユーザは少なからず存在する．既存技術ではこれらの不正なユーザ端末の不良を検出することはできない．本研究ではエッジスイッチの監視と MARS との連携により，ユーザに制限事項を設けることなく端末不良が検出できる．加えて，不正なユーザがネットワークに接続してきた場合でも，それらの端末不良を検出することができる．さらに，ユーザ端末と直接通信をおこない監視する必要がないため，IP アドレスの設定ミスにより正常にネットワークに接続できない端末も監視することができる．したがって，本研究は既存技術よりも優れていると考えられる．

8.2 本提案システムの新規性

2.1 節で述べた統合監視システムは ZABBIX や NAGIOS を代表として数多く提供されている．これらの監視対象は組織内ネットワークにおいてサービスを提供しているサーバやバックボーンネットワークの機器が対象である．つまり，管理者が提供もしくは管理している機器が監視対象となっている．既存技術ではユーザが持ち込んだ端末の存在を正確に把握することが難しく，それらの端末に管理者自ら専用エージェントをインストールすることはできない．よって，既存技術ではユーザ端末の不良を検出することは難しい．本研究のようにユーザ端末の不良を検出するシステムは，調べてみたところ現在は存在していない．これは管理者にとってユーザ端末の不良が重要視されていないためであると考えられる．しかし，端末不良は端末が設置されている現場に行かなければ切り分けることが難しいため，管理者にとって時間がかかる厄介な問題である．よって，端末不良をリモートで診断できる環境設備は重要である．本提案システムを用いることによりユーザ端末の不良をリモートで診断できるため，管理者の負担を軽減し，支援することができる．以上から，ユーザ端末の不良を検出するという点で本研究は新規性があると言える．

6.3 使用する機器に制限がない

2.2 節で述べた Storm Control と L2 ループ検出機能を本提案システムと比較する．StormContol は原因箇所から離れたスイッチで作動してしまうことがある．すなわち，Storm Control は被害範囲を拡大させないためには有用であるが，必ずしも原因箇所を特定できるとは限らない．L2 ループ検出機能はスイッチに L2 ループ検出用の独自機能を搭載している．よって，独自の機能を搭載していないスイッチが存在していた場合，正常に動作しないことがある．加えて，多数の独自機能を搭載したスイッチを導入する必要があるため，既存システムへの適用は現実的ではない．本研究では，エッジスイッチの MAC アドレス誤学習を rsyslog で収集し，MARS と関連付けることで原因箇所を特定した．専用のループ検出用パケットのような独自機能を使用しないため，ユーザがどのようなスイッチを導入し

ても確実に動作する．以上より，既存システムへの適用が容易であり，使用する機器に制限がない点で本研究は既存技術よりも優れている．

9. 考察と今後の課題

9.1 端末不良の検出精度向上

本研究では，エッジスイッチの各ポートが受信するエラーパケットを用いて端末不良を検出した．エラーパケットだけでは本当にその端末が不良であるかどうかを切り分ける情報が不足していると考えられる．精度を向上させるためには切り分ける情報を増やす必要がある．その情報の候補としてブロードキャストパケットや，端末の頻繁なリンクアップとリンクダウンが挙げられる．NIC の不良によってブロードキャストパケットが大量に送信されることや，NIC やケーブルの老朽化により端末がリンクアップとリンクダウンを繰り返すことがある．よって，エラーパケットだけでなくブロードキャストやリンクのアップダウンを考慮することにより，端末不良の検出精度を改善できると考えられる．

9.2 エラーパケット発信端末の特定精度向上

本研究ではエッジスイッチのポート下に複数の端末が存在した場合のエラーパケットと端末の接続状況から発信端末を特定した．しかし，ポート下の複数の端末が常時リンクアップである場合や，多数の端末が存在している場合は発信端末の特定が難しい．よって，発信端末を特定するための情報が不足していると言える．改善策として，発信端末の候補に PING の応答確認を定期的に実施する方法などが挙げられる．しかし，この方法も PING に対して応答しない端末が存在しているため効果的ではないと考えられる．そのため，より正確に特定する方法を今後の課題としていきたい．

9.3 **L2** ループ原因箇所の特定精度向上

本研究では，エッジスイッチの MAC アドレス誤学習を利用してケーブル誤接続箇所を特定した．5.2.1 項で述べたように MAC アドレス誤学習は発信端末が接続されているスイッチとループが形成されているスイッチの間にある全てのスイッチで発生する．しかし，Storm Control の設定によっては L2 ループが発生した直後にポートがブロックされ，L2 ループがすぐさま終息してしまうためにエッジスイッチで MAC アドレス誤学習が発生しない場合があることがわかった．加えて，発信端末の通信先にもエッジスイッチで MAC アドレス誤学習が発生するかどうかに少なからず関係があると考えられる．すなわち，エッジスイッチだけの MAC アドレス誤学習を監視しても，MAC アドレス誤学習が発生しない場合が存在するため，ケーブル誤接続箇所を特定できないことがある．

MAC アドレス誤学習を利用し，より確実にケーブル誤接続箇所を特定するためにはバックボーンネットワークの上位にあるスイッチ(以下上位スイッチ) からも同様にログを収集する必要があると考えられる．エッジスイッチにログが出力されない場合は上位スイッチのログを利用することで，より確実にケーブル誤接続箇所を特定できる．しかし，上位スイッチのログを利用するにあたり問題がある．上位スイッチの下位にどのエッジスイッチが存在しているか把握していなければこの手法は使えないため，どのようにして上位スイッチとエッジスイッチを関連付けるかが問題になってくる．エッジスイッチを集約している上位スイッチをパッチ表などを用いて管理する必要があると考えられる．以上の方法で L2 ループ原因箇所特定の精度を向上できると考えている．

9.4 端末不良のインタフェース改善

6.4.1 項で示した端末不良のインタフェースで出力されるグラフは同時に 1 つしか表示できない．よって，あるエッジスイッチのあるポートに対して過去のグラフを複数出力させ，いつからエラーパケットを受信したかを調べることができない．現状では日付を指定し，グラフを 1 つずつ確認していかなければならない．今後は複数のグラフを出力できるように改良していきたい．

10. おわりに

本研究では物理的な原因による障害をリモートで診断し，管理者を支援するシステムを構築した．エッジスイッチの監視と先行研究の MARS との連携による手法を提案し，端末不良の検出と L2 ループを引き起こすケーブル誤接続箇所の特定ができることを確認できた．今後は，物理的な原因による障害を検出する精度を向上できるようにシステムを改良していきたいと考えている．

参考文献

[1] 吉田祐亮 “ネットワーク接続監視システム MARS の構築”
2012 年度和歌山大学大学院修士論文

[2] ZABBIX
http://www.zabbix.com/

[3] NAGIOS
http://www.nagios.org/

[4] IEEE802.1D
http://www.ieee802.org/1/pages/802.1D-2003.html

[5] “Remote Authentication Dial In User Service (RADIUS)”
http://tools.ietf.org/html/rfc2865

[6] SNMP
http://www.snmp.com/

[7] rsyslog
http://www.rsyslog.com/

[8] “Cisco Systems”
http://www.cisco.com/

[9] Apache
http://www.apache.org/

[10] MySQL
http://www.mysql.org/

[11] Net-SNMP
http://www.net-snmp.org/

[12] highcharts
http://www.highcharts.com/