

Link Layer Discovery Protocol と Cisco Discovery Protocol を利用した ネットワークトポロジーの探索と描画による障害検知システムの構築

堀内 亮汰† 川橋 裕‡
Ryota Horiuchi Yutaka Kawahashi

1. はじめに

一般的に運用されているネットワークでは、ネットワーク機器は経年劣化による故障や復電時の正常な起動の失敗などによってネットワークの遮断が発生する。しかしこの障害は、ネットワーク層の機器と違い **traceroute** を利用できないため、障害が報告された地点からネットワーク図を用いて調べる必要がある。この作業には、時間がかかりネットワークの管理者の大きな負担となっている。この問題を解決するためには、機器間の隣接状態の変化を検知する必要がある。この検知をおこなう既存の手法として、**SNMP(Simple Network Management Protocol)**トラップという機能を利用したものがある。SNMP トラップは、ネットワーク機器に何らかの異常が発生した際に **SNMP** エージェントから **SNMP** マネージャーへその内容を通知する **SNMP** の機能のひとつである。しかし、この機能には問題点があり、**SNMP** エージェントから **SNMP** マネージャーへの通知が **UDP(User Datagram Protocol)**の通信であるため確実な受信ができないことである。そのため **SNMP** トラップのみに依存する障害検知では、障害発生を検知できない場合があり信頼性が高いとは言えない。

本研究では、**SNMP** を用いて **LLDP** や **CDP** の情報を取得し、ネットワークをクロールすることによって現在のネットワークトポロジーを取得することを目的とする。データリンク層のプロトコルには **LLDP** を用いることによって、ネットワーク機器のベンダーによらない検知が可能である。また、**LLDP** に対応していない古いネットワーク機器に対応するため、**Cisco** 社が提供する **CDP(Cisco Discovery Protocol)** も利用する。このプロトコルは、**Cisco** 社の製品と一部の **CDP** 対応製品のみが利用できる。本システムを用いることで、管理者は時間ごとにおけるネットワーク機器の隣接情報の変化を比較的容易に確認することを可能にした。

2. 既存研究

既存研究として、**FDB(Forwarding Data Base)**を用いたネットワークトポロジーの探索が存在する。**FDB** とは、宛先 **MAC** アドレスと送出ポートと **VLAN** の組み合わせを管理するデータベースのことである。**FDB** を用いることによって隣接するネットワーク機器の **MAC** アドレスとそこに割り当てられた **VLAN** を取得することができるため、既存研究ではあらかじめ設定していたネットワーク機器から **FDB** を取得することによってネットワークトポロジーの探索をおこなっている。しかしながら、既存研究の問題点として **FDB** から情報を取得するためスパンニングツリーが設定されてい

る場合に、待機状態のネットワーク機器を発見できないという問題点がある。

3. 研究目的

ネットワークを運用する上で、管理者はネットワークのトポロジーの変化を把握しなくてはならない。しかし、常にこの変化を把握することは現実的に困難である。そのため、これまでは **SNMP** トラップの機能を利用し、ネットワークトポロジーの変化を検知してきた。しかし第 2 章で述べた通り、**SNMP** トラップだけに依存してしまうと情報を取得できずにネットワークトポロジーの変化を検知出来ない場合がある。この問題は、**UDP** というプロトコルで動作する **SNMP** トラップを利用する限り解決することは難しい。そのためこの問題を解決するには、**SNMP** を利用しマネージャー側が能動的にネットワークをクロールし、ネットワークトポロジーを把握する必要があると考えられる。

本研究では、**SNMP** を用いて **LLDP** や **CDP** の情報を取得し、ネットワークをクロールすることによって現在のネットワークトポロジーを取得することを目的とする。さらに、取得したネットワークトポロジーをグラフとして描画し管理者が容易に確認できるようにする。これにより管理者がネットワーク図を用いて調査する手間を省き、ブラウザを通じて得られる情報のみで現在のネットワークトポロジーの情報を把握することが可能となる。

4. 提案システム

提案システムの概要を図 1 に示す。

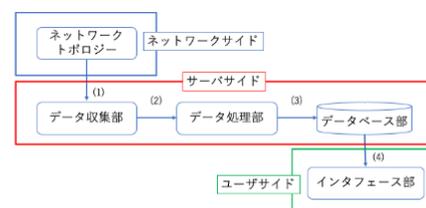


図 1: システムの概要

また、システムの処理手順を以下に示す。

- (1) ネットワークトポロジーのクロール
- (2) クロールによって得られた情報を伝達
- (3) 情報を整形しデータベースへ保存
- (4) 現在のネットワークトポロジーを描画

データ収集部では、**cron** を用いることによって定期的にネットワークトポロジーのクロールを行う。ネッ

†和歌山大学大学院

‡和歌山大学 学術情報センター

トワーク機器が保持しているマネジメントアドレスによってそのネットワーク機器がクローラ済みかを確認しているためクローラによるループ等は発生しない。

データ処理部では、データ収集部で収集されたデータに対して正規化を行い保存する。このときホスト名を用いて重複を削除するため、再度 SNMP を用いて各ネットワーク機器からホスト名を取得する。その後、ホスト名によって重複を取り除いた情報に対して正規化した隣接リストを作成する。このとき、作成した隣接リストは JSON 形式で出力する。

データベース部では、データ処理部で作成された隣接リストを管理する。さらに、ホスト名とマネジメントアドレスの対応も管理する。この 2 つはそれぞれが独立したデータであるため別のテーブルで管理を行う。

インタフェース部は、JavaScript によって実装されている。管理者は Web インタフェースから予め設定した始点となるネットワーク機器からのネットワークトポロジーを確認することができる。さらに、そのネットワークトポロジーにあるネットワーク機器のホスト名とマネジメントアドレスの対応一覧も確認することができる。

5. 実験・評価

実験のため構築したネットワークを図 2 に示す。実験用ネットワークでは、停電時を想定し SNMP マネージャーへの通信を一時的に全遮断させた。さらに、通信の全遮断中に C2960-TS-1 と C2960-TS-2 の接続を切断し、ネットワークトポロジーを変化させた。これによって、全遮断が復旧した後も一部のネットワークを通信できない状況にした。その後、本システムでネットワークの復旧後にトポロジーの変化を検知できるかを検証した。

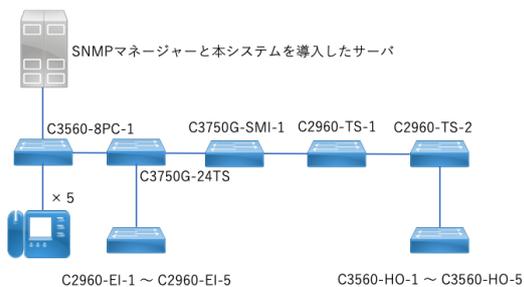


図 2：実験用ネットワーク

通信の全遮断前と全遮断後にそれぞれ本システムを利用し、ネットワークトポロジーを取得した。取得したネットワークトポロジーをそれぞれ図 3 と図 4 に示す。取得したネットワークトポロジーを比較することによって、C2960-TS-1 と C2960-TS-2 の接続が切断されて障害が発生したことが検知できた。

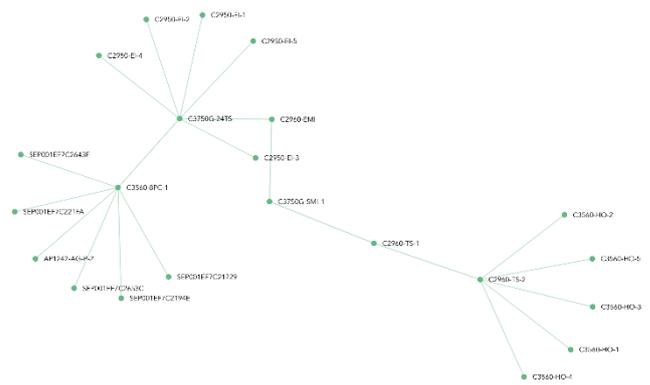


図 3：全遮断前のネットワークトポロジー

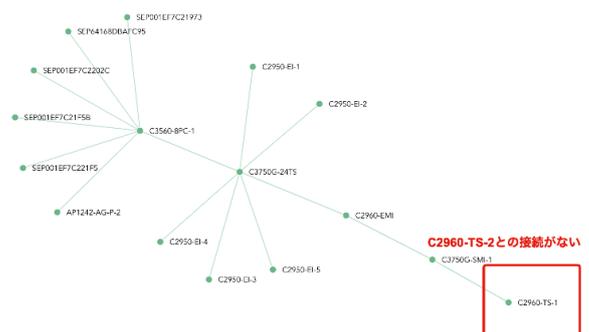


図 4：全遮断後のネットワークトポロジー

6. おわりに

本研究では、SNMP と LLDP および CDP を利用することで、時間ごとにおけるネットワーク機器の隣接情報の変化を比較的容易に確認することを可能にした。しかしながら、現状のインタフェースによるネットワークトポロジーの表示では接続されていないポートの表示などがおこなわれていない。そのため、ネットワーク機器がどのポートで接続されているか表示することにより、ネットワーク機器のどのポートに原因があったかといったより詳しい情報を確認できると考えられる。

さらに、レイヤー 2 におけるネットワークで重要となる VLAN (Virtual LAN) の管理情報も表示することで影響範囲の推定なども容易になると考えられる。そのため、今後はネットワーク機器が接続されたポートやそこに割り当てられた VLAN の情報などを表示できるようにし、より詳細なネットワークトポロジーの把握が可能になるようシステムを改良していきたい。

参考文献

- [1] 吉田 和幸 “Layer2 ネットワーク構成情報の推測アルゴリズムの改良について” 分散システム/インターネット運用技術シンポジウム 2005 論文集 pp.61-66
- [2] 吉田 和幸 “ループを考慮した Layer2 ネットワーク構成情報の推測アルゴリズムについて” 分散システム/インターネット運用技術シンポジウム 2006 論文集 pp.7-12