社団法人　情報処理学会　研究報告
IPSJ SIG Technical Report

2006－DSM－43（7）
2006／9／15

組織内ネットワークにおける Layer-2 トポロジ検出システムの提案

續木　涼太 †　　泉　裕 ††　　齋藤　彰一 †††　　塚田　晃司 †††

† 和歌山大学　システム工学研究科　　†† 和歌山大学　システム情報学センター
††† 和歌山大学　システム工学部

内容梗概　ネットワーク管理における構成管理は，障害管理・性能管理・セキュリティ管理全てに関連する重要な管理項目である．したがって，ネットワーク管理者は巨大な Layer-2 構造になりつつある近年のネットワーク構成を把握する必要がある．Layer-2 のネットワークトポロジを把握するためには，ネットワーク機器同士の接続情報，ネットワーク機器の保持する ARP 情報と MAC アドレスのキャッシュ情報，VLAN に関する情報，冗長化経路に関する情報が必要となる．そこで，本稿では Layer-2 のネットワークトポロジを把握するために，上記した情報をネットワーク機器から収集しネットワーク管理を支援するシステムを提案する．

A Proposal of Layer-2 Topology Detecting System for Internal Network

Ryota TSUZUKI †　　Yutaka IZUMI ††　　Shoichi SAITO †††　　Koji TSUKADA †††

†Graduate school of Systems Engineering, Wakayama University
††Center for Information Science, Wakayama University
†††Faculty of Systems Engineering, Wakayama University

Abstract　Configuration management is a essential item at network management, related to fault, performance and security management. Therefore, the network manager has to grasp the network structure that is going to do huge Layer-2 structure in recent years. As grasping the Layer-2 topology, network manager needs the informations of connection between routers, ARP, MAC-Adresse cache, VLAN and redundant network. In this paper, we propose the system to support the network manager that gathering the above informations to grasp the Lyaer-2 network topology.

1　はじめに

近年インターネットの普及に伴い，一般企業や学術機関など各種団体におけるネットワーク運用の重要性は増している．ネットワークの重要性が増すと同時に，ネットワークに対する機能要求は多くなっており，ネットワーク管理者はネットワークを巨大な Layer-2 構造にし，きめ細やかな設定を行えるようにする場合が多くなっている．このようにネットワークが巨大な Layer-2 構造になるにつれ，ネットワーク構成が複雑になってしまいネットワーク管理者がネットワークを完全に把握するするのは困難になりつつある．しかし，ネットワークの構成を把握すること，つまりネットワーク管理における構成管理は，障害管理・性能管理・セキュリティ管理全てに関連する重要な管理項目であり，ネットワーク管理者はネットワーク構成を把握する必要がある．

しかしながら，ネットワークを設計した本人がネットワーク構成を把握することは容易だが，自分で設計したネットワークだけを管理するとは限らない．また，スパニングツリープロトコル等によって冗長

化したネットワークや，ネットワーク構成を変更した場合はネットワーク構成の把握が困難になる場合がある．

そこで，本稿ではネットワーク管理者を支援するために，ネットワークの Layer-2 トポロジを検出し構成管理を支援するシステムを提案する．提案システムは，できるだけ特定ベンダーに依存しないようにするために SNMP を用いてネットワーク機器から構成情報を収集し，SNMP で収集できない情報に関してはネットワーク機器に telnet 接続を行い情報を収集するものとした．

2 章では，現存するシステムと提案システムについて述べ，3 章ではシステムを構築する際に必要となる機能について述べる．そして 4 章で提案システムに関する考察と問題点を述べる．

2　既存システムの課題と提案手法

現存のシステムでネットワークトポロジを調査するものとして，OpenView[1] のような Network Management System（以下，NMS という）があげられる．しかし，現存の NMS は一般的にネットワークトポロジを Layer-3 的にとらえている[1]．このため，スパニングツリープロトコルによって冗長化されている場合ネットワークトポロジが安定して描画されないこともあり，Layer-2 トポロジを詳しく把握するのは困難である．

したがって，提案システムでは現存のシステムより詳細に Layer-2 情報を把握することを目的とする．提案システムでは，Layer-2 のアドレスである MAC アドレスに関する情報を中心に収集することによって Layer-2 トポロジを調査する．具体的には，ネットワーク機器が使用している MAC アドレス情報，ネットワーク機器が保持している ARP 情報と MAC アドレスのキャッシュ情報，スパニングツリープロトコルによる冗長化経路の情報を収集し，Layer-2 トポロジを把握する方法をとった．上記した情報のうち，スパニングツリープロトコルに関する情報はネットワーク機器に telnet 接続して情報を取得する手法をとったが，他の情報に関しては SNMP を用いて情報を収集した．

[1]OpenView の，ネットワークノードマネージャ Advanced Edition の Extended Topology 機能を用いれば，レイヤー 2 のデバイス情報を検出してデバイス間の接続状況を表示することができると OpenView のマニュアルに表記されている．しかし，実際に OpenView を操作する環境が準備できなかったため，提案システムと同じようなことができるのかどうか判断できなかった．この件に関する調査は今後の課題とする．

3　提案システム

本章では，提案システムの実現性を確認したネットワーク環境，提案システムの機能とその実現方法について述べる．

3.1　ネットワーク環境

提案システムの実現性は，和歌山大学（以下，本学という）の学内ネットワークにおいて確認しており，本学のネットワーク環境に依存している部分がある．本節では，提案システムの各機能の実現性を確認したネットワーク環境について述べる．

ネットワークの基幹となる機器は Cisco 社製の Catalyst スイッチであり，主に同スイッチの Layer-3 モジュールを用いてルーティングを行っている．以下に本学の基幹ネットワークに設置された機器を示す．

- Catalyst 6509, 6506, 4006
- Catalyst 3524, 2950, 2940

本学のネットワークは，これらのスイッチ群を使用し VLAN を用いたネットワークを構築しており，Catalyst スイッチのみが所属している管理 VLAN セグメントが存在する．この管理 VLAN セグメントに接続してある PC 上に，提案システムを構築する．また，これら基幹部のスイッチからエンドユーザの端末が存在する部屋まで配線がされている．これらの簡易構成を図 1 に示す．

Catalyst4006 において，一部 SNMP による情報収集ができないものがあった．このことについては 4 章で詳しく述べる．

3.2　トポロジ把握

本節では，Layer-2 トポロジを把握するために必要となる情報を調査する方法について述べる．SNMP で情報を問い合わせるオブジェクト ID（以下，OID という）は全て mib-2 の情報であるため，mib-2 までの OID は省略して記す．また，今回提案するシステムは前提条件として管理 VLAN セグメントに所属しており，このセグメント内で使用する IP アドレスとデフォルトゲートウェイの情報は保持しているものとする．

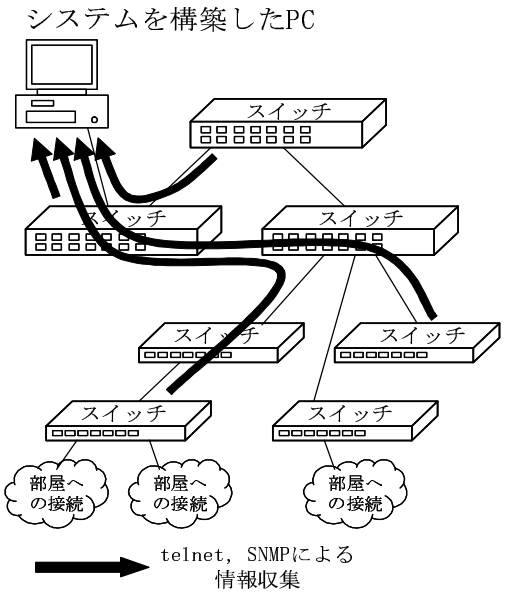

図 1: 簡易構成図

3.2.1 情報を収集する対象に関する情報

本項では，ネットワーク構成情報を収集する対象，つまり組織内ネットワークに設置されたネットワーク機器（以下，スイッチという）に設定された IP アドレス一覧を収集する方法について述べる．

SNMP を用いると，3.1 節で述べた環境において，提案システムに設定した管理 VLAN セグメントにおける IP アドレスと，管理 VLAN セグメントをルーティングしている IP アドレスの情報を保持していれば，管理セグメント内に存在する IP アドレス一覧を取得することが可能である．これら IP アドレス一覧は組織内ネットワークのコアスイッチ群の IP アドレスになっており，これらの IP アドレスから情報を収集すれば，組織内のネットワークトポロジに関する情報が収集可能である．次にこの IP アドレス一覧の取得方法について述べる．

SNMP で管理セグメントをルーティングしている IP に対し，atIfIndex（mib-2.3.1.1.1）のクエリを実行すると，返された OID の下４つの ID が IP アドレスになっている．この返された OID の中から提案システムが管理 VLAN セグメントで使用している IP アドレスを検索し，この IP アドレスに対するインタフェース番号を取得する．ここで得たインタフェース番号と同じ値を持つ IP アドレスが，管理 VLAN セグメントに存在する IP 一覧になる．

図 2 に例を示す．図中の左の枠で囲ってある部分

```
...atIfIndex3.1.1.1.42.1.192.168.1.10 = INTEGER: 42
...atIfIndex3.1.1.1.42.1.192.168.1.11 = INTEGER: 42
...atIfIndex3.1.1.1.42.1.192.168.1.12 = INTEGER: 42
```

図 2: OID 例

が IP アドレスであり，右がインタフェース番号である．

3.2.2 ARP 情報

本項では，組織内ネットワークで使用されている IP アドレスと，この IP アドレスに対応する MAC アドレスの一覧を取得する方法について述べる．

まず，ルーティングを行っているスイッチに対し SNMP で ipRouteNextHop（mib-2.4.21.1.7）のクエリを実行し，組織内ネットワークでルーティングを行っている IP アドレスを取得する．こうして得た IP アドレスに対し atPhysAddress（mib-2.3.1.1.2）のクエリを実行すると，組織内ネットワークで使われている IP アドレスと MAC アドレスの対応情報が取得できる．

3.2.3 インタフェース情報

本項では，組織内ネットワークに設置されたスイッチに存在するインタフェースと，そのインタフェースに対応する MAC アドレス情報を取得する方法について述べる．

SNMP で管理セグメント内の IP に対し ifName（mib-2.31.1.1.1.1）のクエリを実行し，OID の下１つの ID をインタフェース ID として取り出し，この ID に対するインタフェース名を取得する．ここで取得できるインタフェース名は，“FastEthernet1/3”といった物理的なインタフェースに加え，VLAN 番号，チャネルされたポートもインタフェース名として取得することができる．次に，ifPhysAddress（mib-2.2.2.1.6）のクエリを実行し，先に得たインタフェース ID より，各インタフェースに対応する MAC アドレスが取得できる．

図 3 に例を示す．図のように ifName のクエリでインタフェースが取得でき，そのインタフェースに物理アドレスが存在する場合は ifPhysAddress のクエリを実行すると同じインタフェース ID により物理アドレスを取得することができる．

```
...ifName.7 = STRING: 3/1
...ifName.130 = STRING: VLAN-55
...ifName.306 = STRING: GEC-1/1-2,2/1-2
...ifPhysAddress.7 = STRING: AA:AA:AA:AA:AA:AA
...ifPhysAddress.130 = STRING: AA:AA:AA:AA:AA:AB
...ifPhysAddress.306 = STRING: 0:0:0:0:0:0
```

図 3: OID 例

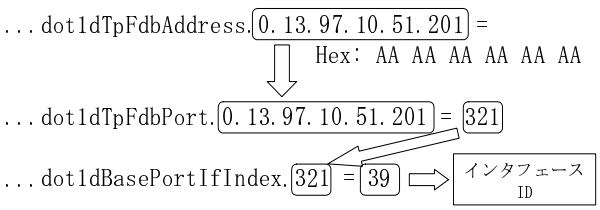

図 4: OID 例

3.2.4 MAC アドレスのキャッシュ情報

本項では，組織内ネットワークに設置された各スイッチに保存されている MAC アドレスのキャッシュ情報を取得する方法について述べる．

以下の SNMP の問い合わせは，問い合わせの際コミュニティ名に “@” と “VLAN 番号” を付け，“コミュニティ名@VLAN 番号” のようにしてクエリを実行する．これにより，スイッチに設定された VLAN 毎に情報が取得できる．

SNMP で管理セグメント内の IP に対し dot1dTpFdbAddress（mib-2.17.4.3.1.1）のクエリを実行し，スイッチの持つ MAC アドレステーブルが取得できる．次に dot1dTpFdbPort（mib-2.17.4.3.1.2）のクエリを実行し，返された OID の下６つの ID が dot1dTpFdbAddress（mib-2.17.4.3.1.1）で返された ID の下６つと対応した値が，各 MAC アドレス所属するインタフェースのブリッジ番号となっている．次に dot1dBasePortIfIndex（mib-2.17.1.4.1.2）のクエリを実行すると，下１つの ID が dot1dTpFdbPort（mib-2.17.4.3.1.2）のクエリで取得したブリッジ番号と対応しており，対応するブリッジポートのオブジェクト値が取得できる．ここで取得したオブジェクト値は，3.2.3 項で得たインタフェース ID と対応している．これにより，各スイッチに保持された MAC アドレスのキャッシュ情報がスイッチのインタフェースと対応づけて取得することができる．図 4 に，上記した情報取得の流れの例を示す．

3.2.5 ネットワーク機器同士の接続情報

本項では，管理 VLAN セグメントにおける Layer-2 のトポロジを取得する方法について述べる．3.2.1 項，3.2.3 項，3.2.4 項で得た情報を組み合わせることにより，管理 VLAN セグメントの Layer-2 トポロジを取得することができる．

Layer-2 の接続情報を調べたいスイッチの IP アドレスをそれぞれ，“A”，“B” とし，各スイッチの MAC アドレスを “a”，“b” とする．この２つのの接続情報を取得する場合，A，B の IP アドレスがお互いに通信を行っている必要がある．お互いに通信を行っている状況で，２つのスイッチが保持している MAC アドレスのキャッシュ情報をインタフェース名と対応づけて取得すると，どのインタフェースの先に a，b の MAC アドレスが存在するか判明し，接続情報を取得することができる．

次に，A，B の間に “C” という IP アドレス，“c” という MAC アドレスを持ったスイッチが存在する場合を考える．この場合は，A，B がお互いに通信を行った場合，C のスイッチには a，b 両方の MAC アドレスがキャッシュ情報として保存されるため，直接接続されていないことが分かる．このように直接接続されてないと判明した場合，C と A，C と B の接続を同じ方法で調べればよい．

このような調査を行うことにより，ネットワークの Layer-2 トポロジを取得することができる．

3.2.6 冗長化経路に関する情報

本項では，スパニングツリープロトコルによって冗長化された情報を取得するための方法について述べる．

スパニングツリープロトコルによって冗長化された経路は，SNMP による情報収集では把握することができない．これは 3.2.4 項で述べた方法により，冗長化されたポートの MAC アドレスのキャッシュ情報を得ようとしても，通信を行っていないためキャッシュ情報が存在しないためである．

したがって，スパニングツリープロトコルによる冗長化された経路を知るためには，ベンダーに依存する調査方法になってしまうが，telnet でスイッチにログインして “show spantree” や “show cdp neighbors” 等のコマンドを実行して調査する必要がある．

3.2.7　エンドユーザの使用する端末情報

3.2.2 項で述べた ARP 情報と，3.2.4 項で述べた MAC アドレスのキャッシュ情報を組み合わせることにより，組織内ネットワークで使用されている端末の Layer-2 的な位置情報が把握できる．

3.3　システムの実現性

3.2 節で述べた各機能を，CPAN に登録されたモジュール“ Net::SNMP ”,“ Net::Telnet::Cisco ”を使用して実現性を確認した．しかし，限られた環境での実現性を確認しただけであり，SNMP と telnet によってテキストデータを取得してトポロジが描画できることを確認するにとどまっている．次章以降で提案システムの問題点や今後の研究予定について述べる．

4　システムの考察と課題

提案システムでは，本学のネットワーク環境下で Layer-2 トポロジを把握するための情報が取得できることを確認した．しかし，完全な Layer-2 トポロジを把握するには機能的に不十分であり，他のネットワーク環境でシステムを構築する場合は考慮すべき点が存在する．これらの考慮する必要があると思われる点を箇条書きにし，それに対する考察を述べる．

Catalyst4006

3.1 節で述べたように，Catalyst 4006 のスイッチからは SNMP による情報取得が一部不可能であった．この Catalyst スイッチの詳細を以下に記す．
WS-C4006 Software, Version NmpSW: 6.1(2)
Hardware Version: 1.4 Model: WS-C4006

取得できなかったのは 3.2.4 項で使用した dot1dTpFdbPort（mib-2.17.4.3.1.2）と dot1dBasePortIfIndex（mib-2.17.1.4.1.2）の情報である．これは，MIB-2 の 1〜11 のグループが 1991 年 3 月に RFC1213[2] で定義されたのに対し，一般的に Bridge MIB と呼ばれている dot1dBridge（mib-2.17）グループは 1993 年 7 月に RFC1493[3] で定義されたため，古いネットワーク機器の場合対応できていないと考えられる．

情報を収集する対象

今回提案したシステムでは，管理対象となるスイッチだけが所属する管理 VLAN セグメントが存在したために，自動で調査対象の IP アドレス一覧を取得することができた．しかし，このような管理 VLAN セグメントが存在しないネットワークの場合，調査対象となるネットワーク基幹部のスイッチに最初から設定された IP アドレスをシステムに与えておく必要がある．

冗長化経路

今回提案したシステムでは，SNMP によって冗長化経路に関する情報は取得することができなかった．したがって，冗長化経路に関する情報は telnet 接続を行いコマンドを実行する方法をとり，提案システムはベンダーに依存する形になってしまった．本学のネットワーク環境では Cisco Systems 社製の Catalyst スイッチだけであったが，今後は他のベンダーのスイッチも調査可能にしていきたい．

冗長化経路に関する情報は取得することができないと述べたが，スパニングツリープロトコルによる冗長化は VLAN 毎に設定を変更し，経路を変更することが可能である．したがって，冗長化している経路も，スパニングツリープロトコルのコスト値を変更して一部の VLAN だけでも通信が行われるようにすれば Layer-2 のトポロジを把握することが可能である．本学のネットワーク環境でも，このようなネットワーク構成になっている部分が存在する．この場合，通信経路上のスイッチの Layer-2 的な配線情報までは取得することができない．

ポートのチャネル

3.2.3 項で得たインタフェース名は，チャネル化されているポートの場合 “GEC-1/1-2,2/1-2” のような文字列として情報を取得することができた．この場合，接続先の 4 つのポート同士の Layer-2 トポロジは把握可能であるが，1 つ 1 つのポートがどのように配線されているかは判断することができなかった．この問題は今後も解決することができないと考える．

スイッチ同士の通信

3.2.5 項で述べた方法は，接続を確認する 2 つのスイッチがお互いに通信を行っている必要がある．今回は 2 つのスイッチに telnet ログインし，Ping を送り合うという方法をとり通信を行った．この方法

は，telnet ログインできないネットワーク機器の場合実行できないのでお互いのポート同士の接続は確認できない．

トポロジの描画

今回提案したシステムは，収集したテキストデータを表示する機能しか備えていない．ネットワークトポロジを把握するためには，テキストデータでの表示だけでなくトポロジの描画も必要だと考える．したがって，今後は提案システムの完成度を上げると同時にトポロジを描画する機能も追加したいと考えている．

5 おわりに

本稿では，ネットワークを Layer-2 的に調査する手法について述べた．全ての環境において完全な Lyaer-2 のトポロジが描画できる情報を取得することはできなかったが，ネットワークを管理する上では有用な情報を取得することができた．今後は，様々なネットワーク環境において同様な機能が実現できるようにしていくとともに，3.2 節で述べた情報を収集する各手法を効率よく実行し情報を収集するシステムを完成させる．また，トポロジを描画する機能を実装すると共に，ネットワークのトポロジ管理とネットワーク上の MAC アドレスを総合的に管理するシステムにしていく予定である．

2 章の脚注で述べた OpenView の，ネットワークノードマネージャAdvanced Edition の Extended Topology 機能に付いての調査も行っていく予定である．

参考文献

[1] Openview, Hewlett-Packard Company http://h20229.www2.hp.com/

[2] K. McCloghrie, M. Rose,:Management Information Base for Network Management of TCP/IP-based internets:MIB-II, RFC1213 (1991).

[3] E. Decker, P. Langille, A. Rijsinghani, K. McCloghrie,:Definitions of Managed Objects for Bridges, RFC1493 (1993).