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

2005－DSM－38（10）
2005／8／5

SNMPによるMACアドレス探索とレイヤ2通過ノード特定ツール

鈴木　聡[†]　湯浅　富久子[†]

ワーム感染対処やレイヤ 2 での通信障害切り分けには当該機器の接続口や経由スイッチを特定することが有効だが、VLAN 多重化とレイヤ 2 スイッチ冗長構成によりループが多数存在する状況では手動の探索は難しい。当機構では MAC アドレス識別によるダイナミック VLAN 環境を運用しており、機器の接続先は変動しうる。SNMP によってブリッジテーブルと隣接スイッチ情報を動的に取得し、レイヤ 2 での経路を探索するツールを作成した。

MAC address finder and layer2 switch tracer by SNMP

Soh Y. Suzuki[†] and Fukuko Yuasa[†]

The detection of physical network port is effective to solve problems such as virus infection or poor thuroughput. Since last year, we started the dynamic VLAN management at the KEK LAN. The dynamic VLAN makes anybody can use any physical network port regardlessly what VLAN is assigned to the port. This makes we can't predict the actual location of the machine. We developed "MAC address finder and layer2 switch tracer" using SNMP query and it shorten the detection time of network port. This paper presents how this finder tool detects the port location and the layer2 path.

1. 動　機

本機構は大学共同利用研究所であるため、職員以外にも大学や他の研究機関からの利用者が数日から数年にわたって滞在し、持ち込み PC 等を通じてネットワークを利用する。居室の存在する建物と実験場が離れているが、実験に関わるネットワーク機器が意図的にサブネット越えを禁止している等の制約があり、居室まで実験場のサブネットが延長されている。

多数の実験グループとサブネットが存在しているため、IP アドレスだけでは端末の場所は特定できない。これまでは新規接続申請時に必ず機器設置場所も記載させていたが、ノート PC が一般化するに至って申請時の場所と現在接続されている場所の不整合が多発していた。

これに加えて当機構では昨年よりダイナミック VLAN の運用を開始した。これはスイッチのポートに最初に到着したパケットの MAC アドレスを元にそのポートが属するべきサブネットを判断し VLAN 番号を変更するものである。これによってどのポートにどの端末を接続しても適切なサブネットが割当てられる。これを適用すると事前に MAC アドレスと VLAN 番号の対応を登録していない端末はどのネットワークにも参加することができず、通信不可能となるのでセキュリティの向上も図れる。

会議室や不定期にユーザーが入れ替わる共同利用者用の居室等で、いったん登録した利用者が再来した場合接続場所を意識することなく空いているポートを見つけたらそこに接続することができる。その代り、IP アドレスを特定しても機器がどこに接続されているか特定できない。

この状態で利用者の持ち込んだ機器がワーム等に感染すると場所の特定に時間がかかるため感染が拡大し、対処の負荷が増大する。本機構 LAN では各サブネットの大きさは/24〜/20 であり、大学で利用されるサブネットにくらべてかなり広いものがある。これは建物と関係なく研究組織単位でサブネットを割当てていること、サブネット越え禁止の機械が多くあること、共同利用者の数が多いこと、組織を細分化していないこと、等の理由による。機構外からの攻撃はファイヤーウォールで遮断しているものの、いったん感染した PC を内部 LAN に持ち込まれると感染が拡大しやすい。WindowsPC にはウイルス対策ソフトのインストールを義務づけているが、感染の拡大を防ぐためウイルスの活動を検知した場合は迅速に該当機器をネットワークから切り放すことが求められている。

また、セキュリティ上の問題とは別にユーザー機器同士の通信が 10Mbps 以下の速度しか出せず苦情が上がってくることがある。ほとんどの場合 100M イーサ

† 高エネルギー加速器研究機構
High Energy Accelerator Research Organization

ネットのネゴシエーションが失敗し半二重になっていることが原因であるので、ユーザー機器の接続されているポートの状態を確認し、全二重固定にすることで解決する。稀に排熱障害等によりスイッチの上流ポートの通信品質が低下している場合もある。さらに不定期にエラー率が変動して一見他のトラフィックに影響されていると誤認しやすい症状も発生したことがある。この切り分けには同一スイッチ配下の機器すべてが遅いかどうかを検定すればよいが、多段接続されている場合に経路を特定することは手作業では繁雑である。

本研究はこの対処、すなわち物理接続ポートとレイヤ 2 での経路を特定する時間を短縮するためのものである。

2. 機構内 LAN の特徴

本機構のネットワークはレイヤ 2 ではコアスイッチとエッジスイッチの 2 種に大別され、ユーザー機器はエッジスイッチに直接接続することを推奨している (図 1)。あらゆるエッジスイッチからすべてのサブネットに参加できる。前述のダイナミック VLAN を有効に機能させるため、エッジスイッチのポート数が足りない場合でもユーザーが自前でスイッチを用いて接続することは推奨しておらず、センターの管理するスイッチ (s ハブと呼ばれる) を用いてポート数を補充している。コアスイッチ同士は 10G、コアスイッチとエッジスイッチは 1G、エッジスイッチと s ハブは 1G か 100M のイーサネットで接続されている。

レイヤ 3 ではネットワークは 2 段階の構造になっており、サブネットのルーティングはコアスイッチ以外では許可していない。

物理層の障害対策の為、すべてのエッジスイッチは 2 つの経路を通ってコアスイッチに到達可能である。あらゆる建物について必ず 2 つのコアスイッチに到達するファイバーを敷設してある。構造上、レイヤ 2 でのループが多数存在するがこれらのスイッチはスパニングツリーで協調しているので正常時にはループガードによって一部の接続がブロックされている。ブロック機能を用いてループ問題を回避しているため、ホップ数では最短経路に見える経路が選択されているとは限らない。

機構内のエッジスイッチはすべて前述のダイナミック VLAN に対応しており、CISCO 社の VMPS (VLAN Management Policy Server) を使用して一元管理されている。現在のところ VMPS に対応しているスイッチは CISCO 社製品しかないため、センターが管理するスイッチはほとんど同社の製品となっている。当センターでは要望に応じてエッジスイッチを増強しているため同社の製品であっても時期により機種および OS が異なる。現在使用されている主な機種は以下のものであり、エッジスイッチは能力も OS も様々である。

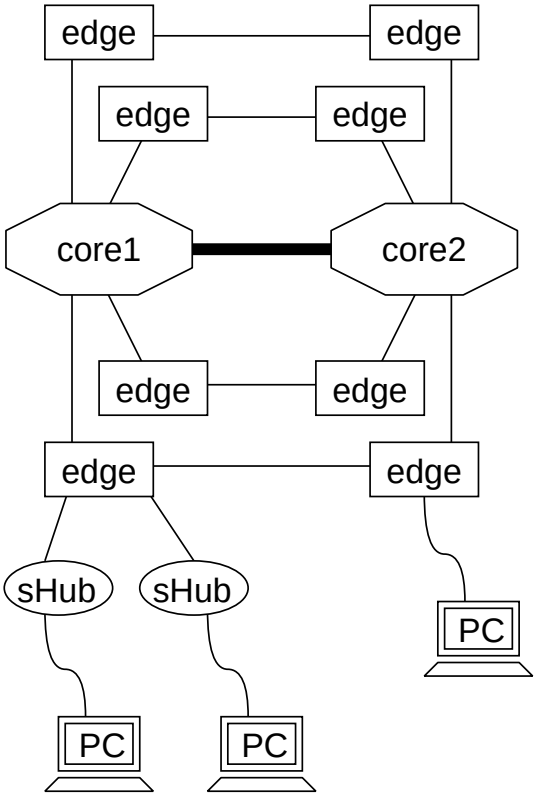

図 1 コアスイッチとエッジスイッチの接続形態

- コアスイッチ
  - Catalyst 6513 Supervisor 720 IOS 12.2(17d)
- エッジスイッチ
  - Catalyst 2948 CatalystOS 7.6(7)
  - Catalyst 3508 IOS 12.0(5)
  - Catalyst 3550 IOS 12.1(6)
  - Catalyst 2970 IOS 12.2(25)

問題の切り分け中に予備のエッジスイッチと交換したり、能力の高い機種と交換・回収したエッジスイッチを s ハブとして使用するなどして配置替えすることがある。そのため、“正しいトポロジー” を定義してそれに基づく調査をすることは難しい。

そこで CDP (CISCO Discovery Protocol) を用いて自動的にトポロジー情報を構築する。CISCO 社のスイッチは CDP を用いて名前・IP アドレス・デバイス情報等を含むパケットをネットワークに定期的に送出することができる。この機能を有効にしておくと、隣接する CISCO 製品を検出することができる。このパケットはイーサネットマルチキャストであり、通常のスイッチやルータを横断しない。したがってこの CDP の情報からレイヤ 2 でのトポロジーを把握することができ、ブリッジテーブルの情報と組合せることによっ

てレイヤ 2 での経路を特定することができる。

以上をふまえて特定の機器がどのエッジスイッチに接続されているか、またそのエッジスイッチに到達する際のレイヤ 2 的経路を特定するツールを作成した。

3. 実　　装

本ツールは Perl の CGI として実装されており、使用者は WWW 経由で調査を行なう。使用する Perl モジュールは CGI, Net::Ping, Net::SNMP, Net::Telnet::Cisco である。いずれも CPAN から取得できる。すべてのスイッチは操作用の VLAN にのみ IP アドレスをもっており、安全のため他の VLAN とはルーティングされていない。通常の SNMP ツールを使用する場合は操作用 VLAN に接続しなくてはいけないが、このツールを経由していればその必要はない。使用者が指定する項目は

- 経路探索開始スイッチ
- 宛先ノード (IP もしくは MAC アドレス)

の 2 つである。

3.1 機器接続ポートの取得

まず宛先ノードとして IP アドレスが指定された場合はこれに対応する MAC アドレスを取得する必要がある。機構内の VLAN はすべてコアスイッチでルーティングされているため、コアスイッチの ARP テーブルを調査すれば MAC アドレスが取得できるはずである。ARP テーブルの取得には

```
.1.3.6.1.2.1.4.22.1.2
            IP-MIB::ipNetToMediaPhysAddress
```

を使用する。この OID 配下には ARP テーブルが

```
.1.3.6.1.2.1.4.22.1.2.A.B.C.D.E
                        = aa:bb:cc:dd:ee:ff
```

の様な形で格納されており、`A` がインターフェース番号、`B` ～ `E` が IP アドレスに対応している。機構内のルーティングはすべてコアスイッチで行なわれているので、ARP テーブルは巨大であり、直接配下を走査すると時間がかかる。そこで `IF-MIB::ifIndex` (`.1.3.6.1.2.1.2.2.1.1`) によってあらかじめインターフェース一覧を取得し使用者が指定した `B` ～ `E` とあわせて OID を合成した後、複数まとめて GETBULK リクエストを発行する。

ただし、エッジスイッチ同士で完結するような通信しか行なっていない端末はコアスイッチにフレームが到着しないため、情報が現れない。そのため IP アドレスが指定されている場合は CGI から ping コマンドを使用して ICMP echo request を送出する。

MAC アドレスを取得後、ブリッジテーブルを取得し該当する MAC アドレスが記録されているか検索する。ブリッジテーブルの取得には SNMP を使用する。既に MATT[1] で述べられているように CISCO 社のスイッチでは VLAN 毎にブリッジテーブルが独立しているので VLAN テーブルを取得し、しかる後各 VLAN についてブリッジテーブルを取得する。機構内 LAN においてはブリッジテーブルは ARP テーブルよりさらに大きいためスイッチの CPU への負荷が無視できない。目的の機器が複数の VLAN に接続している場合、最初に発見された VLAN で調査を終了する。

CISCO の機種・OS によっては SNMP では VLAN 毎のブリッジテーブルが取得できない。最初に機種情報を調査しておき、SNMP が有効でない場合は CGI が telnet 経由で login し CUI のコマンドを用いてブリッジテーブル一覧を取得する。

このブリッジテーブル情報から指定された MAC アドレスがどのポートにフォワードされるかを特定できる。手順は MATT と同様で、`BRIDGE-MIB::dot1dTpFdbPort` と `BRIDGE-MIB::dot1dBasePortIfIndex` を取得してポート番号とインターフェース番号を特定する。

インターフェースが特定できたら CDP テーブルを取得して次ホップを特定する。CDP テーブルについては SNMP の

```
.1.3.6.1.4.1.9.9.23.1.2.1.1.4
             CISCO-CDP-MIB::cdpCacheAddress
.1.3.6.1.4.1.9.9.23.1.2.1.1.6
            CISCO-CDP-MIB::cdpCacheDeviceId
```

の 2 つの配下を走査する。cdpCacheAddress には IP アドレスが、cdpCacheDeviceId には機器本体に設定する名前文字列が格納されている。この IP アドレスが操作用 VLAN のものになっていればセンター管理の機器として識別できる。

それぞれの配下の OID は

```
.1.3.6.1.4.1.9.9.23.1.2.1.1.4.x.y
```

の様に 2 つの数字がつく。上位 (`x`) によって接続されているインターフェースが識別できる。`x` はブリッジテーブルに使用されるポート番号ではなくインターフェース番号である。

機構内 LAN の構造上、たかだか 3 回この操作を繰り返せばセンターの運用するスイッチの終端にたどりつくことが保障される。得られたポートには CDP の隣接ノードが存在しないか、もしくはセンター管理のものでない場合そこで探索を終了する。実際に探索が終了した時点の様子を図 2 に示す。

終端に到達したとき、ブリッジテーブルの該当ポートに複数の MAC アドレスが存在していた場合、使用者が自前の廉価なミニスイッチを接続していることが推測される。何らかの問題が発生して該当ポート配下の機器をネットワークから遮断する事態になった時、

図 2 探索結果の表示

同じミニスイッチ配下の機器は巻き添えになる。事前に巻き添えになる機器を把握しておく必要があるため、複数の MAC アドレスが観測された場合はそれも表示する。

3.2 可 視 化

取得された経路だけではもっともらしい経路が選択されているかどうかは判断しにくいため、迂回路も含めて経路を可視化する。

迂回路は経路上に現れる各エッジスイッチから CDP を用いて隣接スイッチを探索することによって検出する。コアスイッチに到達したらその枝については探索を終了する。エッジスイッチはたかだか 3hop でコアスイッチに到達するため、この探索はさほど時間を要しない。レイヤ 2 の経路に現れるスイッチすべてを含むトポロジーが作成できたら GraphViz[2] を用いて可視化する (図 3)。

すでに述べたように物理障害によって不通になっていない限り、必ず迂回路が存在する。また、スパニングツリーによってブロックされている物理経路であっても CDP による情報交換は行なわれているため、物理障害によって切断されているかどうかが迂回路の有無から判断できる。

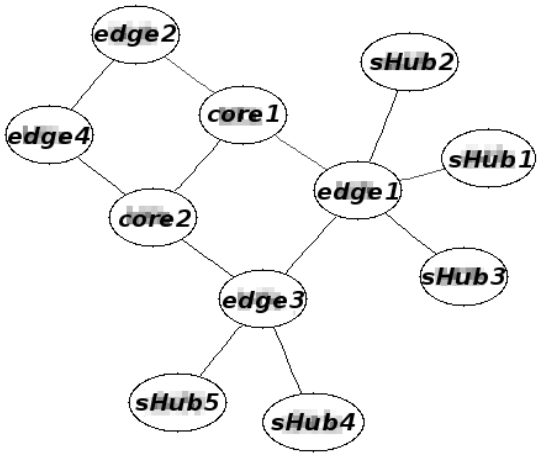

図 3 GraphViz による隣接スイッチのトポロジー表示

4. ま と め

CDP を用いてスイッチのレイヤ 2 トポロジーを自動的に検出し、任意の MAC アドレスの接続ポートとレイヤ 2 での経路を特定する CGI を作成した。MAC アドレスを指定した場合、エッジスイッチに対する query はほぼ 1 秒程度であるがコアスイッチに対する query は VLAN 数が多いためか、2〜3 秒程度の時間がかかる。また、ARP テーブルの探索も同様の時間がかかるため 1 機器の経路を特定するのにだいたい 5〜6 秒の所要時間であった。これまでの telnet で隣接スイッチを渡り歩く作業と比較すると、間違いもなくなり作業時間も大幅に短縮されたと言える。

機構内 LAN の一部では実験データの大量転送が行なわれているが、導入時に 10G イーサネットが間に合わなかった個所では複数の GbE を束ねて一つの仮想インターフェースとして使用している。この仮想インターフェースに限ってはポート番号とインターフェース番号の対応が SNMP からは見えず、現在は対応できていない。また、VMPS サーバと連携して事前に VLAN 番号を取得することができればコアスイッチに対する query を減らすことができるので今後の課題である。

参 考 文 献

1) 續木涼太, 泉裕, 齋藤彰一, 塚田晃司: 組織内ネットワークにおける MAC アドレストレースバックシステムの開発, 電子情報通信学会 研究報告 2005-DSM-36, pp. 13-18 (2005)
2) http://www.graphviz.org/