

ネットワーク構成把握技術の開発

A new technology for visualizing network topologies

太田 貴彦
Takahiko Ohta

神宮 武志
Takeshi Shingu

キーワード

SNMP, MAC アドレステーブル, RSTP, ネットワーク構成, ネットワーク冗長化

システム機器のマルチベンダー化に伴い大規模化・複雑化が進むネットワークシステムに対して、ネットワーク構成を自動把握する技術を開発し、可視化するシステム監視アプリケーションを試作した。本技術はSNMP対応スイッチングハブ（以下、スイッチ）内の情報を解析することにより、ローカルネットワーク内の機器を階層構造で把握することを実現する。本技術により、ネットワークシステムの構築時や運用時においてネットワーク構成把握の確認作業コストを大幅に削減する。

In response to the growth in size and complexity of network systems that accompanies the multi-vendorization of system equipment, we have developed a technology for automatically detecting the configuration of networks, and we have experimentally produced a system-monitoring application that visualizes the configuration. By analyzing the information in an SNMP-compatible switching hub, this technology is able to detect the local network devices in their hierarchical structure. This technology significantly reduces the time and cost required to check the configuration of a network when constructing or operating a network system.

1. はじめに

近年、IoTやクラウドサービスの普及に伴い、ネットワークに接続する機器が増え、ネットワークの大規模化・複雑化が進んでいる。また、新型コロナウイルス感染症（COVID-19）の拡大に伴い、企業では在宅勤務の推進など働き方改革の関心が高まり、人手不足が課題となっている。

多くの組織や企業は、自身のビルや建物内にネットワークを利用しているが、ネットワークの構築や運用、保守において人の手作業が必要なことが課題となっている。ネットワークの新規構築においては、ネットワークが設計図どおりに構成されているか目視や手作業による確認が必要であり、増改築時においては、ネットワークの構成変更が行われた際に設計図の更新が必要となる。また、障害が発生した際には、原因特定のため設計図を参照し目視や手作業による確認作業が必要となるが、設計図の更新がされていないこともあり、さらに確認作業の時間を要することが課題となっている。

以上の課題や背景から、ネットワーク構成を自動で把握する技術を開発し、本技術を利用したシステム監視アプリケーションを試作した。

2. ネットワーク監視における課題

従来のネットワーク構成の自動把握技術においては、IPv4ネットワークの場合、ネットワークアドレスの範囲内のすべてのアドレスに対してアクセスを試みる手法により、システム内のネットワークに接続している機器を列挙するのにとどまっているのが一般的である。例えば、192.168.1.1～192.168.1.254のネットワークセグメントであれば、ARP（Address Resolution Protocol）リクエスト^{注1}を254回送信することにより接続している機器を把握する。しかし、実際に構築したネットワークが設計図どおり正しいかどうか確認するためには、スイッチの階層構造を含め把握する必要がある。そのため、従来の技術では設計図どおりネットワークが構築されているか正確に確認するには不十分であり、規模が大きくなるほど人の目視や手作業による確認作業にコストを要している。

また、近年では、STP（Spanning Tree Protocol）などによる冗長化ネットワークが適用されているシステムも多く、そのようなネットワーク構成において、冗長化構成情報についても正しく構築されているか確認する必要がある。しかし現状では冗長化ラインであるブロッキングポートは容易に把握できるが、ブロッキングポートの接続先については自動把握する技術がないため、人の目視や手作業により接続状態を把握する必要があり、確認作業にコストを要している。

注1 ARPはIPアドレスからMACアドレスを取得するプロトコルであり、ネットワーク上の機器の有無を確認するために使用する。

3. ネットワーク構成把握技術

本章では、ローカルネットワーク内の複数のスイッチの構成を自動把握する技術を説明する。各スイッチがどのスイッチの何番ポートに接続されているか把握することにより、ネットワーク全体の物理的な接続情報を可視化することができる。

このネットワーク構成の自動把握は、SNMP (Simple Network Management Protocol) によってネットワーク上に存在する全スイッチのMACアドレステーブル^{注2}を取得、解析することによって実現する。なお、本技術は、ネットワーク上の全スイッチがSNMP対応かつMACアドレステーブルの取得が可能であることを前提とする。

3.1 SNMP (Simple Network Management Protocol)

SNMPは、IPネットワークに接続された機器を管理するためのプロトコルである。管理対象は、スイッチやルータ、サーバ、パソコン、セキュリティ機器やネットワークプリンタなど多岐にわたり、管理対象から、インターフェース、ARPテーブル、MACアドレステーブル、ポートステータスなど様々な情報を取得できる。管理情報はMIB (Management Information Base) として標準化されている。

3.2 MACアドレステーブル

MACアドレステーブルは自身の物理ポートと接続先機器のMACアドレスの対応表であり、各スイッチがそれぞれ保持している。MACアドレステーブルの情報は、スイッチを通じた通信が行われる際に自動で学習し、スイッチが効率良く通信を行うために利用される。なお、一定時間通信が行われない場合、自動で消去される。

3.3 ネットワーク構成把握

本技術は主に次の2ステップで構成される。

- (1) MACアドレステーブルへの学習
- (2) MACアドレステーブルの解析

3.3.1 MACアドレステーブルへの学習

各スイッチのMACアドレステーブルに、他の全スイッチの情報を学習させる。各スイッチにブロードキャストメッセージを送信させ、他の各スイッチのMACアドレステーブルに自身のスイッチMACアドレスを記憶させる必要がある。そのためには、ネットワーク上に存在しないダミーのIPアドレスを送信元に設定したpingを利用する。pingを受信したスイッチは送信元へ返答を行おうとするが、ネットワーク上に存在しないIPアドレスは自身のARPテーブルに登録されていないため、MACアドレスを取得するためにARPリクエストをブロードキャストする。例えば、図1のようなネットワーク構成において、MACアドレステーブルが空の状態、スイッチCに対して、ネットワーク上に存在しないダミーのIPアドレスを送信元に設定したpingを送信すると、各スイッチのMACアドレステーブルは図2のようになる。なお、図2ではMACアドレステーブルのうち、スイッチに関する情報のみ抽出している。このように、全スイッチに対して

ネットワーク上に存在しないダミーのIPアドレスを送信元に設定したpingを送信することで、ネットワーク上の全スイッチ同士が通信することとなり、各スイッチのMACアドレステーブルに、他の全スイッチの情報が学習された状態となる。そのMACアドレステーブルを図3に示す。図3ではMACアドレステーブルのうち、スイッチに関する情報のみ抽出している。

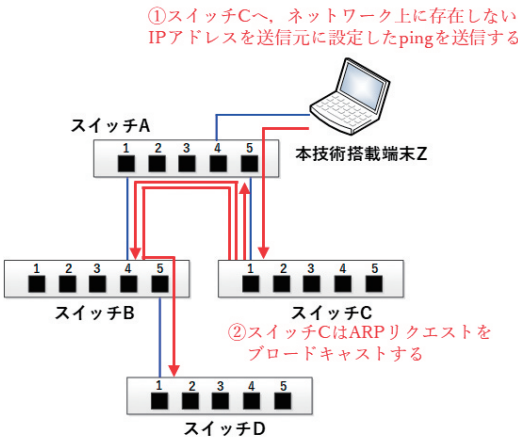


図1 存在しないIPアドレスを利用したping

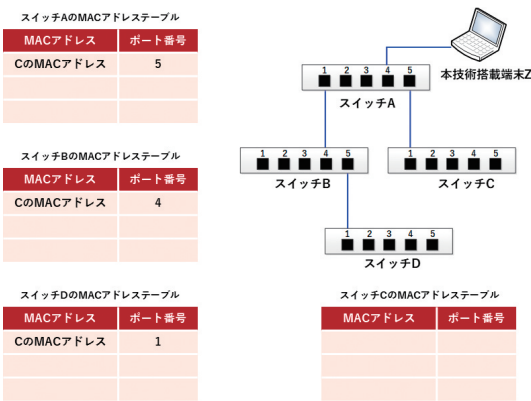


図2 MACアドレステーブルへの学習例

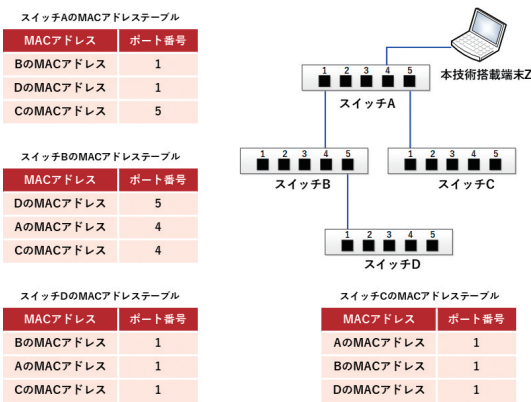


図3 MACアドレステーブルへの学習結果

3.3.2 MACアドレステーブルの解析

3.3.1で学習させたMACアドレステーブル情報をネットワーク上の全スイッチから収集し、解析を行う。MACアドレ

注2 MACアドレスはネットワーク機器固有の識別番号であり、ローカルネットワーク内の機器同士が通信するために使用する。MACアドレステーブルに関しては3.2に記述する。

ステابل情報からネットワークの末端となるスイッチを判定し、その上位に接続しているスイッチの探索を繰り返すことにより、ネットワーク構成を把握する。

はじめに、ネットワークの末端にあるスイッチを探索する。各スイッチのMACアドレステーブルを参照し、図4の赤枠のような任意の1つのポートに自身以外の全スイッチのMACアドレスが登録されているものを、ネットワーク末端のスイッチと判定する。図4ではMACアドレステーブルのうち、スイッチに関する情報のみ抽出している。

次に、この末端のスイッチと直接接続している上位のスイッチを探索する。各スイッチのMACアドレステーブルを参照し、任意の1つのポートに末端のスイッチのMACアドレスのみが登録されているものを、直接接続していると判定する。接続が確定したスイッチの情報を、各スイッチのMACアドレステーブル情報から削除し、前述の上位スイッチの探索を繰り返すことで、ネットワーク構成を把握することができる。

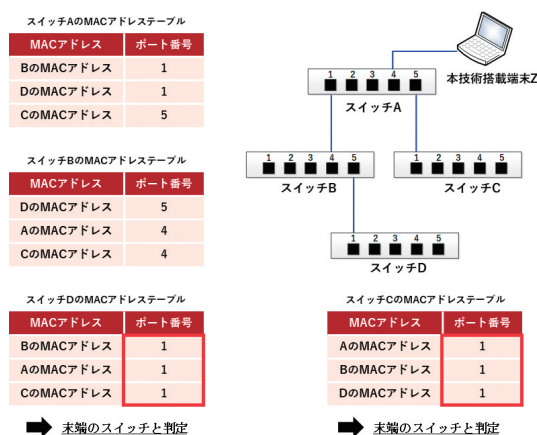


図4 末端のスイッチの判定

4. ネットワーク冗長化構成把握技術

本章では、冗長化が構成されたネットワークにおいて、STP(Spanning Tree Protocol)などの冗長化プロトコルにより、ブロッキング(Blocking)状態となったポートの物理的な接続先ポートを自動把握する技術を説明する。

このブロッキングポートの接続先ポート自動把握は、各スイッチのポートステータス情報とMACアドレステーブルを解析することによって実現する。なお、本技術は、3章と同様に、ネットワーク上の全スイッチがSNMP対応かつMACアドレステーブルの取得が可能であること、および冗長化構成が1つであることを前提とする。

4.1 STP (Spanning Tree Protocol)

STPはネットワークにおいて、冗長化構成を可能とするプロトコルである。冗長化とは、障害発生時の迂回路として、ネットワーク上に複数の経路を物理的に設けることである。しかし、ネットワーク上にループ状の経路がある場合、ブロードキャストストームによるネットワーク停止を招くため、そのままでは使用できない。そこでSTPを用いることで、ループの一部のポートをブロッキング状態とし論理的に切

断することで、ループを防ぎ、障害発生時に一部の経路が不通になった際には、ブロッキング状態だったポートをフォワーディング(Forwarding)状態として通信可能にすることで、新たな経路に切り替えることができる。STPはIEEE 802.1Dで規格化されており、複数の異なるベンダー機器で構成されているネットワークにおいても適用可能である。また、高速化・高機能化されたRSTP(Rapid STP)やMSTP(Multiple STP)もそれぞれIEEE 802.1w, 802.1sで規格化されており、現在は一般的にRSTPが使用されている。

4.2 ネットワーク冗長化構成把握

本技術は主に次の2ステップで構成される。

- (1) MACアドレステーブルへの学習
- (2) ブロッキングポートおよび接続先の探索

4.2.1 MACアドレステーブルへの学習

各スイッチのMACアドレステーブルに、他の全スイッチおよび全機器の情報を学習させる。4.2.2にて後述するブロッキングポートおよび接続先の探索において、各スイッチの全ポートのステータス情報と接続している機器を参照する必要があるため、スイッチと機器の情報をMACアドレステーブルに学習させる必要がある。スイッチの学習は3.3.1と同様に、ネットワーク上に存在しないダミーのIPアドレスを送信元に設定したpingを利用して行う。機器の学習は、IPv4機器に対してはARP、IPv6機器に対してはMLD(Multicast Listener Discovery)を利用した機器検索⁽¹⁾を行い、各機器からの返信により、MACアドレステーブルへの学習を行う。

4.2.2 ブロッキングポートおよび接続先の探索

ネットワーク上の全スイッチから全ポートのステータス情報を収集する。はじめにブロッキングポートを探索する。収集した全ポートのステータスを見ると、ブロッキング状態となったポートが1つ見つかり、それ以外のポートはフォワーディングとなっていることがわかる。なお、接続されていないポートは「ディセーブル(Disable)」となる。図5に冗長化ネットワークの構成例と各ポートのステータスを示す。STPによりスイッチDの5番ポートがブロッキング状態となり、スイッチC-D間の接続が論理的に切断された状態となる。

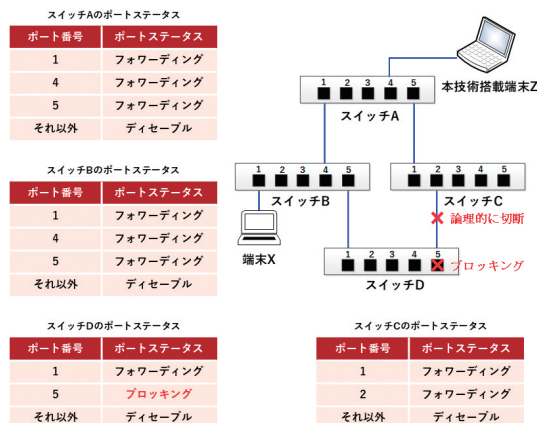


図5 冗長化ネットワークにおけるポートステータス

次に、MACアドレステーブル情報をネットワーク上の全スイッチから収集し、ブロッキングポートの接続先を探索する。各スイッチのMACアドレステーブル情報を参照し、「フォワーディング状態かつ対応するMACアドレスが登録されていないポート」をブロッキングポートの接続先ポートと判定する。これは、ブロッキングポートの接続先ポートは物理的なケーブルが接続されておりフォワーディング状態となるが、接続先のポートはブロッキング状態で、この両ポート間は論理的に切断された状態となり、実際にはデータ通信が行われないからである。図6に図5と同じ冗長化ネットワークにおける各スイッチのMACアドレステーブルを示す。スイッチCの2番ポートのみが「フォワーディング状態かつ対応するMACアドレスが登録されていないポート」に該当し、ブロッキングポート（スイッチDの5番ポート）の接続先であると判定する。

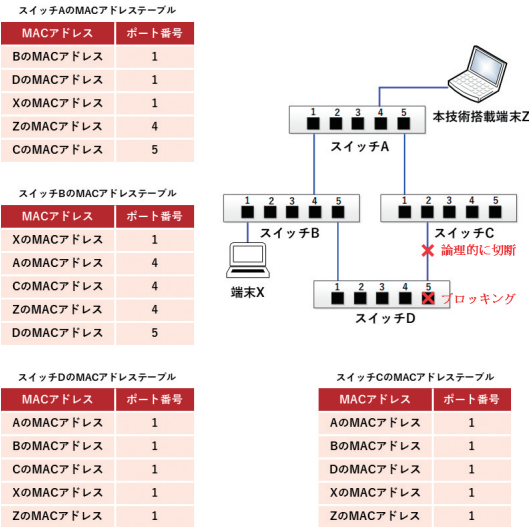


図6 冗長化ネットワークにおけるMACアドレステーブル

5. 成果

SNMP対応スイッチ内の情報を解析することによりローカルネットワーク内の機器を階層構造で把握できる技術の開発およびネットワーク冗長化の構成を把握できる技術の開発を開発した。また、それを利用したシステム監視アプリケーションの試作を行うことで、ネットワークシステムの新規構築時・増改築時において、従来図面を参照しながら目視や手作業で確認していたネットワーク構成の確認作業コストを大幅^{注3}に減らすことおよび、運用時において、障害が発生した際に、障害箇所を早期に特定できることを検証可能とした。

- システム監視アプリケーションの実装機能を以下に示す。
- (1) スwitchの多段構成の把握機能
- ローカルネットワーク内のスイッチの階層構造を自動把握しツリー形式で表現することで、ネットワーク全体の構成を把握可能となった。

注3 クラスCで254台を想定した環境においては、これまで数日を要したが、1分以内に把握可能。

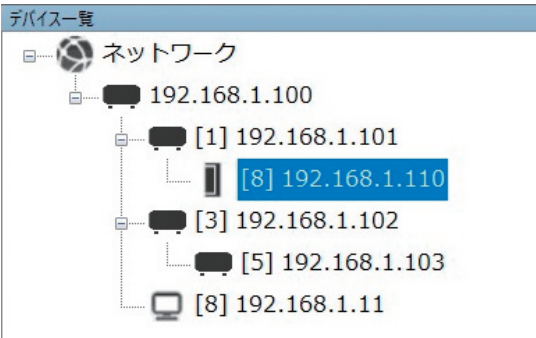


図7 把握したネットワーク構成のツリー表現

図8はシステム監視アプリケーションが障害を検知した際の表示例である。新規構築時や運用開始時など正常な状態でネットワーク全体を探索し、ネットワーク内に存在する機器のアドレス情報をホワイトリストとして保持しておく。運用時にネットワーク内のパケットを監視し、パケットの送信元アドレス情報をもとに、ホワイトリストに存在しない機器を見つけた場合、その機器を未許可機器として上部に警告を表示し、左部の赤枠のように障害が発生した場所をすぐに把握可能である。

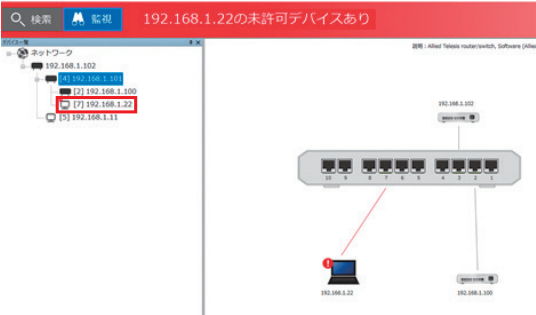


図8 障害箇所の特定

(2) ネットワーク冗長化構成把握機能

冗長化のネットワーク構成において、図9に示すようにルートブリッジ、ブロッキングポートおよび接続先ポートが把握可能となった。

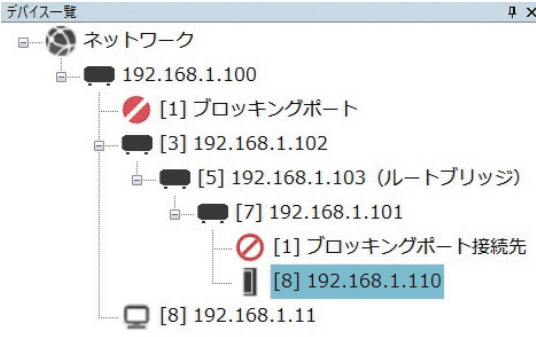


図9 冗長化構成情報の把握

6. おわりに

ネットワーク内の機器を階層構造で把握する技術を説明した。

今後の課題は、汎用的に適用可能なネットワーク構成把

握技術の開発である。この背景は、今後5Gを活用したネットワークや機器が普及し、さらにネットワークの大規模化・複雑化が考えられるからである。本稿で説明した技術は、ネットワーク内の全スイッチがMACアドレステーブルの取得に対応していることを前提とし、有線で接続されている機器の構成把握のみを行っているが、今後はスイッチの種類や接続機器の有線・無線を問わず、どのようなネットワーク構成であっても適用可能とすることを目標とする。

<参考文献>

- (1) 佐々木太一, 太田貴彦, 佐内大司, IPv6におけるノードの発見とプロミスキュスモードの検出, azbil Technical Review, 2020年4月, pp.15-18

<著者所属>

太田 貴彦	アズビル株式会社 ビルシステムカンパニー開発本部開発2部
神宮 武志	アズビル株式会社 ビルシステムカンパニー開発本部開発2部