Vol.2022-OS-157 No.2
Vol.2022-IOT-59 No.2
2022/9/13

接続端末把握のためのネットワークテレメトリにおけるネットワーク機器からの情報収集に関する一考察

大森 幹之[1,a)]

概要：コンピュータネットワークにおいて，障害やセキュリティインシデントを迅速に検知し，対応するために，接続端末を把握することは重要である．接続端末の把握のためにはネットワーク機器からの情報収集が必要である．そして，情報収集する 1 つの概念として，ネットワークテレメトリが注目されている．ネットワークテレメトリでは，従来のポーリング型といった手法と異なり，低負荷で情報収集できることが期待されている．しかし，ネットワークテレメトリの一意の定まった手法が存在する訳ではない．新しい手法だけでなく，改善した既存手法なども組み合わせ，既存手法の課題を解決することが予想される．そこで，本稿では，接続端末把握のためのネットワークテレメトリにおけるネットワーク機器からの情報収集について考察する．

キーワード：ネットワークテレメトリ，ストリーミングテレメトリ，ポーリング型，出版-購読型

Consideration on Collecting Information from Network Equipment in Network Telemetry for Identifying Connected Hosts

Motoyuki Ohmori[1,a)]

Abstract: In computer networks, it is important to identify hosts connected to a network in order to quickly detect and respond to failures and/or security incidents. To identify the connected hosts, it is necessary to collect information from network equipment. Network telemetry has been, then, attracting attention as a concept for collecting information. Unlike conventional polling or other methods, network telemetry is expected to be able to collect information with a lower load on network equipment. There is, however, no well-defined method for network telemetry so far. In network telemetry, it might be expected that not only newly developed methods but also improved existing methods will be combined to solve the problems of existing methods.
In this paper, we discuss the collection of information from network equipment in network telemetry for identifying connected hosts.

Keywords: network telemetry, streaming telemetry, polling, pub/sub

1. はじめに

コンピュータネットワークにおいて，障害やセキュリティインシデントを迅速に検知し，対応することは重要である．迅速な検知と対応のためには，ネットワークに接続している端末の IP アドレスや MAC アドレス，接続箇所の把握が欠かせない．これらの把握には，ルータやスイッチ，ファイアウォールといったネットワーク機器などから情報を収集しておく必要がある．この情報収集のためにはこれまで SNMP (Simple Network Management Protocol) [1], [2], [3] や syslog [4] などがこれまで広く用いられてきた．しかし，従来手法では，ポーリング型のデータ取得によるネットワーク機器への負荷の増大やデータの

[1] 鳥取大学 情報基盤機構
Organization for Information and Communication Technology, Tottori University
[a)] ohmori@tottori-u.ac.jp

Vol.2022-OS-157 No.2
Vol.2022-IOT-59 No.2
2022/9/13

粒度が粗いなど様々な課題がある．

従来手法の課題を解決するため，テレメトリが提唱されている [5]．テレメトリでは出版-購読型やストリーミングといった新しいデータ取得手法や概念を用いることにより，従来手法の課題の解決が期待されている．しかし，ネットワーク機器におけるテレメトリ，すなわち，ネットワークテレメトリを実現するために必要となるアーキテクチャや構成要素は明らかになってはいない．そこで，本稿では，接続端末を把握するためにネットワークテレメトリに必要なネットワーク機器に求められる機能などについて考察する．特に，有線 LAN においてネットワークへ接続している端末を把握するために，以下の情報を収集することに着目する．

(1) 端末に付与されている IP アドレスと MAC アドレス
(2) 当該端末の接続箇所 (スイッチと収容ポート)

IEEE802.1x 認証で比較的容易に上記の情報を取得できる無線 LAN については本稿では論じない．また，バーストトラフィックの検知などネットワークテレメトリの 1 つの事例として挙げられることの多い他の情報収集については本稿の対象外とする．

本稿の構成は以下のとおりである．2 節では，従来のデータ取得手法と課題を述べる．3 節では，課題を解決するために必要なネットワークテレメトリに必要な機能を挙げる．4 節では，常時認可する MAC アドレス認証を用いた接続端末の把握手法を提案する．5 節では，ネットワークテレメトリに必要な機能について考察する．6 節では，関連研究に言及する．最後に，7 節で本論文をまとめる．

2. 従来のデータ取得手法とその課題

2.1 SNMP による ARP テーブル取得と高負荷

ネットワークに接続している端末の IP アドレスから接続箇所を特定するためには，MAC アドレスが必要となる．これらを収集するため，IP アドレスと MAC アドレスの組からなる ARP テーブルの情報を取得することが従来から広く行われている．これは，SNMP によってコアスイッチの ARP テーブル上のエントリを定期的に収集することが多い．しかし，SNMP による ARP テーブルの情報収集はスイッチの CPU 負荷を高騰することが知られている [6]．

そこで，より詳細な CPU 負荷を明らかにするため，鳥取大学の湖山キャンパスのコアスイッチにて CPU 負荷を計測した．コアスイッチはアラクサラネットワークス株式会社 (以降 AlaxalA) の AX8616 であった．当該コアスイッチでは最大で約 6,000 個の MAC アドレスが観測されていた．そして，SNMP によって ARP テーブルを 5 分に 1 回取得した．1 秒毎の CPU 負荷を 1 日に渡って計測した結果を図 **1** に示す．図 1 から分かる様に，接続していたホスト，つまり，MAC アドレスの数が多い時間帯で，最大で 1 秒間で 48%の CPU 負荷が発生していた．一方，SNMP による情報取得を実施しない場合では，CPU 負荷は 5%未満であった．

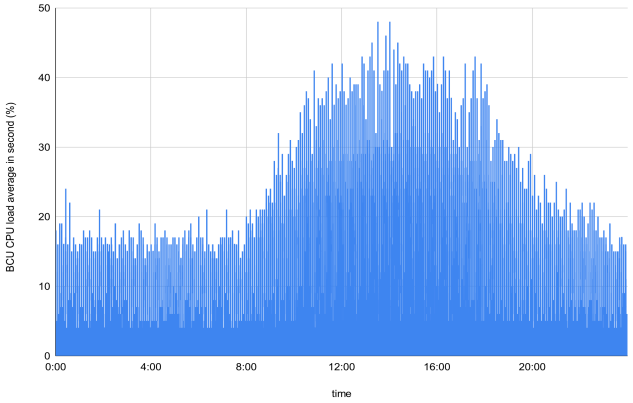

図 **1** AlaxalA AX8616 の CPU 負荷 (2022 年 8 月 4 日 0:00-23:59, 1 秒平均, CLI による 60 秒毎の計測)

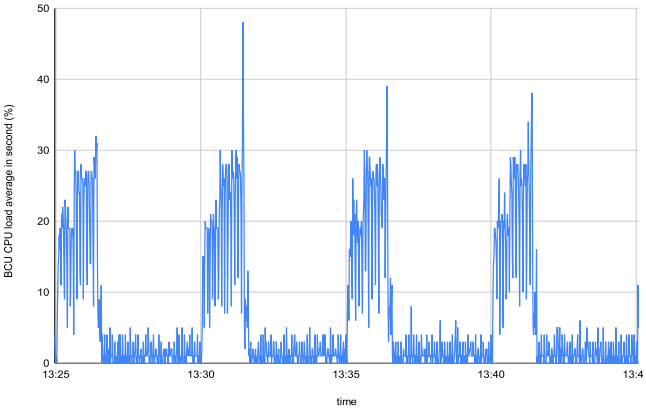

図 **2** AlaxalA AX8616 の CPU 負荷 (2022 年 8 月 4 日 13:25-13:45, 1 秒平均, CLI による 60 秒毎の計測)

1 回の ARP テーブルの情報収集に要する時間を明らかにするため，図 1 の一部を拡大したものを図 **2** に示す．図 2 から分かる様に，13:30:03 から CPU 負荷が 6%になり高騰が始まり，13:31:27 に 48%の最大値となった．そして，13:31:39 に 1%となり，CPU 負荷の高騰が収まった．この様に，実に 1 分 36 秒もの間 CPU 負荷の高騰が持続していた．

今回計測したスイッチの CPU は，経路制御や ARP，STP，転送テーブルの更新といったパケット転送に必須の機能を担うため，その負荷は低い方が望ましい．48%の CPU 負荷は高負荷過ぎる可能性があり，他の機能に一時的に影響を与えていた可能性も否定できない．また，約 6,000 台の端末しか接続していなかった計測環境よりも大規模なネットワークでは，より高負荷を招くと推察される．例えば，12,000 台の端末が接続している場合は，CPU 負荷は 96%以上になることも考えられ，他の機能への影響を与える可能性も高くなる．

実際に，情報処理学会 インターネットと運用技術シンポジウム 2018 (IOTS2018) の会場ネットワークでの実験で

Vol.2022-OS-157 No.2
Vol.2022-IOT-59 No.2
2022/9/13

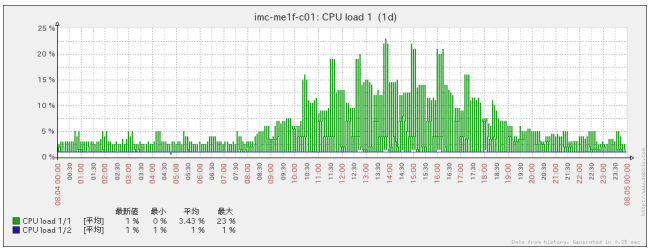

図 **3** AlaxalA AX8616 の CPU 負荷 (2022 年 8 月 4 日 0:00-23:59, 5 分平均, zabbix による 5 分毎の計測)

は, SNMP による情報収集によって実運用に支障が生じた. IOTS2018 の会場ネットワークでは，AlaxalA の AX8608 により対外接続を収容し，BGP によってフルルートを受信していた．そして，200 台程度しか端末が接続していなかったにも関わらず, 対外接続回線のパケットカウンタのデータ取得に失敗し, スループットをグラフ化できなくなる事象が発生した．これは, SNMP によって ARP テーブルの情報を収集する AlaxalA の AX-SC (AX-Security-Controller) [7] を適用した場合に発生していた．AX-SC による情報収集を停止することで復旧した．そのため，IOTS2018 の様な小規模な会場ネットワークであっても，AX-SC の SNMP による情報収集がスイッチに高負荷を招き，他の基本的な運用に影響を与えていたと考えられる．この様に，SNMP による ARP テーブルの情報収集は好ましくない言える．

また，同様な課題が，MAC アドレステーブルの情報収集にも存在していると言える．

2.2 ポーリングによる情報損失

ネットワーク機器からの従来の情報収集は，ポーリング型であることが多い．そして，情報収集の間隔は，慣例的に 5 分であることが多い．この様なポーリング型の情報収集では，情報が失われたり，重大なイベントを見過してしまう可能性がある．例えば，コアスイッチの CPU 負荷の収集を考えると，瞬間的な負荷の高騰を見逃す可能性がある．実例として，2.1 節の図 1 で示したコアスイッチの CPU 負荷を 5 分間隔で zabbix により取得し可視化したグラフを図 **3** に示す．前述の図 1 では 48%であった最大の CPU 負荷が，図 3 では 23%と示されていた．示された CPU 負荷が半分未満になっていたのは，5 分間隔で情報を取得しており，CPU 負荷の 5 分間の算術平均になっていたことに起因する．これは，情報が失なわれたことを意味し，ポーリングによる情報収集の限界とも言える．ポーリングの間隔を短くすることで，この種の情報の損失は軽減できるが，逆にコアスイッチの CPU 負荷を増加を招く．

また，ARP テーブルのポーリングによる情報収集では，別の原因で情報が失われ得る．例えば，ポーリングの間隔より短い時間で，コアスイッチ上の ARP テーブルのエントリが変化する場合，IP アドレスと MAC アドレスの組の情報を失い得る．これは，異なる端末に同一の IP アドレスが重複して付与されてしまった場合に発生し得る．実際，鳥取大学においては，2018 年に発生したセキュリティインシデントにおいて，疑義のある通信を発生させた IP アドレスが重複して別の端末に付与されていた．その結果，疑義のある振舞いをしていなかった端末をセキュリティインシデントの原因として検出してしまうことがあった [6].

2.3 ポーリングによるデータ量の増加

ポーリングによる情報収集では，変化の無い (つまり，重複した) 情報も収集するため，データ量が増大する．ARP テーブルの情報取得で考えると，鳥取大学の湖山キャンパスのコアスイッチでは，非圧縮のテキストで保存した場合，1 年で約 4.9GB のデータ量が必要となる [6]．変化の無い情報，つまり，連続する同一の IP アドレスと MAC アドレスの組が重複して記録されるため，データ量も増加してしまう．

3. 接続端末把握のためのネットワークテレメトリに求められる機能

本節では，2 節で紹介した課題を解決するために必要と考えられる機能を示す．

3.1 スイッチからの情報送信

2.1 節で示した様に，ポーリングではスイッチに負荷を増加させてしまう．そこで，スイッチへ情報取得するのではなく，スイッチから自律的に情報を送信することで，スイッチへの負荷を削減できる必要がある．スイッチから自律的に送信できない情報の場合は次節で言及する機能により補完する必要がある．

3.2 詳細な情報のスイッチでの保持

2.2 節で示した様に，ポーリングによる情報収集では収集間隔によっては CPU 高騰といったイベントを検知できない場合がある．その様な場合でも，図 1 で示した様に，情報に対して時刻を付与することにより，1 秒毎の情報を 10 分間隔のポーリングでも収集できる可能性がある．

3.3 情報送信の分散

図 2 で示した様に，スイッチから一度に大量の情報を送信すると高負荷の時間が続いてしまうことがある．その様な状況を防ぐために，スイッチからの情報の送信は可能な限り，分散させることが望ましい．

3.4 差分情報のみの送信

2.3 節で示した様に，ポーリングでの情報送信の様に，同一の情報を送信すると，データ量が増加する．そのため，できる限り差分情報のみ送信できることが望ましい．

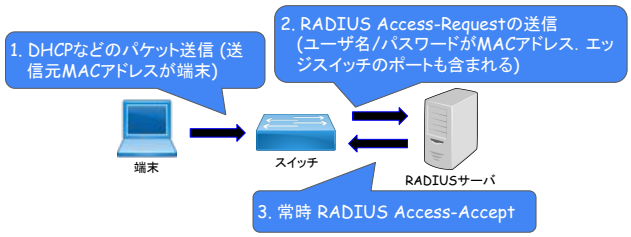

図 4　常時認可 MAC アドレス認証

4. 常時認可 MAC アドレス認証

ここでは，ネットワーク全体に MAC アドレス認証を適用することに依って接続端末を把握する**常時認可 *MAC* アドレス認証**を提案する (図 4)．常時認可 MAC アドレス認証は一般的な MAC アドレス認証である．ただし，事前に登録されていない MAC アドレスも常に認証し，ネットワークへの接続を認可することで，端末を収容しているスイッチとポートを収容する．なお，常時認可 MAC アドレス認証では 3 節で挙げた機能を RADIUS によって実現している．

端末の IP アドレスは，RADIUS のアカウンティング時に送信される Framed-IP-Address 属性により検知する．これにより，コアスイッチから ARP テーブル上の情報を取得する必要が無くなる．

5. 考察

5.1 RADIUS アカウティングでの IP アドレスの送信

提案した常時認可 MAC アドレス認証では，RADIUS のアカウンティング時に端末の IP アドレスが Framed-IP-Address 属性が送信されることを前提としている．少なくともシスコシステムズ合同会社 (以降 Cisco) 製のスイッチでは，MAC アドレス認証の RADIUS アカウンティングに Framed-IP-Address 属性が含まれる．しかし，鳥取大学において導入している AlaxalA のスイッチでは，Framed-IP-Address 属性が送信されない．そのため，コアスイッチから ARP テーブルの情報取得が必要となってしまう．

6. 関連研究

ネットワーク機器からの情報収集には SNMP や syslog が広く用いられていた．しかし，Google, AWS (Amazon Web Services)，Microsoft などのデータセンター事業のいわゆる Hyperscale Player (超大規模データセンター事業者) らによって，SNMP や syslog による情報収集の限界が指摘された．例えば，SNMP によるポーリングでは，トラフィックのマイクロバースト，つまり，極めて短い期間でのリンクの通信帯域を超えたトラフィックの発生を検知することが難しいと言われている．

そこで，ポーリングではなく，イベント駆動型でネットワーク機器から能動的に情報を送信するストリーミングテレメトリが提案された．ストリーミングテレメトリでは，同一の情報はネットワーク機器から一度だけ送信される．一方，SNMP によるポーリングでは，同一の情報に対する異なる要求全てに対して，ネットワーク機器が応答する必要があった．そのため，ネットワーク機器への負荷が低いと言われている．

情報の表現としては，SNMP では ASN (Abstract Syntax Notation).1 BER (Basic Encoding Rules) を用いており，バイナリ形式で表現される．ネットワークテレメトリでは，GPB (Google Protocol Buffers) [9] が用いられ，SNMP と同様バイナリ形式で表現される．メーカ独自のネットワークテレメトリ機能の実装では，テキスト形式の JSON (JavaScript Object Notation) が用いられることもある．

ネットワーク機器上における設定項目などのデータ表現としては，YANG (Yet Another Next Generation) [10], [11] が挙げられる．YANG は OpenConfig [12] で用いられており，現在では設定項目だけでなく，ネットワークテレメトリに必要なデータの表現にも用いられることもある．

データ転送に関しては，SNMP では UDP もしくは TCP が用いられる．一方，ネットワークテレメトリでは，gRPC (Google Remote Procedure Call) [8] を用いられることが多い．

7. おわりに

本稿では，接続端末把握のためのネットワークテレメトリにおけるネットワーク機器からの情報収集について考察した．まず，従来の SNMP による情報収集の課題について示した．次に，接続端末を把握するためのネットワークテレメトリとして必要な機能を示した．そして，MAC アドレス認証を用いた接続端末の把握手法を提案した．

謝辞　本研究の一部は JSPS 科研費 22K11992 の助成を受けたものである．また，本研究の一部はアラクサラネットワークス株式会社との共同研究により実施した．

参考文献

[1] Harrington, D., Presuhn, R. and Wijnen, B.: An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks, RFC 3411 (Standard) (2002). Updated by RFCs 5343, 5590.
[2] Case, J., Harrington, D., Presuhn, R. and Wijnen, B.: Message Processing and Dispatching for the Simple Network Management Protocol (SNMP), RFC 3412 (Standard) (2002). Updated by RFC 5590.
[3] Presuhn, R.: Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP), RFC 3416 (Standard) (2002).
[4] Gerhards, R.: The Syslog Protocol, RFC 5424 (Proposed Standard) (2009).
[5] Tan, L., Su, W., Zhang, W., Lv, J., Zhang, Z., Miao, J., Liu, X. and Li, N.: In-band Network Telemetry: A Survey, *Computer Networks*, Vol. 186, p. 107763 (online), DOI: https://doi.org/10.1016/j.comnet.2020.107763

(2021).
[6] Ohmori, M., Miyata, N. and Okamura, K.: AXARPSC: Scalable ARP Snooping Using Policy-based Mirroring of Core Switches with ARP Log Contraction, *Journal of Information Processing*, Vol. 29, pp. 198–204 (online), DOI: 10.2197/ipsjjip.29.198 (2021).
[7] ALAXALA Networks Corporation: AX-Security-Controller, `http://www.alaxala.com/jp/news/press/2017/20170601.html` (2017). Accessed: 2017/06/03.
[8] Google: gRPC, `https://grpc.io/`. Accessed: 2022/8/3.
[9] Google: Protocol Buffers, `https://developers.google.com/protocol-buffers/`. Accessed: 2022/8/3.
[10] Bjorklund, M.: YANG - A Data Modeling Language for the Network Configuration Protocol (NETCONF), RFC 6020 (Proposed Standard) (2010).
[11] Bjorklund, M.: The YANG 1.1 Data Modeling Language (2016).
[12] OpenConfig: OpenConfig, `https://www.openconfig.net/`. Accessed: 2022/8/3.