C-08

MARS を利用した使用されていない IP アドレスの検出

山下 和志†　　川橋 裕‡
Kazushi Yamashita　　Yutaka Kawahashi

1. はじめに

近年ネットワーク環境の急速な普及に伴い，IP アドレスの利用形態は多様化され，需要は増加している．IP アドレスは有限な資源であり，現在主に利用されている IPv4 アドレスの運用では，IP アドレスの枯渇が問題となっている．[1]

和歌山大学 (以下，本学) では有線接続を用いて IP アドレスを使用する際，ユーザ側で固定の IP アドレスを設定する必要がある．IP アドレスをユーザ側で設定する場合，複数端末に同じ IP アドレスを設定してしまう可能性がある．本学では IP アドレスの競合を避けるため，利用者が IP アドレスを利用する際，申請書の提出を義務付けている．しかし申請書の提出をしないユーザが少なからず存在する．そのため，管理者は IP アドレスの利用状況を正しく把握することが困難である．

IP アドレスの利用状況の確認をおこなう方法として，ネットワークコマンドを用いて疎通確認をおこなう手法がある．しかしながらこの手法では，IP アドレスを利用する端末の電源を入れていない場合疎通確認がおこなえないため，利用頻度の低い端末を検知することが難しい．さらに機器に設定されたファイアフォールによって検知できない場合も存在する．

本研究では管理するネットワーク内の IP アドレスがいつ使用されたか把握することで，長期間使用されていない IP アドレスを検出することを目的とする．

2. 既存技術

2.1 MARS の概要

本学では MARS(Monitoring, Analysis and Response System)[2]を運用している．MARS では，ユーザがインターネットに接続する際，ユーザが接続するエッジスイッチから RADIUS 認証プロトコル[3]を用いて端末の IP アドレス，MAC アドレス，接続時刻や端末の位置等の接続情報を取得している．さらに取得した接続情報をブラウザを通じて管理者に提示することで，管理者が障害に対して迅速に対応することを可能とする．MARS では RADIUS 認証で得られた情報に加えてパッチ情報と対応させることで以下の項目を管理している．

- セッション ID
- 端末の DNS ホスト名
- 端末の IP アドレス
- 端末の MAC アドレス
- エッジスイッチの IP アドレス
- エッジスイッチのポート番号
- 棟名
- 部屋名
- 接続開始時刻
- 接続終了時刻

MARS で収集される接続情報は，エッジスイッチと RADIUS サーバ間の RADIUS 認証で取得できる．すなわち，ユーザの利用する機器の設定に依存せず収集可能であり，IP アドレスの管理をする上でも有用である．

2.2 MARS の動作

MARS のエッジスイッチと RADIUS サーバ 間の動作を図 1 に示す．

(1) ユーザの端末がエッジスイッチに接続
(2) エッジスイッチは接続要求を RADIUS サーバに送信
(3) RADIUS サーバは受信した情報を基に認証し，結果をエッジスイッチに通知
(4) エッジスイッチは通知された認証結果を基に，端末の接続を許可
(5) エッジスイッチは端末の接続が終了したことを RADIUS サーバに通知

2.3 MARS の問題点

現在の MARS はデータ量が多く複雑な SQL を実行するには長い時間を要する問題がある．また MARS で収集できる接続情報は，端末がエッジスイッチへの接続を開始したときと終了したときである．しかし，接続を終了した際の記録が収集されていない記録が複数確認された． MARS 上で接続終了時刻がない記録の中には，現在も接続中である端末だけでなく，ネットワーク上の不具合などの原因で接続終了の際の RADIUS 認証を取得できなかった場合の 2 種類が存在する．このため終了時刻のない接続記録が現在も接続中であるか判断できない．

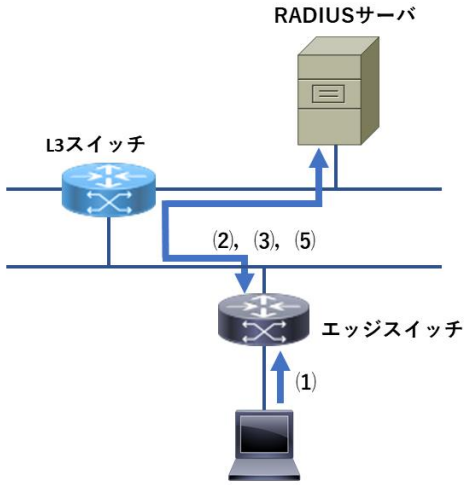

図 1　エッジスイッチと RADIUS サーバ 間の動作

† 和歌山大学大学院，Graduate School of Systems Engineering, Wakayama University

3. 研究目的

IP アドレスを管理するには，どの IP アドレスが利用されているか把握する必要がある．旧来の IP アドレス検知方法では IP アドレスの利用を把握することは困難であったが，MARS を利用することで IP アドレスの利用を正確に把握することが可能であると考えられる．本研究では IP アドレスの利用を正確に把握することで，長期間使用されていない IP アドレスを発見し，無駄な IP アドレスの割り振りを検出することを目的とする．

4. 提案システム

MARS のデータベースに対して複雑な SQL を実行するには長い時間をようする．そのため提案システムではバックグラウンドで定期的に MARS のデータベースから各 IP アドレスの最新の接続情報のみを取得し，システムのデータベースに保存する．そのためシステムを利用する際には簡易な SQL で IP アドレスの最新の接続情報を取得可能となる．終了時刻のない接続情報については，接続情報にある端末が現在も接続されているかシステムで自動的に判断する．コマンドは「show ip device tracking」というものを用いる．このコマンドでは ARP 情報を基にしたデータの取得をおこない，スイッチに接続された端末の IP アドレス，端末の MAC アドレス，ポートに設定された VLAN の値，接続されているポート，現在の接続状態を表示する．コマンドを用いた判定のフローを図 2 に示す．まず終了時刻のない接続情報にあるエッジスイッチの IP アドレスに接続する．そして show ip device tracking コマンドを用いて端末の接続されているポートを指定する．得られた実行結果の端末の IP アドレス，MAC アドレスが MARS の接続情報と一致すれば，現在の状態とその時刻をデータベースに保存する．

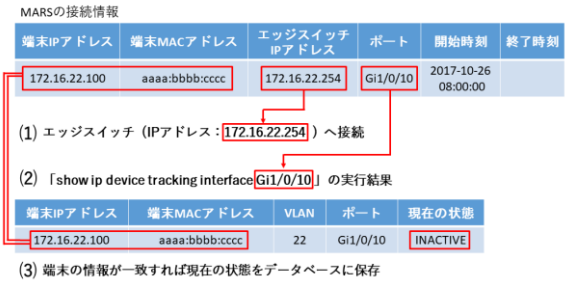

図 2　判定フロー

5. 実験

提案システムを，MARS の運用されている本学のネットワークに設置し，運用実験をおこなった．MARS には 2016 年 8 月以降の接続記録が保存されており，1 月 26 日～28 日の間運用実験をおこなった．さらにサブネットマスク長が 24 である 1 つのネットワークに対して，インタフェースを用いて IP アドレスの利用状況の調査をおこなう．なお，管理者の持つ申請書に基づいたデータでは，74 個の IP アドレスが現在使用中という扱いである．

図 3 に実験結果をベン図を用いて示す．サブネットマスク長が 24 のネットワークには 254 個の IP アドレスが存在する．そのなかで MARS を用いて利用を検出できた IP アドレスは 57 件存在した．申請書による

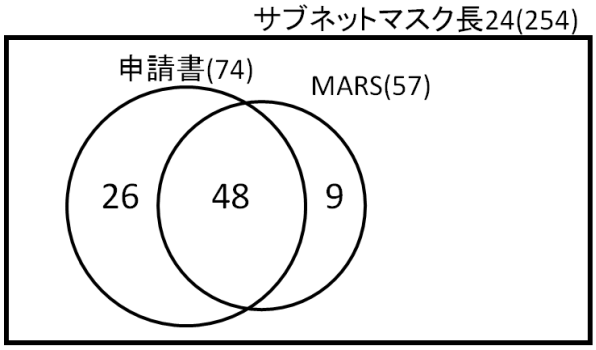

図 3　実験結果ベン図

データと分類したところ 9 件の IP アドレスは申請書の中に含まれず，MARS で検知することができた．これは申請書を出さず無断で IP アドレスを利用されていたとわかる．申請書が出されており，MARS で検出した IP アドレスが 48 件存在した．この IP アドレスは正規に利用されていたが既に 1 年以上利用されていない IP アドレスが 8 件存在していることが確認できた．また 26 件の IP アドレスは利用申請されているが全く使用されていないことが確認された．この IP アドレスが本当に使用されていないか別方法で調査したところ 4 件の IP アドレスが使用されていたことが確認された．4 件の IP アドレスについて追加で調査したところ，この IP アドレスは普段利用されている場所と離れた部屋で利用されており，スイッチに Radius 認証の設定がされていないことが原因となり，システムで利用を検知することができていなかった．

6. 評価

6.1　従来の IP アドレス検知手法との比較

従来では IP アドレスの利用を検知するためにネットワークコマンドを用いた疎通確認がおこなわれていたが．しかし端末の利用時間やファイアウォールの設定によって利用の検知が困難な場合があった．本研究では MARS を利用することで端末をいつ利用されても検知することが可能であり，加えて機器の設定に依存することなく IP アドレスの利用を検知可能なネットワークを構築することができたため，従来手法より正確に IP アドレスの利用を把握できると考えられる．

6.2　今後の課題

6.2.1　ネットワークの構築

提案システムでは MARS の RADIUS 認証の仕組みを利用することによって，IP アドレスの利用状況を把握することを可能とした．しかしながら RADIUS 認証の設定がされていない環境下では，この手法で，IP アドレスの利用を正確に検知することができない．したがって管理をおこなう環境に RADIUS 認証の設定を正確に施さなければいけないという難点がある．

6.2.2詳細な利用時間の表示

提案システムでは利用時間について最新の接続時刻のみを表示している．過去の利用時間を直感的に可視化することで，その IP アドレスがどのように利用されているか詳細に知ることができると考えられる．

7. おわりに

本研究では IP アドレスの管理に MARS を用いることで，より正確に IP アドレスがいつ使用されていたか把握できるシステムを提案した．今後は，管理するネットワークの環境を整備し収集した接続情報をさらに有効活用することで，IP アドレスがどのように利用されているか，より正確に把握できるよう改良していきたい．

参考文献

[1] “IPv4 アドレスの在庫枯渇に関して “(2018)
https://www.nic.ad.jp/ja/ip/ipv4pool/

[2] 吉田祐亮 “ネットワーク接続監視システム MARS の構築 “
2012 年度修士論文　和歌山大学大学院システム工学研究科

[3] “Remote Authentication Dial In User Service (RADIUS） “(2018)
https://tools.ietf.org/pdf/rfc2865.pdf