東北工業大学地域連携センター紀要 EOS
Vol.27 No.1 p.97 ～ p.103, 2015

〔技術報告〕

ARP 要求の送受信特性に着目したネットワーク機器の分類に関する検討

角田　裕[1)]，太田　耕平[2)]，キニ グレン マンスフィールド[2)]

Categorizing networked devices by focusing volume of ARP requests

Hiroshi Tsunoda[1)] , Kohei Ohta[2)] , Glenn Mansfield Keeni[2)]

Abstract

Configuration management, one of the important aspects of network management, is getting more and more complex because a number of and a variety of devices connect to intranets in recent years. Network administrators have to find those devices and have to identify the types of the devices for configuration management. In this research, we discuss a simple method to roughly categorize the types of devices in intranets by focusing volume of ARP requests. Since ARP requests are broadcast to an intranet, we can easily monitor and analyze them. This paper reports analysis results of ARP requests monitored in real environment. The analysis results show that different types of devices have different characteristics in sending or receiving ARP requests. It indicates that the volume of ARP request can be useful metrics for categorizing networked devices.

1．はじめに

近年，ネットワークに繋がる機器の数は爆発的に増加し，その種類も多様化している。従来のネットワークにおける主たる機器はサーバやクライアント，スイッチ，ルータなどであった。しかし最近では，従来では周辺機器に過ぎなかったプリンタやストレージがネットワークに接続され，ネットワークプリンタや NAS（Network Attached Storage）となっている。また，スマートフォンやタブレット PC が急激に普及し，無線 LAN を通じてネットワークに繋がることが一般的となっており，企業でも社員が個人で所有するそういった機器を業務に利用する BYOD（Bring Your Own Device）という考え方が認知されている。一方，家庭に目を向ければ，テレビや据置型ゲーム機や携帯型ゲーム機などがネットワークにつながる新たな機器となっている。さらには，M2M（Machine-to-Machine）や IoT（Internet of Things：モノのインターネット）という言葉が生まれ，家電製品や各種センサに代表されるあらゆるモノがネットワークに接続され，ネットワークを介して監視・制御される時代が到来しつつある。

1）東北工業大学 工学部 情報通信工学科　准教授，Department of Information and Communication Engineering, Faculty of Engineering, Tohoku Institute of Technology
2）株式会社サイバー・ソリューションズ，Cyber Solutions Inc.

このようにIT機器の増加と多様化が進んだ結果，ネットワーク管理の一要素である構成管理は複雑化し課題のひとつとなっている。構成管理では，接続機器を検知し，その種別や役割を識別し，機器の論理的・物理的位置を把握することが求められる。特に機器の識別は，各機器がそれぞれ異なる特性を持ち，それに応じたリスクを内包しているために重要である。例えば，スマートフォンが持つ持ち運びの容易さという特性は，それがひとたびイントラネットに持ち込まれれば情報漏えいの要因にもなり得るという危険性を秘めている。その結果，イントラネットのセキュリティ管理という観点からも，機器を識別しその特性やリスクに応じて適切な対策を施すことが強く求められ，新たなニーズとなっている。機器が増加・多様化した現代のネットワークにおいて，特に専任の管理者のいない場合には構成管理は大きな課題となる。

本研究では，構成管理の一要素である機器の識別においてARP（Address Resolution Protocol）[1]の要求パケットの活用を検討する。ARPはネットワーク内でのアドレス解決用のプロトコルであり，インターネット技術をベースとしたあらゆるネットワークで利用されている。従来，ARP要求の情報は接続機器の検知に利用されているが，本研究では各機器のARP要求の送受信特性に着目する。それは，アドレス解決は通信に先立って行われるためARP要求の送受信量やパターンに各機器の用途に基づく特性が反映されていると考えられるためである。本稿では，実運用ネットワークにおいてARP要求を収集し，そのデータを利用して，機器毎のARP要求の送受信量から機器の種別の分類の可能性を検証する。

以下，2ではARPの概要とアドレス解決の流れについて説明し，それに基づいてARP要求の送受信量が用途によって変わりうることを指摘する。次に3ではARP要求の収集を行った本学の情報処理演習室の環境について説明する。そして，4では収集したデータの分析結果に基づいて，本学の情報処理演習室の機器がARP要求の送受信量から分類可能であることを示す。5では関連研究について説明する。6はまとめである。

2．Address Resolution Protocol

ARPは同一LAN上にある端末のMACアドレスの調査に使われるアドレス解決プロトコルである。サブネット内の通信では，宛先端末のIPアドレスだけではなく，そのIPアドレスが割り当てられているNIC（Network Interface Card）のMACアドレスが必要である。そのため，送信元ホストは宛先ホストのIPアドレスに対応するMACアドレスをARPによって解決する。

図1にARPによるアドレス解決の流れを示す。ある機器がIPアドレス192.168.1.1を持つ機器と通信したい場合，その機器のMACアドレスを知るために，ARP要求パケットをブロードキャストにより送信する（図1左）。このARP要求パケットは同一LAN上にの全機器が受信する。ARP要求パケットを受信した機器の中でIPアドレス192.168.1.1を持つ機器があれば，その機器は自身のARP応答パケットを要求パケットの送信元に返信することでMACアドレスを通知する（図1右）。

このように，ARP要求は同一LAN内の全機器に送信されるため，LANにトラヒック観測用機器（トラヒックモニタ）を接続するだけで，特別な機器や設定の必要なくARP要求を観測できる。各ARP要求パケットからは以下の情報が得られ，ネットワークに接続している機器の検知に利用されている[2]。

- 送信時刻

- 送信元機器の IP アドレス
- 送信元機器の MAC アドレス
- 宛先機器の IP アドレス

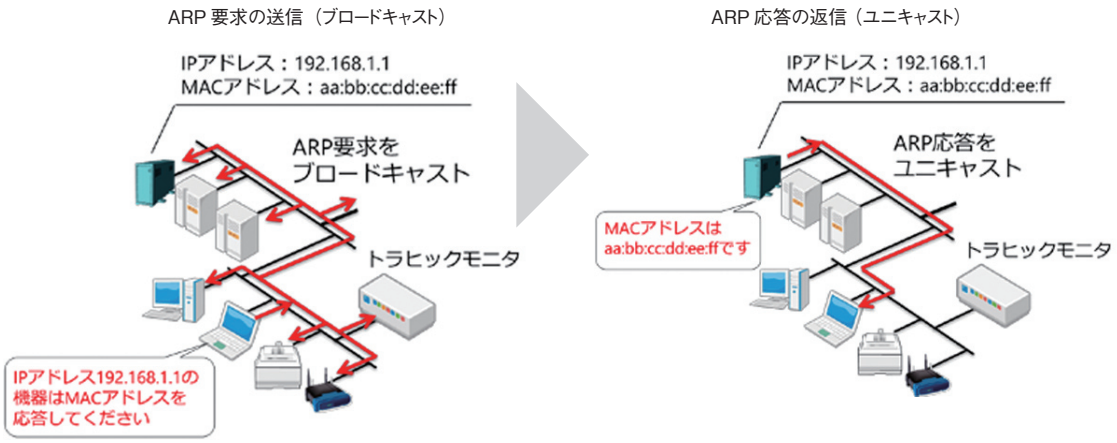

図 1　ARP による MAC アドレス解決の流れ

ARP 要求は他の機器との通信を開始する機器が送信するものであるため，サーバ・クライアント通信においてはクライアント機器がサーバ機器の MAC アドレスを解決するために送信する。すなわち，クライアント機器は ARP 要求の送信回数が多く，その一方でサーバ機器は少ない，といった特徴が表れる。本研究では，このように ARP 要求の送信先や送信頻度，間隔など送受信の特性に機器の特性が反映されることに着目し，送受信特性に基づいて機器の役割の推定と分類を試みる。

3. ARP パケットの収集

実ネットワークにおける ARP 要求の特性を調査するため，実運用ネットワークである本学情報処理演習室（812 教室）で ARP 要求を収集し分析した。情報処理演習室は朝 8:30 から夜 8:00 まで開放されており，講義で使用されている時間のほかにも，解放時間内であれば講義で使用している時間帯以外は学生･教職員ともに自由に利用できる。そのため，実際の利用状況を反映した ARP 要求のデータが得られる。なお，ARP 要求自体には通信内容に関わる情報は含まれていないため，この収集によってプライバシーを侵害する恐れはない。

演習室のネットワークには演習用端末，プリンタ，スイッチの合計 130 台程度のホストが接続されている。以下にその内訳を示す。

- 演習用端末：116 台
  （DELL:OPTIPLEX 780）
- ネットワークプリンタ：5 台
  （RICHO:IPSiO SP 6220,IPSiO SP C821）
- スイッチングハブ：7 台

ネットワーク構成は図 2 のようになっており，演習用端末とプリンタがつながった 6 台のスイッチをその上位のスイッチ 1 台が束ねる構成になっている。

本学情報処理演習室では端末ごとに静的に IP アドレスが設定されており，ネットワー

クプリンタとスイッチングハブにはそれぞれ1つずつ決まったIPアドレスが割り当てられている。なお，演習用端末ではホストOSであるLinux上にゲストOSであるWindows 7が稼働しており，それぞれのOSに異なるIPアドレスが割り当てられている。そのため，1台の物理端末が2つのIPアドレスを持っている。

データの収集期間は2012年5月21日から12月19日の夏季休業を含むものである。期間中に観測したARP要求の総数は5,445,036個であり，1日平均で25,684個のARP要求が流れていることになる。

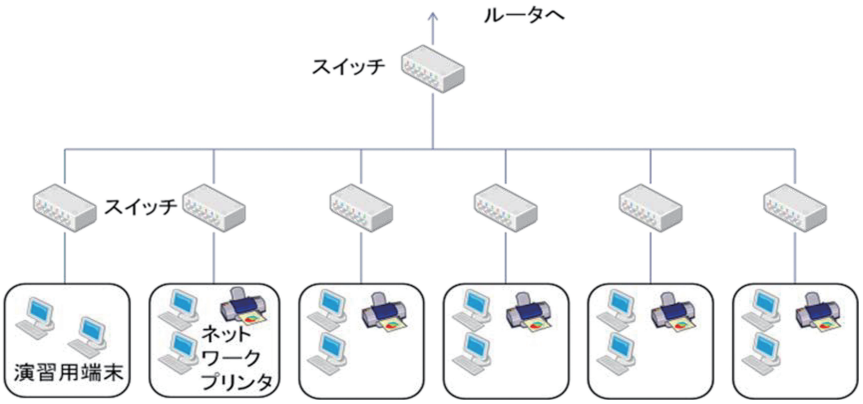

図2　812演習室のネットワーク構成

4．ARP要求の送受信特性に基づく機器分類の検討

まず，収集したARP要求の送信元と送信先から送受信回数をIPアドレスごとに月単位で集計した。図3は2012年5月21日～31日に観測したARP要求について，横軸を受信回数，縦軸を送信回数としIPアドレス毎にプロットした散布図である。1つの点が1つのIPアドレスを示しており，点の色の違いは機器の種類の違いを表す。ただし，この期間に約40万回受信している2つのホストOSについては，他の機器に比べて明らかに受信回数が多いために何らかの異常が発生していると考え，今回は除外している。

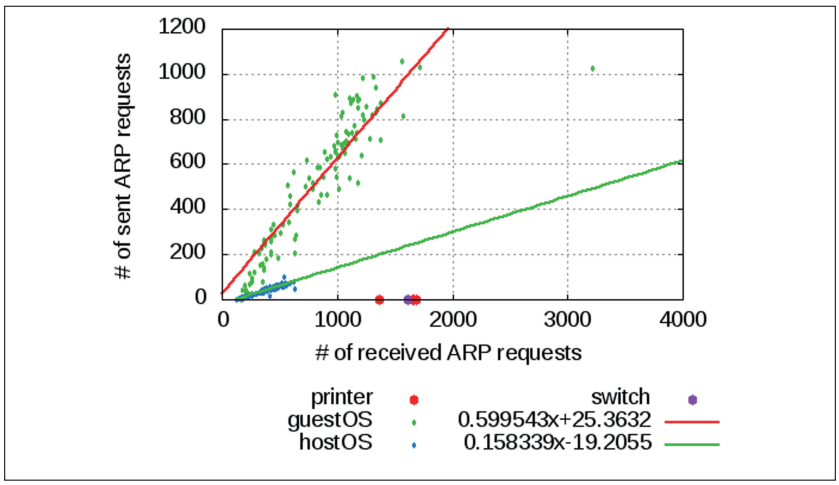

図3　機器毎のARP要求送受信回数（2012年5月）

図3より，各点は（1）プリンタとスイッチングハブ，（2）ゲストOS，（3）ホストOSという機器の種類毎に分布していることがわかる。プリンタとスイッチングハブを表

す点は近い位置に分布しており，いずれも ARP 要求を受信しているが送信はしていないことがわかる。これらの機器はプリンタは印刷機能，スイッチングハブはネットワークへの接続性というサービスを他のホストに対して提供する機器と考えられサーバとみなせる。このことから，ARP 要求の送受信特性からサーバを識別できる可能性があることがわかった。また，ゲスト OS とホスト OS の点の集合は，ある傾きを持つ直線上に点が分布している。2 つの点の集合について最小二乗法により求めた回帰直線の傾きはそれぞれ約 0.60 と約 0.16 となった。この傾きの違いの原因が，Windows と Linux による OS の差によるものか，ゲスト OS とホスト OS の役割の差であるかを今後の課題とする。この直線の傾きの違いが表れる原因を調査することによって，端末上で稼働している OS またはホスト OS やゲスト OS の存在を判別することが可能になると考える。

他の月において同様なグラフを作成した結果，ほとんどの月で図 3 と同じように点が機器の種類ごとに直線上に分布する形になった。例として図 5 に 6 ～ 7 月および 10 月～ 11 月のグラフを示す。図 5 内の各図においても図 3 と同様の分布が見られており，5 月の結果が特殊なケースではないと言える。また，すべての図おいてゲスト OS とホスト OS の分布の傾きはいずれも類似しており，ARP の送受信回数の比率に特徴が反映されていると言える。

次に図 6 に 2012 年 8 月，9 月における ARP 要求送受信回数を示す。この 2 ヶ月のデー

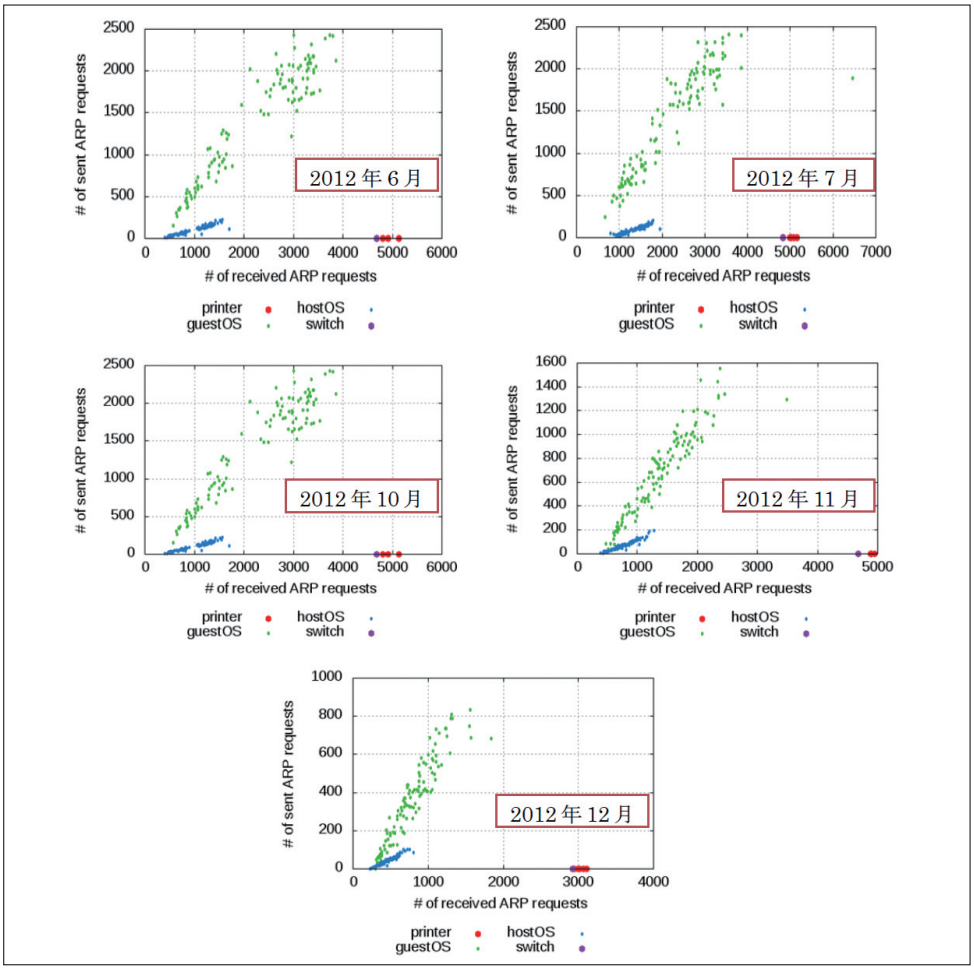

図 4　機器毎の ARP 要求送受信回数（2012 年 6 ～ 7 月，10 ～ 11 月）

タは他の月と異なり，ゲストOSとホストOSの点は直線上に分布しなかった。この違いが生じた原因として，この2ヶ月は夏季休業期間を含んでおり使用する演習用端末に偏りがなかったためと考えられる。講義で演習室を使用する際，学生は指定された端末を使用するため，よく使われる端末とそうではない端末が出てくるが，講義での使用でない場合，どの端末を使用してもよいため使用する端末に偏りが出にくかったと推測される。また，夏季休業中にシステムのメンテナンスが行われるため，すべてのホストが均等に外部との通信が行われたため，講義期間中の他の月とは異なる通信状況であったと推測される。しかし，分布の形状は違うが，種別の異なる機器の点は異なる位置に分布しており，対象ネットワークにおける機器の分類は依然として可能であると考えられる。

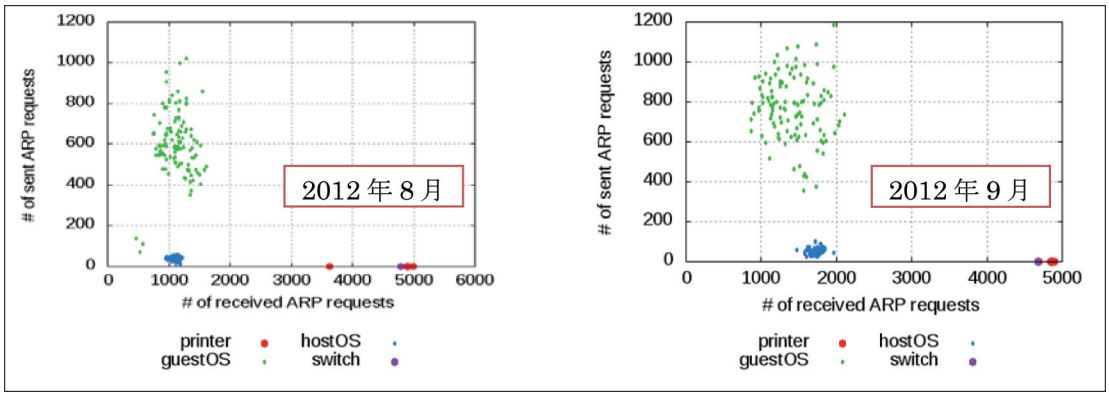

図5　機器毎のARP要求送受信回数（2012年8～9月）

以上の結果より，特定のネットワークにおける検証の段階ではあるが，機器毎のARP要求の送受信回数の情報のみから，機器を種別毎に大別できる可能性があるといえる。今後は，1台の機器からのARP要求の送信回数の宛先毎の集計や，ARP要求の送信間隔の評価，時間帯別の送受信量のパターンの評価など，ARP要求からさらに多くの情報を得ることで分類の詳細化や高精度化を図る。また，他のネットワークにおけるデータ収集を行い，同様に機器分類の可能性を検証する。

5．関連研究

既存のイントラネット内の機器の識別技術・ツールについて主要なものを表1に示す。各ツールは機器識別に利用するパケット情報の収集方式によって2種類に大別できる。一方は日常的に流れているパケットを捕捉する受動的な方式，他方は識別対象となる機器にプローブパケットを送信しその応答を捕捉する能動的な方式である。受動的な方式は，ネットワークや識別対象機器に負荷を与えず識別対象が気づかれにくいが，識別対象の機器を指定することができない。能動的な手法は対象機器に能動的にパケットを送信し，そのパケットに対する応答パケットの観測データに基づいてOSを識別する手法である。この手法では対象の機器を明確に指定できるが，識別のために送信するデータがネットワークに負荷を与えてしまう。各ツールが着目するパケットはARP，ICMP，TCP，DHCPのパケットであり，セキュリティ監査やペネトレーションテストにも利用されるnmap［3］のみがパケット情報に加えて対象機器が使用しているポートの種類や使用状況を考慮している。

表 1　既存ツールの特徴

ツール名	パケット情報の収集方式	識別に使用する情報
nmap [3]	能動的	対象機器が使用しているポートの種類 TCP の各種パケット
xprobe [4]	能動的	TCP SYN, TCP SYN/ACK, ICMP の各種要求に対する応答
arp-fingerprint [5]	能動的	ARP 応答
p0f [6]	受動的	TCP SYN，TCP SYN/ACK
satori [7]	受動的	DHCP Discovery

本研究は受動的に収集した ARP 要求を使用して機器の識別を試みるものである。既存のツールでは arp-fingerprint [5] が ARP 応答を利用しているが，ARP 要求に着目したツールや技術は提案されていない。また，既存技術は主にパケット内部のデータにのみ着目しており，本研究で着目した送信量や受信量などの特性については識別の材料として十分に検討されていない。

6. おわりに

本研究では，ネットワークの接続機器がアドレス解決のために送受信する ARP 要求に着目し，各機器の ARP 要求の送受信量の特性に基づいた機器の分類可能性を検証した。ARP によるアドレス解決はネットワークにおける通常動作の一つであり，それによって送信される ARP 要求はブロードキャストされるため観測が非常に容易である。そのため，ARP 要求が機器の分類に活用できれば多くのネットワークで広く構成管理に活用できる技術となる。実運用ネットワークである本学の情報処理演習室で収集した ARP 要求を分析した結果，機器の種別によって ARP 要求の送信量と受信量に関係が異なっているという特徴が見られた。このことから，ARP 要求の送受信量に着目することで機器の分類が可能であると言える。

今後は他のネットワークにおけるデータ収集を行い，機器分類の可能性をより一般的に検証すると共に，分類の詳細化と高精度化の方法を検討する。

謝辞

本研究は，東北工業大学新技術創造研究センターの地域・産学連携プロジェクト研究費の援助により行われたものである。ここに記して謝意を表する。また，卒業研究としてデータ分析に取り組んだ 2013 年度研修生・齋藤綾君の貢献に感謝する。

参 考 文 献

1） David C. Plummer, “An Ethernet Address Resolution Protocol,” RFC826, November 1982
2） H. Tsunoda and G. M. Keeni, “Security by Simple Network Traffic Monitoring”, Proc. of The 5th ACM International Conference on Security of Information and Networks, pp. 29-32, Oct. 2012 8
3） Nmap - Free Security Scanner For Network Exploration & Security Audits., http://nmap.org/
4） X probe - active OS fingerprinting tool, http://sourceforge.net/projects/xprobe/
5） Arp-scan Documentation, http://www.nta-monitor.com/wiki/index.php/Arp-scan_Documentation
6） p0f v3 http://lcamtuf.coredump.cx/p0f3/
7） Satori Download http://chatteronthewire.org/satoridownload.htm