6U-6

ネットワークに接続されたマシンの通信内容に基づくグループ化について

守谷紘樹† 古川善吾‡

（香川大学）

1. はじめに

ネットワークの運用管理において個々の機器が正常に動作しているかどうかに注意を払う必要がある。また、障害の発生や不正な通信の検出を行った場合には、対象となる機器を特定しその対処が必要となる。このような問題に対処するためにネットワーク構成を把握し、物理的な位置情報を取得するための方法が議論、提案されている。しかしながら、ノート型コンピュータの普及によって動的に位置が変化する場合が増えている。その場合には、機器を特定するだけでなく、その機器の利用者あるいは管理者を特定する必要がある。[1]

一方、ネットワークに接続されたネットワーク機器やコンピュータ（これらを「ネットワークに接続されたマシン」あるいは誤解のないときは単に「マシン」と呼ぶことにする）のグループ化としては、サブネットあるいは VLAN でのグループ化が行われている。その他には個々のマシンを IP アドレスや MAC アドレスで識別しているだけである。そのために、管理者の組織体系とサブネットあるいは VLAN でのグループ化が対応していれば、障害や不正通信を行ったマシンへの対処を依頼する際に、管理者の組織体系内で連絡を取ることが可能である。しかしながら、機器のグループ化と管理の体系とは必ずしも対応していないのが現状で、機器の障害や不正通信への対処については、個々の利用者に直接連絡する必要がある。

そこで、本研究では、コンピュータやネットワーク機器の管理を円滑にするために、ネットワーク上のパケットから判別できる利用方法に基づいてそれらをグループ化する方法を提案する。

Making to computer groups based on packets from/to the computers connected with networks

†Hiroki Moriya (Kagawa University)
‡Zengo Furukawa(Kagawa University)

2. ネットワーク接続マシンのグループ化

現在、ネットワークに接続されているマシンは、いくつかのグループとして識別することが可能である。ここで述べるグループは、ネットワーク機器やネットワークに接続されたコンピュータの集合のことを言う。

例えば、香川大学というグループに所属するマシンとの通信であるか否かは、パケットのソースアドレスあるいはディスティネーションアドレスが 133.92.*.* によって判断できる。同じように香川大学内のサブネット 133.92.145.0 というグループに所属するマシンとの通信は、IP アドレスが 133.92.145.*であるマシンであると考えることができる。

さらに、最近では、前もって設定されたグループに所属するマシンを VLAN のアドレスとして割当それらをグループとして考える試みが行われている。

現在の情報では上記のような形でネットワークに接続されたマシンのグループ化が行われている。さらに、例えば、大学内の研究室やプロジェクト単位というグループ化ができれば、障害や不正パケットの発信などを行うマシンへの対処などの、ネットワーク管理を円滑にする上で有効であると考えられる。

3. グループ化の基準

従来のネットワークに接続されたマシンのグループ化と異なる新しいグループを作成するためには、従来のものとは違う基準に基づいてグループを定義する必要がある。そこで本研究では、コンピュータの利用方法をネットワーク上のトラフィックから抽出し、その利用方法に基づいたグループ化を提案する。グループを定義するために以下に示す 3 つの利用方法に基づくグループ化を検討した。

(1) 認証システムによるグループ化
認証方式によるグループ化は、LDAP などの認証システムを利用しているマシンと認証サービスを提供しているサーバとの通信を解析しグループ化を行う。

(2) ファイル共有によるグループ化
ファイル共有によるグループ化は、対象となるサーバと NFS や Samba などのファイル共有システムを用いてファイル共有を行っているマシンを特定しグループ化を行う。
(3) 遠隔利用によるグループ化
遠隔利用によるグループ化は、ssh や telnet などの遠隔利用を用いて対象となるサーバと通信を行っているマシンを特定しグループ化を行う。

4. パケット収集実験

遠隔利用によるグループ化（前節(3)）に関する実験を実施した。

4.1 実験の概要

今回の実験においては、古川が担当する講義での学生に関する情報を収集した。その理由として、この講義では、出欠の確認を gin と呼ばれる香川大学内の Linux サーバを利用している。講義に出席している学生は、DHCP を用いて IP アドレスが割り当てられる自分のノート型コンピュータから gin に ssh あるいは telnet を用いてログインすることで、授業への出席が認められる。このことから授業時間中の gin の通信内容から、講義に出席している学生のコンピュータをグループ化できる。

4.2 実験の詳細

今回の実験では通信するパケットを収集するために tcpdump コマンドを使用した。この実験では送信元または送信先のホスト名が gin のパケットで通信に ssh を用いているパケットのみを対象にして情報の収集を行った。また、パケット情報の詳細についての取得を避けるために、パケットの先頭から 48 バイトに制限して情報を取得し、パケットのソースアドレスとディスティネーションアドレスと通信方式のみ記録した。

4.3 実験結果と考察

tcpdump を用いて収集したパケットの一部を図 1. に示す。

これらの情報は左からパケットの取得時間、パケットのソースアドレス、パケットのディスティネーションアドレスの順に表示されている。また、今回の実験でパケット取得の対象となるサーバが gin であることが明確なので、gin の IP アドレスは表示せず、ホスト名のまま出力している。

```
13:37:25 gin.ssh > 133.92.164.134.1181:
13:37:25 133.92.164.134.1181 > gin.ssh:
13:37:28 133.92.157.170.2043 > gin.ssh:
13:37:28 gin.ssh > 133.92.157.170.2043:
13:37:29 133.92.157.135.1089 > gin.ssh:
13:37:29 gin.ssh > 133.92.157.135.1089:
13:37:31 133.92.157.165.3040 > gin.ssh:
13:37:31 gin.ssh > 133.92.157.165.3040:
13:37:49 133.92.157.233.1159 > gin.ssh:
13:37:49 gin.ssh > 133.92.157.233.1159:
13:37:52 133.92.157.152.1642 > gin.ssh:
13:37:52 gin.ssh > 133.92.157.152.1642:
13:38:00 133.92.157.243.1041 > gin.ssh:
13:38:00 gin.ssh > 133.92.157.243.1041:
```

図 1. tcpdump を用いて収集したパケットの一部

この結果では講義室に割り当てられている 133.92.157.0 のサブネットから通信している 135, 170, 165, 233, 152, 243, の IP アドレスを持つマシンが、対象となった講義に出席している学生のノート型コンピュータとしてグループ化できる。ただし、この時点ではコンピュータの利用者自身を特定していないので、講義の出席者リストに用いることはできない。

133.92.164.134 のコンピュータは、異なるサブネット上で割り当てられたコンピュータであることが分かるので、グループから除外することができる。

5. おわりに

一定の条件の下でネットワーク上の通信パケットを解析し、サーバを遠隔利用(ssh)しているコンピュータのグループ化ができることが判った。ただし、実際にこれらの結果に基づいて管理者グループとの連携を行うためには、コンピュータの識別とその利用者とのデータベースが必要になる。

今後の課題としては、認証やファイル共有を行っているマシンのグループ化など、他の利用方法に基づくグループ化を行う必要がある。さらに、グループ化した情報の精度がどの程度であるか評価するための方法の検討や、グループ化した情報の具体的な利用方法を検討する必要がある。

【参考文献】

[1] 水野 忠則, 井手口 哲夫, 石原 進, 岡崎 直宣,”コンピュータネットワークの運用と管理”, ピアソン・エデュケーション, 2002.4