DHCP サーバ自動検出システムの構築

Construction of a DHCP server automatic detection system

白清　学，谷内田　昌寿
Manabu Hakusei, Masatoshi Yachida

hakusei@vos.nagaokaut.ac.jp, yachida@ipc.nagaokaut.ac.jp

長岡技術科学大学 情報処理センター
Information Processing Center Nagaokauniversity of Technology

〒940-2188 新潟県長岡市上富岡町 1603-1
Kamitomioka1603-1, Nagaoka, Niigata , 940-2188　JAPAN

概要

長岡技術科学大学の学内 LAN では，MAC アドレスに対して固定の IP アドレスを発行するネットワーク管理形態を採用しており，IP アドレスの割り当ては情報処理センターの DHCP サーバの集中管理により行われている．したがって，学内 LAN では利用者単位による DHCP サーバの利用は認められない運用となっているが，NAT を使用できる無線 LAN アクセスポイントなど DHCP サーバ機能を有するネットワーク機器の誤設定により，不測の DHCP サーバが接続される事例があり，他の利用者に影響を及ぼす障害を引き起こしている．この問題を早期に発見し，障害時間の短縮を図るため，学内 LAN の各セグメントに関して DHCP サーバの存在の有無を自動検知するシステムを導入した．また，MAC アドレスを元に設置場所を特定する手法と組み合わせることにより効果的な運用を実現している．

キーワード：学内 LAN，DHCP，VLAN，telnet，自動検出

1.はじめに

長岡技術科学大学は構成員約 2700 人の工科系単科大学である．各構成員が充分にネットワークを利用できるよう，表 1 に示す Cisco 社製のネットワーク機器が導入されており，基幹ネットワークを構成している．情報処理センター(以下センター)にはルーティングを担う 3 台のスイッチが設置されており，この中央スイッチの配下へ 36 台の Layer2 スイッチが分散して接続されている．これらのネットワーク上で論理的な構成として 46 のネットワークセグメントへ分割した形態にて学内 LAN の運用を行っている．現在は約 5100 のグローバル IP アドレスを発行しており，各セグメントにおいて適切な利用ができるようセンターが IP アドレスの管理を行っている．IP アドレスの発行は，MAC アドレス，設置場所，使用者などの情報を事前にセンターへ申請するものとし，設置場所のセグメントに応じた固定の IP アドレスを割り当てる方式を採用している．

表 1　学内 LAN の機器構成

機器名称	設置台数
Catalyst 6506	2
Catalyst4006	9
Catalyst4506	1
Catalyst3548XL	18
Catalyst3524XL	7
Catalyst3512XL	1

アドレス割り当て時は，DNS サーバへの登録の他，センターが管理する DHCP サーバへも登録を行っており，一元的に管理が行われている．したがってセンター管理下のセグメントでは，DHCP サーバは構成することはできない状況であるが，誤った形態での DHCP サーバの設置は他の利用者にも悪影響を及ぼすため，ネットワーク運用上の大きな問題となっている．近年は様々なネットワーク機器が利用されており，NAT 機能を備えるルータ機器や無線 LAN アクセスポイント，パソコン上で仮想マシンを実現するソフトウェアなどに DHCP サーバ機能が組み込まれている．これらの機器が多数利用されるようになった結果，設定の誤りやケーブルの接続箇所の誤りにより，当該セグメントにおいて DHCP サーバをサービスをするケースが増えている．DHCP サーバの設置が為された場合，同一セグメントの利用者が自動取得によりネットワーク接続を試みると，ネットワークが正しく利用できない状況となり，周辺の利用者の利便性が大きく低下する．従来は，このような障害に遭遇した場合，照会者に対して不具合箇所の周辺の調査を依頼する程度の対応であったが，容易に障害機器を特定できないケースもあり，より速やかに障害機器を特定するシステムの導入が望まれていた．このような背景の下，DHCP サーバ自動検出システムを構築し，さらに，設置場所を調査する仕組みを取り入れることで，このようなネットワークの障害の発生時に短時間で障害機器を特定し，学内 LAN から切り離すことで，ネットワーク運用に貢献できるものと考えている．

2.システムの構築

2.1　システムの構成

DHCP サーバの検出にはサーバのサービスポートである 67/udp のサービス状況を調査する方法が考えられるが，その調査にはあらかじめ IP アドレスを知る必要がある．センター管理下の IP アドレスであればサービスポートを対象とする調査も可能であるが，プライベートアドレスによってサーバが構築され，IP アドレスの発行も為されている場合は，同様の方法での調査は困難である．

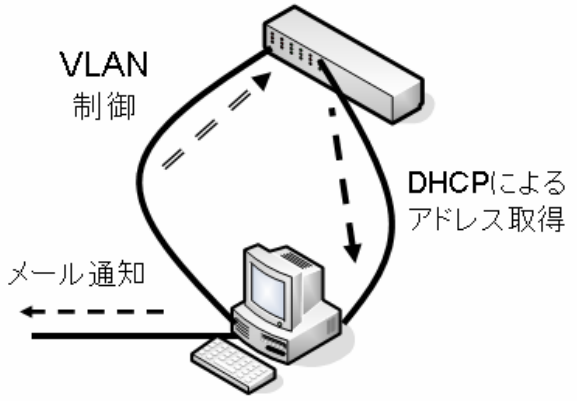

図 1 システム構成

プライベートアドレスを使用する DHCP サーバにも対応するため，各セグメントにおいてアドレスを自動取得するクライアントを配置し，その取得情報を確認することによって調査を行うこととした．セグメント数に応じて多数の機器を備えるのは非効率であることから，VLAN 機能を使用することとし，これに対応したスイッチを用いることによって各セグメント毎の DHCP サービスの確認を実現する．したがって VLAN による制御が可能なスイッチおよび，スイッチの制御および DHCP クライアントとして動作可能なクライアントマシンを備えた単一のシステムを用いることでネットワーク全体を調査することができる．そこで本システムでは，図 1 に示すように 3 つのネットワークインターフェースを持つ PC を使用し，VLAN 制御とアドレスの取得のほか，検出時のメール送信のために利用することとした．

これらの機能が実現できるよう，スイッチには Cisco 製の Catalyst3524XL，PC はマザーボードに NIC を備えかつ PCI スロットを通じて 2 ポートの NIC が増設可能な機器を用いている．クライアントとなる PC の OS には FreeBSD6.2，各機器の制御にはスクリプト言語 ruby を用いている．本システムをセンターの Layer3 スイッチへ接続し配下の VLAN を束ねて利用できるポートへ接続することで，学内全体の調査を行うこととした．

2.2 VLAN 切替

本システムで用いる Catalyst3524XL では，telnet コマンドでログインし，switchport access コマンドを用いることで，VLAN 設定の変更を行うことができる．制御プログラムにて使用している ruby では，Net::Telnet ライブラリが備えられており，こちらを利用することで容易に制御コマンドを実行することができ，スイッチ設定の変更を行うことができる．telnet コマンドでのスイッチの制御の

際は，パスワードの利用が不可欠となるが，セキュリティの観点から他の一般利用ユーザのセグメントとは異なる VLAN 管理専用のセグメントを用いている．

2.3 dhclient によるアドレス取得

クライアント PC の OS として使用している FreeBSD ではDHCPのクライアントとして標準で備えられている dhclient コマンドがあり，こちらをアドレス取得で用いることとした．このコマンドには dhclient.conf と呼ばれる設定ファイルがあり，アドレス取得を試みる回数やタイムアウト値，取得を行う NIC の名称を指定することで，特定のスイッチポートから希望の VLAN 内でのアドレス取得を試みることを実現できる．アドレス取得後は，dhclient.leases.NIC 名 のファイルに取得情報が保管され，DNS 情報は resolv.conf へ反映される．これらの情報を確認することで，VLAN 内の DHCP サーバの有無を確認するものとしている．図 2 は取得した設定情報の例である．

```
lease {
  interface "fxp2";
  fixed-address 192.168.11.2;
  option subnet-mask 255.255.255.0;
  option routers 192.168.11.1;
  option domain-name-servers 192.168.11.1;
  option dhcp-lease-time 86400;
  option dhcp-message-type 5;
  option dhcp-server-identifier 192.168.11.1;
  renew 6 2007/8/11 12:38:24;
  rebind 6 2007/8/11 21:38:24;
  expire 0 2007/8/12 00:38:24;
}
```

図 2 dhclient.leases の例

2.4 MAC アドレス取得

調査対象のセグメントにアドレス取得が確認された場合，DHCP サーバのハードウェアを特定することによって，以降の対応を速やかに進めることができるものと考えている．アドレス取得時に得られる dhclient.leases ファイル内には dhcp-server-identifier として，サーバのアドレス情報が含まれていることから，こちらのアドレスに対して ping コマンドを用いて応答を確認後，arp コマンドを利用することで，MAC アドレスの確認を行っている．

```
#arp 192.168.11.1
 (192.168.11.1) at 00:07:40:XX:XX:XX on fxp2 [ethernet]
```

図 3 arp による Mac アドレス取得の例

2.5 システムの処理の流れ

本システムの処理の流れを(1)～(7)に示し，さらに具体的な機器に対する処理の様子を図 4 に示す．

(1) VLAN 切替：アドレス取得を行うスイッチのポートを調査対象の VLAN へ設定変更を行う．
(2) アドレス要求：dhclient コマンドによりアドレスの要求を行う．
(3) アドレス取得の確認：dhclient.leases 情報の有無を確認する．存在していない場合は，(1)へ戻り，以降の VLAN に対して調査を継続する．存在する場合は(4)以降の処理を継続する．
(4) ping 応答確認：確認された dhcp サーバのアドレスに対して ping コマンドを実行し，応答を確認する．
(5) MAC アドレスの取得：arp コマンドにより MAC アドレスを取得する
(6) メール通知：取得した dhclient.leases および MAC アドレスを電子メールにより管理者へ通知する．
(7) (1)へ戻り，以降，全ての VLAN の調査を行う．

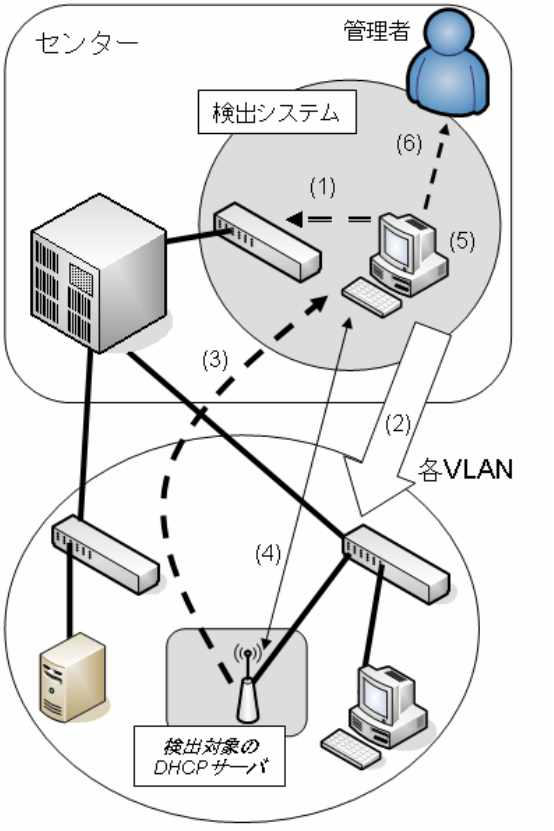

図 4 システムの処理の流れ

2.6 設置場所の特定

センターで管理している IP アドレスが障害の機器となっている場合，申請時の登録情報により使用者および設置場所を特定することが可能であるが，プライベートアドレスを用いてDHCPサーバが動作していた場合には，異なる手段により設置場所の特定を行う必要がある．

本システムで対象としている Cisco 製のスイッチでは，show mac-address-table および show cam dynamic コマンドを利用することで MAC アドレスとスイッチの接続ポートの情報を取得することができる[1]．別途作成しているスイッチの接続ポートと設置場所の情報を組み合わせることで，設置場所の特定を行っている．設置場所を特定できることで使用者への連絡を速やかに行うことができ，連絡体制の強化を実現している．

3.システムの運用

プログラムにて自動的にDHCPサーバの検出を行う機能が構築できたことから，スケジュール機能を利用して定期的に繰り返し調査を行っている．対象としているセグメントの調査には 9 分程度の時間を要しており，現在は 1 時間に 2 回の調査を実施している．短時間の障害機器の接続の場合には検出できない可能性もあるが，継続的な利用の場合が大きな問題となることから，現行では十分な調査間隔と考えている．

これまでの DHCP サーバの障害事例では，学内利用者からの問合せによってのみ各セグメントにおける障害の動向を認識することができる状況であったが，定期的な監視体制が構築できたことから，今後は積極的に調査を行うことが可能であり，従来は検出できなかった潜在的な障害についても明らかにできるものと考えている．

4.おわりに

ユーザの接続や設定の誤りによって発生するDHCPサーバ設置のネットワーク障害を短時間で解消することを目的として，学内 LAN の複数のセグメントに対して，自動的に DHCP サーバを検出するシステムを構築した．テスト目的にて設置したDHCPサーバでは適切に検出動作を行っており，運用に耐えるものが構築できたものと考えている．但し DHCP サーバの検出は可能であるものの，取得情報に差異が見られる事例があることから，今後，具体的な検出状況を踏まえてプログラムの更改を実施したいと考えている．

現時点では設置場所の特定に関連する作業の自動化は行っていないが，スイッチにおける MAC アドレス情報のエージングタイムにより，接続ポートが特定できないケースが想定される．このような問題を回避するために，障害となる DHCP サーバを検出した際に，速やかに設置場所の確認を行うことが望ましいと考えている．

また，VLAN 切替によりセグメントの変更が実現できていることから，各セグメント内における未登録ホストやプライベートアドレスの利用についても検出する仕組みを別途構築することも可能と考えている．本システムをより有効に活用し，ネットワーク障害や不適切な利用を検出することによって，適切な形態でのネットワーク運用を実現したいと考えている．

参考文献

[1] 續木涼太，泉裕，齋藤彰一，塚田晃司:組織内ネットワークにおける MAC アドレスとレースバックシステムの開発，情報処理学会研究報告 IPSJ-2005-DSM-36, pp.13-18(2005)