IPv6 における DHCP と DNS 動的更新を用いた 移動 PC の利用制限

2011SE216 太田 詞大
指導教員 後藤 邦夫

1 はじめに

現在, 南山大学瀬戸キャンパスでは Dynamic Host Configuration Protocol(DHCP) サーバ，Domain Name System(DNS) サーバを使用し，Media Access Control アドレス (MAC アドレス) を登録しておく事で許可された PC だけがネットワークを利用できるシステムになっている．しかし，現行のシステムは IPv4 環境で動作するが，近年利用者が増えている IPv6 環境では動作しない．

高機能スイッチを使用すると費用がかかってしまうので，本研究では現行と同等のシステムを IPv6 で実現する．具体的には，既存の DHCP Version 6[1](DHCPv6) サーバプログラムと DNS サーバプログラムを利用し，DHCP と DNS の連携部分のプログラムを作成することで現行の瀬戸キャンパス同等の機能を IPv6 で実現する．また，プログラムを作成することで来客者の臨時のネットワーク利用を可能にする．ソフトウェアネットワークエミュレータ Common Open Research Emulater[2](CORE) を用いて仮想ネットワークを構成し，実験を通じて動作を確認する．ネットワークネームスペースが使用できる点から OS は Linux を使用する．

2 DHCP/DNS 動的更新システムの概要

この節では IPv4 で DHCP と DNS 動的更新を用いた現行のシステム，また IPv6 用のシステムの概要を示す．

2.1 IPv4 用現行システム

システムの目的は移動 PC のネットワーク利用制限である．DHCP サーバに接続を許可する PC の MAC アドレスを登録しておくことにより，許可されている PC にのみ DHCP サーバからネットワークの接続に必要な情報が付与される．さらに，情報を付与されたクライアントのドメイン名を DNS 動的更新で登録する．事前にアプリケーションサーバ類では逆引き情報をもたないクライアントへのサービスを拒否する設定にしておくことで，DHCP を用いずに手動で IP アドレスを設定した場合でも DNS 逆引き情報がなく実質的にネットワークを使用できない．

また，ユーザ名と MAC アドレスを対にしたユーザ表とルータと教室名を対にした教室対応表を作成しておくことでどこで誰が使用しているかをドメイン名を見ることで分析できる．ドメイン名の付与の具体例として現在南山大学瀬戸キャンパスの教室 A401 教室で学生番号 2011SE789 の学生が PC を接続したとき付与されるものを表 1 に示す．

表 1 接続したとき付与されるもの

IP アドレス	ドメイン名
10.64.6.99	11SE789.A401.nanzan-u.ac.jp

2.2 IPv6 用システム

IPv6 では Router Advertisement(RA) という機能があり，DHCP を用いずにルータからの RA で各 PC の IPv6 アドレスの自動設定ができる．本研究では IP アドレスは DHCP での管理が必要なので，RA は DHCP を用いてステートフルに管理するようにクライアントに送信する．

IPv6 用システムではプライベート IP アドレスではなく割り当て範囲からグローバル IP アドレスを付与する．また，グローバル IP アドレスであっても IPv4 の現行南山大学瀬戸キャンパス同様にルータの通過には別途ユーザ認証を求めることとする．DHCPv6 では MAC アドレスではなくそれと同等の DHCP Unique Identifier(DUID)-LL で制限をかける．

DNS は IPv6 では AAAA レコードと PTR レコードで登録することで正引き/逆引きとなる．

3 IPv6 用 DHCP/DNS 動的更新システムの実現

この節では IPv6 用 DHCP/DNS 動的更新システムの実現方法について示す．

3.1 ネットワーク構成

DHCP サーバ, relay とクライアントには dibbler, DNS には BIND[3], NSD[*1] というオープンソースソフトウェアを使用する．RA には UNIX 系 OS に標準搭載されている radvd を使用する．作成したネットワークの構成を図 1 に示す．各ルータは dibbler の relay 機能を持たせることでサーバとクライアント間通信の中継をする．

3.2 DHCP サーバ・ルータと DNS 設定

relay する各ルータ，マルチポートルータの教室側のインターフェースに複数あればそれぞれ interface-id を設定しておき，設定も interface-id 毎に記述しておく．DHCP サーバでは interface-id 毎に割り振る IP アドレスのプール範囲，接続許可 DUID を記述しておく．

DNS には管理するドメインと DHCP でリースする IP アドレスの正引き/逆引きのゾーン情報を記述しておく．

[*1] http://www.nlnetlabs.nl/projects/nsd/

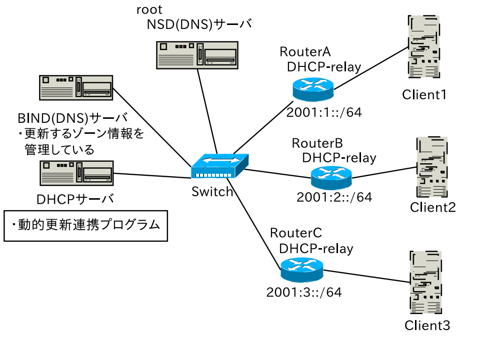

図 1 ネットワーク構成図

3.3 DHCP/DNS 連携プログラム

希望のドメイン名を登録するために DHCP サーバと DNS 動的更新の連携部分を Perl で約 160 行のスクリプトを作成した．DHCP サーバの log を動的に読みこみ情報を付与したクライアントを DNS に動的更新要求を送信するという仕様である．IP アドレスの付与から動的更新までの処理のシーケンスを図 2 に示す．IP アドレスをリリー

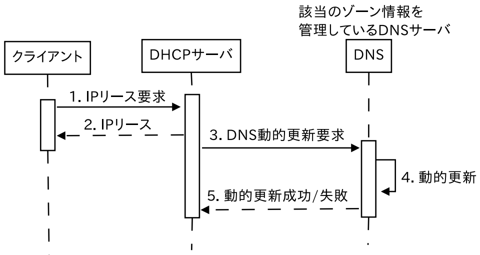

図 2 動的更新通信手順

スした場合も同様で，log ファイルでリリース確認しだい DNS へ該当レコードの削除を動的に要求する仕様とした．

3.3.1 ゲスト用設定

ゲストの持ち込んだ PC を利用可能とするために PC 臨時登録システムを作成した．作成したプログラムは 3 つであり，3 つで約 200 行のプログラムとなっている．

1. 認証サーバプログラムの DDNS.js
2. DHCP サーバがゲストの情報を取得するプログラムの get.pl
3. DHCP サーバ設定ファイルを更新するプログラムの conf.pl

DDNS.js は認証サーバとする PC で動作させる HTTP サーバプログラムであり，ゲストは Web ブラウザで認証サーバに接続しパスワード使用して認証を通過する．また，DDNS.js はサーバサイド JavaScript 環境である Node.js で作成した．

4 実験

本研究では OS が Ubuntu Linux14.04, CPU が Intel(R) Core(TM) i5 2.67GHz の PC で実験した．CORE 上で前節で示した構成図を仮想ネットワークとして作成し，client1 と client2 は接続を許可する PC，client3 を接続を許可しない PC とする．BIND は “nanzan-u.ac.jp.”のドメインを管理し，DHCP は IP アドレスを 2001/124 の範囲で管理している．エミュレータをスタートさせ，各クライアントの端末上で ifconfig コマンドを使用して接続を許可された PC にだけ IP アドレスが付与されているか確認する．また，dig コマンドを使用してドメイン名が DNS へ登録されているかを確認する．client1 の結果を下に示す．

client1

IP アドレス：2001:1::5b/64
dig 正引き結果：classroom.A401.nanzan-u.ac.jp. 86400 IN AAAA 2001:1::5b
dig 逆引き結果：b.5.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.1.0.0.0.1. 0.0.2.ip6.arpa. 86400 IN PTR classroom.A401.nanzan-u.ac.jp.

client3 には IP アドレスが付与されず，client1,2 には IP アドレスが付与され DNS にドメイン名が登録されていた事が確認できた．つまり利用制限のシステムとして正しく動作しているといえる．

5 おわりに

本研究によって IPv6 における移動 PC の利用制限システムが作成できた．ゲスト利用設定において Web ブラウザでの IPv6 リンクローカルアドレスの指定方法が定まっていないので，ループバックアドレス::1 で接続することでゲスト登録の実験をしたところプログラムは正しく動作した．また，ユニークローカルユニキャストアドレスを認証サーバに静的に付与しておくことでゲストは Web ブラウザでの接続ができると思われる．MAC アドレスの偽装には認証サーバを用意しておき，クライアントは Web ブラウザを使用した認証をはさむことで対策になると考えられる．

今後の課題は DHCP 負荷テストである．tap を数百個作成しカーネルブリッジと接続して DHCP にリクエストを大量に送ることで負荷テストになると考えられる．

参考文献

[1] Droms, R., Bound, J., Volz, B., Lemon, T., Perkins, C. and Carney, M.: Dynamic Host Configuration Protocol for IPv6 (DHCPv6), RFC 3315 (Proposed Standard) (2003).

[2] U.S. Naval Research Laboratory Networks and Communication Systems Branch: Common Open Research Emulator web page (accessed: Jan. 2015). http://www.nrl.navy.mil/itd/ncs/products/core.

[3] Internet Systems Consortium: BIND web page (accessed: Jan. 2015). http://www.isc.org/downloads/bind.