

2H-03 Dynamic LAN Configuration Protocol の作成と評価*

松澤 智史 武田 正之†

東京理科大学大学院 理工学研究科 情報科学専攻‡

1 はじめに

従来、ほとんどの LAN は固定マシンで構成されていた。しかしながらモバイル機器の発達と普及により、現状では多くの LAN にノート PC 等の移動ノードが接続するようになってきた。移動ノードはその名の通り時間によって設定されている情報が異なる。この移動ノードの設定を自動で行うために作られたのが DHCP[1] である。DHCP はノードの IP アドレスだけでなく、ネットワーク情報なども自動で設定するため、管理者の手間を軽減することに成功している。しかしながら、DHCP は移動ノードの属する LAN の設定までは行うことができない。結果として、移動ノードの接続によって変わるべき LAN の設定を自動で行う手法が必要になってくる。

本研究では、DHCP の利点である動的設定を移動ノードに限定せず、LAN を構成する各種サーバマシン等にも適用させるのを目的とし、そのための新プロトコルの作成、実装、評価を行う。つまり DHCP によって動的に変わるネットワーク (LAN の構成) 情報を用いて LAN に存在する各ノードの設定を動的に行うためのプロトコル DLCP (Dynamic LAN Configuration Protocol) を提案する。

本実装では、このプロトコルを用いて LAN 構成の変化をあたえる項目として、DHCP によって割り当てられた IP アドレスによる DNS の動的更新と DHCP サーバによって認証されたノードの LAN 内におけるアクセス制御という 2 つのプロトコルを作成し、これを評価する。

2 DLCP プロトコル概要

本研究で開発するプロトコルは概ね DHCP のプロトコルフォーマットを基にしている。これは DLCP は DHCP の拡張プロトコルであり、つまり、DHCP は LAN を動的に構成するために必要な、移動ノードの設定を行うためのプロトコルという位置づけをする。プロトコルフォーマットについては DHCP と同じであるが、解

*Implementation of Dynamic LAN Configuration Protocol and Its Evaluation

†Tomofumi Matsuzawa, Masayuki Takeda

‡Department of Information Sciences, Science University of Tokyo

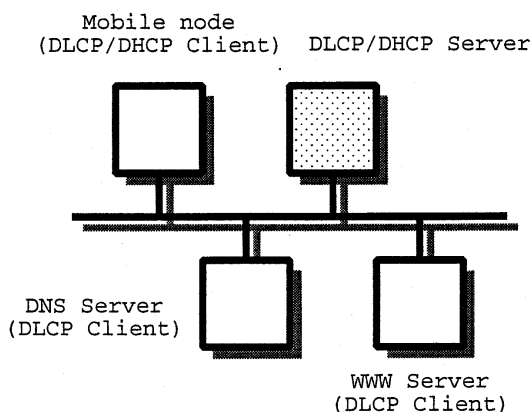


図 1: DLCP を使用している LAN

釈の仕方は各プロトコルによって異なる。

DLCP を用いた LAN では、DHCP サーバ以外のすべてのノードが DLCP クライアントである。(図 1) DHCP によって割り当て状況が変わった場合に DHCP サーバからすべて、あるいは任意の DLCP クライアントに対して変更情報を通知することによって各ノードの設定を変更する。

DLCP サーバとクライアントは、DHCP プロトコルフォーマットの op フィールド¹の値によって、²DHCP と各プロトコルの判別を行う。

3 DNS UPDATE プロトコル

DLCP に乗せるプロトコルとして、まず DNS UPDATE プロトコルを考案した。このプロトコルは、DHCP サーバと DNS が連携することによって、移動ノードの割り当てられる IP アドレスは毎度異なるが、常に固定的なホストネームを使用することを可能とする。[3]

DNS UPDATE のプロトコルで独自の部分は、DNS

¹DHCP プロトコルの一番最初の 1 オクテット。

²具体的な値としては、BOOTPREQUEST=1, BOOTPREPRY=2, DNSUPDATEREQUEST=3, DNSUPDATEREPRY=4, FILTERREQUEST=5, FILTERREPRY=6 がある。DHCP では最初の 2 つを使用している。

サーバの IP アドレス (これは明示しなくても良い), DNS に登録する IP アドレス, DNS に登録するホスト名, option フィールド³の追加があげられる。

DHCP にはない option は DLCP MESSAGE TYPE と DLCP LEASE TIME で, それぞれオプション番号として 53 と 51 が割り当てられている。これは DHCP のオプション DHCP MESSAGE TYPE と IP ADDRESS LEASE TIME に相当する番号である。DLCP MESSAGE TYPE には update delete ack nak prolong の 5 種類が用意されており, これらはそれぞれ DNS に新たなエントリを加える要求 (update), 削除する要求 (delete), クライアントからの返答 (ack, nak), 登録延長要求 (prolong) として使用される。DLCP LEASE TIME は, 32 ビットの整数値が使用され, 使用できる期間をミリ秒単位で指定する。リースをタイムアウト方式にした理由は, DHCP サーバから DNS に通知する際の通信経路になんらかの異常が発生し, 通信が正常に行われなくなった場合に, 移動ノード用の DNS エントリが永久に使用されるのを防ぐためである。

4 ACCESS FILTER プロトコル

DLCP に乗せるもう一つのプロトコルとして, ACCESS FILTER プロトコルを提案する。これは LAN に存在する各ノードが, DHCP サーバによってアドレスを割り当てられた移動ノードからの TCP/IP を利用したアクセスを許可するためのプロトコルである。具体的な流れは, DHCP サーバによって移動ノードが認証され, IP アドレスを割り当てた後, DHCP サーバは LAN に存在する各ノード (DLCP クライアント) に対して DHCP サーバが割り当てたノードを通知する。これによりクライアント側は自ノードのアクセス制御を変更し, DHCP によって設定された移動ノードからのアクセスを許可するようにする。また, IP アドレスが回収された後, その回収した IP アドレスからのアクセスを不許可にする。これによって動的に LAN 上に存在する各ノードのアクセス制御状況をコントロールすることが可能になる。今回の実装では, TCP/IP のアクセス制御の部分には tcpd を用いている。

ACCESS FILTER のプロトコルの独自部分はアクセス制御させるノードの IP アドレス, DHCP によって割り当てた IP アドレス (アクセス制御する IP アドレス), option フィールドの追加の 3 つである。

³DHCP プロトコルの最後の可変長のフィールド。option 番号が決められており [2] 様々な追加情報を挿入することができる。DLCP にも同じく option フィールドが存在する。

option フィールドには DLCP MESSAGE TYPE, DLCP LEASE TIME, PORT の 3 種類あり, DLCP MESSAGE TYPE には, regist delete ack nak prolong の 5 種類が存在し, 用途は DNS UPDATE と同様である。DLCP LEASE TIME も DNS UPDATE のと同様である。PORT は, アクセスさせる PORT を任意に指定し, これによってアクセス許可するノードのポートまで細かく設定することができるようになっている。

5 評価

本実装はすべて Solaris 2.5.1 上で行った。DHCP サーバは SUN Ultra1 上で稼働し, ホストにかかる負荷を調べた。DHCP サーバからのパケット送信量は, 平均して DHCP パケットの約 1.5 倍～3 倍ほどになる程度でほぼ問題にはならなかった。プロトコルの拡張性については, 本稿で 2 つの新 DLCP プロトコルを提案したが, この他にも, ルータで外部からのパケット制限やファイアウォールの動的コンフィグレーション等にも使用できる。また DLCP 自体は DHCP サーバが主体でなくても問題ないため, プロトコルに拡張性がある。

6 まとめ

本プロトコルを実装したクライアントによって, DHCP による IP アドレス割り当てから DNS のエントリ更新, ノードのアクセス制御までユーザや管理者の手を煩わすことなくスムーズに動的な設定を行うことができた。この手法は DHCP サーバからのメッセージが絶対的な存在となるため, DHCP サーバからのメッセージの信頼性を高めることが今後の課題となる。

参考文献

- [1] R. Droms, "Dynamic Host Configuration Protocol" RFC2131, March 1997.
- [2] R. Droms and S. Alexander, "DHCP Options and BOOTP Vendor Extensions" RFC2132, March 1997.
- [3] 松澤 山崎 武田, "DHCP 環境におけるネットワーク情報更新手法" 電子情報通信学会投稿中, Nov 1999.