マルチメディア通信と分散処理 78－9
（1996．9．27）

DHCP環境におけるアクセス制御についての考察

小林 和真　　山口 英

奈良先端科学技術大学院大学情報科学研究科

内容梗概

IETFで議論されInternet Draftで公開されているDHCPメッセージ認証方式では、過去に割り当てた情報やネットワークから直接得た情報をもとに不当にネットワークにアクセスしようとするクライアントを防ぐことができない。そこで本稿ではDHCP環境での移動ホストに対するアクセス制御の必要性について議論し、不当なアクセスを行うクライアントに対してネットワークの利用を制限する方法について考察する。またこの問題を解決するための手法としてアクセス制御ゲートウェイを提案しその設計・実装と有効性について述べる。

Network Access Control for DHCP Environment

Kazumasa Kobayashi　and　Suguru Yamaguchi

Graduate School of Information Science, Nara Institute of Science and Technorogy

Abstract

The DHCP message authentication method which was released by the IETF as Internet Draft has a problem for access protection from unauthorized clients that have expired or invalid resource obtained through tapping. This paper focuses technical requirements of the network access control for DHCP Environment. The need for the protection mechanism of unauthorized clients access to the network was also considered in our research. This paper also discusses the design, implementation and validation of the Network Access Contorol Gateway for DHCP environment.

1　はじめに

コンピュータ関連技術の進歩により持ち運びのできるノート型コンピュータの普及が急速に進んでいる。従来のコンピュータは基本的に固定され、ネットワーク的にも移動しないものとみなされていた。しかしノート型のコンピュータは利用者とともに移動し(「移動ホスト(Mobile Host)」)、移動先でもネットワークに接続される。こうした新しい利用形態の出現により、移動先でもネットワークに容易に接続できるメカニズムが必要とされはじめた。

こうした中でマイクロソフト Windows95にも標準で採用されたDHCP(Dynamic Host Configuration Protocol)[1][2][3] は、この要求を満たす技術として急速に普及し数多くのネットワークサイトで利用されている。しかしながら現在普及しているDHCPは、セキュリティについてまったく考慮されておらず、ネットワークに接続しようとするすべてのクライアントの要求を同じように処理し、接続情報の割り当てを行ってしまう。つまり誰にでもネットワーク

アクセスを許してしまうのが現状である。

インターネットの普及とともにネットワーク環境におけるセキュリティの必要性も同時に認識され、Firewall を構築し内部ネットワークに対するアクセス制御を行なうサイトが急速に増加している。こうした背景から IETF(Internet Enginiaring Task Force) でも DHCP におけるセキュリティの重要性が議論され IETF Draft[4] をはじめとする幾つかの方向性が示されつつある。またサーバとクライアントとの間で認証処理を行うための方法がこれまでにもいくつか提案されている [5]。

しかし IETF Draft や関連する提案で述べられている方法では、DHCP サービスを提供しているネットワークを物理的に盗み見て接続に必要な情報を入手しアクセスしようとする不当なクライアントや、過去に入手した情報をもとにアクセスしようとするクライアントに対する有効な対処法がまったく述べられていなかった。現実に運用する DHCP ネットワークを構築する場合には、こうした不当アクセスの排除は明らかに必要な機能である。

そこで本稿では、こうした不当なアクセスを行おうとするクライアントからの通信を排除し、DHCP サーバによって接続のための資源を正当に割り当てられたクライアントのみが通信できるメカニズムを実現する手法について述べる。

2 関連技術

2.1 移動ホストのアドレス

インターネットでは、ネットワークに接続されたホストを IP アドレスで識別している。移動先での接続で新たに IP アドレスを割り当てた場合、結果的に移動前と別のホストとして識別される。この問題を解決するためにいくつかの提案が行われている。

IETF の Mobile-IP WG では、ホストの IP アドレスを変更せず移動先のネットワークとの間でトンネリングの技術を用いて仮想的に本来のネットワークに接続し、移動する前と同じアドレスで通信する方法について提案している [6]。

WIDE プロジェクトでは、接続位置に関する情報のみを IP アドレスで表現しホストの識別を別の VIP アドレスで表現する VIP(Virtual Internet Protocol)[7][8] を提案し移動ホスト環境を実現している。

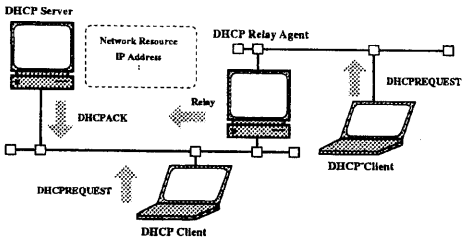

図 1: DHCP

2.2 資源の割り当て

移動の前後で同一のホストとして識別するための Mobile-IP や VIP の提案では、移動先のネットワークに接続するための何らかのネットワーク資源を必要とする。また、ネットワークに接続することが重要であり、移動の前後で異なるホストとして識別されてもかまわないとしても、移動先での接続のために IP アドレスなどの情報を割り当てなければならない。こうした要求に対応するためにインターネットでは BOOTP(Bootstrap Protocol)[9] や DHCP などの資源割当機構が提案されている。

本稿で着目している DHCP は、BOOTP 上位互換の資源割り当てプロトコルであり、ユーザの介在無しに動的な資源の割り当てができ、かつ割り当てた資源の回収が可能なプロトコルである。DHCP はネットワーク資源の割り当てを行う DHCP サーバと資源を要求するクライアント、要求を中継するリレーエージェントから構成される (図1参照)。

2.3 ホスト認証の必要性

BOOTP プロトコルや DHCP プロトコルでは、資源の割り当てに際して割り当てるホストの認証をまったく考慮していない。これらのサーバはどのようなクライアントからの割り当て要求に対しても要求に応じて資源を割り当ててし

まうため、セキュリティの観点から問題視されている。逆に割り当てられたアドレスが正当なDHCPサーバから割り当てられたものなのかという問題もあるためクライアントによるサーバの認証も考慮する必要がある。

3 DHCPメッセージの認証

DHCPのメカニズムにおいてセキュリティ上重要なポイントは、DHCPサーバとDHCPクライアントの間のDHCPメッセージの交換の安全性にある。この安全性を確保する手法として、サーバ・クライアント間の一連の処理において交換するDHCPメッセージにディジタル署名を付加することが考えられる。これを用いればDHCPサーバとDHCPクライアントとの間で認証処理を行ない、正当なクライアントにのみネットワーク資源の割り当てを行なうことが可能である。これらの認証情報はDHCPに関連する分野ではMessage Authentication Code(MAC)と呼ばれている。

一般的なディジタル署名では受信者Rと送信者Sの間で次の3つの条件を満足する必要がある。

1. Rが受信したメッセージが確かにSが送信したものであると確認できること。
2. Rを含む第三者TがSのメッセージを偽造できないこと。
3. SがメッセージをR宛に送信した事実を送信後に否定できないこと。

3.1 IETF Draftにおける認証

IETFで議論されているDHCPメッセージの認証方式は、サーバとクライアントで暗号鍵を共有しこの鍵を利用して生成されるMACにより認証処理を行うものである。

実際に伝送されるDHCPメッセージには次の情報が含まれる。

DHCP Message, counter,
$f(K$, MD5(message + counter))

DHCP Messageは、DHCPサーバとクライアントの間で交わされるネットワーク資源を割り当てる処理のための通常送られるメッセージである。counterはリプレイアタック(繰り返し攻撃)を防止するための情報で通常は時間などを含んだ値を設定する。これらの情報に加えて、共有している鍵K、DHCP Messageとcounterから生成されるメッセージダイジェスト(MD5)[10]を一方向関数fで変換した値がディジタル署名として付加される。

あらかじめDHCPサーバとこれを利用するクライアントの間で秘密鍵Kを共有しておくことにより、サーバとクライアントの双方で、送られてきたDHCPメッセージをもとに正当なサーバ／クライアントであることを認証することができる。また共有する秘密鍵Kの生成においてDHCPにおけるクライアントIDなど固有の情報を用いれば、送られてきたメッセージからクライアントを完全に特定することも可能である。

DHCPにおける認証については、現在IETFで議論されている最中でありInternet Draftとして"Authentication for DHCP Message"が公開されている。

4 アクセス制御機構の設計

本稿で提案するアクセス制御機構は、DHCPサーバがネットワーク接続のための情報を割り当てるサービスセグメントと、正規に割り当てられたクライアントからのみアクセスを許可する内部ネットワークとの間にゲートウェイを用意し、このゲートウェイによるアクセス制御を実現する。

4.1 基本的なアイデア

DHCPメカニズムの認証処理の流れを図2に示す。DHCPクライアントはまずDHCPサーバを探すためDHCPDISCOVERメッセージを送信する。これを受けたDHCPサーバはアドレスの割当が可能ならDHCPOFFERメッセージをクライアントに対して送信する。クライアントはアドレスを要求するサーバを決めDHCPREQUESTメッセージをサーバに対して送信する。

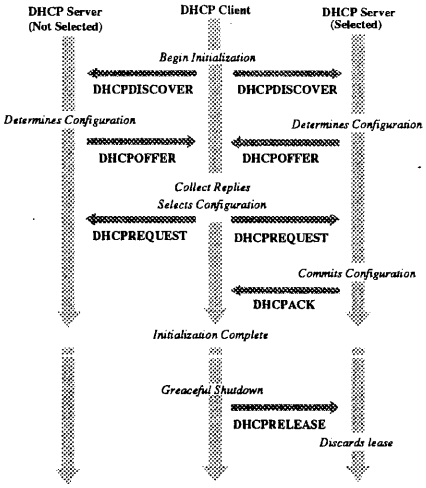

図 2: DHCP プロトコルの処理の流れ

これを受けとった DHCP サーバは割り当てる情報を DHCPACK メッセージとともにクライアントに送信し、クライアントは受けとった情報に従ってネットワークなどの設定を行なうことになる。

一連の DHCP サーバとクライアントの間で交換される DHCP メッセージの中で、具体的に割り当てられた情報が交換されるのは DHCPACK メッセージである。しかもこの情報はブロードキャストされるため同一ネットワーク上に存在するゲートウェイでも当然ながら受信できる。そこで DHCP サーバがサービスを提供するセグメントと、アクセスの許可を必要とする内部のネットワークとの間にアクセス制御ゲートウェイを用意して、DHCP サーバから DHCP クライアントへの DHCPACK メッセージをゲートウェイでも受信する。そして受信したメッセージに含まれるアドレスに対して必要ならば認証処理を行い、アクセスを許可してパケットの中継処理を実行する。つまりアクセス制御ゲートウェイでは正当に DHCP サーバによって割り当てられたクライアントの情報を実際の DHCP サーバの資源割り当てパケットから得てアクセス制御を実行することになる (図 3参照)。

アドレス割り当て時に DHCP サーバからア

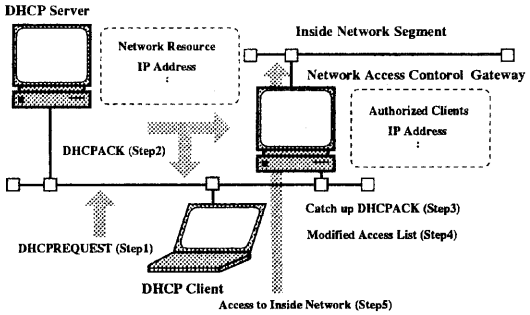

図 3: アクセス制御ゲートウェイのしくみ

クセス制御ゲートウェイに対して割り当てた旨の情報を伝送しなくても、通常の割り当て処理を監視することで正確な割り当て情報を得ることが可能である。

4.2 DHCP メッセージの認証

IETF Draft の"Authentication for DHCP Message" では、資源の割り当て処理に必要な情報に加えて、MAC(Message Authentication Code) と呼ばれるディジタル署名を、一連の割り当て処理で伝送する DHCP メッセージに付加している。実際の実装方法については Internet Draft では述べられていないが、DHCP プロトコルのオプションに記述することで伝送することが可能である。本稿で述べる実装では DHCP オプションのひとつである Class-identifier オプションに MAC を記述することにより、サーバとクライアントの間で認証処理を行なっている。DHCP プロトコルでは、このオプションを用いてサーバ固有の処理を行わせることが許されている。本来ならば MAC を記述するためのオプションが規定されるべきであるが現在の DHCP オプションでは規定されていない。そのため本稿の実装においては、正規の DHCP オプションとして定義されても最小限の変更で対応できるよう互換性のあるフォーマットを採用した。DHCP Class-identifier オプションに記述した MAC の Format を図 4に示す。

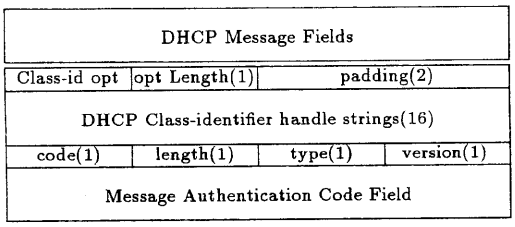

図 4: DHCP MAC Header Format

4.3 アクセス制御ゲートウェイの実装

アクセス制御ゲートウェイにおいて DHCP サーバの認証を厳密に行うならば DHCP メッセージの認証機構を必要とする。しかし厳密に認証する必要が無い場合でも適用できるアプローチを選択し実装を行った。すなわちアクセス制御機構を実現するうえで変更が必要な部分は、大部分がアクセス制御ゲートウェイに関するものであり、既存の DHCP サーバの変更を行なわなくてもすむよう配慮している。

アクセス制御ゲートウェイは 4 つの部分から構成される。

1. DHCP パケットの監視
2. アクセスコントロールデータベースの管理
3. アクセス制御
4. パケットの中継処理

DHCP パケットの監視には bpf(Berkelay Packet Filter) などの低レベルインターフェースから直接データを入手するメカニズムが必要である。またアクセス制御と中継処理の主要な部分については、フィルタリング機能を持つ既存のソフトウェアである ip_fil3.1.0 を利用した。

実装を行った dhc_fild プログラムは DHCP メッセージを監視し DHCP サーバからクライアントへ送られる DHCPACK メッセージから割り当てられたアドレスを抽出し、これを ip_fil に登録する処理を行うプログラムである。同様に DHCP クライアントからサーバに DHCPRELEASE メッセージが送られた時に、返却されるアドレスを ip_fil から削除する処理も行っている。

DHCP サーバでの DHCP メッセージの認証が行われている場合には、DHCP サーバと dhc_fild プログラムで秘密鍵を共有することにより認証処理を行うことができる。また認証処理の有無を dhc_fild.conf ファイルに定義しておくことにより認証を行わない通常の DHCP サーバに対する処理方法も選択できるよう配慮した。認証処理において DHCP サーバのメッセージ認証で必要な一方向関数 f には暫定的に MD5 を使用した。

5 評価

移動ホストからの割り当て要求に応じて DHCP サーバにより正当な割り当てを行ったクライアントのみアクセスを許可するアクセス制御ゲートウェイを実現できた。また本稿で提案したメカニズムでは、これまでに利用されてきた DHCP サーバ、クライアントとの互換性を重視しており、従来の DHCP 環境でもそのまま利用することが可能である。

5.1 安全性

DHCP では DHCP メッセージにディジタル署名を含むため DHCP オプションフィールドの大きさの制限から利用できる暗号化方式や鍵の長さに制限がある。IETF で提案されている方式は秘密鍵をサーバとクライアントで共有する方式で、その認証メカニズムはオプションフィールドの利用を考慮したものである。

秘密鍵を共有する場合の問題点としてクライアント側での鍵の漏洩が指摘されている。そのためユーザ自身にも解読できない鍵生成関数を用意してこれによる鍵の自動生成の必要性も議論されている [4]。

本稿で実現したアクセス制御機構の安全性は、DHCP のメッセージ認証の強度に依存する。DHCP サーバからのメッセージを偽造することが出来なければ、それと等価に安全であると言える。アクセス制御ゲートウェイで DHCP サーバからのメッセージ認証を行うため、DHCP サーバとクライアントに加えてアクセス制御ゲートウェイでも秘密鍵を共有する必要がある。この部分での安全性の低下が考えられるがゲートウェイ自身の安全性に依存するので考慮の対象

外とした。

5.2 性能

DHCP メッセージの認証処理によるフィルタの設定に必要な時間は、DHCP サーバからクライアントへの送信データをそのまま利用しているため無視できる範囲であると考えられる。

実際にアクセス制御ゲートウェイを経由して内部ネットワークと通信する場合のゲートウェイ処理のオーバヘッドについては、本稿で示している実装では IP フィルタ機能をフリーソフトウェアである ip_fil3.1.0 を利用して実現しているため ip_fil とその実装ハードウェアの処理能力に依存する。

5.3 問題点

本稿で提案しているメカニズムでは、アクセス制御ゲートウェイが起動した時点で、すでに DHCP サーバによってネットワーク接続のための資源が割り当てられているクライアントを認識することが出来ない。しかしながら内部ネットワークとの接続がアクセス制御ゲートウェイを経由してしか出来ないネットワーク環境での利用を想定しているため、それ以前の割り当てを考慮せず起動後の割り当て処理のみで十分であると考えている。またこの問題はクライアントから再度の更新要求を DHCP サーバに出すことにより正常な認証処理を行わせることができ、運用で対応することが出来る問題でもある。

6 今後の課題

現在の実装では、割り当てられたまま返却されないアドレスについての対応が不十分である。DHCPACK メッセージにはアドレスの有効期限も含まれている。こうした情報を有効に利用して有効期限の切れたアドレスについては中継処理を行わないようにする必要がある。またサーバ側で指定した最大有効期限を越えているアドレスについても同様な処理を行う必要がある。

さらに IETF で議論されている DHCP メッセージの認証機構以外の認証機構への対応とアドレス以外のリソースに対するアクセス制御について考える必要がある。

7 まとめ

ノート型のコンピュータによる移動先でのネットワーク接続を容易に実現するために、ネットワーク接続を自動化するメカニズムとして DHCP が提案され普及しつつある。しかしながら、現状の DHCP ネットワークでは、正当に DHCP サーバから入手した接続情報かどうかをまったく考慮しておらず、アドレスさえ設定すれば自由にネットワークを利用できてしまっている。

こうした現状を踏まえ、本稿では DHCP サーバから正規にアドレスの割当を受けたホストのみの通信路を確保するメカニズムの提案を行い、実際に動作するアクセス制御ゲートウェイの実装と評価を行った。

参考文献

[1] R. Droms: "Dynamic Host Configuration Protocol", RFC 1541 (1993).

[2] R. Drams and S. Alexander: "DHCP Options and BOOTP Vendor Extensions", RFC 1533 (1993).

[3] 富永, 寺岡, 村井："動的ホスト設定プロトコル (DHCP) の実装の評価", 情報処理学会マルチメディア通信と分散処理ワークショップ論文集 (1993).

[4] R. Droms: "Internet Draft — Authentication for DHCP Message" (1996).

[5] 小林, 山口, 山本："移動ホスト認証を考慮した資源割り当て機構の提案", 情報処理学会 マルチメディア通信と分散処理研究会 (1995).

[6] C. Perkins: "Internet Draft — IP Mobility Support" (1996).

[7] F. Teraoka and M. Tokoro: "Host Migration in Virtual Internet Protocol", Proceedings of Inet'92 (1992).

[8] W. Project: "移動ノード", 1992 年度 WIDE プロジェクト研究報告書 (1993).

[9] B. Croft and J. Gilmore: "Bootstrap Protocol(BOOTP)", RFC 951 (1985).

[10] R. Rivest: "The MD5 Message-Digest Algorithm", RFC 1321 (1992).